IBM Security Identity Governance and Intelligence
Version 5.2.2

Glossary Topics

IBM Security Identity Governance and Intelligence
Version 5.2.2

Glossary Topics

Table of contents

Table list

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC) module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is

fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential
1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.

2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished

name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic

user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines

whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key

cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

"A" on page 1 "B" on page 6 "C" on page 7 "D" on page 9 "E" on page 11 "F" on page 12 "G" on page 13 "H" on page 14 "I" on page 15 "J" on page 16 "K" on page 17 "L" on page 17 "M" on page 17 "N" on page 18 "O" on page 19 "P" on page 20 "Q" on page 24 "R" on page 24 "S" on page 27 "T" on page 32 "U" on page 34 "V" on page 34 "W" on page 35 "X" "Z"

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource

1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource

1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource

1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource

1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF

1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource
1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Glossary

This glossary provides terms and definitions for the [product name] software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

AC See access certifier.

access The ability to read, update, or otherwise use a resource. Access to protected resources is usually controlled by system software.

access analytics
A role engineering tool that combines the concept of risk analysis with the role mining process.

access certifier (AC)
A module that certifies users in an organization. The access certifier (AC)

module provides a complete and flexible workflow for certifying permissions that are associated to a user through a specific role, according to the role-based access control (RBAC) standard and separation of duties (SoD) policies that are enforced by the IBM Security Identity Governance platform.

access control
In computer security, the process of ensuring that users can access only those resources of a computer system for which they are authorized.

access control list (ACL)
In computer security, a list associated with an object that identifies all the subjects that can access the object and their access rights.

access governance core (AG core)
A module that manages digital identities and delineates and implements access rights based on the role-based access control (RBAC) model.

access management
The process of controlling access to IT services, data, or other assets.

access optimizer (AO)
A module that does risk analysis and role mining. Access optimizer (AO) is fully integrated with IBM Security Identity Governance role management features to support continuous role development and optimization as business processes evolve.

access request (AR)
A module that manages authorization workflows.

access risk
A concept that measures the probability of encountering several types of vulnerabilities when access is granted to resources in a large company or organization. Different policies for reducing risk probability are based on access risk evaluation.

access risk control (ARC)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model.

access risk controls for SAP (ARCS)
A module that defines SoD enforcements through the chain Business Processes - Activities - User Entitlements and is based on the RBAC model, according to the SAP authorization model.

account
An entity that contains a set of parameters that define the application-specific attributes of a user, which include the identity, user profile, and credentials.

account configuration
The configuration of a multi-application account on target systems. It supports functions such as password policies (creation, expiration, or propagation). It also supports user lock and unlock policies. An account can be configured for many applications.

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

ACL See access control list.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification
A second authentication factor and presence detector. See also radio frequency identification.

activity
A group of actions, which are guided by an operator, a software system, or both, that determines the part of a process to run. In the ARC context, an activity can have a hierarchical structure. In the PD context, an activity is the basic element that is used to define and configure the behavior of an authorization workflow (ARM workflow).

AD See Active Directory.

adapter
An intermediary software component that allows two other software components to communicate with one another.

adapter clause
A clause in a firewall rule that attaches the rule to a specific adapter.

adapter file
See target definition file.

admin domain
See administrative domain.

administrative domain (admin domain)
A logical collection of resources that is used to separate responsibilities and manage permissions. See also permission.

advanced persistent threat (APT)
A multiphase, and long term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

advanced threat protection (ATP)
A form of security protection that detects network anomalies and flags abnormal events to address more complex attacks and safeguard key assets and data.

advisory
A document that contains information and analysis about a threat or vulnerability.

AG core
See access governance core.

alert A message or other indication that signals an event or an impending event that meets a set of specified criteria.

alias An alternative name used instead of a primary name.

anomaly
A deviation from the expected behavior of the network.

anomaly detection
The process of monitoring and isolating activity that falls outside of normal patterns across time, location, and user and traffic behavior.

AO See access optimizer.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application security
The practice of using software, hardware, and other methods to protect a web and mobile application from malicious threats.

application server
A server program in a distributed network that provides the execution environment for an application program.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

APT See advanced persistent threat.

AR See access request.

ARC See access risk control.

ARCS See access risk controls for SAP.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN See autonomous system number.

asset A collection of artifacts that provide a solution to a specific business problem. Assets can have relationships and variability or extension points to other assets.

asset test
A test that is used to identify potential risk indicators that signal when assets on a network violate a defined policy or introduce risk into the environment.

ATP See advanced threat protection.

attack Any attempt by an unauthorized person to compromise the operation of a software program or networked system. See also attacker.

attacker
A user (human or computer program) that attempts to cause harm to an information system or to access information not intended for general access. See also attack.

attack path
The source, destination, and devices associated with an attack.

attack pattern
Two or more related events that might indicate a specific type of attack, such as an unauthorized scan, a break-in attempt, or activity on a compromised asset.

attestation campaign
A process for checking if the authorizations held by a user are valid.

attribute
Data that is associated with a component. For example, a host name, IP address, or the number of hard drives can be attributes associated with a server component.

attribute group
An organizational view in a hierarchical notation that is based on a specific user attribute. An extra hierarchy can be created at any time by grouping users by attribute values.

audit A process that logs the user, administrator, and help desk activities.

audit trail
A chronological record of events or transactions. An audit trail is used for examining or reconstructing a sequence of events or transactions, managing security, and recovering lost transactions.

authentication
A security service that provides proof that a user of a computer system is genuinely who that person claims to be. Common mechanisms for implementing this service are passwords and digital signatures. See also authorization, credential.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization
The process of granting a user, system, or process either complete or restricted access to an object, resource, or function. See also authentication.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

authorization owner
A group of users who can define access control information (ACI) within the context of the organizational unit to which they belong.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

back door
A hole in the security of a system. It can be used by hackers to access sensitive information, or by programmers for maintenance and testing.

behavior
The observable effects of an operation or event, including its results.

big data
A data set whose size or type is beyond the ability of traditional relational databases to capture, manage, and process with low-latency. Four key dimensions of big data are volume, veracity, variety, and velocity.

binary security token
A security token that is binary encoded using a value type and an encoding type to interpret the token.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory. See also distinguished name.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

blacklist
A list of IP addresses or email addresses that are always identified as sources of spam.

block response
A default response that prevents attacks by dropping packets and sending resets to TCP connections.

BRole See business role.

brute force attack
An attack that uses a repetitive method of trial and error to obtain the user name and password for a valid account on a web application. If successful, the attacker can then access credit card numbers, cryptographic keys, profile data for confidential documents, and tools that are used to manage the user privileges and content of the web application.

buffer overflow
An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer overflows are a common cause of malfunctioning software.

business activity
See activity.

business process
A defined set of business activities that represent the required steps to achieve a business objective. A business process includes the flow and use of information and resources.

business role (BRole)
Any combination of application permissions, IT roles, and other business roles. Different business roles can be defined within the same organization unit.

C

CA See certificate authority.

candidate role
An aggregation of entitlements that are provided as output of the role mining process (see also access optimizer). It can be considered an "advised role" to be added into the role set of a company or organization.

CAPI See cryptographic application programming interface.

CDP See collateral damage potential.

cell security
The access control level assigned to a single cell in a cube.

centroid
A virtual point in an organizational unit hierarchy that is geometrically collocated close to the area of the hierarchy where the presence of a certain entitlement is a concentrated.

certificate
A digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate, Secure Sockets Layer.

certification campaign
See attestation campaign.

challenge-response authentication
An authentication method that requires users to respond to a prompt by providing information to verify their identity when they log in to the system. For example, when users forget their password, they are prompted (challenged) with a question to which they must provide an answer (response) in order to either receive a new password or receive a hint for specifying the correct password.

chief information security officer (CISO)
A person responsible for the protection of enterprise information and assets.

CIDR See Classless Inter-Domain Routing.

CISO See chief information security officer.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

clause A set of conditions and variable expressions that represent specific layers in a protocol stack.

cluster
A group of appliances in which one appliance acts as the central appliance, and the other appliances act as its clients.

collateral damage potential (CDP)
A measurement of the potential impact of an exploited vulnerability on a physical asset or on an organization.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

communications protocol
In networking, a set of standards defining how computers are to exchange information.

communications security
A system option that requires the identity of a remote location to be verified before that location can run programs on a system.

community
In SNMP, the relationship between an agent and one or more managers. The community describes which SNMP manager requests the SNMP agent should honor.

connector
A plug-in that is used to access and update data sources. A connector accesses the data and separates out the details of data manipulations and relationships.

console
A graphical user interface that simplifies the tasks for managing network security, such as monitoring events and scheduling scans.

contributing test
A test that examines the risk indicators that are specified in a question.

credential

1. A declaration of authorization or other security attributes of a subject that is typically validated and signed by a trusted third party. See also authentication, principal.
2. Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources. See also shared access.

credential pool
A group of credentials with similar access privileges. The pool can be defined as a service group or a set of service groups.

credential vault
A configured repository that stores credentials for shared access management.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

criticality
A rating, assigned by the user, which represents the potential vulnerability of an asset to a malicious exploit. The criticality rating contributes to the overall risk score of an asset.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

Cryptographic Service Provider (CSP)
A feature of the i5/OS operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

cryptography
A method for protecting information by transforming it (encrypting it) into an unreadable format, called ciphertext. Only users who possess a secret key can decipher (or decrypt) the message into plaintext.

CSP See Cryptographic Service Provider.

CVSS See Common Vulnerability Scoring System.

cybersecurity
The protection of computers, computer networks, related hardware devices, and the information they contain and communicate, including software and data.

D

daemon
A program that runs unattended to perform continuous or periodic functions, such as network control.

dark web
A network of thousands of websites that use anonymity tools to purposely conceal their IP addresses. See also deep web.

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

data model
A description of the organization of data in a manner that reflects the information structure of an enterprise.

data security
The protection of data against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

data set
The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

data warehouse
1. A central repository for all or significant parts of the data that an organization's business systems collect.
2. A subject-oriented collection of data that is used to support strategic decision making. The warehouse is the central point of data integration for business intelligence. It is the source of data for data marts within an enterprise and delivers a common view of enterprise data.

decrypt
To decipher data.

deed The presence of an event, a user, or both, in the working memory.

deep web
Any web content that is not indexed, and therefore cannot be found, by a standard search engine. See also dark web.

demilitarized zone (DMZ)
A configuration that includes multiple firewalls to add layers of protection between a corporate intranet and a public network, such as the Internet.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

destination
Any point or location, such as a program, node, station, printer, or a particular terminal, to which information is to be sent.

DHCP lease
The length of time that a DHCP server allows a client to use an assigned IP address.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

directory
A file that contains the names and controlling information for objects or other directories.

directory server
A server that can add, delete, change, or search directory information on behalf of a client.

directory service
A directory of names, profile information, and machine addresses of every

user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region. See also bind distinguished name.

DMZ See demilitarized zone.

DN See distinguished name.

DNS See Domain Name System.

domain
A set of data on which conflict analyses are carried out. It can be identified by a set of applications (or by a set of permissions that are related to applications). A single application can be included in several domains.

domain administrator
The owner of an administrative domain.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

dynamic organizational role
An organizational role that is assigned to a person by using an LDAP filter. When a user is added to the system and the LDAP filter parameters are met, the user is automatically added to the dynamic organizational role.

E

Encapsulated Security Payload (ESP)
In a virtual private network (VPN), a security protocol that provides data confidentiality and integrity.

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

encryption key
A mathematical value that allows components to verify that they are in communication with the expected server. Encryption keys are based on a public or private key pair that is created during the installation process.

enterprise connector (ERC)
A module that aligns the Access Governance Core module with the peripheral target systems and vice versa.

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

entitlement
The identification of a structured set of rights that are assigned to a generic user for access to the resources of a company or organization. There are four types of entitlement: business role, IT role, permission, and external role.

ERC See enterprise connector.

escalation
A course of action that runs when a task is not completed satisfactorily within a specific period of time. See also escalation limit.

escalation limit
The amount of time, for example hours or days, that a participant has to respond to a request, before an escalation occurs. See also escalation.

ESM See external security manager.

ESP See Encapsulated Security Payload.

ESSO See enterprise single sign-on.

event An occurrence of significance to a task or system. Events can include completion or failure of an operation, a user action, or the change in state of a process.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

event collector
A component that manages real-time events from sensors and vulnerability data from scanners.

event marker
A marker that represents the target system as the sender or recipient of connected events to or from IBM Security Identity Governance.

event notification
The process of notifying a user about an event.

expression
A variable in a firewall rule that specifies adapter numbers, network addresses, port numbers, ICMP parameters, or IP datagram protocol numbers.

external role
A particular type of entitlement, which is built on a set of permissions and roles that are received from an external application (or target). It is conceptually like a business role, but is received directly from a connected target.

external security manager (ESM)
A security product that performs security checking on users and resources. RACF is an example of an ESM.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

false positive
A test result classed as positive (indicating that the site is vulnerable to attack), that the user decides is in fact negative (not a vulnerability).

false positive exception rule
A rule specific to low-risk vulnerabilities that minimizes the volume of vulnerabilities that are managed.

farness
A numeric index that provides an estimate of the virtual distance between OUs which have the same entitlement/candidate role, for example the distance between OUs in which different registered users are aggregated to the same entitlement/candidate role.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

file security packet (FSP)
In z/OS UNIX, a control block containing the security data (owner user identifier (UID), owner group identifier (GID), and the permission bits) associated with the file. This data is stored with the file in the file system.

File Transfer Protocol (FTP)
In TCP/IP, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter A device or program that separates data, signals, or material in accordance with specified criteria.

FIPS See Federal Information Processing Standard.

firewall
A network configuration, typically both hardware and software, that prevents unauthorized traffic into and out of a secure network.

firewall rule
A chain of statements matching specific criteria that define the types of traffic to block on a network.

firmware
Proprietary code that is usually delivered as microcode as part of an operating system.

FSP See file security packet.

FTP See File Transfer Protocol.

fulfillment
The function through which requests to create, update, or remove accounts are initiated.

G

gateway
A device or program used to connect networks or systems with different network architectures.

GINA See graphical identification and authentication.

global security
Pertains to all applications running in the environment and determines whether security is used, the type of registry used for authentication, and other values, many of which act as defaults.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

ham An email message that does not contain advertising or inappropriate content. See also unsolicited email.

hardening
The process of protecting security data from exposure to vulnerabilities by establishing restricted access to the data.

hardware security module (HSM)
A hardware component that provides secure storage for RSA keys and accelerates RSA operations.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

health check
A process that monitors system resources and conditions to determine whether the system is running efficiently. The health check can be configured to report potential problems and to display warnings and fail levels before the integrity of the system is compromised.

heartbeat
A signal that one entity sends to another to convey that it is still active.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

HSM See hardware security module.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

IAG See Identity and Access Governance.

IAG activity
A step, such as generation, authorization, or execution of a request, in an authorization workflow.

IAG actor
Any user that can operate or is associated with an administrative role.

IAG administrator
An administrator that can assign IAG roles.

IAG operator
See IAG actor.

IAG process
A set of activities that support an authorization process.

IAM See identity and access management.

ICMP See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

Identity and Access Governance (IAG)
The strengthening of compliance and reduction of risk by protecting and monitoring user access in today's multi-perimeter environments.

identity and access management (IAM)
The process of controlling access of authorized users to data and applications, while helping companies comply with various regulatory requirements.

identity management
A set of enterprise search APIs that control access to secure data and enable users to search a collection without being required to specify a user ID and password for each repository in the collection.

identity policy
The policy that defines the user ID to be used when creating an account for a user.

IDS See intrusion detection system.

IIOP See Internet Inter-ORB Protocol.

incident
An event that has been defined by a site administrator as a possible attack.

information disclosure attack
An attack that attempts to obtain system-specific information about a website, such as software distribution, version numbers, patch levels, and the location of backup files or temporary files.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Inter-ORB Protocol (IIOP)
A protocol used for communication between Common Object Request Broker Architecture (CORBA) object request brokers.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

Internet Protocol Security (IPsec)
A set of protocols that provide cryptographic security services at the network layer. See also virtual private network.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention
A set of policies and rules for detecting suspicious behavior in network traffic and for alerting system or network administrators.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP See Internet Protocol.

IPS See intrusion prevention system.

IPsec See Internet Protocol Security.

IT role
A collection of permissions that are defined within the context of a single system or application. It can contain other IT roles of the same application. See also application role.

J

Java Database Connectivity (JDBC)
An industry standard for database-independent connectivity between the Java platform and a wide range of databases. The JDBC interface provides a call level interface for SQL-based and XQuery-based database access.

JDBC See Java Database Connectivity.

job A separately executable unit of work.

job group security
A security model in which groups of users can access and control a common set of jobs owned by that group.

join directive
The set of rules that define how to handle attributes when two or more

provisioning policies are applied. Two or more policies might have overlapping scope, so the join directive specifies what actions to take when this overlap occurs.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

LDAP Data Interchange Format (LDIF)
A format used by the ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries in a standard portable text form.

LDAP directory
A type of repository that stores information on people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the repository are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP Directory Interchange Format (LDIF)
A file format that is used to describe directory information as well as changes that need to be applied to a directory, such that directory information can be exchanged between directory servers that are using LDAP.

LDIF
1. See LDAP Directory Interchange Format.
2. See LDAP Data Interchange Format.

lifecycle
Passage or transformation through different stages over time. For example markets, brands and offerings have lifecycles.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Citrix/Terminal Server and improves the single sign-on startup duration.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

malicious file execution attack
An attack that uses SMB file wrappers in PHP scripting language to run code, install a root kit, or compromise an entire system on a web server remotely.

malware
Software that is designed to disrupt or gain unauthorized access to a system, gather information that compromises a person's privacy or assets, or other behavior that is harmful to the user.

managed resource
An entity that exists in the runtime environment of an IT system and that can be managed. See also resource.

Management Information Base (MIB)
A definition for management information that specifies the information available from a host or gateway and the operations allowed.

man-in-the-middle attack
An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions.

MIB See Management Information Base.

minability
An indicator of the efficiency of aggregating assignments into roles. Minability provides a measure of how to easily build and define a role.

mitigation control
A policy that can be associated with a user to perform a work task, that is unauthorized by an SoD analysis or by other risk scenarios.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

multilevel security
A security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. The system imposes mandatory access controls restricting which users can access data based on a comparison of the classification of the users and the data.

multiple-context device
A single appliance that is partitioned into multiple virtual devices. Each virtual device is an independent device, with its own security policy.

N

namespace
Space reserved by a file system to contain the names of its objects.

NAT See network address translation.

National Vulnerability Database (NVD)
A catalog of publicly-known information security vulnerabilities and exposures maintained by the National Institute of Standards and Technology (NIST).

nested group
A group that is contained within another group.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

netmask
See network mask.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network mask (netmask)
A number that is the same as an Internet Protocol (IP) address. A network mask identifies which part of an address is to be used for an operation, such as making a TCP/IP connection.

network object
A group of predefined settings that can be shared among multiple network access policy rules to control traffic flow, communication, and access between hosts, segments, or subnets on a network.

network security layer
The protection of a network from malicious activity through monitoring, collecting, and analyzing network activities.

NVD See National Vulnerability Database.

O

object security
A security level that allows the user to control access to specific objects in the directory, using an access control list (ACL).

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

on-demand scan
A scan that runs only when initiated by the user. The types of scans include full scans, discovery scans, patch scans, PCI scans, database scans and web scans.

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

operation
A specific action (such as add, multiply, or shift) that the computer performs when requested.

operational window
A configured time period within which a scan is permitted to run.

organization
A hierarchical arrangement of organizational units, such that each user is included once and only once.

organizational role
In identity management, a list of account owners that is used to determine which entitlements are provisioned to them.

organization tree
A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organization unit (OU)
Primary component of an organization, providing a context for its management. Organization structure relates a parent unit to its subsidiaries in a hierarchy, and each unit is responsible for collections of other business components.

orphan account
On a managed resource, an account whose owner cannot be automatically determined by the provisioning system.

OSI See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

OU See organization unit.

P

packet A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet.

packet capture
The process of intercepting and logging network traffic.

Padding Oracle On Downgraded Legacy Encryption (POODLE)
A security vulnerability that affects the SSL protocol 3.0 (SSLv3). An attacker can get clear text data by exploiting this vulnerability.

PAM See Protocol Analysis Module.

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process.

parm See parameter.

participant
In identity management, an individual, a role, a group, or a JavaScript script that has the authority to respond to a request that is part of a workflow.

passive authentication
A configuration option that automatically logs users into a system when they log on to a network using a directory service, such as Active Directory.

passphrase
A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for added security.

password
In computer and network security, a specific string of characters used by a program, computer operator, or user to access the system and the information stored within it.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

path traversal attack
An attack that uses special character sequences to exploit a URL and gain access to restricted files, directories, and commands that are located in the web document root directory or the CGI root directory.

Payment Card Industry Data Security Standard (PCI DSS)
A worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments to prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

PCI DSS
See Payment Card Industry Data Security Standard.

PCI severity level
The level of risk that a vulnerability poses to the payment card industry.

PD See process designer.

permission
Authorization to perform activities, such as reading and writing local files, creating network connections, and loading native code. See also administrative domain.

permission inheritance
An option that automatically assigns an asset subgroup the same permission settings as the asset group above it in the group hierarchy.

persona
A user archetype based on role and other characteristics that influence how a user interacts with the offering.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

phisher
A person who engages in a type of email fraud called phishing. See also phishing.

phishing
The act of tricking a user into providing personal or financial information by falsely claiming to be a legitimate entity. See also phisher.

physical security
The protective measures that restrict access to a site, provide stability through hardware redundancy, and ensure network restoration in case of an outage or disaster.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

plug-in
A separately installable software module that adds function to an existing program, application, or interface.

policy A set of considerations that influence the behavior of a managed resource or a user.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

polyarchy
See attribute group.

POODLE
See Padding Oracle On Downgraded Legacy Encryption.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

principal
An entity that can communicate securely with another entity. A principal is identified by its associated security context, which defines its access rights. See also credential.

process
In the context of a PD module, a group of activities that manage the lifecycle of an authorization request. A process can consist of a single activity (direct process) or a series of activities (workflow process).

process designer (PD)
A module that designs and defines the authorization processes managed by the ARM module (front-end authorization workflows). The PD module provides a modeler capable of outlining every type of workflow for building custom authorization processes.

profile
Data that describes the characteristics of a user, group, resource, program, device, or remote location.

programmatic security
A collection of methods used by applications when declarative security is not sufficient to express the security model of the application.

protection domain
A group of access permissions to interfaces, VLans or IP addresses that are used to define policies for multiple network segments that are monitored by a single appliance.

protection interface
An access point on a network appliance that is used to monitor, inspect, and block network traffic as it passes through the appliance.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Protocol Analysis Module (PAM)
A deep-pack inspection engine that stores handling specifications for a comprehensive list of vulnerability checks. PAM interprets the vulnerability checks, processes the results as security events, and then sends the security events to the appliance in X-Press Updates.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning policy
A policy that defines the access to various managed resources, such as

applications or operating systems. Access is granted to all users, users with a specific role, or users who are not members of a specific role.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

proxy server
A server that receives requests intended for another server and that acts on behalf of the client (as the client's proxy) to obtain the requested service. A proxy server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but should be permitted some services.

public key
The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures and to encrypt data that can be decrypted only with the corresponding private key.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

Q

quarantine rule
A set of responses that block DDoS attacks, prevent worms from spreading, and deny access to systems that are infected with backdoors or Trojan horses.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RBAC See role-based access control.

RD See report designer.

RDP See Remote Desktop Protocol.

realm A named collection of users and groups that can be used in a specific security context.

reconciliation
The process of ensuring consistency between the original data repository and the larger system where the data is stored for backup. Examples of larger systems where the data is stored for backup are storage servers or other storage systems. During the reconciliation process, data that is identified as no longer needed is removed.

recording
A collection of information about user actions performed on a monitored application for some time.

recording daemon
A privileged process running on the same endpoint as the monitored application, which performs operations that require elevated privileges.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

registry
A repository that contains access and configuration information for users, systems, and software.

relevance
A measure of relative impact of an event, category, or offense on the network.

remediation process
A process of assigning, tracking, and fixing vulnerabilities that have been identified on an asset.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

Remote Desktop Protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

repo See repository.

report designer (RD)
A module that designs and defines reports. The RD module's front-end component provides a modeler capable of outlining every type of report. Using this modeler, the administrator can visually represent the report creation process.

repository (repo)
A persistent storage area for data and other application resources.

request
An item that initiates a workflow and the various activities of a workflow. See also workflow.

request for information (RFI)
A workflow activity that requests additional information from the specified participant.

resource

1. A hardware, software, or data entity. See also managed resource.
2. A logical or physical object that is useful for access governance and that can be associated to a certain user. For example, a resource can be a current bank account, a transmission device in a telecommunications system, a network folder, or a document.

response
The reaction of an appliance to an event. Responses include sending an email message to a responsible party, triggering an SNMP trap, creating a log of the activity, quarantining the activity, or using a custom (user-specified) action, such as running an application or running a command.

revoke
To remove a privilege or an authority from an authorization identifier.

RFI See request for information.

RFID See radio frequency identification.

rights The permission to perform a certain action on a specific resource.

risk A possible threat or potential damage that can be classified inside a company or organization. Risks are modeled by rules and constraints of business activities into a data model.

risk indicator
A measure of the potential exposure of a system to a security breach.

risk score
A measure of how much risk an asset poses to a site, based on how critical the asset is and the amount and severity of attacks made against the asset.

risky protocol
A protocol that is associated with services that run on an open port in inbound communications from the internet to the DMZ.

Rivest-Shamir-Adleman algorithm (RSA)
A public-key encryption technology developed by RSA Data Security, Inc, and used in the IBM implementation of SSL.

role

1. The part played by an organization that is understood by all of the other organizations that are associated with that particular hub.
2. A job function that identifies the tasks that a user can perform and the resources to which a user has access. A user can be assigned one or more roles.
3. A collection of access rights that can be assigned to a user, group of users, system, service, or application that enable it to carry out certain tasks.

role-based access control (RBAC)
The process of restricting integral components of a system based on user authentication, roles, and permissions.

role-based security
Security that provides access rights to certain files, business processes, web templates, and features, according to the permissions associated with the user account.

root The user name for the system user with the most authority.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

rootkit
Malicious software that enables a hacker to gain administrator-level access to a computer or computer network.

RSA See Rivest-Shamir-Adleman algorithm.

rule A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

SAML See Security Assertion Markup Language.

scanner
The software used to gather hardware information and software information from systems and devices.

scan profile
The configuration information that specifies how and when the assets on a network are scanned for vulnerabilities.

schema
A collection of database objects such as tables, views, indexes, or triggers that define a database. A schema provides a logical classification of database objects.

scope In identity management, the set of entities that a policy or an access control item (ACI) can affect.

SECMEC
See security mechanism.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Shell (SSH)
A network protocol for secure data exchange between two networked devices. The client can use public-key and private-key authentication, or password authentication, to access the remote server.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. See also certificate authority.

security
The protection of data, system operations, and devices from accidental or intentional ruin, damage, or exposure.

security as a service
The delivery of security services through the cloud.

Security Assertion Markup Language (SAML)
An XML framework for exchanging authentication and authorization information.

security audit
A manual or systematic measurable technical assessment of a system or application.

security category
A non-hierarchical grouping of sensitive information used to control access to data.

security certificate
A certificate containing information used by the SSL protocol to establish a secure connection. The information can include who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate.

security constraint
A declaration of how to protect web content, and how to protect data that is communicated between the client and the server.

security dimension
A collection of related values that can be used to label a user according to their role or security clearance, with the aim of affecting their access to information.

security entity
Entities used to specify what a user is authorized to do. Security entities include roles and users.

security event
Any network occurrence or activity that may have an impact on the security of the network.

security group
A group defined for the purpose of providing access to applications and optionally to collections of data.

security intelligence
The advanced analytics, expert analysis, and swift remediation of security risks to safeguard the enterprise from dangerous events and attacks without sacrificing innovation and growth.

security list
A set of users and user groups matched with permissions or permission groups and optional organization restrictions. It defines who can access an object, action, or feature that contains it, and what they can do once accessed.

security mechanism (SECMEC)
A technical tool or technique that is used to implement a security service. A mechanism might operate by itself, or in conjunction with others, to provide a particular service. Examples of security mechanisms include access control lists, cryptography, and digital signatures.

security object
An object such as a user, group, or role that is created for authentication and authorization purposes.

security officer
A person assigned to control all of the security authorizations provided with the system. A security officer can, for example, remove password or resource security or add, change, or remove security information about any system user.

security operations center (SOC)
A centralized enterprise unit that monitors security threats, manages incident reporting, recruits and manages security personnel, develops and documents processes, and leads the strategy for handling emerging threats.

security policy
A set of rules that determine the type of security event an agent detects, the priority of each event, and the way an agent responds to an event.

security profile
A role-based security model that supports classes of service, which have different levels of access to system and repository information.

security risk
The potential success of a threat and the damage that could ensue.

security service
A service within a computer system that protect its resources. Access control is an example of a security service.

security template
A set of security settings that can be applied to a document, folder, or custom object. Security templates are components of security policies.

security token (STOKEN)
In RACF, a collection of security information that represents data to be accessed, a user, or a job. A security token contains a user ID, a group ID, a security label, the node of origin, and other information.

Security Token Service
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

segregation of duties (SoD)
A conflict of interests that arises after the assignment, to a user, of a specific entitlement that is incompatible with the already assigned entitlements.

self-care
A method that supplies a set of operations so users can create and administer their own accounts, which they can provision into business-to-consumer environments.

sensor Software that monitors security networks, applications, or systems for security-related information, possibly indicative of suspicious activity.

separation of duties (SOD)
A principle of organizing complex structures by dividing tasks and responsibilities between the members of an organization in order to prevent any member from having complete control of any transaction from initialization to completion.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use it as a second factor in AccessAgent.

service selection policy
A policy that determines which service to use in a provisioning policy.

severity
A measure of the relative threat that a source poses on a destination.

share A folder or file that is made accessible to multiple components or users on a network.

shared access
Access to a resource or application using a shared credential. See also credential.

shared access policy
A policy that authorizes role members to share access by credentials or credential pools. A policy can be defined for a specific credential pool, a specific credential, or all pools or all credentials with the same organization container context.

shared secret
An encrypted value that is used to retrieve the initial password of a user. This value is defined when the personal information for the user is initially loaded into the system.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB). See also SNMP manager, SNMP trap.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

site The set of components that monitor and control agents.

site database
The database where security data, command and control jobs, and asset information are kept.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
An image that is an exact copy of the original files or directories from which it was created.

SNMP
See Simple Network Management Protocol.

SNMP manager
A host that collects information from SNMP agents through the SNMP. See also Simple Network Management Protocol.

SNMP trap
An SNMP message sent from the SNMP agent to the SNMP manager. The message is initiated by the SNMP agent and is not a response to a message sent from the SNMP manager. See also Simple Network Management Protocol.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

SOC See security operations center.

SoD

1. See separation of duties.
2. See segregation of duties.

SOD See separation of duties.

spam

1. See unsolicited email.
2. To send unsolicited email to a large number of addresses.

spear phishing
A targeted phishing attack that is directed at a particular company, organization, group or government agency.

SPI See service provider interface.

spoofing
The practice of masquerading as a trusted system to try to obtain confidential information. For example, when a would-be intruder sets up a client system with an IP address that is trusted by another system, it is called IP spoofing.

spyware
Malicious software that is designed to transmit information or take partial control of a computer without the informed consent of the user of the computer.

SSH See Secure Shell.

SSL See Secure Sockets Layer.

SSO See single sign-on.

static organizational role
An organizational role that is manually assigned to a person.

STOKEN
See security token.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

supply chain security
The protection of products, facilities, equipment, information, and personnel from theft, damage, or terrorism and the prevention of the introduction of unauthorized material, people, or weapons of mass destruction/effect into the supply chain.

system security
A system function that restricts the use of files, libraries, folders, and devices to certain users.

T

target A technical view of an IT application (for example, active directory). A target can refer to several applications.

target definition file
A Java archive file that defines managed resource types.

target profile
See target type.

target type
A category of related targets that share schemas.

task A set of jobs (TP module) that are linked together to form a complex function to be run.

task planner
A module that is used to manage asynchronous processes that can be completed at a future time (for example, processes involved in the production of reports or for some type of batch processing).

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

threat A security issue, or a harmful act, such as the deployment of a virus or illegal network penetration.

TLS See Transport Layer Security.

to-do list
A collection of outstanding activities.

token A particular message or bit pattern that signifies permission or temporary control to transmit over a network.

topology graph
A graph that describes subnets, devices, and firewalls.

topology model
A virtual representation of the arrangement of network assets that is used to simulate an attack.

traceroute
A utility that traces a packet from a computer to a remote destination, showing how many hops the packet required to reach the destination and how long each hop took.

traffic In data communication, the quantity of data transmitted past a particular point in a path.

transparent screen lock
A feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

Transport Layer Security (TLS)
A set of encryption rules that uses verified certificates and encryption keys to secure communications over the Internet. TLS is an update to the SSL protocol.

transport protocol
A specification of the rules that govern the exchange of information between components of a transport network; for example, the User Datagram Protocol (UDP).

trap In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

Trojan horse
A computer program that appears to perform a useful and innocent function but contains hidden functions that use approved authorizations assigned to users when they start the program. For example, it may copy internal authorization information from a computer and send it back to the originator of the Trojan horse.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for

authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

UME See user multiple entries.

Uniform Resource Identifier (URI)
A compact string of characters for identifying an abstract or physical resource.

unsolicited email
Unwelcome and bothersome email. See also ham.

URI See Uniform Resource Identifier.

user Any individual, organization, process, device, program, protocol, or system that uses the services of a computing system.

user-account matching
The Identity Governance and Intelligence module that manages orphan accounts and account mismatching with company policies.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user multiple entries (UME)
A user that has more than one account on the same target system.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

violation
An act that bypasses or contravenes corporate policy.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual member manager
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure. See also Internet Protocol Security.

VPN See virtual private network.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web filter inspection object
A filter that is used to control the types of web pages that users can access on a network.

web security
The theory and practice of information security relating to the World Wide Web, HTTP and web application software.

Web Services Security (WSS, WS-Security)
A flexible standard that is used to secure web services at the message level within multiple security models. SOAP messages can be secured through XML digital signature, confidentiality can be secured through XML encryption, and credential propagation can be secured through security tokens.

whaling
A phishing attack that is directed against high-level executives within a single organization, or executive positions common to multiple organizations.

whitelist
A list of approved websites which are ignored by the software to block pop-up ad windows and allowed to function without interference.

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.

workflow
The sequence of activities performed in accordance with the business processes of an enterprise. See also request.

worm A self-replicating standalone malware program that spreads across a network through security vulnerabilities.

WSS See Web Services Security.

WS-Security
See Web Services Security.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

X

X-Press Update (XPU)
A software update that is issued between major releases to protect a network against the latest security vulnerabilities and threats.

XPU See X-Press Update.

Z

zero configuration networking
A set of techniques or technologies used by an application to automatically discover devices on a network and configure network settings.

zeroize
To erase electronically stored data, cryptographic keys, or CSPs from a cryptographic module.

Index

G

Printed in USA