Realize business value by choosing the right identity and access assurance solution

IBM

Organizations need to manage an increasing number of users, applications and access points, all while trying to ensure regulatory compliance. They need a security infrastructure that can address short-term requirements, such as costs reduction, integrating mergers and acquisitions, and effectively managing changes in workforce, but also longer-term goals, such as enabling the organization to implement growth initiatives through new portal and Web services projects, and positioning the organization to quickly leverage new delivery platforms such as cloud computing and service-oriented architecture (SOA).

Executives increasingly want to see the business value that can be delivered by an identity and access assurance solution because how effectively an organization addresses these challenges can have a significant impact on its competitive posture and profitability. They want to innovate and provide convenient access to applications and systems while ensuring strong security and compliance. To remain competitive, they want to facilitate collaboration of employees, customers or constituents, and partners through role-based portals, and quickly roll-out new services to these users.

To achieve these goals, organizations must be able to:

- Authenticate and authorize users before allowing access to resources.
- Address access control policies that range from simple decisions based on group membership to real-time decisions based on business conditions and data.
- Monitor that the access follows appropriate use policies and is consistent with regulations.
- Take corrective action where compliance policy violations are detected.
- Protect access to critical data across the organization.
- Integrate new identities from mergers and acquisitions.
- Ensure that user entitlements are revoked in a timely manner once they are no longer needed.
- Free up budget for new initiatives by controlling costs in areas such as help desk, application development security coding, and compliance reporting.
- Support requests for new initiatives, such as cloud computing, portal and SOA projects.
- Improve employee, administrator and user productivity.

An effective solution for identity and access assurance brings together complete capabilities from a trusted partner for administering, securing and auditing user access to resources. Such a solution can help an organization realize business value and achieve both short- and long-term objectives.

This buyer's guide can help you select the right solution to attain identity and access assurance by successfully managing and controlling access within, across and between organizations. It outlines the most common identity and access management challenges organizations face from the perspective of CSOs, IT operations staff, line-of-business managers and enterprise architects. It then provides information about the capabilities required to directly address the challenges of complexity, compliance and cost. This information will help you assess whether a particular vendor's offerings best address the challenges you've prioritized.

Getting started with identity and access management

When selecting a solution that will deliver identity and access assurance, these main categories should be addressed:

1. Managing users and user information throughout the entire lifecycle

2. Maximizing user productivity by ensuring efficient access to resources

3. Managing and enforcing access control policies across every application, data source, operating system and organizational boundary consistently

4. Monitoring and auditing user access

5. Accelerating time to value

6. Selecting the right identity and access assurance provider

For each category, you'll find checklists below that you can use when evaluating vendors and their products.

1. Managing users and user information throughout the entire lifecycle

IT staff often spend an inordinate amount of time managing user permissions and policies that can exist in hundreds of different places. Adding user roles, identities and access rights on a case-by-case basis can be a complex undertaking that can take from hours to weeks. Removing these rights can take just as long and brings the additional risk of missing a user whose access should have been terminated.

And even after the initial user rights have been assigned, IT staff must perform ongoing reconciliation, recertification and reporting to ensure that access points such as portals and Web sites are secure and that data remains safe. Every time a person changes jobs, roles or employment status, all of their existing rights must be evaluated and altered accordingly, while maintaining appropriate separation of duties.

Centralized, automated solutions enable you to manage tasks for administering and auditing user roles, identities, credentials, accounts and access permissions more efficiently. Automation reduces costs by relieving IT staff of repetitive tasks, thereby helping to ensure that security is administered in a uniform manner from the initial onboarding of users to the eventual offboarding.

User lifecycle management

Look for a solution that:	IBM	Other vendor
Provides a single, secure, auditable identity repository.	✓	
Provides an integrated Web-based interface that includes both simple wizards and a rich configuration editor to enable you to easily create, modify and view configuration objects and their relationships.	✓	
Delivers flexible account adoption methods needed to effectively and securely map accounts to their users.	✓	
Provides integrated role-based access control (RBAC), rule/attribute-based access control (ABAC), and request-based provisioning options.	✓	
Offers operational role management as an embedded functionality within the user provisioning platform.	✓	
Tightly integrates user provisioning with role management, separation of duties, and recertification with open interfaces for integration with continuous business controls systems.	✓	
Offers role hierarchy to simplify mapping of users and permissions.	✓	
Delivers preventive and detective separation of duties to mitigate the risk generated by conflicting user access rights.	✓	
Enables recertification of a user's role, account and group membership as a single, simple activity.	✓	
Supports identity management on a group basis, simplifying and reducing the cost of user administration.	✓	
Supports tools to build user provisioning workflows using both simple wizard-based navigation and a drag-and-drop GUI for more advanced business processes—all from a common Web interface.	✓	

User lifecycle management

Look for a solution that:	IBM	Other vendor
Manages distributed sets of users and includes the ability to assign these users to single or multiple roles.	✓	
Reconciles accounts automatically and in an on-demand way to rapidly and reliably discover invalid "orphaned" accounts and unnecessary entitlements, and to initiate either automatic or manual remediation processes.	✓	
Automates user lifecycle management, from onboarding to offboarding.	✓	
Leverages identity integration capabilities to establish rules that identify which groups and individuals have the authority to change which data fields.	✓	
Maintains accurate records of configuration and changes to user access rights for auditing purposes.	✓	
Provides access to both approval and operational workflows, allowing customization of the provisioning activity.	✓	
Supports provisioning intranet and extranet profiles equally well.	✓	
Supports manual services out of the box so that individuals can quickly and easily automate business processes related to phone orders and other manually administered items, and so they can gain governance over targets while still performing provisioning tasks manually.	✓	
Provides a customizable role-based user GUI with views such as Manager, End User, Auditor, and Help Desk out of the box.	✓	
Provides lifecycle management of privileged and shared identities to ensure individual accountability.	✓	

2. Maximizing user productivity by ensuring efficient access to resources

Giving employees timely, straightforward access to applications and services can make them more productive, while protecting access to business-sensitive data on a need-to-know basis can help protect the organization from growing threats and vulnerabilities. Opening access for customers, constituents and partners carries with it the promise of new value and growth opportunities. But increasing the number of legitimate users creates complex environments and significant security challenges. Users will not be satisfied or productive if security controls block access to the resources they need or make access excessively cumbersome by requiring multiple logins and authentications.

Entering, changing and resetting passwords add up to a significant amount of employee and IT staff time—with resulting increases in operational costs. Single sign-on (SSO) capabilities across enterprise, Web-based and federated systems can minimize a number of password-related problems and improve user productivity.

Federated SSO capabilities enable users to navigate seamlessly among Web sites across domain boundaries. Reducing both frustration and user administration costs, federated SSO capabilities promote a seamless collaboration environment with partner organizations.

Self-service capabilities can further enhance the user experience by allowing users to manage their own accounts and reset passwords. With these capabilities, users can get back up and running quickly without the added time and cost of calling the IT help desk.

Core capabilities for user access management

Look for a solution that:	IBM	Other vendor
Offers an intuitive, customizable administration GUI with point-and-click capabilities that enable you to easily create new user GUI views.	✓	
Includes a multitasking feature within the administration GUI that enables you to start a task, open a second task and then toggle back to the original task and complete it.	✓	
Allows you to submit and track status requests and monitor workflow tasks from a single GUI.	✓	
Delivers wizards and templates for fast, easy configuration along with easy GUI access to the generated script for granular customization.	✓	
Provides out-of-the-box authentication integration using a documented integration path with open APIs for a wide variety of authentication solutions.	✓	
Provides a complete and integrated federation and trust management solution that includes a general-purpose security token service for common standards-based identity propagation within a Web services/SOA environment.	✓	
Provides standards-based development for extension of the security token service via Eclipse-based plug-ins.	✓	
Offers strong integration with enterprise service bus (ESB), including IBM WebSphere® Enterprise Service Bus, to facilitate and secure federated access to the ESB.	✓	

Core capabilities for user access management

Look for a solution that:	IBM	Other vendor
Includes robust directory and directory integration and synchronization products at no additional charge.	✓	
Supports designating the authorization level required for access to protected resources and enforcing a step-up policy when users must provide the next level of authentication.	✓	
Provides standards-based (XACML) entitlements management (roles, rules, attributes) for data security and fine-grained access control.	✓	
Provides SOA security policy management (message protection policies support).	✓	
Offers a completely configurable authentication mechanism, along with an external authentication interface to accommodate Web applications written in any language.	✓	
Addresses password policy, login policy, file access control, TCP port access control, application protection and accountability for Linux® and UNIX® environments, including virtualized environments (IBM AIX® LPARs/WPARs, Solaris Zones, VMware).	✓	
Integrates widely with identity servers, applications, middleware, operating systems and platforms.	✓	
Offers closed-loop access and audit management support including integration with existing security information and event management tools.	✓	

Web and federated single sign-on (SSO)

Look for a solution that:	IBM	Other vendor
Delivers unified SSO to users across desktop applications, Web applications and more, including IBM WebSphere, Microsoft®, Oracle and many other portal and application environments.	✓	
Provides direct SSO support for Microsoft .NET environment applications such as Microsoft SharePoint and Exchange servers.	✓	
Simplifies Microsoft user logins by honoring password changes for Active Directory (AD), supporting the use of AD alternate userPrincipalName (UPN) e-mail addresses for authentication and Active Directory Application Mode (ADAM) as a user registry.	✓	
Supports multiple standards for cross-site authentication, including Security Assurance Markup Language (SAML), Liberty Alliance and Web Services Federation Language (WS-Federation) token-passing protocols.	✓	
Supports SAML 2.0 Attribute Query and Authentication Authority for secure collaboration with business partners.	✓	
Supports OpenID Attribute services for secure collaboration with consumers.	✓	
Supports the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) protocol to enable users to access multiple Web resources with just one login.	✓	
Supports WS-Security Policy for Web Services authorization as well as WS-Metadata Exchange and WS-Notification for secure IT integration.	✓	
Supports Java™ EE and .NET application and Web services integration using existing application identity (e.g. LTPA, Kerberos, and SAML) protocols.	✓	

Web and federated single sign-on (SSO)

Look for a solution that:	IBM	Other vendor
Supports mainframe application and Web services integration including using RACF PassTicket protocol.	✓	
Builds fault tolerance into the solution, rather than relying on optional third-party tools.	✓	
Centrally controls access to on- and off-premise applications including SaaS and cloud-based services.	✓	
Offers a Java administration API to manage large scale users and groups.	✓	
Supports HTTP 1.1 for persistent application connections.	✓	
Supports combined TCP and SSL junctions for Web protection.	✓	
Integrates with WebSphere DataPower® for Web-services support in the demilitarized zone.	✓	
Provides business-to-consumer (B2C) self-service interfaces for user enrollments, user validation, account updates, and password resets and synchronization.	✓	
Provides high availability by replicating policy (versus caching only), so that policy enforcement can take place even if the link to the policy server is down.	✓	
Utilizes a Web authorization approach that offers high performance and scales to user implementations in the tens of millions as well as to hundreds of applications.	✓	
Offers a flexible Java Web-based architecture that can protect resources using either a hardened reverse proxy, or a plug-in module to an existing Web server. (In certain cases, a dedicated proxy can offer a higher level of security.)	✓	

Web and federated single sign-on (SSO)

Look for a solution that:	IBM	Other vendor
Offers proven reverse proxy technology (as demonstrated by more than 1,000 customer installations), which is a superior approach from a change and configuration management perspective.	✓	
Includes session management services that can improve performance by limiting the number of sessions created on a per-realm basis, eliminating server restarts and allowing multiple server instances to share user sessions.	✓	
Provides session management services that allow for the immediate termination of all active sessions for a malicious user.	✓	
Offers a post office (anti-spam) feature that aggregates like e-mails and user work items.	✓	
Supports a lightweight federation solution to enable smaller organizations to quickly establish federations with a large organization.	✓	
Supports B2C federation with emerging user-centric identities including OpenID and Information Card Profile using identity selectors such as Microsoft CardSpace or Higgins identity framework.	✓	
Supports user access across Web 2.0 and Web services, including out-of-box integration with existing XML gateways (e.g. WebSphere DataPower).	✓	
Supports broad and flexible integration with strong third-party authentication solutions.	✓	

Automating access to enterprise applications

Look for a solution that:	IBM	Other vendor
Includes an enterprise single sign-on (ESSO) solution that is distinguished in the marketplace by its advanced capabilities to work with many different kinds of applications, integration with strong authentication, flexible approach to session management, and ability to log and audit end-user activities.	✓	
Includes a leading ESSO solution that is fully integrated, developed and supported by the same vendor providing comprehensive identity and access assurance.	✓	
Offers an ESSO solution built on a Java EE architecture.	✓	
Provides an ESSO solution that integrates with Web, desktop, teletype and mainframe applications, as well as many client device platforms such as Microsoft Windows® CE and Windows XPe to accommodate the broadest possible range of applications.	✓	
Takes automation beyond simple SSO through the ability to automate the logon, password change and logoff processes through workflow extensions.	✓	
Provides an ESSO solution that includes a wide variety of session management capabilities including support for personal desktops, shared desktops (kiosk), private desktops (kiosk with multiple sessions), terminal clients, dial-up sessions, pervasive devices, and roaming desktops.	✓	
Provides fast user switching and full AD policy enforcement with a true private desktop between users on the same shared workstation so that one can log off and another log on with minimal downtime.	✓	

Automating access to enterprise applications

Look for a solution that:	IBM	Other vendor
Offers a wide choice of authentication factors, including user IDs and passwords, USB smart tokens, building access badges, active RFID, biometrics and an open authentication devices interface for easy integration of third-party devices.	✓	
Provides an ESSO solution that supports desktop password reset functionality.	✓	
Supports ESSO without placing additional load on the directory infrastructure or modifying the directory schema.	✓	
Provides wizards for automatically generating SSO profiles and provides visual profiling for advanced users for automation of complex applications.	✓	
Goes beyond SSO to control the user interface of applications without the need to change the applications.	✓	
Provides full enforcement of AD GPO settings for all session management modes to ensure security.	✓	
Enables account usage auditing by tracking application logins/logouts.	✓	
Provides the ability to customize application tracking.	✓	
Is integrated with provisioning to provide automated check-out/check-in of shared and privileged identities for privileged identity management.	✓	
Is fully integrated with other identity and access management components such as provisioning, compliance tracking and reporting, Web SSO and federated SSO to provide an end-to-end identity and access assurance framework that can grow with your needs.	✓	

3. Managing and enforcing access control policies across every application, data source, operating system and organizational boundary consistently

As the number of users increases exponentially, organizations need an efficient solution to manage and enforce access control policies. These policies need to integrate with core business systems and keep identity information synchronized across multiple sources. But just as important, they need to align business rules with access control decisions and be able to simulate policy changes before they are implemented. The organization must be able to put into place access control policies that help ensure regulatory compliance, and do it in a cost-effective manner.

Users need to be tracked across multiple sessions while enforcing access policies such as inactivity timeouts. And the access control business rules need to be maintained and managed outside the application code to increase flexibility. Resources also need to have meaningful descriptions to make it easier to manage them.

As more users rely on these applications, the scalability and availability of the security solution becomes paramount. Organizations need a solution that will scale to a very large number of users and that provides the right level of technology support and failover capabilities to maintain the availability of business-critical applications.

Data and application entitlements and access control policies

Look for a solution that:	IBM	Other vendor
Provides flexible, quickly configured and extensible identity feed methods that push identity data from either a single authoritative source or pull and aggregate data from multiple sources.	✓	
Provides business managers and auditors with a business-friendly description of what users can do with their access rights for better decision making in new access approval requests, recertification and audit reviews.	✓	
Allows administrators to apply a meaningful description to a fine-grained resource, categorize it for quick reference and search, assign an owner to it, define unique approval and recertification workflows, and provide detailed reports on these resources.	✓	
Allows enterprise architects to model security policies and create security policy templates for use that is consistent across the organization.	✓	
Allows application owners to create data entitlements using application roles and attributes without requiring knowledge of the IT operations environment.	✓	
Has a workflow that seamlessly integrates with SAP and Oracle ERP, and fine-grained separation-of-duties checking with flexible exception-handling methods.	✓	
Provides a centralized management GUI for control and making modifications, eliminating the need to manually update each individual adapter to reflect changes in authentication and authorization methodology.	✓	

Data and application entitlements and access control policies

Look for a solution that:	IBM	Other vendor
Includes a what-if policy change simulation analysis to identify who and what entitlements will be impacted before a change is made. Provides an in-depth impact analysis and preview of policy changes, with the ability to drill down on accounts, attributes and values.	✓	
Incorporates business rules into access control decisions and evaluates these rules dynamically at run time.	✓	
Manages access control business rules outside the application code to enable you to change policy parameters that affect access without having to rewrite and recompile applications.	✓	
Keeps track of what a user is doing across multiple concurrent sessions so that when a user logs out once, the solution can log the user out everywhere to avoid concurrent logons.	✓	
Enforces access policies for inactivity timeouts, three-strikes rules and other options across multiple enforcement points.	✓	
Offers unified policy management to centrally manage and control access from operating system resources to Web-based application SSO.	✓	
Defines policy-based rules that allow you to easily set security policies that apply to different systems, users, storage or information.	✓	
Sets an access policy that automatically detects and remediates both intentional and inadvertent noncompliance events in real time.	✓	

Data and application entitlements and access control policies

Look for a solution that:	IBM	Other vendor
Automatically escalates and redirects workflow processes to alternate participants when timely action is not taken.	✓	
Scales to tens of millions of users for authentication and authorization; also scales to meet the needs of intranet, extranet and Internet user populations.	✓	
Provides scalability and availability through support for nonstandard, secure IP load balancers, intelligent load balancing over replicated servers and included clustering support.	✓	
Ensures availability by replicating the full set of policy rules where they are locally accessible by decision-making components.	✓	
Enables multiple policy enforcement points in a Web-services infrastructure, for DataPower®, WebSphere and other Web Services resources.	✓	
Enables multiple policy enforcement points for application and data sources such as SharePoint, WebSphere Portal, WebSphere Application Server, IBM FileNet®, IBM DB2® and other application and data resources.	✓	
Leverages SSL accelerator card technology by securing hardware key-stores, and providing a failover capability that allows automatic switchover to backup Web servers.	✓	

4. Monitoring and auditing user access

Organizations must not only be able to control access to data and applications, they must also be able to demonstrate the strength and consistency of their access controls to close the identity and access lifecycle and provide auditable proof of compliance. In today's complex computing environments, organizations need a closed-loop view of who has access to what, why they have access to it, and what they are doing with that access. This visibility must extend to privileged and trusted users, because these accounts are particularly vulnerable to abuse.

Monitoring reports can be used to understand if user activities align with the rights and policies of the organization. Any abnormal or out-of-policy activity should be highlighted so it can be addressed and corrected. Including monitoring as part of your overall compliance process closes the loop and helps ensure that the right level of security is in place.[1]

Whether users gain access through portals, Web sites, or the enterprise network, a centralized, policy-driven approach based on the right solution can provide the visibility to track everyone who has access to systems, align the degree of access granted with organizational priorities and needs, manage access with greater accountability, and ensure that access policy is enforced.

And to help govern SOA environments, enterprise architects should also be able to expand the capabilities of an enterprise service bus (ESB) through the ability to efficiently and effectively manage and provision user identities across the SOA.

This approach creates an "identity-aware" ESB, enabling organizations to ensure that users have access to applications, data and information based on their security credentials and access level, regardless of which application they are accessing.

Monitor and audit user access

Look for a solution that:	IBM	Other vendor
Provides automated log management to efficiently collect, store, investigate and retrieve logs.	✓	
Includes a scalable log collector to ensure the reliable and verifiable collection of native logs from virtually any platform, including syslog, Simple Network Management Protocol (SNMP) and other security log types including operating systems, databases and security devices.	✓	
Utilizes a single, secure identity repository from which virtually all identity events are tracked and can be audited.	✓	
Centrally collects, simplifies and correlates security-related events and alerts across a wide variety of perimeter security devices.	✓	
Offers audit logging of all activity automatically and out-of-the-box, including administrative activities such as policy modifications.	✓	
Provides true closed-loop policy compliance enforcement that both detects and remediates access entitlements granted outside the provisioning process, instead of a complex, multiple-step serial process that could have multiple points of failure.	✓	

Monitor and audit user access

Look for a solution that:	IBM	Other vendor
Includes out-of-the-box automated, configurable and sophisticated attestation/recertification processing to help address requirements such as Sarbanes-Oxley (SOX) 404 recertification of access requirements.	✓	
Provides a single identity GUI through which all administrative functions are performed and through which identity events are tracked and can be audited.	✓	
Includes workflows as an integral part of the solution so that all lifecycle and provisioning events are managed and monitored by the solution, which can then log all transactional data for forensic audit and reporting.	✓	
Establishes a central framework to govern and protect your SOA environment.	✓	
Enacts and governs proper access controls for each services application.	✓	
Translates and maps a diverse set of user identities across different services.	✓	
Manages application-specific identities across organizational silos and firewalls.	✓	
Establishes an identity trust management framework to ensure transactions are performed securely.	✓	
Propagates the required credentials end to end—from a point of contact such as an XML gateway through ESB to the back end such as an ERP or mainframe application.	✓	

Monitor and audit user access

Look for a solution that:	IBM	Other vendor
Tracks and collates all login events, allowing you to audit application access.	✓	
Provides extensive auditing and detailed reports you can give to regulators, external and corporate auditors.	✓	
Provides an audit trail of who has access to what and who approved those access rights.	✓	
Is integrated with provisioning to provide automated check-out/check-in of shared and privileged identities for management of privileged identities.	✓	
Offers privileged user monitoring, reporting and auditing on databases, applications, servers and mainframes.	✓	
Supports major regulations and best practices out of the box, including ISO 27001, SOX, GLBA, FISMA, PCI-DSS, Basel II, HIPAA, NERC and COBIT.	✓	
Provides organization-wide monitoring for both distributed and mainframe environments to detect policy non-compliance exceptions.	✓	
Translates captured native log data into easy-to-understand reporting that can be used by regulators and external and corporate auditors without the need for any platform knowledge.	✓	
Provides an easy-to-use interface for creating custom reports, including summary and detail, Top-N, and threshold reporting.	✓	
Offers a common reporting system for scheduling, distributing, viewing and customizing reports across all solution components.	✓	

5. Accelerating time to value

As you're evaluating different identity and access assurance solutions, it's important to select one that offers rapid time to value. A cost-effective solution includes a number of key features designed to provide easy configuration, integration and maintenance, even in a complex enterprise environment.

Time to value

Look for a solution that:	IBM	Other vendor
Provides all necessary infrastructure adapters, leading commercial versions of middleware and software components (including any necessary databases), Lightweight Directory Access Protocol (LDAP) servers, and Web and application servers.	✓	
Offers full-featured, out-of-the-box capabilities without limited versions of components, such as a workflow that must be upgraded to get the rich full features needed.	✓	
Bundles a best-of-breed directory and data integration and synchronization tool with the solution to elegantly solve integration challenges.	✓	
Demonstrates mature, proven capabilities tested through hundreds of worldwide customer installations.	✓	
Makes experienced services teams available to ensure productivity remains high during the implementation.	✓	

Time to value

Look for a solution that:	IBM	Other vendor
Has the ability to address your heterogeneous target needs.	✓	
Includes embedded integration with the industry-leading IBM WebSphere Application Server.	✓	
Allows custom authentication so existing Web-based authentication applications can be swiftly integrated into the authentication process for all users without the use of third-party development tools.	✓	
Includes a broad set of capabilities for integration with applications (including SAP, PeopleSoft and Siebel), as well as support for multiple directories/user repositories and heterogeneous middleware (including Oracle WebLogic Server and Microsoft SharePoint).	✓	
Supports local languages and incorporates dynamic language support to display deployment-specific content such as password challenge/response questions or e-mail notifications in each user's preferred language.	✓	

Time to value

Look for a solution that:	IBM	Other vendor
Provides breadth of platform support, including Windows, UNIX, Linux on distributed, Linux on IBM System z® and IBM z/OS®.	✓	
Allows customization of branding (look and feel) and layout of the self-service user interface, while protecting your investment by retaining any existing customizations during fixpack application or other upgrades.	✓	
Provides common criteria certification of Evaluation Assurance Level 3 or higher for key capabilities for Web access control, user provisioning and LDAP Directory.	✓	
Supports standard configuration and programming languages, instead of requiring proprietary scripting or workflow definition languages.	✓	
Includes tools to monitor the health and availability of the identity and access management solution.	✓	
Integrates self-service password reset with the service desk (help desk) system, including generation and closure of incidents (trouble tickets).	✓	

6. Selecting the right identity and access assurance provider

The provider you choose should be a trusted partner who can support the full breadth of your identity and access assurance solution—helping you address the issues of complexity, compliance and cost. Ideally, you'll also want a provider who can support you throughout the implementation process. So before you select a provider, make sure to ask these questions:

Does your vendor support your organizational goals through their technology?

Look for vendors whose solutions align with your organization's objectives. Do their solutions promote efficiencies, reduce business service deployment time, reduce costs, enhance compliance and speed time to market?

Does your vendor offer part of the total solution or the complete solution?

With a vendor who is focused too narrowly on a solution that addresses only a particular environment, you can run into the "islands of security" problem. Solution costs, and the time it takes to manage multiple vendors, can rise dramatically when multiple vendors are involved. Look for a vendor with a complete portfolio for identity and access assurance, including UNIX and mainframe access controls, Web Services security and federation.

Are your vendor's products tightly integrated for seamless functionality?

The better integrated the solution, the less work you need to do to manually integrate the technology.

What type of global presence does your vendor have?

If your organization has international offices, you should look for a vendor with a global presence and proven international experience. Make sure the vendor can support your offices abroad with their own local resources.

Is the solution supported by a mature support organization with the expertise and bandwidth that can be relied on when you need them?

Your vendor should offer highly responsive and highly effective customer support. Find a vendor who has a proven support organization to help you maximize the value of your software investment.

Are the vendor's solutions consistently rated highly by the analyst community?

Look for solutions that are recognized through independent analysis and examination across multiple dimensions by leading analysts.

How sure are you of your vendor's stability and staying power in today's tough economy?

A big issue in today's economy is vendor stability and viability. You should consider a vendor who has a long history in the industry, a solid, forward-looking strategy and the resources to overcome adverse economic times.

Can your vendor deliver products that are strategically designed and technically superior?

When comparing various security solutions, look for technical superiority—well-designed functionality, an intelligent architectural design and broad support for industry standards.

Address your identity and access assurance needs with IBM

When you begin to evaluate identity and access assurance vendors, you'll find that IBM offers not only best-of-breed solutions, but also unsurpassed breadth and integration across the security portfolio. Only IBM enables you to focus on driving innovation by reducing the complexity of securing the organization through a flexible and adaptable approach across the entire realm of IT security risk. When you're ready to expand into other areas of security management, IBM is the trusted partner you need to support your long-term security goals.

IBM Tivoli® Identity and Access Assurance provides efficient, secure and compliant access, helping organizations ensure that the right users have access to the right information in a timely manner. The solution provides comprehensive identity management, access management and user compliance auditing capabilities. It centralizes and automates the management of users, then closes the identity and access loop, providing industry-leading capabilities not only for assigning and enforcing user access rights, but also for monitoring user activity and for detecting and correcting situations that are out of compliance with security policy. Organizations have the option of implementing the Tivoli Identity and Access Assurance solution, or starting with a subset of these capabilities to address specific immediate requirements and then expanding the solution to provide additional capabilities as their needs grow.

IBM Tivoli Identity and Access Assurance interoperates with a broad set of identity repositories, easily handles large volumes of users and enables automation of process workflows, improving administrative efficiency and minimizing costly errors. To support compliance, it automatically captures and centrally collates user access activities, and summarizes the information on a security compliance dashboard. Monitoring reports lets you know if user activities align with the rights and policies of your organization. The dashboard and reporting also highlight abnormal or out-of-policy activity, so it can be addressed and corrected.

IBM Tivoli Identity and Access Assurance empowers organizations to improve service by enabling collaboration through role-based portals, facilitating the quick roll-out of new services and enabling single sign-on. Tivoli Identity and Access Assurance helps organizations reduce costs for managing accounts, groups, policies, credentials and access rights throughout the user lifecycle by providing a single-vendor solution that reduces complexity and total cost of ownership (TCO) while giving users quick access to the resources they need. Finally, organizations can better manage risk with the integrated support the solution provides for compliance efforts, including centralized and automated compliance reporting, robust user activity monitoring, and strong password policy enforcement capabilities.

IBM can help provide the infrastructure necessary to support today's security requirements, whether for access provided via cloud computing, SOA, portals, Web sites, or enterprise networks. Beyond managing user identities and access to resources, establishing a centralized and automated infrastructure for identity and access assurance can ultimately become a business enabler—helping you:

- Minimize the complexity of providing a secure environment that safeguards your data.
- Comply with internal and external requirements for secure access to assets and information.
- Optimize productivity and costs by automating best practices for repeatable tasks.
- Free IT staff to focus on higher-value activities.
- Attain the agility needed to capitalize on new business opportunities by removing barriers to innovation.

For more information

To learn more about IBM identity and access assurance solutions, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
June 2010

Please Recycle

[1] For more information about selecting the right security information and event management solution, please see IBM security information and event management solution buyer's guide at **ibm.com**/common/ssi/fcgi-bin/ssialias?infotype=PM&subtype=RG&appname=SWGE_TI_SE_USEN&htmlfid=TIO14001USEN&attachment=TIO14001USEN.PDF