IBM Software Group

Deliver effective governance for identity and access management.

June 2009

June 2009

Deliver effective governance for identity and access management.

Today, companies face many hurdles to driving consistent profitability and managing organizational risk. Compliance regulations like Sarbanes-Oxley, Basel II, the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), Model Audit Rule (MAR) and the Payment Card Industry Data Security Standard (PCI/DSS) add to those challenges by mandating processes and controls that are typically geared toward industry-specific objectives.

The cost of addressing compliance requirements also impedes corporate profit objectives, since managing the information life cycle is a significant financial burden due to:

- Explosive growth of structured and unstructured data.
- Ubiquitous information access.
- The growth of richer, Internet-based collaboration.

Implementing a cohesive strategy for access control and preventing data and information leakage is difficult, since access controls must extend across the entire IT and data center fabric while integrating with a broader enterprise risk management approach. Poor visibility, ineffective controls and escalating administrative costs impede an organization from maintaining its core business and delivering new, revenue-generating services. Organizations need a strategic approach to understanding digital identity and addressing challenges in managing, sharing and validating identities and entitlements[1] claims.

Governance, risk management, compliance are at the business forefront

Controlling access to data and applications is vital. Escalating security and privacy concerns and a renewed focus on corporate oversight drive governance, risk management and compliance (GRC) to the business forefront. Organizations must prove they have strong and consistent access controls.

"Identity and access management governance" (IAM governance) describes how organizations administer, secure and monitor identities and access to applications, information and systems. It further extends the value delivered by core identity and access management functions like user provisioning, Web access management and the directory infrastructure. This white paper reviews common, yet fragmented approaches to IAM governance, as well as the IBM approach, which holistically addresses each IAM governance requirement.

Choose a policy-driven approach to managing people, applications and data

Organizations should consider a thorough approach to IAM governance that meets the requirements of discovering, documenting and analyzing user access; establishing a process for user access governance; ensuring that constraints help manage business conflict; enforcing policies; and continuous monitoring.

Such an approach should provide IT and line of business (LOB) personnel with automated ways to identify, cleanse and collate identity data; discover, classify and analyze identity and entitlement data across applications in a reusable, business-friendly format to facilitate role[2] creation; and define and manage roles, identity attributes[3] and entitlements throughout their life cycles.

Also essential for effective IAM governance are:

- A policy governance layer that applies business and IT policies in a controlled, centralized manner.
- A policy enforcement and remediation layer that drives workflow, task and process automation.
- Monitoring, reporting and auditing to help ensure access rights are used properly and to provide a feedback loop into both policy governance and the organizational identity and role structure.

A policy-driven approach, using the right solution, provides the required visibility, control and automation to manage business-specific user access requirements with greater accountability, and to ensure access is governed and enforced.

For more information

To learn more about building a holistic IAM governance strategy, contact your IBM representative or IBM Business Partner, or visit the following Web sites:

- **ibm.com**/tivoli/products/identify-access-assurance
- **ibm.com**/tivoli/products/identity-mgr
- **ibm.com**/services/gbs
- **ibm.com**/services/us/index.wss/offering/iss/a1030826

About IBM Service Management

IBM Service Management solutions help organizations manage their business infrastructure and deliver quality service that is effectively managed, continuous and secure for users, customers and partners. Organizations of every size can leverage IBM services, software and hardware to plan, execute and manage initiatives for service and asset management, security and business resilience. Flexible, modular offerings span business management, IT development, operations management and system administration, and draw on extensive customer experience, best practices and open standards–based technology. IBM acts as a strategic partner to help customers implement the right solutions to achieve rapid business results and accelerate business growth.

[1] Entitlement—access rights to applications, services or data, such as authorization to access the SAP financial application or modify customer database financial records.

[2] Roles can vary in type. Business roles represent collections of users (for example, financial analysts) while application roles represent collections of resources or entitlements (for example, "approve purchase order").

[3] Identity attribute—a piece of data that is tied to users, such as job code, division number, and so on.

Contents

Current products offer a fragmented approach

The IAM governance market today is fragmented, with point products for access certification, separation of duties, role management, entitlement management and privileged identity management that do not holistically address IAM governance requirements.

Address each IAM governance requirement

Driven by GRC and the need to share information with many stakeholders, organizations must address each IAM governance requirement, including:

1. Share the right information, at the right time, with the right people, for the right purpose.

2. Apply policies and regulations to business operations.

3. Document users whose access to critical processes, information systems and data should be managed as a foundational risk management control.

4. Understand the level of access users have to services, applications and data. Ensure and document that user access has a valid business reason and prevents separation-of-duty conflicts.

5. Define and manage governance over physical and logical access rights,[4] including a certification process that ensures valid user access and access revocation when needed.

6. Deploy governance with accountability, manageability, sustainability and reporting to business and IT owners while allowing delegation. Develop an understanding between business and IT that specifies how IT can effectively administer this process repeatedly, while the business oversees access accountability.

7. Leverage a systematic IT architecture and platform to enforce policy as designed and make a feedback loop available so both business and IT understand the results of continuous compliance in the broader risk management strategy.

Sample scenario: JK Enterprise

To help explain why gaps exist in point products today, we will refer to JK Enterprise—a fictional health care consortium. We will focus on a maternity ward nurse and an emergency room nurse.

Access certification

Access certification products are incomplete when they define access as an account on a server or group membership on an application, without knowing whether the native access control policy on that server or application has been properly configured or enforced.

Analyzing and validating who has access to what resources typically starts with reconciliation that connects users to existing IT access. User access to IT resources must be analyzed to determine if access should remain. From there, certification policies establish a regular review process and validate that access remains appropriate.

Much access certification product value is derived in the access cleanup, which is performed during initial reconciliation, as well as ongoing certification data capture, which is used for auditing and compliance. Certification helps establish a continued review of users, roles and associated entitlements. While these

address IAM governance requirements 1-3, access certification products are incomplete when they define access as an account on a server or group membership on an application, but do not properly configure or enforce the native access control policy on the server or application.

For instance, JK Enterprise has patient information stored on its admission, discharge and transfer (ADT) application, and they associate access with user membership to a group on that application, assuming the native access control policy is properly administered. But when an emergency room nurse is assigned membership to the ADT application emergency room nurse group, no validation checks are performed. Has the native access control policy been properly configured and enforced? If user access is invalid, no remediation is provided without user provisioning. Unlike user provisioning, access certification alone does not grant or remove user access, but establishes a method for sanitizing and reviewing whether the user access is valid. Furthermore, certifying user access through entitlements can be tedious. If they are applied without using roles, the large volume of entitlements poses an administrative problem. The number of roles an organization has should be substantially fewer than their entitlements.

Separation of duties

To manage access conflict within an organization, consider the example of a finance department clerk who is responsible for establishing new hospital suppliers and approving supplier payments. Separation of duties helps define and enforce policy on conflicts at both the role and entitlement levels. For example, at JK Enterprise, an accounts payable clerk cannot also have the role of accounts receivable clerk. This applies at the entitlement level too, where the accounts receivable clerk cannot also perform the “issue check” function within the enterprise resource planning (ERP) system.

To most effectively avoid conflicts, an organization should combine:

- *Preventative separation of duties*, when policy prevents granting overlapping responsibilities that present a potential conflict to the organization.
- *Detective separation of duties*, analysis to see if conflicts already exist.

Standalone separation-of-duties products may deliver robust policy constraints at a transaction level, but are insufficient, as they predominantly focus on ERP application roles. Separation-of-duties functionality is often bundled inside role-management or user-provisioning products. While they address identity governance requirement 5, they typically only deliver controls at the role and group levels and assume that users assigned to a group represent an entitlement. That assumption is not always valid. Delivering business context to separation of duties is a better practice. For instance, JK Enterprise prefers for emergency room nurses to admit and discharge the same patient on weekends, when they are short-staffed.

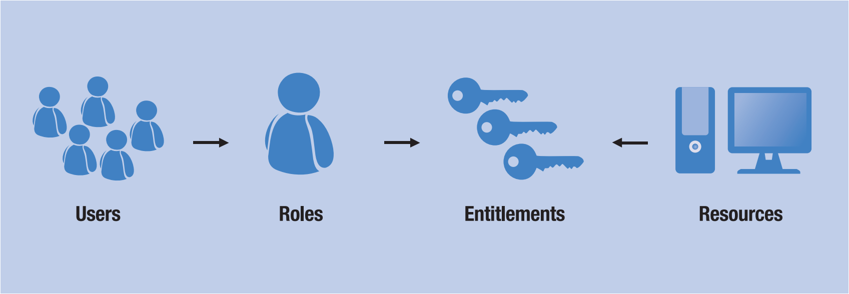

Figure 1: Role management enables discovery, creation and ongoing change control in an organizational role structure that governs user access to resources.

Role management

Role management enables discovery, creation and ongoing change control in an organizational role structure that governs user access to resources, but does not grant or remove user access. It establishes a role structure and process to more efficiently manage:

- *Roles,* which represent collections of users—often described by job functions and responsibilities—and entitlements.
- *Collections of users,* often referred to as business or organizational roles (such as physician, lab technician, and so on); they describe what a user does in his job.
- *Collections of entitlements,* known as application or IT roles, grouped together when they perform a specific function within an application (such as "update a patient record"). Together, business and application roles govern the access needed to perform a job.

Unlike access certification, role management adds an abstraction layer that streamlines automation by providing fewer objects to manage user resource access. By integrating with user provisioning, remediation can be automated.

Organizations seeking a role management solution typically:

- Establish role definitions and structure by analyzing business objectives, business processes and user access.
- Initiate approval and recertification workflows to govern operational change control over whether the role, as defined, still applies.
- Assign role membership, defining who is entitled to the defined roles.

- Establish workflows to consistently revalidate role membership.
- Deploy role structure and integrate it with a user provisioning solution.
- Use ongoing monitoring to help address compliance requirements for auditing and reporting (as well as establish a potential feedback loop for refreshing the role structure to ensure proper mapping between IT and the business).

Common role management pitfalls

Compliance, security and automation are key drivers behind a role management solution. However, role management projects that are too technically focused can end in failure. Success requires continuous collaboration with the business, to ensure business roles and processes are adequately integrated with application roles. While role-based access control is useful, a policy- and context-driven approach is necessary.

Context can include:

- Identity context (such as location and department name).
- Service context (such as data classification and service location).
- Environmental context (such as intranet request and time of day).

Access controls must extend across the entire IT and data center fabric while integrating with a broader enterprise risk management approach.

Many role management products provide substantial value in modeling and operational management. They may partially address client identity governance requirements 1-5, but fail to address underlying identity associations—through roles—to applications and data that determine how governance is managed.

Role management products often equate IT or application roles to user membership in a group on an application. As previously discussed in the section “Access certification,” native application access control policies are assumed adequately configured to ensure an entitlement. But “an emergency room nurse can read patient information” would be better expressed as “an emergency room nurse can read confidential patient information within the corporate network.” The latter delivers fine-grained business context and metadata tagging. “Within the corporate network” indicates a policy is defined and enforced that determines where a user can access the application containing patient information. And “confidential” is a metadata tag describing how sensitive data is classified. When policy governs people, applications and data, end-to-end governance with accountability is achieved.

Role mining[5] is one important step in role modeling, but its value is often overestimated. Role modeling requires substantial collaboration between business and IT personnel. Role mining has limited value without collaboration. Most value is derived in the initial organizational role structure, and less in a production environment.

In addition, as organizations collaborate within supply chains, business processes are more intertwined with those of partners. Consequently, controls need to be applied at the data and information levels—not just at the system or process levels. Information access is becoming more peer-based, which leads to decentralization of security information management and dynamic relationships between partners. There exist critical needs for rich semantics to define tailored, fine-grained access policies such as dynamic quality of protection parameters (for example, threat-level consideration, transaction at hand and community of interest).

Prevalent access management forms, like discretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC), are static and do not address these needs. For instance, RBAC, which typically relies on centralized management of user-to-role and entitlement-to-role assignments, is not well suited for a highly distributed environment, since management is difficult when the subject and resource belong to different security domains.

Entitlement management

With role-based access to key business applications and services, organizations face critical application security challenges. Increasing industry regulations, compliance requirements and risk of intellectual property theft drive the need to control user access to applications using role-, rule- and attribute-based entitlements. A policy-based entitlement management solution helps centrally capture the application roles, author and manage entitlements, and enforce the appropriate data-level access control. It also offers an "application-driven" approach to the traditional role management task and helps address operational governance needs.

For example, JK Enterprise wants to deploy a new call center application for patient and customer service and creates a "patient record reviewer" application role. Rules defined and associated with that application role may contain permissions (such as "open record" and "view record"), data-level access controls (including "restrict access to patients' personally identifiable information") and additional business context (for example, "time of day" and "location").

Given its granular access control focus, entitlement management on its own can be difficult to scale across the organization. Standards like Extended Access Control Markup Language (XACML) can help alleviate this concern.

Privileged identity management

Privileged identity management governs the heightened risk introduced by IT administrators and C-level officers with significant access levels within an application or across the organization. For example, the JK Enterprise root administrator on the ADT application will have access to sensitive patient data. Without proper controls, he could easily access patient data and then erase the audit logs showing that he accessed them. Organizations should consider separate processes and policies for user lifecycle management, password management, access control and ongoing user activity monitoring to manage this potential risk.

IBM delivers a policy-driven approach to managing people, applications and data

Organizations should consider a holistic approach to IAM governance that meets the requirements of discovering, documenting and analyzing user access; establishing a process for user access governance; ensuring that constraints help manage business conflict; enforcing policies; and continuous monitoring. A policy-driven approach to manage people, applications and data provides the consistency and breadth needed for IAM governance.

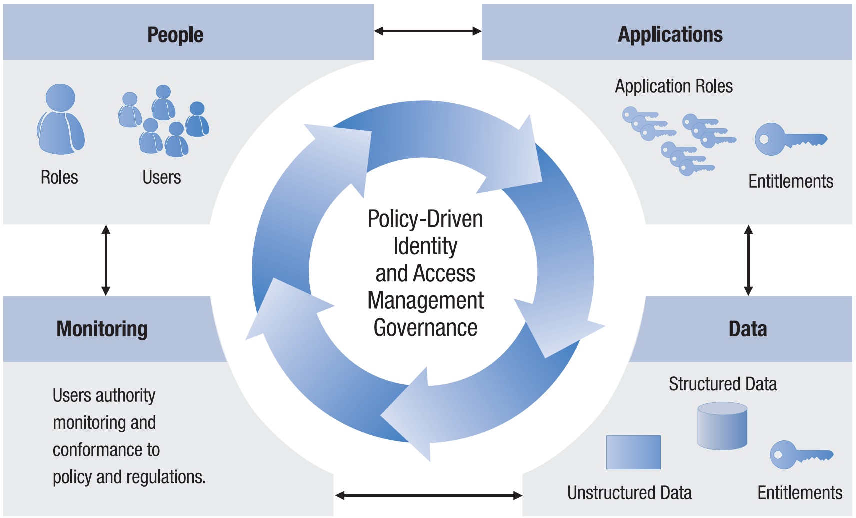
People
Roles
Users
Applications
Application Roles
Entitlements
Policy-Driven Identity and Access Management Governance
Monitoring
Users authority monitoring and conformance to policy and regulations.
Data
Structured Data
Unstructured Data
Entitlements

Figure 2: IBM delivers a policy-driven approach to IAM governance.

A policy-driven approach to manage people, applications and data provides the consistency and breadth needed for effective IAM governance.

People, identity attributes and associated roles provide critical links between the business and processes that deliver organizational visibility, accountability and improved efficiency. Applications and associated roles provide important entitlement links to users, so they can work through appropriate access to systems and information. Because of this:

- Management of application and data entitlements should leverage the business contexts of identities, services and the surrounding environment.
- Data, whether structured or unstructured, must be managed effectively to ensure proper intellectual property governance, customer data and so on.
- Ongoing user activity reviews not only aid policy and regulation conformance, but also can help organizations correct abnormal user behavior.

To help execute this holistic approach to IAM governance, organizations should consider the life cycle shown in Figure 3. Achieving IAM governance does not demand a specific chronology.

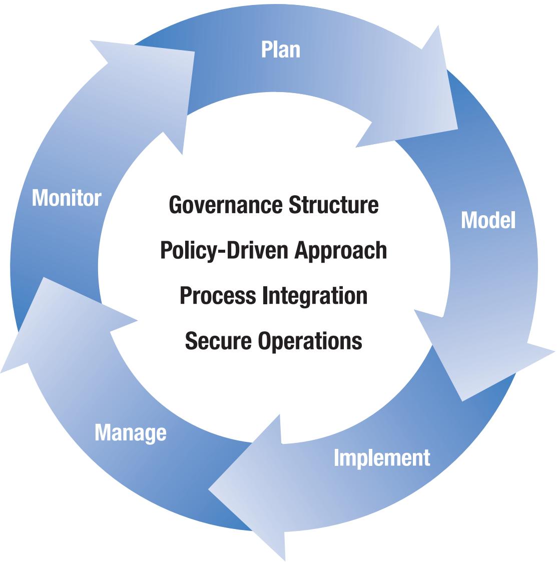

Figure 3: A viable IAM governance plan requires a multi-step, closed-loop process.

Plan

The first step in IAM governance is establishing agreed-upon business objectives and priorities, including executive sponsorship for consistent oversight. Then the organization should perform an internal process and data discovery assessment—across people, applications and data infrastructure—and examine processes for bringing users into and out of the organization or division. What data is needed to determine and provide access? To establish a baseline, organizations should also document how business operations are performed and leverage user data and access management policies.

Business role creation should target a department or division. IT should also communicate with key LOB personnel, using a comparative analysis of key business processes, to show how the current organizational role structure supports them. In parallel, IT should clean user and entitlement data to match known users to known accounts and entitlements. This data cleanup includes identifying and collecting relevant user and entitlement data from target systems such as user provisioning solutions, Microsoft® Active Directory, Lightweight Directory Access Protocol (LDAP), ERP applications and IBM Resource Access Control Facility (RACF®).

Model

At this stage, an organization should have the foundation of application data and job and business process information needed to model and engineer a role structure. A good guideline is to have 70-80 percent of entitlements covered by roles.

Organizations should determine how they want to map candidate business roles to candidate application roles, and then analyze data for common authorization sets. For example, the ADT application at JK Enterprise reveals that emergency room nurses commonly transfer patients from the emergency room to another department. The “transfer patient” functions within the ADT application should be a candidate application role mapped to the business role of emergency room nurse.

Application and business roles should be separate, so a single technical change does not require a change to the entire role structure. Role definitions may include a business-level description of what the role actually does (for example, a maternity ward nurse cares for newborn babies) and its association to IT (a maternity ward nurse can start and change diagnostics for the heart monitoring system). Associations can occur through the role hierarchy,[6] separation-of-duties policies, access certification policies and user provisioning policies. Access right provisioning can be assigned through application roles and XACML policies for administering fine-grained entitlements.

Emergency room nurses at JK Enterprise need to update patient records when transferring a patient, but the hospital recognizes patient privacy constraints and defines a fine-grained data-level entitlement policy that states emergency room nurses can only edit confidential patient data in that location and must initiate editing within the corporate internal network. This policy governs:

- Information context (confidential patient data).
- Identity context (nurse location and patient location match).
- Environment context (within the corporate network).

After mapping, role modeling begins. Modeling should include simulation so the organization can see what-if scenarios based on the proposed role structure. The final structure should be approved by both business and IT. For entitlements not governed by roles, the end user should request access through a self-service portal. Approval and recertification workflows can be associated with the access request process to invoke or revoke entitlement after approval or recertification. Modeling the workflow and access remediation beforehand is critical.

Policy design and modeling should include user activity monitoring. For example, emergency room nurses often need to administer medication quickly and do not have time to gather approvals—a risky clearance level. JK Enterprise invokes user activity monitoring to validate whether application roles mapped to emergency room nurse are being leveraged as intended. This is a key feedback loop as organizations review role structure to adjust role definitions.

This approach helps define and model a process to govern user access across people, applications and data through multiple policy management layers. It also delivers an abstract data model focused on role and entitlement management to manage various entitlement definitions.

Implement

Role and policy assignment ties users to roles and policies and designates role and policy owners. The implementation step includes controls around user assignment, as well as integration with user provisioning solutions, applications and systems.

Complementing policy management is policy enforcement, including checks and balances in business processes and run-time enforcement in the infrastructure. Run-time policy enforcement should take into account in-depth approaches, so intermediaries can enforce both coarse-grained access and fine-grained control closer to applications and data. A service oriented architecture (SOA) approach supports consistent run-time management, as well as policy and identity enforcement across heterogeneous systems, applications and data, rendering identity and security as services. This way, enforcement, decision and policy information points are loosely coupled and can be integrated within and across organizations.

Manage

Once an organization starts operational management, change control processes help ensure proper change governance for organizational role and policy structure. They also help organizations make sure that any organizational compliance requirements have a system to collect audit proof points.

Approval and recertification policies deliver change control at the user, role and entitlement levels, which can be managed with little business impact. If a business or application role definition change is required, it is initiated proactively or, as a result of the recertification event, it asks the role owner whether the role definition is still accurate. If not, the role owner can trigger steps to delegate changes required for remediation and return for approval. Entitlement enforcement is critical—not just associating user or role membership with a group on an application—but also run-time, predefined policy enforcement.

Monitor

Ongoing monitoring, auditing and reporting provide organizations with two key benefits. First, key IAM governance reports, granular enough to identify fine-grained permissions, enable organizations to meet audit requirements for external regulatory mandates and internal corporate security policies.

Second, user compliance auditing and monitoring deliver a litmus test on the organizational role and entitlement structure: Does the role structure align with what users are doing with their access? This critical link creates a feedback loop into role definitions, policies and ongoing change control.

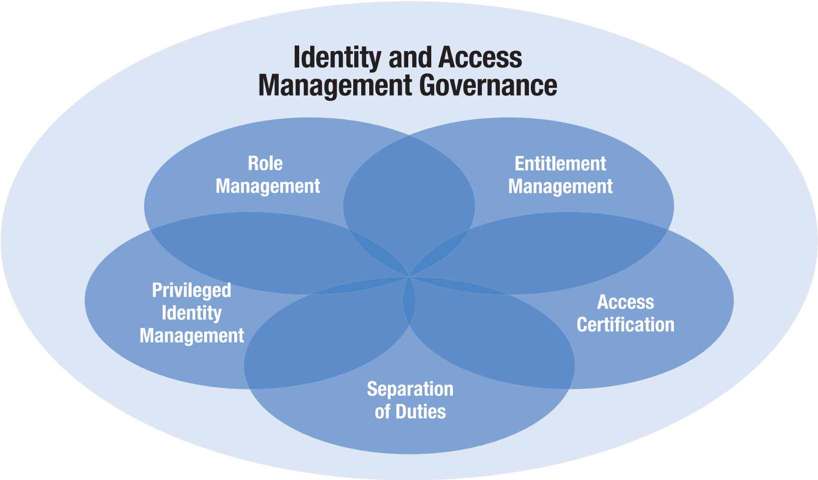

Figure 4: Based on their business priorities, organizations should begin with a subsegment of identity management, as shown here, then develop a plan for complete IAM governance.

IBM IAM governance provides the required visibility, control and automation to manage business-specific user access requirements with greater accountability, helping to govern and enforce access.

Deliver IAM governance with accountability

IAM governance solutions today deliver value but are incomplete. As organizations seek to administer, secure and monitor user access to resources, they should consider a policy-based approach to managing people, applications and data. IBM provides the visibility, control and automation needed to manage business-specific user access with greater accountability. Based on their business priorities, organizations should begin with a subsegment of identity management (see Figure 4), then develop a plan for a complete IAM governance solution. IBM can help.

For more information

To learn more about building a holistic IAM governance strategy, contact your IBM representative or IBM Business Partner, or visit the following Web sites:

- **ibm.com**/tivoli/products/identify-access-assurance
- **ibm.com**/tivoli/products/identity-mgr
- **ibm.com**/services/gbs
- **ibm.com**/services/us/index.wss/offering/iss/a1030826

About IBM Service Management

IBM Service Management solutions help organizations manage their business infrastructure and deliver quality service that is effectively managed, continuous and secure for users, customers and partners. Organizations of every size can leverage IBM services, software and hardware to plan, execute and manage initiatives for service and asset management, security and business resilience. Flexible, modular offerings span business management, IT development, operations management and system administration, and draw on extensive customer experience, best practices and open standards–based technology. IBM acts as a strategic partner to help customers implement the right solutions to achieve rapid business results and accelerate business growth.

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

Produced in the United States
June 2009

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

[4] Access rights—access to various IT and physical resources (such as IT systems and buildings), business process resources (business applications) and information systems (including files, databases, content management systems and file shares).

[5] Role mining—process used to analyze target systems for common sets of permissions that can be grouped and used to define application roles.

[6] Role hierarchy—inheritance between business roles. For example, a JK Enterprise employee assigned to the emergency room nurse role inherits the general nurse and permanent employee roles.