IBM Software
IBM Security Systems

Manage identities and access for continuous compliance and reduced risk

Administer, control and monitor user access to resources, applications and information

IBM

Highlights

- Validates the authenticity of all users who access resources
- Monitors that user access follows appropriate use policies and is consistent with regulations
- Takes corrective action where violations exist
- Provides accountability and transparency for user entitlements throughout the user lifecycle
- Enables ongoing audits of user activity to enforce policies and aid compliance.

As organizations strive to securely deliver high-quality, high-availability services to their user communities, they grapple with cost control and ever-changing user populations, access points, and applications. But that is only part of a larger challenge related to identity and access management (IAM). Services must be delivered solely to the right people, with the right privileges—whether employees, suppliers, partners or customers. This is becoming more important, yet more difficult to achieve.

Compliance regulations such as 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) stress the importance of visibility and control for individuals' entitlements and access privileges. Simultaneously, advances in computing make it harder, including:

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

The complexity of IAM and the pressure of risk and compliance demand a new approach—and the solutions to make that approach a reality. What organizations require is policy-driven IAM governance that improves visibility, control and automation to protect assets from unauthorized access without diminishing productivity.

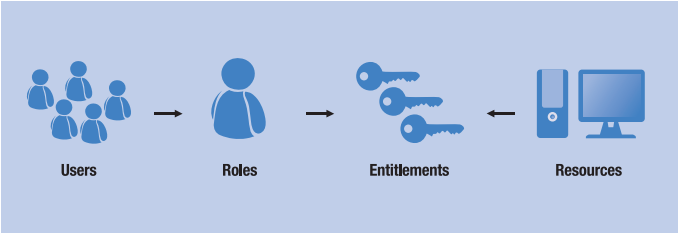

Figure 1: IAM governance helps deliver the right resources to the right people with the right privileges.

Establishing the front line of enterprise defense with IAM Governance

IAM governance is part of the front line of enterprise security. It is the fundamental technology for determining who has authorized access to what resources, for what purpose and for how long. In addition to technologies and policies for granting, updating and removing access, IAM governance also includes the tools to monitor, audit and report on what users do with their access rights. Without IAM governance, other security tactics such as entitlement management, data leakage prevention and fraud detection may have little or no point of reference to enforce access policy. IAM governance is also a fundamental part of the drive to optimize enterprise protection with security intelligence.

Most organizations have invested in security tools and techniques. But layered defenses are not the same as building security intelligence into your environment. What about a proactive approach to security that integrates risk control into its very fabric? IBM identity and access management governance can help address these questions, and provide value beyond risk

control alone—with accountability and transparency for user entitlements throughout the user lifecycle. When identity management is more directly integrated with business goals and priorities, IT can deliver services more finely tuned to the individual—enabling the business to capitalize on opportunities. IAM governance solutions can also enhance other security and policy control technologies, and contribute to comprehensive security management.

IAM governance describes how organizations administer, secure and monitor identities and access rights 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. IAM governance solutions discover, analyze and establish user access, drawing on workflows, reporting tools and analytics. This creates a process for user access governance in which entitlement constraints help manage business conflict. IAM governance includes the following practices:

- User lifecycle management (user provisioning and de-provisioning)
- Password management and single sign-on (SSO) to applications (including self-service options to reduce help desk call volume)
- Role management (assigning users to roles based on job function and business needs, and managing separation of duty conflicts)
- Certification policies that establish a regular review process and validate that user access remains appropriate
- Access management (enforcing policy-based access to internal and external users, including business partners and third-party service providers)
- Entitlement management (enforcing fine-grained roles-, rules- and attributes-based access to applications and services)
- Ongoing audits and reports to monitor user activity, enforce policies and aid compliance

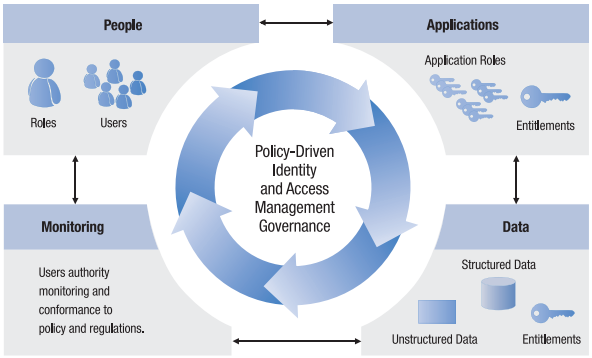

Figure 2: IBM delivers a policy-driven approach to IAM governance.

Facilitating consistency and compliance with a policy-driven approach to IAM

Controlling access to data and applications is vital considering escalating security and privacy concerns and an ongoing focus on compliance and corporate oversight. Organizations must prove they have strong and consistent access controls. They also want to ensure that decisions made about user entitlements are in line with their business goals and policies. IBM IAM governance provides the resources to manage business-specific user access requirements with greater accountability and transparency, helping to govern and enforce user access more effectively. The IBM policy-driven approach to managing people, applications and data provides the consistency and breadth needed for effective IAM governance and also helps facilitate compliance.

IBM guides clients through a proven, policy-driven approach that encompasses five phases of the identity and access management lifecycle, including:

- Defining controls
- Enrolling and proofing users
- Issuing and managing user rights

- Managing and enforcing access control
- Monitoring, auditing and reporting on user rights and activities.

Each of these phases provides an opportunity for clients to generate business value from IBM IAM governance solutions by improving service, reducing costs and better managing risk. IAM governance solutions from IBM help provide efficient and compliant access for the right people to the right resources at the right time. They do this by streamlining user authentication, optimizing application access and managing user provisioning and de-provisioning activities. Clients can draw on deep IBM security expertise to create an end-to-end IAM solution that supports and enhances other security components, and boosts efficiency in problematic areas such as compliance, usage policies and reporting. By simplifying user lifecycle management and providing better visibility into user entitlements, IBM Identity and Access Management governance can help maximize IT staff productivity and reduce the cost and complexity of security and compliance.

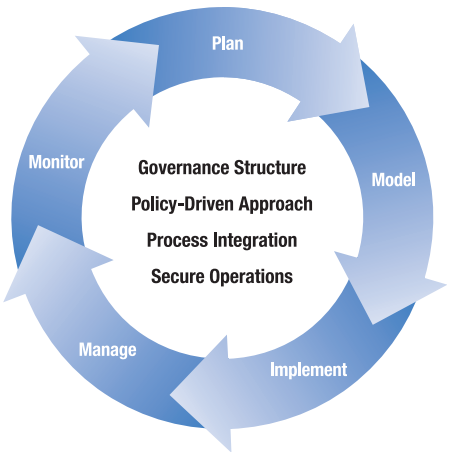

Figure 3: A viable IAM governance plan requires a multi-step, closed-loop process.

Exploring IBM solutions for IAM governance

Compliance regulations are driving organizations to adopt IAM technology, based on the need to prove accountability for data access and management. IAM can also help prevent fraud and improve operational efficiency. Consistent identity and access management help protect data integrity and facilitate compliance—even with the complexities of cloud-based user communities, large data stores and increased mobility. IAM governance solutions from IBM quickly provide users with authorized access to the resources they need to do their jobs, while protecting applications and data. IBM solutions for IAM governance include:

Identity Management

Identity management is the process of managing information used to identify users, control user access, determine user privileges and delegate administrative authorities. When it comes to end users, one size does not fit all. User lifecycles are in constant motion because people's roles and responsibilities often change. As employees are given new responsibilities or transfer within the organization, their access privileges need to be reviewed, approved and updated—and previous access privileges potentially suspended or removed. Customer access profiles can also evolve. For example, auction-site power sellers or stock investors who reach a specified trade volume need their profiles and authorizations to be updated seamlessly.

The speed of authorization is just as important as accuracy. New employees may remain idle until they can access business or email applications. And cloud-based customer communities and users also demand immediate access to resources.

Security policies are dynamic too, so identity management solutions should include tools that streamline policy creation and enable administrators to assess the potential impact of policy changes without introducing them to a production environment. Compliance and oversight requires the ability to manage identity and access data. Predefined reports and audit events should help auditors quickly gain an accurate view of an organization's security posture and state of compliance.

With its ability to deliver policy-based user and role management across the IT infrastructure, Tivoli® Identity Manager is a key driver of identity and access governance. Tivoli Identity Manager helps automate the creation, modification, and termination of user privileges throughout the entire user life cycle. It provides capabilities such as user self-care, provisioning and de-provisioning of user accounts, and recertification. Its role and policy modeling feature delivers comprehensive life cycle management with role mining and modeling, separation of duties, and group management capabilities, coupled with the ability to simulate various access scenarios.

Access Management
Access management is the ability to manage consistent sets of access control policies in line with security policies and compliance regulations across enterprise systems, including policy administration, monitoring and enforcement.

Access management solutions manage the day-to-day access to resources by authorized persons. Effective solutions integrate formal security policies into the access management workflow to automate management of access to operating systems, networks, servers, storage devices, databases, desktop applications, online commerce systems and enterprise applications. Access management also unifies the many user names and passwords that users typically have for various resources and applications into a single, security-enhanced authentication and authorization process—typically through the use of single sign-on (SSO) technologies.

Access management offerings enforce access policies throughout the user's lifecycle—authenticating and providing access to authorized users across multiple environments and security domains, while enforcing security policies and protecting against internal and external threats. Access management products from IBM help support the consistent execution of security policies across multiple applications and users. They enable SSO to improve the user experience and reduce help desk costs. They can also provide fine-grained access enforcement with entitlement management. IBM Access Management products include:

- IBM Tivoli Access Manager for e-business—acts as the hub for authentication and authorization for web and other applications, centralizing access management and making it easier and more cost effective to deploy secure applications.
- IBM Security Access Manager for Enterprise Single Sign On—simplifies, strengthens and tracks access by integrating enterprise single sign-on with strong authentication, access workflow automation, fast user switching and audit reporting.
- IBM Tivoli Federated Identity Manager—provides user-centric, federated single sign-on to securely share information between trusted partners and simplify application integration using open standards for SOA and web services deployments across distributed portal and mainframe environments.
- Tivoli Security Policy Manager—centralizes security policy management and fine-grained data access control for applications, databases, portals and services.
- QRadar Security Intelligence Platform—provides a unified architecture for collecting, storing, analyzing and querying log, threat, vulnerability and risk-related data to help protect against insider threats and control the cost of demonstrating compliance.
- IBM Security zSecure suite—improves an organizations' ability to facilitate security compliance, monitor and audit incidents and automate routine administrative tasks for the mainframe.

IBM Security Identity and Access Assurance
IBM offers a bundled software solution to help streamline identity management and enforce access policies throughout the user lifecycle. This solution also includes log management and privileged user monitoring to enhance insider threat detection, improve audit capabilities and facilitate compliance initiatives.

IBM Identity and Access Management Services is a comprehensive portfolio of capabilities that covers virtually every aspect of identity management—from identity proofing to user provisioning to access control.

IAM governance offerings from IBM are part of a holistic approach that helps meet critical business and security requirements, including:

- Discovering, documenting and analyzing user access
- Establishing a process for user access governance
- Ensuring that constraints help manage business conflict
- Enforcing policies in a controlled, centralized manner
- Driving workflow, tasks and process automation
- Monitoring, reporting and auditing to help ensure proper access and facilitate compliance

Achieving tangible benefits with IAM governance solutions from IBM

A policy-driven approach, using the right IAM governance solutions, provides the required visibility, control and automation to manage business-specific user access requirements with greater accountability. The following IBM clients have benefited from this approach in terms of streamlining IT efficiency, enhancing security and reducing risk, and facilitating compliance.

Latin American bank

A Brazilian bank offers payroll loans and credit solutions to more than 100,000 customers from numerous offices and over 1,000 points of sale. With a diverse set of security standards and sign-on procedures across dozens of applications, the staff struggled to ensure that its employees were provided with proper and quick access, and to demonstrate compliance with Brazilian regulatory standards.

The client deployed an integrated identity management and single sign-on solution from IBM to strengthen security while simplifying access to information.

This solution ensures that users have access to the appropriate applications and provides simplified access to IT resources. Now, staff and agents can log into the bank's network once and gain immediate access to all the applications they're authorized to use. Previously users had to separately log in to 15 - 30 different applications to build a loan package for a client. As employees leave the company or agents change roles, the security team can immediately de-provision access across all systems with a few keystrokes to keep the bank's data secure.

As a result, the bank reduced help desk costs by approximately R$32,000 (US$20,000) per year. It also decreased time to provision new users from up to five days to just two hours, and to reset passwords from four hours to seconds. System security has been improved through fast de-provisioning of users when needed, which also enables the security team to support new projects without hiring additional staff.

European city

A Czech city has a rich history and has become a growing commercial and tourist center. Ensuring comprehensive IT security for a growing city requires the centralization and intelligent automation of many processes, including monitoring and preventing unauthorized access to the city's IT systems.

The city has implemented a rules-based identity management system that automates employee account access based on employee position, role and department. The system then uses an automated account reconciliation process to detect and correct (or remove) any accounts that are not in agreement with the predefined rules. A closed-loop reconciliation process identifies "orphan" or out-of-date accounts, and automatically removes account access when an employee leaves. The city can now be confident that employees who need access to accounts get it quickly and efficiently, while the security of its IT systems is assured.

Benefits of the solution include:

- A 100 percent improvement in the speed of new employee activation—new employees become productive with access to all systems in a few hours instead of several days.
- Improved administrative efficiency and lower costs; one full-time employee can now manage all user accounts, while the rest of the IT staff develop and enhance the IT environment of the organization.
- Improved system security by removing orphan accounts and deactivating employee accounts within a few hours of termination of employment.

South American social services agency

In Uruguay, an exciting pilot program is underway that enables hospitals to notify government social security and social service agencies online when a child is born. It's one of a number of e-government programs the country is launching to replace paper-based processes and provide greater efficiency and transparency. About 50,000 government employees and two million citizens will ultimately use these online services.

Working with IBM and an IBM Business Partner, the organization has implemented a multi-tier architecture that provides a comprehensive security solution for its e-government services and addresses transport security, access control and identity management. To maintain the confidentiality and integrity of web services, IBM WebSphere® DataPower® Integration Appliance acts as the policy enforcement point, receiving policies from IBM Tivoli Security Policy Manager. Security tokens are issued by Tivoli Federated Identity Manager to confirm that the individuals claiming to send a message are who they say they are. IBM Tivoli Access Manager for e-business provides the centralized authentication, policy management and access control services to give citizens and government employees fast and secure access to online services. And IBM Tivoli Directory Server and IBM Tivoli Identity Manager provide the trusted identity data to support the authentication process across all web services.

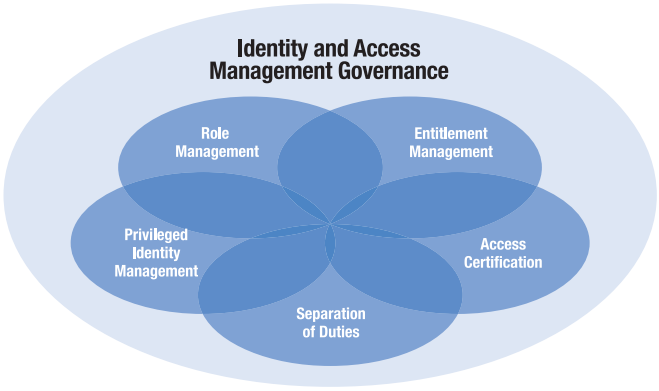

Figure 4: Based on business priorities, organizations should begin with a sub-segment of identity management, as shown here, then develop a plan for complete IAM governance.

Getting started—improving security and business efficiency with IAM governance

As regulatory hurdles multiply, data volumes expand and social business continues to transform access requirements, IAM governance solutions are becoming more important to an organization's day-to-day security and business operations—as well as ongoing compliance efforts. With a strategic, policy-driven approach, identity and access management can help you respond to change, reduce management costs and protect your most valuable information assets.

Given these factors, it is not surprising that IAM has moved from the periphery to the forefront of IT priorities. IBM solutions for IAM governance are helping clients realize a variety of security and business-oriented benefits, including:

- Improved compliance posture with centralized views and business processes for verifying identities and granting access rights

- Reduced costs resulting from the sunset of separate, custom identity administration solutions
- Improved security and reduced cost resulting from fewer employee logins and credentials
- Improved productivity, reduced help desk costs and increased employee and/or customer satisfaction through single-sign-on (SSO) experiences and on-demand access provisioning
- Improved business flexibility resulting from a faster time to market and a centralized, standardized security infrastructure
- Centralized audit views of runtime authorization events, enabling easier detection of malicious behavior

Why IBM?

Consistent identity and access management governance protects data integrity and facilitates compliance. IBM is a recognized leader in the worldwide IAM market space, with a global perspective and understanding of constantly evolving regional requirements across industries. In addition, IBM is consistently recognized by analysts and the security community for solution excellence, with analyst rankings of "leader" in several different reports and recognition as 2011's Best Identity Management solution by SC Computing magazine. Many IAM vendors provide only portions of a comprehensive IAM governance solution, requiring customers to deploy and manage separate products from several vendors. But IBM offers an extensive, integrated suite of identity and access management software and services that can support third-party environments such as Oracle, Microsoft and SAP.

For more information

To learn more about IBM Security Systems, please contact your IBM sales representative or IBM Business Partner, or visit the following website: **ibm.com**/security

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

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

Produced in the United States of America
January 2012

WGB03002-USEN-00