IBM Security Identity Governance and Administration

IBM helps you bridge the gap between business and IT with streamlined identity governance processes

Highlights

- Align auditors', line-of-business managers' and IT teams' perspectives with one consolidated platform for identity governance and administration
- Deliver easy access certification and access request capabilities to meet compliance goals with minimal IT involvement
- Enhance role mining and separation-of-duties (SoD) reviews using a visualization dashboard and business-activity mapping
- Support in-depth SAP governance with SoD, access-risk and fine-grained entitlements reviews
- Leverage easy-to-deploy virtual appliances for adapting to different access requirements

In any organization, it's more important than ever to verify people are connected to IT resources with the appropriate credentials and level of assurance. But in today's constantly changing environments—where people are frequently joining, leaving or moving to new positions, and technology is constantly evolving to meet business opportunities and challenges—how do you ensure that the access you've established for users stays current and appropriate? How can you confirm that SoD rules and other policies are being enforced? And how do you prove it to regulators and compliance auditors?

These identity management challenges can be difficult, especially as an organization's user populations and application infrastructures grow. Granting a person access in one area requires a provisioning process that includes application-specific information about the user's business role and work requirements. Then, when the user requires additional access elsewhere, the organization needs to provision again. And the cycle goes on and on—with each user requiring new access entitlements to support new job requirements, group membership or applications. The result is an exponential increase in the complexity of the identity management infrastructure and the risk that security and compliance might be compromised.

Now IBM® Security Identity Governance and Administration can help organizations mitigate access risks and SoD violations with business-driven identity governance and end-to-end user lifecycle management. It provides an integrated, streamlined approach for managing user roles, access policies and risk, ensuring that appropriate levels of access are applied and enforced across enterprise and cloud applications. The solution automates the administration of user access privileges across an organization's resources, throughout the entire identity management lifecycle—from initial on-boarding to final de-provisioning. By delivering improved visibility into how access is being utilized, it helps to answer critical compliance questions such as "Who has access to what resources and when?" and "How did users get access to resources and why?"

Support identity administration and governance with broad capabilities

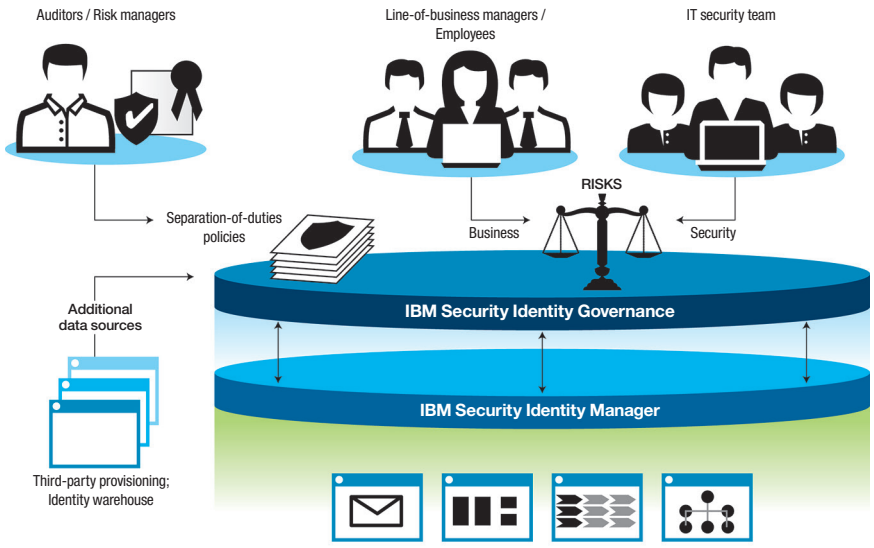
IBM Security Identity Governance and Administration is a business facilitator on multiple levels—helping IT staff contribute to meeting business goals with sophisticated capabilities for controlling who is entitled to access what, identifying those attempting access, and making sure that only those with proper authorization are allowed access—and helping line-of-business managers support the business by enforcing security policies, complying with regulatory requirements and protecting data.

Its wide range of self-service functions are business-user friendly and include a shopping cart-like experience, allowing easy management of profiles and access with an easy-to-use interface. Designed to simplify processes for managing user entitlements while strengthening the ability to meet security compliance concerns such as SoD violations, the solution helps bridge the gaps between business, IT and compliance processes with capabilities ranging from business-driven identity governance to end-to-end user lifecycle management.

The solution brings together capabilities that help organizations adopt a business-centric approach to identity and access governance, simplifying the review and certification of user access while it prevents governance from being an afterthought. With identity management tools that are easy to install, configure and use, line-of-business managers are now better able to create appropriate user roles and assign access privileges to each with a view toward supporting business and compliance goals. At the same time, IT staff can automate the creation, modification and termination of user privileges with audit trails and detailed reports, automatic recertification of privileges, and detection and correction of noncompliant accounts.

IBM Security Identity Governance and Administration can help organizations mitigate access risks, managing people as well as applications by targeting user roles, accounts and access permissions. Now compliance, provisioning and access management processes can leverage a common governance framework that consolidates entitlements within a central repository and structures them into business roles. The solution also helps reduce costs and improve productivity with self-service access requests and password management.

IBM Security Identity Governance and Administration is offered as a unified solution comprising IBM Security Identity Governance Foundation and IBM Security Identity Manager. IBM Security Identity Governance helps organizations understand, control, and make business decisions related to user access and access risks. IBM Security Identity Manager helps increase the efficiency and accuracy of user entitlements and profile administration. By integrating the capabilities of these two products, IBM provides a single-vendor solution that helps improve an organization's governance posture, while also reducing total cost of ownership and overall complexity.



IBM delivers an integrated identity governance approach designed to help organizations mitigate user access risks and support regulatory compliance.

Simplify access governance with a business-focused approach

Today, even small and midsized organizations deploy dozens of business applications. And each application has its own data requirements for defining user roles and processes for providing access. The challenge comes in managing these entitlements—especially when an organization ends up with more roles than people. Each application can have multiple roles that match its technical functions, but those roles often don't match business functions because they're defined differently. There may be four variations of "accountant" in different applications, for example, while the business may have only one.

The resulting jumble of roles can tremendously complicate SoD configurations, where each entitlement or role needs to be mapped and matched against each application. This can lead to an unmanageable number of combinations *and* serious consequences when it comes to compliance. Even if an individual commits no inappropriate actions, the fact that she has access to certain IT resources can violate SoD rules, increase exposure to fraud, compromise validity of access-certification processes and result in noncompliance. To help control these situations, organizations need to define roles from the business-activity point of view—rather than application capabilities—and align the roles with access policies established by business leaders.

Such a business-activity centric approach to access governance can significantly reduce management challenges—because it places the emphasis on the user's role and activities, which can be structured in a common framework, rather than according to diverse IT applications. For example, all tellers in a bank can belong to the same business role, with clearly defined business activities they perform as a part of their job description. Then, SoD rules can be defined on the business role and activity level. Therefore, a teller who becomes a loan officer can simply switch to a different business role; the underlying mapping to IT entitlements changes automatically, reducing the possibility of an SoD violation.

This approach also enables IT administrators and line-of-business managers to work together to better understand and control access—and to prove compliance with regulatory standards. It can help organizations avoid "entitlement creep," in which a user retains unnecessary and perhaps inappropriate access privileges from a previous position because the SoD rules have been incorrectly managed within applications.

Address key issues that are driving change in identity management

IBM Security Identity Governance and Administration provides an effective response to changing demands for greater security and regulatory compliance. Specifically, compliance regulations are requiring that organizations focus on how and why user access is granted in addition to how management complies with security policies and standards.

The resulting shifts in how organizations handle access fall into three core areas:

- **Governance** is now a fundamental component across all identity and access management processes—not something auditors work on after the fact. By embedding policies and controls throughout all identity processes, organizations are better able to achieve ongoing, sustainable compliance and can reduce the need for expensive, after-the-fact remediation.
- **Regulatory compliance** is increasing and tightening in response to ongoing security breaches and threats to sensitive data. Organizations today must comply with regulations or face penalties. Maintaining and proving compliance with government regulations demands effective controls over access privileges and activities.
- **Role management,** which classifies users by their organizational roles or group membership, job activities and access needs rather than as individuals, makes it easier to handle exceptions and identify abuse. Role and policy modeling, which maps entitlements to a user's role and access needs, can streamline management with automation and help ensure both security and business goals are met. By carefully monitoring how user entitlements align with business roles and responsibilities—outside of IT applications—organizations can better support compliance policies and minimize inappropriate access.

Better understand, control and make business decisions related to access

Part of the IBM Security threat-aware identity and access management portfolio, IBM Identity Governance and Administration helps organizations automate the process of provisioning users with access rights to the data and applications they need.

The bundled solution helps address access management and governance requirements, including:

- **Separation of duties:** IBM Security Identity Governance and Administration offers advanced support for modeling conflicts based on users' activities rather than their roles. The activity-based approach is designed to simplify the definition of violations by reducing the number of policy constraints administrators must manage. The solution also provides components specific to transactions and authorization in SAP environments.
- **Role management and mining:** IBM Security Identity Governance and Administration allows translation of complex access rights into business-readable, easy-to-manage roles. With a visual role-mining interface, it enables business managers and IT staff to work together to establish role criteria, such as the number of constituents and entitlements in a role. The solution can make adjustments as business processes evolve so that roles and permissions align with changing requirements. It supports real-time responses to policy violations in order to define policies for role visibility, SoD, access certification and access risk mitigation. The solution also helps to proactively enforce pre-established business policies for how access should be granted throughout the access request and provisioning processes.
- **Compliance reporting:** The solution provides auditing and reporting on user entitlements and access activities for actionable IT operations and effective compliance reporting. IBM Security Identity Manager includes native IBM Cognos® reporting capabilities and audit trail collection, correlation and detailed reporting to help address compliance mandates. These enhance the solution with predefined reports and audit events, which can help auditors quickly gain an accurate view of an organization's security posture and state of compliance.
- **Access review and certification:** The solution also helps centralize and automate tasks for administering user identities, credentials, accounts and access permissions throughout the user lifecycle. Powerful access-rights recertification features automatically trigger periodic review processes for recertification of user access while providing granular, auditor-friendly details for compliance. It enables scheduling and monitoring of access review and certification campaigns to help identity policy violations and remediate risks by assuring that users have only the entitlements that are justified by business activities.
- **User management and self-service:** The solution provides broad, out-of-the-box support for managing user access rights and passwords on applications and systems. User requests, such as password changes, profile updates and requests for new access rights, can be viewed, modified, approved or rejected through an easy-to-use interface. Plus, users can be automatically notified of the status of their requests. IBM Security Identity Manager can help enforce policy-based password controls, such as hard-to-guess passwords and frequent password changes. Its web-based, self-service administration features and embedded workflow engine enable administrators to group users according to business needs and delegate functionality as needed. For example, administrators can easily specify who can add, delete, modify and view users and reset user passwords.
- **Ease of use and request management:** The solution provides an intuitive, self-service interface that makes it easier for business managers to make informed access-related recommendations or requests for their employees, while helping to improve visibility and accuracy of user authorizations. It empowers users to actively participate in and manage their own access privileges and passwords while providing them with full visibility into active requests, thereby reducing the workload on help desk and IT operations teams.

IBM Security Identity Governance and Administration delivers the best of both worlds—empowering users and managers with the self-service tools and rapid entitlements they crave, while delivering the improved visibility, compliance and risk management demanded by organizations. By integrating policy and governance controls with identity management processes, the solution helps organizations understand, control and make better business decisions related to access and risk—and respond more effectively to the latest security challenges.

Why IBM?

IBM Security solutions are trusted by organizations worldwide for identity and access management. These proven technologies enable organizations to protect their most critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions.

IBM has worldwide service delivery expertise in some of the most highly regulated industries, including government, healthcare and financial services. As a strategic partner, IBM empowers organizations to reduce security vulnerabilities and manage risk across the most complex IT environments.

For more information

To learn more about IBM Security Identity Governance and Administration, please contact your IBM representative or IBM Business Partner, or visit **ibm.com**/security

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2014

Please Recycle

WGS03042-USEN-00