Making intelligent decisions about identities and their access

Provision users and mitigate risks with IBM Security Identity Governance and Intelligence

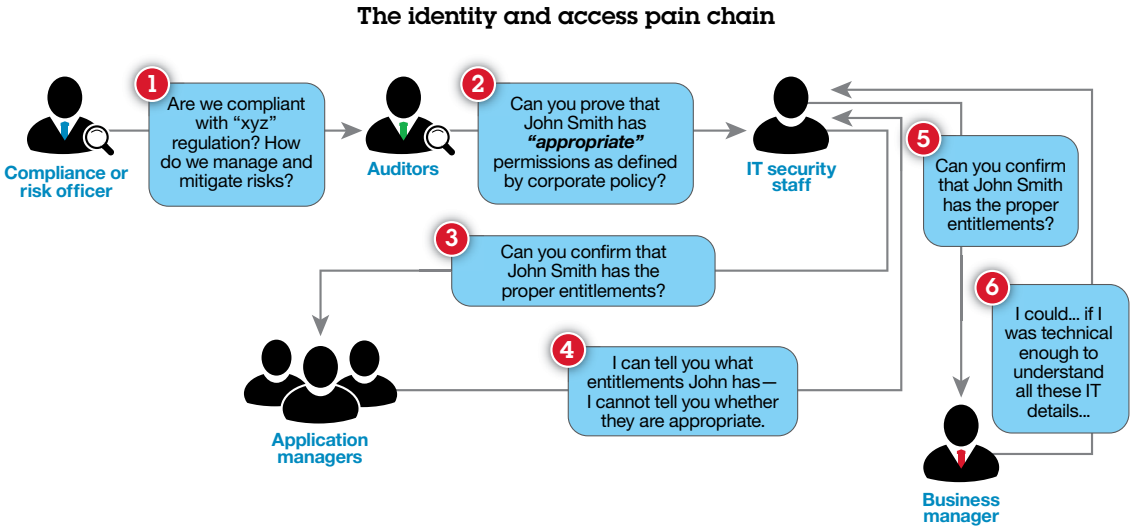
Highlights

- Provide a business-centric approach to risk-based identity governance and management
- Use analytics to provide deep insight into users and entitlements
- Enable end-to-end user lifecycle management with provisioning capabilities
- Help increase efficiency with self-service and with business- and auditor-friendly dashboards
- Facilitate communication between auditors, business managers and IT staff to automate segregation-of-duties (SoD) policies across enterprise applications
- Align line-of-business, IT and compliance perspectives with a consolidated platform for identity governance and administration

As security threats increase and government regulations require more control over users and data, it is important for organizations to evolve their security measures. As enterprises rapidly expand their footprints into cloud, mobile and social, they must ensure that the right users have the right access to sensitive data and applications. Strong as well as optimized identities are becoming increasingly important as insider threat and tightened regulations become more prevalent.

Additionally, granting and managing access has traditionally been the domain of IT professionals, leaving the rest of the organization with little visibility into how user access actually aligns with security and compliance requirements, as shown in the "pain chain" flow chart (below).

With identity governance and management, organizations can better protect their "crown jewels." They can maintain strong control over user access to applications and carefully monitor how access entitlements align with business roles and responsibilities. As roles grow, this becomes increasingly difficult. For example, a stock trader working in a financial institution may be promoted and given access to approve trades in a new system while retaining access to enter trades in the previous system. This dual access may constitute an SoD violation, which can result in more than an audit failure. It can expose the institution to insider threat and fraud, leading to both financial losses and damage to the corporate reputation.



Additionally, 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. The cycle continues 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.

IBM® Security Identity Governance and Intelligence is designed to help organizations effectively grant and manage identities and application access throughout the user lifecycle by bridging the gaps across compliance, business and IT infrastructure operations. As a result, organizations can help reduce the risk of fraud, toxic combinations of access and human error in business processes.

The solution enables organizations to adopt a business-centric approach to identity governance and administration. This can significantly simplify the provisioning process as well as the review and certification of user access. It also delivers detailed analysis of user roles and entitlements, and how they align with business processes and rules. IBM Security Identity Governance and Intelligence helps ensure that the appropriate levels of access are applied and enforced across all types of enterprise applications, making it an integral part of an organization's compliance and risk strategy.

Simplifying identity governance and intelligence

Identity governance has often been an afterthought, something the IT or security teams work on after other identity and access management controls are in place. But by aligning governance-related policies and rules with all identity management processes, organizations can achieve continuous, sustainable compliance, thereby reducing the need for after-the-fact fixes and expensive, error-prone manual remediation. A more innovative and effective approach is required to streamline all of these efforts—one that leverages an enhanced governance framework for roles, policy and risk management—across all resources. This way, from the factory floor to the boardroom, leaders have the insight they need to secure users and their access.

IBM Security Identity Governance and Intelligence delivers a single identity governance and administration platform to help organizations understand, control and make business decisions related to user access and access risks. The solution helps organizations to:

- Centralize and automate tasks for administering user identities, credentials, accounts and access permissions throughout the user lifecycle, from provisioning to deprovisioning
- Periodically review and recertify user access, identify SoD policy violations and remediate risks associated with user access
- Provide visibility into user entitlements, including who has access to what, when they got that access, who they got it from, why they have access to it, and whether it is compliant with external and internal policies and regulations
- Deliver a single identity governance and administration platform to help organizations understand and control access—and make business decisions related to user access along with risk and compliance
- Provide a business-activity based solution approach to help auditors to determine SoD violations across SAP and non-SAP environments and enterprise applications
- Automatically trigger the access review and recertification process required by regulation; drive the workflow to coordinate access certification campaigns
- Analyze and optimize business roles and permissions in an existing user-provisioning system and in enterprise applications not covered by the deployed user provisioning system

Mapping business activities

Traditionally, IT has utilized roles not only as a way to organize IT-centric access permissions and to provision user access into applications but also to manage access and SoD policies. However, auditors and business leaders have had little understanding of how those roles correlate with business operations. In addition to verifying that users have the appropriate access rights, compliance officers need to identify potential access risks, such as combinations of access rights that result in an SoD violation—for example, the ability to both create and approve purchase orders. Therefore, one of the key audit requirements is to report on controls in place to enforce the necessary SoD.

However, such audit requirements can trigger a confusing, time-consuming chain of conversations, where IT staff cannot see all the dependencies that apply for a specific business case, application managers cannot easily confirm if the access rights are appropriate for a user, and business leaders cannot understand what the access rights mean.

To overcome this organizational challenge, IBM Security Identity Governance and Intelligence provides a centralized platform for collecting user and permission information from a variety of sources, including business applications, human resource systems and existing provisioning platforms.

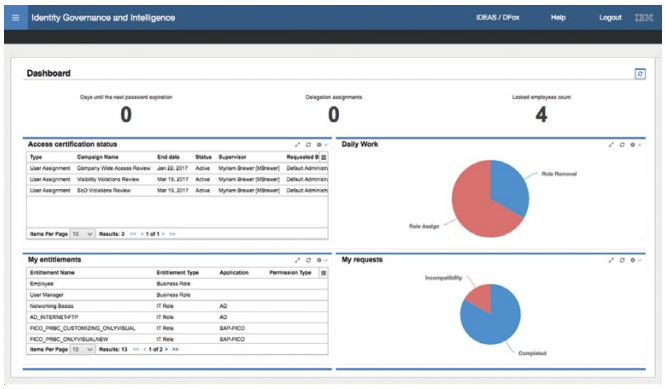
Sophisticated algorithms are applied to identify business-relevant roles and risks, and to help translate technical permissions into user-friendly business activities and/or business roles. These activities and roles are then displayed within audit-friendly dashboards to help the entire organization evaluate access risk and activity-based SoD across enterprise-wide applications.

IBM Security Identity Governance and Intelligence features an innovative, visual role-mining interface that allows business leaders, together with IT staff, to implement the continuous optimization of roles as business processes evolve. As a result, different groups can collaborate on how roles and permissions align with evolving security and compliance requirements.

Automating user provisioning

IBM Security Identity Governance and Intelligence 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.

In addition, IBM Security Identity Governance and Intelligence has robust identity management and user lifecycle capabilities. This helps to manage the user lifecycle with provisioning and business-centric access request management. IBM Security Identity Governance and Intelligence utilizes its business-centric identity management platform to empower both the end user and line-of-business manager by giving them the tools and information needed to make compliant and secure decisions regarding user access.



The IBM Security Identity Governance and Intelligence dashboard shows key metrics in a format useful for both daily operations and audit purposes.

Getting off spreadsheets and into smooth recertification

With a 7,000-member workforce and 400 applications in play (including PeopleSoft, Facets claim software and other healthcare-related applications for data and claims), a large organization in the healthcare/insurance field faced the need to simplify identity management and governance. Recertification was painful for users: twice yearly, the firm had to execute an arduous 4-month process, using spreadsheets to track end-user data. Just as pressing was the critical need to reach compliance with SOC 2 for the 36 applications currently SOC 1 certified. Now they're deploying IBM Security Identity Governance and Intelligence to help reach that compliance and, beyond that, to save time and money with a smoother access recertification process. From there, with IBM Security Identity Governance and Intelligence as a linchpin, the organization plans to implement SoD management and risk-based access control.

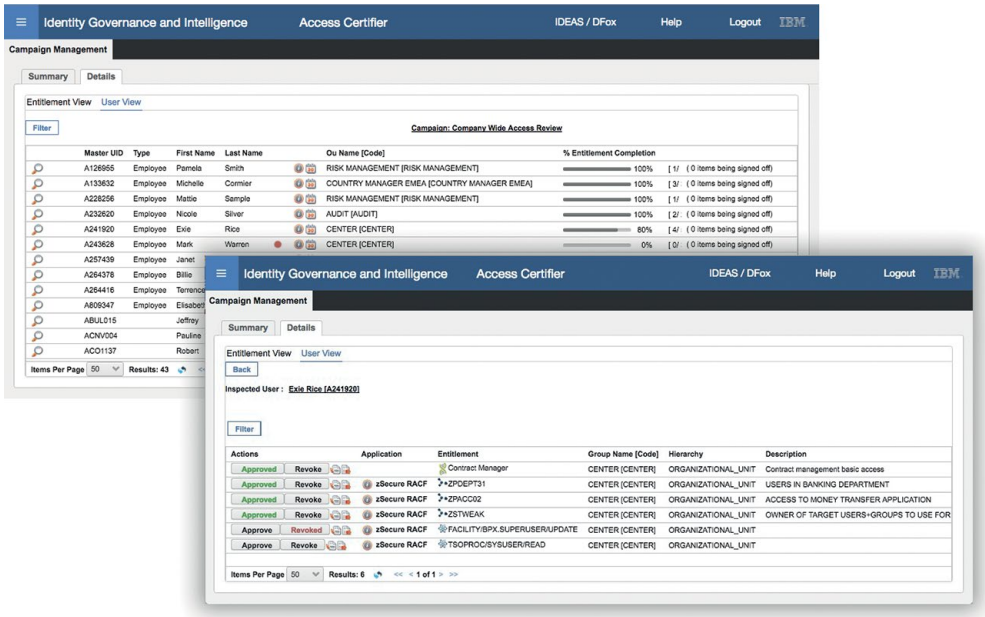
Ensuring that users have the access they need as quickly and efficiently as possible is critical. The right solution can automate provisioning and get users the proper access quickly, saving the organization time and money, while also maintaining compliance and security. Automating deprovisioning is just as important, ensuring that users or user accounts no longer have access or can be compromised once the users are no longer with the organization. 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?"

Certifying user access

Regulations frequently require that authorizations be periodically reviewed and explicitly recertified as still appropriate for individual users and user groups. IBM Security Identity Governance and Intelligence enables compliance managers to design the access certification campaigns that will automatically trigger the review process and drive the workflow to coordinate access approval and re-certification.

From a single screen, business managers can trigger approval or revocation of access rights, review SoD violations, and track the status of access certification campaigns across the organization.

IBM Security Identity Governance and Intelligence also helps improve productivity with self-service access requests. Using an online catalog, employees and managers can amend currently assigned permissions or "order" new permissions. These requests are entered into an automated approval workflow, which varies according to the risk level of the requested access.



The IBM Security Governance and Intelligence Access Certifier module helps safeguard resources by letting administrators quickly inspect and modify user permissions.

Managing segregation of duties

IBM Security Identity Governance and Intelligence enables organizations to enforce SoD controls to meet the specific requirements of auditors—rather than IT staff. The solution provides SoD controls based on pre-defined business activities, which themselves are aligned with individual business processes. This way, conflicts can be easily discovered and described, so it is no longer necessary to resolve them at the IT application entitlement level.

IBM Security Identity Governance and Intelligence supports fine-grained SoD in enterprise resource planning (ERP) applications by connecting to the appropriate features within the ERP system, so organizations can have unified controls across heterogeneous environments. With regard to SAP SoD, IBM delivers integrated support for managing roles with pre-defined rules, down to the level of SAP transactions and authorization objects. With an activity-based modeling approach, conflicts can be easily discovered and described. With granular support for both SAP and non-SAP environments, enterprises can help reduce the costs of SoD adoption.

In addition, IBM Security Identity Governance and Intelligence offers real-time analysis of SoD rules, enabling organizations to continuously monitor for potential conflicts. Risk scoring can be part of the access request workflow, where specific conflicts can be escalated for mitigation and other conflicts allowed as exceptions—helping to focus attention on the areas that pose the greatest risk.

Each organization has a unique and specific mix of applications, resources, users and access polices that need to be addressed differently while still maintaining a unified management approach. For example, two of the most important systems in many organizations are SAP applications and IBM z Systems™ mainframes. Due to the complexity of access control in these two systems, managing SoD can be a difficult task.

IBM Security Governance and Intelligence provides specific controls to help simplify the management process for SAP and mainframe-based systems. Not only can IBM help manage fine-grained SoD in SAP and mainframe environments, it also can manage those SoD conflicts across platforms. In order to keep SAP applications and the mainframe secure, user access must be governed using an identity governance and intelligence solution that works across multiple environments. Each organization needs a “single source of truth” for user access and identities—and the best way to achieve it is with a business-centric solution that integrates with your current environment and adds to it a layer of governance.

Why IBM?

Governance and administration is difficult—and traditional approaches are failing. However, a business-centric identity governance and intelligence solution that uses business activities and operates across multiple platforms can make the process easier by enabling the business manager to make the right decision. With the right governance and intelligence solution, organizations can take a big step in the right direction toward remaining compliant and securing their environments.

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. In addition, IBM Security solutions can integrate with third-party environments, including Oracle, Microsoft and SAP, for robust protection.

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 Intelligence, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

WGS03041-USEN-02