

Making intelligent decisions about identities and their access



Gain insight and mitigate risks with IBM Security Identity Governance and Intelligence

Highlights

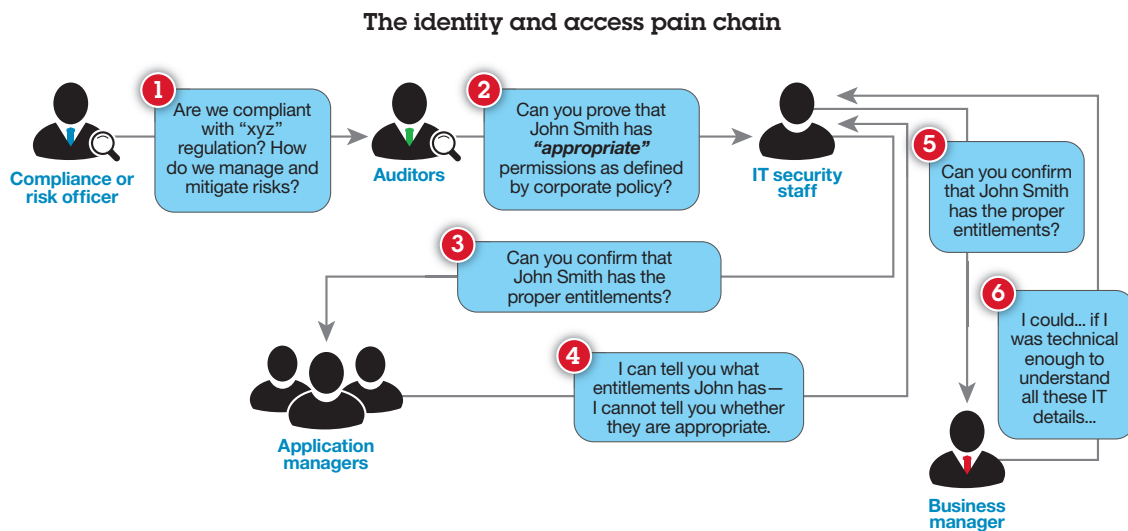
- Deliver value with a business-centric approach to risk-based access governance
 - Use analytics to gain deeper insight into users and entitlements to strengthen security and meet compliance requirements
 - Help increase efficiency with auditor-friendly dashboards, delegated administration and self-service
 - Facilitate communication between auditors, business managers and IT staff to automate segregation-of-duties (SoD) policies across enterprise applications, including SAP and mainframe
 - Simplify access review and certification processes with centralized governance
 - Enable end-to-end user lifecycle management with provisioning capabilities
-

In a world of increasingly sophisticated security threats and increasingly stringent government regulations, it is important for organizations to evolve their security measures. As enterprises rapidly expand their footprints into the cloud, they must ensure that the right users have the right access to sensitive data and applications. With increased software-as-a-service (SaaS) adoption and users logging in from anywhere under bring-your-own-device (BYOD) policies, existing infrastructure protection is not as available as it used to be. Strong identity and tight entitlements are becoming increasingly important, as defense in depth is not there to fall back on.

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.

With identity and access governance, organizations can better protect their “crown jewels”—the critical data that is vital to brand protection and effective operations. They can maintain strong control over user access to applications and carefully monitor how access entitlements align with business roles and responsibilities. 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 a segregation-of-duties (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.





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

The solution enables organizations to adopt a business-centric approach to identity and access governance. This can significantly simplify the review and certification of user access. It also delivers detailed analysis of 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 foundation 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
- 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, why they have access to it, and whether it is compliant with external and internal policies and regulations
- Deliver a single identity governance 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 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.

A corporate spin-off gains control with identity governance

With a workforce composed of employees, interns and contractors, a leading packaged food and beverage company needed to gain control of its identity and access governance processes after a recent spin-off from its parent corporation. In addition to having manual access certification processes that were not scalable or reliable, the company also lacked the remediation and reporting capabilities required for audits. By deploying IBM Security solutions, including IBM Security Identity Governance and Intelligence, the company can now monitor enterprise-wide access from a single view. The solution can automatically revoke access when necessary for remediation and streamline access certifications, freeing up IT staff for other activities.

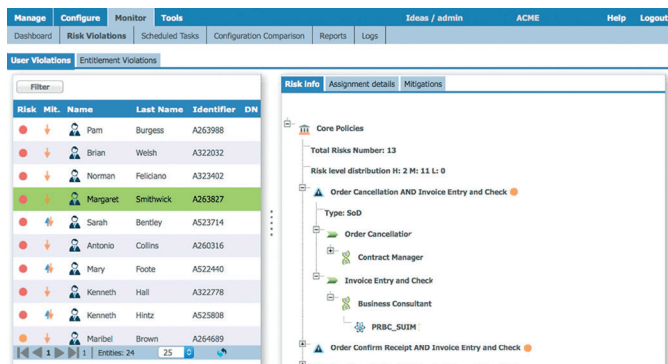
However, such audit requirements can trigger a confusing, time-consuming chain of conversations, where IT staff cannot see all the dependencies that apply for a specific business case, application managers cannot easily confirm if the access rights are appropriate for a user, and business leaders cannot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

Managing identities and certifying access

In addition, IBM Security Identity Governance and Intelligence has 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 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.



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 then approve or revoke 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.

Managing segregation of duties

IBM Security Identity Governance and Intelligence enables organizations to define SoD controls to meet the specific requirements of auditors—rather than IT staff. The solution provides SoD controls based on pre-defined 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 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. Conflicts can be easily discovered and described within a business context using

an activity-based modeling approach. 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 policies 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.

Campaign ManagementIDEAS / AETT383HelpLogout

SummaryDetails

Entitlement ViewUser View

Filter

Campaign : Company Wide Access Recertification_Short

Master UID	Type	First Name	Last Name		Ou Name [Code]	% Entitlement Completion	
A015700	Employee	Marina	Thomas		CORPORATE / Administration, Finance and Control [CORPORATE / Administration, Finance and Control]	100 %	1 / 1
A126204	Employee	Randy	Zielinski		CORPORATE / Administration, Finance and Control [CORPORATE / Administration, Finance and Control]	100 %	2 / 2
A228147	Employee	Kathryn	Robinson		CORPORATE / AUDIT [CORPORATE / AUDIT]	100 %	1 / 1
A229607	Employee	William	Baltazar		CORPORATE / AUDIT [CORPORATE / AUDIT]	100 %	1 / 1
A230704	Employee	Patricia	Whiteman		CORPORATE / AUDIT [CORPORATE / AUDIT]	75 %	3 / 4
A232021	Employee	Dorothy	Fultz		PRODUCT DIVISION / CENTER [PRODUCT DIVISION / CENTER]	0 %	0 / 1
A232586	Employee	James	Livingston		SALES / MAR		7
A241920	Employee	Exie	Rice		PRODUCT D		1
A242158	Employee	Maria	Doss		PRODUCT D		2
A243628	Employee	Mark	Warren		PRODUCT D		3
A247479	Employee	Harry	Peck		INTERNATIO		1
A252344	Employee	Alexis	Ross		SALES / MAR		2

Entities: 2625

Entitlement ViewUser View

Back

Inspected User : Patricia Whiteman [A230704]

Filter

Actions	Application	Entitlement	Description	
ApprovedRevoke	Pivotal	Gas Report		
ApprovedRevoke	Pivotal	Quality Manager	Quality and Audit support and management entitlement set	
ApprovedRevoke	Pivotal	SER Report		
ApprovedRevoke	AD	Networking Basics	Core networking services including Mail and VPN access	

Entities: 425

Why IBM?

Governance is hard—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. 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, health-care 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



© Copyright IBM Corporation 2015

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
November 2015

IBM, the IBM logo, ibm.com, and z Systems are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



Please Recycle
