IBM Software
Thought Leadership White Paper

July 2012

Intelligent role management for improved security and compliance

IBM Security Identity Manager contributes to closed-loop identity and access management governance

IBM

Contents

Managing user access entitlements and activities has become increasingly critical to the security of today's organizations. Having visibility into who has access to what—data, systems, applications and resources—and associated governance policies to control those accesses is necessary to prevent unauthorized use and to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or Sarbanes-Oxley. Organizations need effective and efficient tools to provide identity management—the administration of user entitlements and access privileges—that enables individuals to quickly access the resources they need to do their jobs, and nothing more. Failure to do so can result in audit failures or worse yet, a high-profile security breach.

The IBM strategy for addressing this need is with a continuous, closed-loop, access-entitlement process called identity and access management (IAM) governance. IAM governance starts with the identity and access planning process, and continues with identity lifecycle administration. It goes on to include the real-time enforcement of user access. The last critical piece is providing feedback to this looping process via user activity monitoring, to track how access entitlements are really being used. Throughout all of this, IBM infuses the process with security intelligence, including advanced role analytics from IBM Research, advanced algorithms for entitlement reconciliation and context-sensitive, risk-based, real-time authentication.

The need for role management

In dynamic environments with employee turnover, new business requirements or ongoing compliance challenges, user-access entitlement needs can change rapidly and become difficult to manage. As employees change jobs or leave the enterprise, their entitlements need to be updated in a timely manner to reflect their changes in status and access privileges. As companies or departments merge or split, or new security regulations are imposed, business roles and application access privileges must be adjusted.

For IBM, business-centric role management is a cornerstone to an effective IAM governance strategy. Role management—assigning user access per role instead of per individual—helps streamline the governance process through automation. Effective role management improves productivity, while ensuring that business priorities and compliance goals are met. It also enhances visibility into user-access entitlements, enabling managers to see whether the access privileges are appropriate and in line with their business policies and regulations. For role management to be effective, it must be aligned with an organization's business needs. Business managers should be closely involved in making the role decisions for their employees and providing input for areas including role definition, access rights and compliance requirements.

As part of the IBM Security Identity Manager solution, IBM Security Role and Policy Modeler provides powerful role-management capabilities that help organizations assess their current user entitlements and plan for an effective role structure to support their business needs. With a design that focuses on the business user, this solution supports role management best practices—helping to ensure alignment with business goals and success in role management projects.

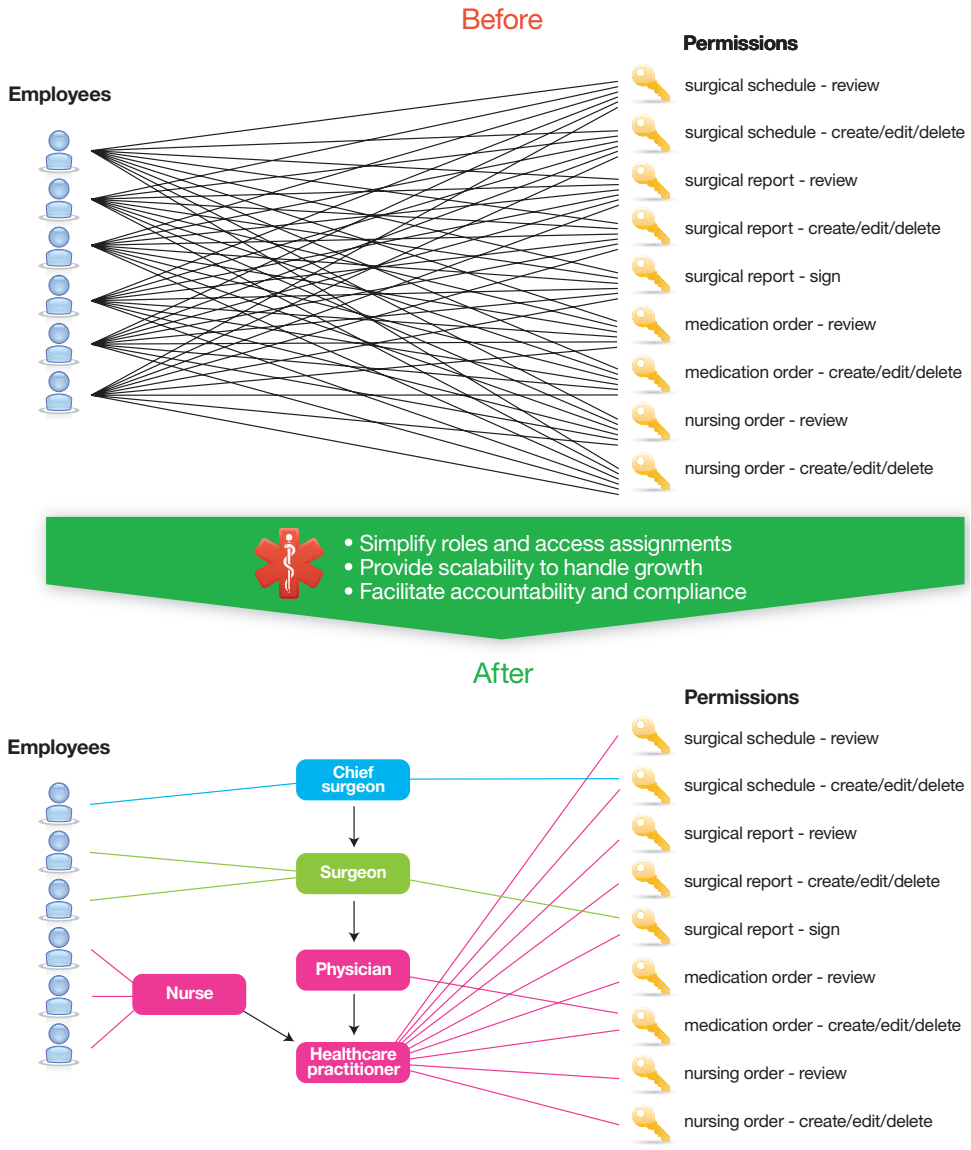

Figure 1: Role management can greatly simplify and expand automation for user access. In healthcare environments, employees are entitled to permissions such as reviewing and approving medical reports and medications. Implementing a role hierarchy can streamline the user-access process and provide more control and visibility.

Best practices address the challenges of role management

Role management can be an important component of an organization's governance posture. It can help organizations maintain focus on their security goals as their business needs change over time, as well as help streamline and strengthen the governance process. However, role management projects can fail or stall, often from the sheer complexity of defining dozens, or even hundreds, of roles and mapping those roles to access privileges and restrictions. A better approach is needed. Let's look at how IBM supports best practices to help role management implementations succeed and remain relevant as business needs change over time.

Support the governance lifecycle

One of the first priorities for an organization should be to gain visibility into and define its existing, but sometimes implied, role structure as business policies. Once a clear picture of the current situation is understood, the role analyst needs to collaborate with business managers to ensure that the correct entitlements are implemented. Even after a role structure is established, there needs to be continued maintenance through regular review cycles (recertification). And after entitlement policies are put into place, organizations should implement user provisioning to execute these policies.

By including the Role and Policy Modeler as an embedded component, Security Identity Manager supports the entire lifecycle of these projects, from policy definition, role mining and planning, to role analytics and provisioning enforcement, through to periodic user assignment recertification.

Promote business collaboration

For role management to be effective, it must be aligned with an organization's business needs. Collaboration between IT analysts and business managers is an important factor in successful role-management projects. Role design and deployment needs to be a collective effort between line-of-business managers and the providers of requested application services. Including appropriate business unit decision makers throughout the entire role-management lifecycle helps ensure that role structures support the organization's business needs.

However, some IAM governance solutions are designed for IT administrators instead of line-of-business managers, eliminating these key business decision makers from the role-management process. To be truly effective, a role-management solution must be tailored toward business managers to allow them to easily participate in these projects.

Taking this approach toward role management, the Role and Policy Modeler component of Security Identity Manager is targeted toward business users. It provides easy-to-understand visualization of proposed role structures and shows how they fit into the current organization. It also provides collaboration tools to ensure easy review by business managers.

Start with small successes

When planning a new role-management project, it can be helpful to start small—address one department or group at a time. Once a structure is successfully established and an ongoing review cycle is in place, then the role strategy can be applied to the parent group or its other sub groups. This helps ensure that the process is sufficiently tested and established before it is applied to the larger organization, and can help make the potential complexity of the role structure more manageable. IBM Security Role and Policy Modeler supports this approach—helping organizations to establish strong role management strategies.

Use accurate data to create roles

When using role mining to identify current roles and role modeling to create a structure, role analysts need to make sure that the mined information is accurate. Although role mining and role modeling can be useful methods for establishing a structure, the mined information could be based on outdated information. It might include employees who have left the organization, or may reflect the outdated entitlements of employees who have changed positions. Or, as is frequently the case, the mined information could be inconsistent across an organization, containing inconsistent job titles or responsibilities. So, the incoming data must be reviewed and cleansed (updated) to ensure its accuracy, and then normalized (made consistent across the organization) to be useful for the enterprise-wide project.

The Security Identity Manager Role and Policy Modeler provides an analytics catalog to help filter the raw, mined data and spot inconsistent entitlements that may indicate outdated assignments or cross-departmental inconsistencies. This enables role analysts to better understand the existing access data before using it to model new roles. Highlighting issues can help resolve them, leading to more effective role assignments and assignment criteria. For example, existing data might highlight a separation-of-duties conflict that could require either a reassignment of existing access or modification to the separation-of-duties policies in order to accommodate a common-exception condition.

Create an ongoing review process

Once organizations establish business-oriented roles, they need to create an ongoing review process to help maintain governance. A role structure cannot be truly effective unless it can adapt to changing environments and business needs. If roles and entitlements are not properly updated, this can lead to security issues and potential compliance failures. Roles should be periodically reviewed by business managers and resource owners to make sure they remain valid, and then user assignments recertified to ensure that users have appropriate access entitlements.

With its built-in support for ongoing reviews and recertification of role assignments, Security Identity Manager enables organizations to establish well-defined roles and entitlements and to periodically review and update them as needed. This helps organizations maintain security and compliance by enforcing governance on an ongoing basis.

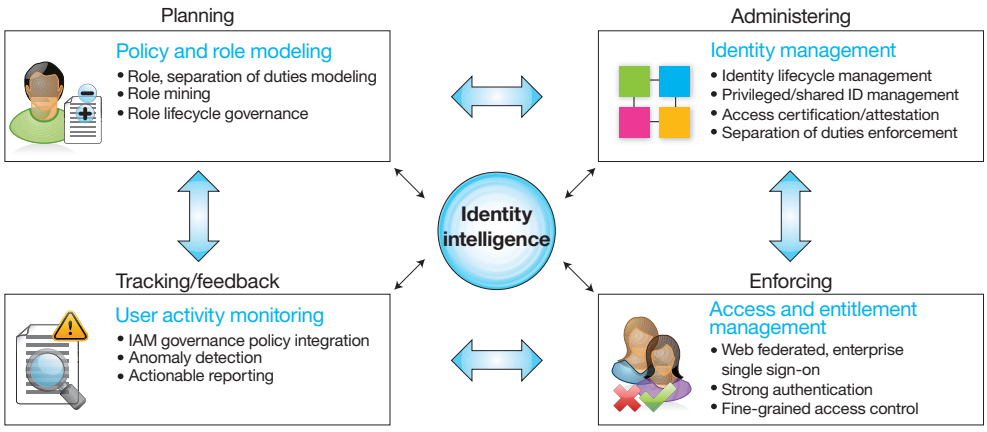

Figure 2: IBM takes a closed-loop approach to identity and access management governance by addressing all stages of the user-lifecycle process—from planning and administering to enforcing and user monitoring.

The IBM governance solution in practice

One example that illustrates how the IBM role-management solution supports best practices involves a multinational pharmaceutical company. Due to insufficient and inconsistent controls on sensitive applications, including the lack of an audit trail for user privileges, the company failed a compliance audit.

To begin addressing the situation, the company's first priority was to gain visibility into their current application access environment. They needed to gather and report on the existing user privileges in order to identify and address missing controls. The company's second priority was to create a business-role structure they could use to consistently enforce user access going forward.

The company was already using Security Identity Manager to manage passwords and provision users to various systems. However, as the company grew, the entitlement management process had become quite complex, and the company hadn't kept up with the organizational dynamics. They needed to implement a governance system to continuously monitor entitlement information, conduct periodic reviews and enforce appropriate controls.

Taking advantage of the integrated Role and Policy Modeler component of Security Identity Manager, the company was able to efficiently gather existing data on users and their access rights. They were able to use the advanced analytics of the Role and Policy Modeler to better understand the gaps and inconsistencies in roles and entitlements. The company was then able to review the findings with key business managers, using generated reports, and converge on appropriate entitlement changes. During the process, the company identified thousands of unnecessary entitlements. This also helped them to understand the required role model going forward. After addressing the deficiencies, the company implemented a recertification program to ensure regular reviews of user access.

The company next plans to take advantage of the Role and Policy Modeler built-in intelligence to suggest business roles for organizing and assigning user access and roles going forward. They plan to use the analysis capabilities to run various "what-if" scenarios on the user access data to build the most suitable role structure—including separation-of-duties policies—to test the structure prior to implementation.

An intelligent approach to role management

It is clear that role management can be instrumental to the IAM governance process, especially for organizations with complex access structures. Role management can significantly improve security and ensure compliance. As part of the flagship IBM Security Identity Manager solution, IBM Security Role and Policy Modeler provides powerful role-management capabilities. Designed for the business user and in support of role management best practices, this solution helps organizations strengthen their role-management process and maintain alignment between user provisioning and their business goals. Today's security challenges demand intelligent solutions, and IBM builds intelligence into security solutions to provide organizations with the proactive security they require.

For more information

To learn more about IBM Security identity and access management solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security Systems software

The IBM Security portfolio provides the security intelligence to help organizations holistically protect their people, infrastructure, data and applications. IBM offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates the world's broadest security research, development and delivery organization. This comprises nine security operations centers, nine IBM Research centers, 11 software security development labs and the IBM Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 13 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
July 2012

Please Recycle

WGW03007-USEN-00