IBM Security

For better access governance, look beyond roles to entitlements

IBM Security Identity Governance and Intelligence can improve access control by integrating your existing systems—without compromise

IBM Security White Paper

Why roles exist—and why they're no longer enough

Not long ago, job roles were relatively easy to define and control. A person was an "accountant" or a "graphic designer" or a "business partner." But as organizations grew and business software became more sophisticated, new roles were added. "Accountant, New York" might require different access to applications and data than "Accountant, Chicago."

Roles were invented to make the provisioning and deprovisioning of users easier. And they worked; they still do. The ability to give a new user all (or most) of the access needed to perform a job role is leaps and bounds better than manually provisioning individual users for their specific duties on an ad-hoc basis.

The challenge comes from the recent explosion in the numbers and types of business roles. Organizations became so focused on having the perfect role for every user group that even slight variations in a person's profile or access needs would lead to the creation of an entirely separate role. The problem was: If the IT-enabled constraints that controlled user entitlements—the permissions they are granted to take action—were linked only to general titles, the more specialized roles might go overlooked, with no controls at all.

With identity governance, one multinational manufacturer manages

430 million

potential entitlement conflicts using a few hundred policies.

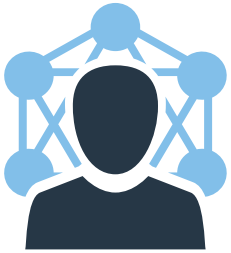
It's important to ensure that access needs and rights align

The creation of roles and the deployment of identity management tools gave organizations the ability to understand which users had access to which applications, along with when users were granted access.

This basic information, however, is no longer enough to ensure security and control. Organizations also need to know if the access users have is the *right* access. More importantly, they need to ensure that users do not have the *wrong* access.

The explosion of specific roles means that roles have increased not only in quantity but also in complexity. And roles are constantly changing. As a result, roles are no longer the right tool to govern user identities. Organizations need to look deeper into who has what entitlements and how they're using them.

One important—and effective—way to gain the necessary insight into users and their entitlements is to think like an auditor. This can help mitigate problems by ensuring that the necessary controls are in place to prevent violations. Has Bob not used a particular entitlement in the past six months? That's often a good reason to revoke the privilege. Does Nancy have the ability to initiate a request—say, for an equipment purchase—and then approve her own request? Another reason to revoke.



With IBM, a global online retailer removes almost

80% of user access privileges

after discovering infrequent access.

Thinking like an auditor addresses both business and IT needs

An auditor-friendly identity governance solution is key to effectively managing users and their entitlements. Auditors place heavy importance on having the right rules in place to identify segregation-of-duties violations. They also require controls to remove and prevent those violations.

But there's more. To be most effective, it's necessary not only to think like an auditor, but also to speak like one. The most commonly used language in identity governance uses terminology from the worlds of both IT and business. This combination can be an issue, however, for auditors who don't understand IT-speak and who prefer instead to use business terms. The right identity governance solution brings together the worlds of business and IT to help organizations understand whether or not users have access to the proper applications—and to support business decisions and actions that rely on appropriate access.

IBM® Security Identity Governance and Intelligence gives you the ability to look beyond roles for a detailed view into entitlements and business activities. The IBM solution provides the intelligence you need to accurately and effectively revoke, reassign or add entitlements—helping you meet business needs without compromising security.

A bank in France reduces its entitlements catalog, showing users

10-15 items

rather than hundreds.

Why business activities are a better basis for governance

Think of a role as a collection of entitlements. It's a way to define the types of access that people doing the same job or similar jobs need. These entitlements can range from access to email software (granted to everyone), to access to an application that manages intellectual property (granted to only a few), to access to very specific application functions (with the most limited access).

It's a multi-tiered process: An employee is assigned a role (for example, stock broker). That role comes with entitlements allowing access to software capabilities (such as entering the order for a trade). That capability enables a specific business activity (placing the trade). The stock broker, however, is blocked from approving that same trade. That entitlement is granted only to personnel who do not have permission to place a trade. Duties are segregated to avoid conflict.

The problem with roles is that they constantly evolve. Within each role there can be multiple other roles or nested roles, which can lead to confusion, breaches in compliance and security vulnerabilities. An auditor creating or enforcing a rule, however, may not have an in-depth understanding of roles. The result? Some segregation-of-duties violations may slip through the cracks.

A European insurance and financial firm governs access for

75,000 users

of SAP, distributed and mainframe applications.

Here's how the business activity-based approach works

What would happen if you segregated the duties of two roles—"web design" and "payroll"—to prevent posting employee salaries on the company website? Imagine, however, that someone from the payroll team also worked on website side projects that gave them the ability to post on the website without giving them the "web design" role. To prevent this scenario, every possible role (and sub-role) combination of the web design and payroll roles would need to be managed—a virtually impossible task without the proper, automated identity governance tools.

Rather than governing identities and segregating access with the abstract concept of roles, why not use something simpler? That's where governance based on business activities comes in. Rather than roles titled "web design" and "payroll," use plain language to describe activities, such as "Ability to edit the website" and "Ability to see payroll information."

In this approach, the organization and the auditor know exactly which capabilities each user has. What's more, sub-categories of activities (such as "editing graphics on a website") are automatically considered part of a larger category (such as "editing a website"), so there is no need for the manual management that is necessary when using roles. In many cases, an auditor will not understand which specific roles can and cannot overlap without conflict. However, auditors will understand which *business activities,* when used together, could present a segregation-of-duties violation and a security risk.

The right identity governance solution helps you control your users' access to business activities with consolidated, fine-grained visibility into entitlements—not just roles. Roles change, roles overlap, and roles increase. As a result, access must be governed at the entitlements level, allowing a view into the specific capabilities the user has, rather than relying on the confusing groupings of access given to a role. The right solution can deliver the intelligence you need to make the right decisions about who has—and who should have—access to what.

In summary: Controlling with intelligent IBM solutions

IBM Security Identity Governance and Intelligence sets the stage for business improvement by enabling you to grant the right entitlements to the right people. Using its deep visibility into entitlements, you can better enforce segregation-of-duties policies to ensure that currently authorized users don't have conflicting entitlements. You can manage orphan accounts to ensure that former users don't retain access after they leave the organization. And you can automate controls and reporting. The IBM approach enables you to govern using business activities—shining a light on complex roles to make management easier for auditors and to simplify governance tasks.

IBM Security Identity Governance and Intelligence connects the IT, compliance and business points of view to mitigate access risks. By consolidating fine-grained access entitlements from enterprise applications in a central repository and structuring them into business roles, for example, it delivers better visibility into actual user access.

As an integral part of the IBM commitment to leadership in identity and access management, IBM Security Identity Governance and Intelligence plays a key role in the IBM IT security portfolio. IBM solutions, including comprehensive security resources and insight provided by IBM X-Force® research and development, are designed to help protect business-critical applications and data from security threats, including conflicts made possible by gaps in controls.

E.ON Global Commodities needed to prevent

rogue trading.

With IBM, it can better:

- **manage segregation of duties**
- **provide reports to auditors**
- **understand the flow of information in the company**

Watch the introductory E.ON video from IBM.

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

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

WGW03177-USEN-02