Role Management and Risk

Jackie Gilbert, CMO & Founder of SailPoint, discusses how Role Management and Risk work as a Key Enabler for Accountability, Policy Alignment and Transparency in the World of Compliance.
Managing Risk with Roles

You may have heard recently that your organization needs a role management solution, most likely from your identity management team, an industry analyst, your external auditor or even all three. Role-based access control (RBAC) is not a new concept for IT security professionals, so you may be wondering “Why all the hoopla?”

The National Institute of Standards and Technology (NIST) formalized the RBAC concept – assigning access privileges in logical groups based on a user’s business role – in the early 1990’s. As a means to simplify and reduce the costs of user administration in complex computing environments, RBAC holds the promise for scalable user management in large, complex enterprise environments, which explains why the idea has persisted over the years.

But the renewed excitement about roles has little to do with administrative efficiency. The new driving force reigniting interest in role management is compliance with government and industry regulations such as Sarbanes-Oxley, Gramm-Leach-Bliley, PCI, and HIPAA. In the world of compliance, effective role management can provide the business context necessary for non-technical personnel to oversee and verify user access policy. Role management helps organizations manage information security risk and ultimately corporate risk in three key areas: accountability, policy alignment and transparency.

Accountability

In the wake of corporate scandals like Enron and the passage of the Sarbanes-Oxley Act, new demands for accountability require organizations to clearly assign responsibility for oversight and governance to the appropriate individuals in authority. From an information technology perspective, this means that the business owners of information (not IT security) are ultimately accountable for issues like fraud prevention and information integrity. These individuals understand the business risks facing the organization and can make the appropriate tradeoffs between business benefits and risk.

The growing involvement of business managers and business process owners in the information security process is elevating the importance of role management. When business managers are required to attest to the correctness of user access to critical business applications and sensitive data in quarterly access reviews, organizations must find ways to bridge the communication gap between business and IT personnel. By translating cryptic, technical access rights into higher-level business context, role management enables business managers to make more accurate decisions about who should have access to what resources. Roles also improve the efficiency of corporate oversight by reducing the number of items under review from dozens of individual access rights to a much smaller number of business roles.

“Role management helps organizations manage information security risk and ultimately corporate risk in three key areas: accountability, policy alignment and transparency.”
Policy Alignment

Effectively managing business risk related to IT security requires the active participation of business managers in the definition of access policy and controls. Business personnel understand the risks associated with sensitive applications based on asset value, privacy requirements, or potential for fraud or misuse, and they are best equipped to define the control objectives needed to mitigate business risk. But business managers must collaborate with IT personnel to effectively configure user access permissions (access to transactions, programs, tables, documents, etc.) based on business process rules and organizational restrictions.

Role management facilitates business and IT policy alignment by making it easier to translate business process rules into technical IT controls without delving into detailed IT entitlements. Defining access policy at the role level (a higher-level abstraction that maps to technical access privileges) allows business and IT groups to more effectively collaborate on separation-of-duty (SOD) conflicts and other access policy rules. For example, business managers can use business terms to define roles that cannot be held simultaneously by the same user (e.g., the ability to both approve a payment and change payment approval rules). Role management also makes it easier for business managers to align and enforce access policy across diverse application environments by centrally defining and managing the access privileges of all users who have access to critical resources.

Transparency

Transparency strengthens an organization’s internal controls by enabling better visibility into IT data and operations. In the face of regulatory compliance, it’s no longer acceptable for the IT department to be a “black box” to business users and executive management. In order to meet compliance mandates, there must be a level of visibility — in the form of audit data and compliance metrics — that can be understood and approved by business managers and executives.

The need for transparency has amplified the importance of roles and given them new relevance. Roles provide the business context necessary for non-technical compliance and audit personnel to verify user access policy and to determine if the actual state of user access matches the desired state as defined by compliance and governance policy. With role management, organizations can more effectively audit and report on the effectiveness of controls, including all approvals, authorizations, and certifications, and can identify potential risks, such as inappropriate access or policy violations.
Role Management in Perspective

As you consider the technologies required to meet your IT governance, risk management, and compliance (GRC) requirements, it’s important to remember that role management is not an end goal in itself, but rather a means to an end. By providing valuable business context and facilitating collaboration between business and technology groups, roles can help your organization move in the direction of stronger accountability, policy alignment, and transparency. However, in and of itself, a role management project will not help you address IT security risk.

To effectively manage user access across complex IT environments, role management must work hand-in-glove with automated workflow, policy enforcement, analytics and reporting, and risk management capabilities. This holistic approach helps organizations automate compliance processes, detect and prevent policy violations, remediate and mitigate control weaknesses, and provide auditable evidence of compliance. Think of role management as one key component in the overall compliance solution set you will need to reduce compliance costs, focus controls, and better manage access to critical resources in the context of true business risk.

About SailPoint

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of the world’s largest organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. The company’s innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information, visit www.sailpoint.com.