Bridging the Gap between Business and IT: How to Engage Business Managers in Identity Management Compliance and Security Processes

Learn the three best practices IT should follow to ensure that business managers actively and effectively participate in identity management compliance and security processes.
Identity Management Is Now a Key Business Process

Recently, global corporations have begun to recognize that identity management is very much a business process that underpins compliance and security efforts. Identity management has always been an extension of core business processes, ensuring that users have the access they need to do their jobs and that access is promptly removed when users leave the organization. But in the last decade, government regulations have added new security and compliance demands that require companies to demonstrate and prove strong controls over “who has access to what.”

This shift has made it all the more imperative that IT organizations work closely with business managers. Because they are the ones who understand the business risks facing the organization, business managers can and should make the appropriate tradeoffs between benefits and risks to the organization.

Alignment of Key Players Is an Imperative

Many people in technology talk about bridging the gap between business and IT, or more accurately, aligning business and IT. But the reality is that engaging business users in security and compliance processes is no easy task. Addressing this difficulty can help organizations ensure the effectiveness of IT controls in managing risk and reducing corporate liability. To get organizations started in the right direction, this paper sets out to explain three best practices that IT managers should follow to ensure that business managers are active and effective participants in identity management processes.

First, let’s examine the key business drivers for getting the business more involved.

Escalating compliance requirements. The coming years will bring more IT challenges than the industry has seen in a long time. Many companies are struggling with outdated compliance and security practices, and they will fall farther behind when additional regulatory mandates are put into effect. To achieve sustainable compliance, organizations must get the right people involved in the process, both business and IT, and should proactively address collaboration issues to eliminate the blind spots, redundant activities, and reactive decision-making caused by departmental silos.

Escalating business risk. Companies also face increased risk in the current economic climate because layoffs, stagnant wages, hastily completed mergers, and other events have increased the number of employees (and contractors) who pose an “insider threat.” Some threats have come from cases of unauthorized access, abuse of privileges, or theft, and alteration or deletion of proprietary data. Others have involved more extreme instances of sabotage, espionage or financial fraud. These “insider attacks” represent a real business risk that must be managed by every organization.

“I believe the shift toward more business involvement is a positive one for the IdM industry. It will help companies better address security and compliance requirements, and create more visibility with executive management.”

Mark McClain, CEO & Founder, SailPoint
Steps that Enable Business Participation

In order for this business and IT integration to succeed, participants from both sides need to come together and communicate.

Here are three recommended best practices to help you ensure that your company’s business managers are active participants in your identity management processes:

1. Build a culture of business accountability.
   Good identity governance ensures that organizations have full visibility into who has access to each critical application and system – and the risk this represents. The better managers understand the potential risks associated with access privileges, the better the company can mitigate those risks. Business managers provide valuable insights into business risk, so a good program of identity governance should regularly include review and approval of access privileges by business managers. By establishing a regular, automated process for business managers to review access, you can begin building a culture of accountability and be well on your way to ensuring controls that prevent fraud and enforce corporate policy.

2. Focus on policy alignment.
   Business managers understand the risks associated with sensitive applications based on asset value, privacy requirements, or potential for fraud or misuse, thus they are best equipped to define the control objectives needed to mitigate business risk. At the same time, the IT organization is ultimately responsible for ensuring that access configurations (who can access programs, tables, documents, etc.) conform to those business policies. Both sides must be involved in order to achieve policy alignment at the implementation level (i.e., not just captured in binders that sit on a shelf). Business-friendly tools that allow business managers to understand how policy is implemented and that highlight when policy violations are detected can help ensure that IT controls properly reflect compliance policy.

3. Make transparency a priority.
   The final step to engaging business managers is perhaps the most important one. The organization must take steps to ensure the required level of transparency into the organization’s identity data, in a way that is easily understood by business users. It’s simply not practical to expect business managers to be able to interpret cryptic access privileges as they natively occur in directories, operating systems, applications, and databases – and make any meaningful decision about these privileges. To ensure good decisions and effective oversight, business managers require business-oriented user interfaces, glossaries and help facilities that turn IT data into “business intelligence.”

“IAM should be (among other things) about clarity. How do we make clear to the business that there is intelligence on those logs, waiting to be mined, and that intelligence may make all the difference in their decisions? The best way is to deliver it, to provide that IAM intelligence is more knowledge for IT users to make IT users’ lives easier. IAM intelligence can be part of the business intelligence realm if properly analyzed and presented to the right audiences.”

Earl Perkins, Research VP, Gartner, Blog post: “Time for Intelligence and Clarity in IAM,” August 24, 2010
Identity Governance Technology Facilitates the Process

When organizations deploy the right identity management tools in accordance with the three best practices outlined above – building an accountability culture, aligning policy and providing full IT transparency – they can successfully engage business managers in a traditionally IT-centric process. Having business managers participate in identity management processes leads to more accurate compliance and security efforts and, ultimately, a better risk posture for organization.

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.

© 2013 SailPoint Technologies, Inc. All rights reserved. SailPoint, the SailPoint logo and all techniques are trademarks or registered trademarks of SailPoint Technologies, Inc. in the U.S. and/or other countries. All other products or services are trademarks of their respective companies. 0713-3920