Compliance Week
April 24, 2012

COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

Rethinking Segregation-of-Duties Systems

Jaclyn Jaeger

April 24, 2012

Nearly all companies assessed their strategies for segregating duties to improve internal controls as part of their Sarbanes-Oxley compliance effort that started a decade ago. Many haven't updated them since.

Changes to job descriptions, organizational structure, and technology can quickly render segregation-of-duties (SoD) policies outdated, yet many companies fail to periodically reassess them.


Barken

"They tend not to refresh segregation-of-duties controls often enough to reflect changes in the organization," says Lee Barken, IT practice leader at accounting and auditing firm Haskell & White. "As companies evolve and change, their internal controls and governance, risk, and compliance systems must be updated to mirror and reflect these changes."

Other companies rely too much on SoD practices for internal controls. "Segregation of duties is just one component to mitigate some of these risks," says Vasant Balasubramanian, vice president of product management at MetricStream, a GRC solutions provider. "It needs to be thought of as a comprehensive part of an overall governance, risk, and compliance program."


Balasubramanian

At smaller companies segregation of duties can be a problem due to lack of resources. The smaller the company, the more hats people must wear and the less likely that proper segregation-of-duties controls will be in place.

If enforcing certain controls is not practical because of a lack of resources—whether people or systems—then more vigilant detection of controls such as periodic reviews are necessary. That often means either monthly, quarterly, or annual reviews, depending on the control, IT experts agree.

New technology systems are cropping up that monitor SoD structures in real time and make some SoD plans unnecessary. At larger companies technology is becoming an increasingly important component to remediate control weaknesses by keeping track of where specific business processes reside within an organization and documenting who has access to those

controls at all times. The problem is that many first-generation GRC tools that companies adopted a decade ago in the wake of Sarbanes-Oxley may not necessary be up to par with today's compliance demands.


Wilhelms

One drawback with first-generation GRC tools is that some required their own set of servers and infrastructure, driving up costs, explains Dan Wilhelms, founder and president of software solutions provider ControlPanelGRC. Second-generation GRC tools reside within the ERP systems, so deploying a separate set of servers isn't necessary.

Another drawback is that business users had to go to IT to access customized reports every time they had a simple question, Wilhelms says. With second-generation GRC tools—such as those provided by ControlPanelGRC, CrossIdeas, Oracle, and others—business users can now go into these systems themselves and immediately drill down to see who has access to what transactions.

Older systems also fail to provide a holistic view. First-generation GRC technology addressed segregation-of-duties, identity, access, audit, and compliance tests in individual silos across the enterprise, explains Balasubramanian. “The evolving trend in technology has been to bring segregation of duties together under the common umbrella of governance, risk, and compliance platforms, so that organizations are able to get a complete picture of segregation of duties,” he says.

Second-generation tools also satisfy higher levels of compliance reporting requirements. New functions offered in GRC tools like ControlPanelGRC, for example, provide for “what if” modeling capabilities that allows for real-time modeling of all requested user and role changes prior to the changes being implemented. This functionality allows users to stay “clean” by identifying SoD risks and remediating or mitigating them on a continuous-control monitoring basis.

Outdated SoD System?

But how do you know when your SoD technology functions aren't at the level they need to be? Wilhelms says that companies should watch for the following five warning signs that may mandate a change to how your company currently tracks and reports SoD controls:

Wilhelms points out that external auditors increasingly are broadening their scope of inquiry into SoD controls, making it essential that processes remain up-to-date. “Where companies may have gotten away with a cursory audit of their SoD controls in the past, that's not the case anymore,” he says.

A change in auditors can also trigger the need for a review of SoD policies. For example, one company that used to produce only semi-annual reports from its core enterprise resource

planning system at the request of its old audit firm, changed auditors and the new firm now requires that the company produce quarterly SoD reports out of all its SAP applications—an eightfold increase in compliance efforts.

IT experts recommend that companies consider the cost of an automated solution versus the cost of manually preparing the enterprise for an audit.

A review doesn't mean that all companies need to go out and purchase the latest GRC system. When deciding whether to upgrade or replace a current GRC solution, first determine whether the organization's system has functionality available that isn't currently being used. "Sometimes applications have built-in features that just aren't enabled or configured," says Barken.

Keep in mind too, that the cost of purchasing a second-generation system could be recouped in savings on IT staff. "Another factor that comes into play is the IT staffing levels required to support first-generation GRC solutions," says Wilhelms. "Many require a level of resources that the organization cannot justify, particularly at a time when IT is being asked to do more with less."

Second-generation GRC solutions are easier to manage and use, reducing the amount of IT intervention required. Users can set up and generate reports themselves rather than having to place requests for IT support and then wait for the reports to be run.

Companies also should identify which controls to track and ensure that good policies and procedures are formalized and documented in the organization. Ensure that the software package the company is considering does, in fact, provide the functionality and reporting needs of the company based on the controls that you wish to track and monitor.

Regardless of which GRC application you choose, the underlying IT systems need to be configured to mirror the written policies of the company. "Just having really good policies, or just having really good IT systems, isn't enough," says Barken. "They have to complement one another."

"Technology is only a part of the overall solution," agrees Balasubramanian. Organizations must plan and develop a strong GRC and segregation-of-duties program with a long-term vision and strong management level backing, by defining clear policies, establishing processes, and having people own and adhere to them.