

Understanding Compliance Time, Needs

By: Elizabeth Millard

May 6, 2011

Processor

“Many organizations experience compliance groundhog days, meaning they find themselves living through the same compliance and audit procedures over and over again,” says Torsten George, vice president of worldwide marketing at Agiliance (www.agiliance.com).

In terms of average time spent on compliance issues, the Verizon 2010 Payment Card Industry Compliance Report gives examples related to PCI compliance, where the coping process takes about 30 days, gap analysis and remediation take 90 days, and certification takes an additional 60 days. “This illustrates that as soon as one audit/compliance project is done, organizations have to almost start immediately with the preparation for the next audit,” George says.

Sound familiar? Regulatory compliance is a never-ending process, and sometimes it feels that way. Finding ways to increase staff skills and decrease time requirements can help, however.

Time Bandits

The amount of time spent on compliance depends on which regulatory issues are involved, notes Ken Vander Wal, international vice president for ISACA (www.isaca.org), a non-profit association focused on developing knowledge and practices for information systems.

“If one considers Sarbanes-Oxley as one of those regulatory compliance issues, hundreds to thousands of hours are spent annually to comply, depending upon the size of the enterprise and its organizational structure,” he says. For example, he adds, a centralized organization with centralized controls may not require the same amount of time and effort as a decentralized enterprise where controls have to be tested at multiple points.

There’s been a tendency to decentralize IT to ensure that user needs are being met more efficiently, Vander Wal says, but this creates additional work when ensuring compliance, so centralizing may be a better option for some organizations.

He adds that Sarbanes-Oxley is one of the regulations that will require the most effort in terms of examining the compliance issues and testing them. There are other regulatory compliance laws that are more specific and therefore won’t require the same degree of effort, Vander Wal notes.

Efficiency Through Automation

According to George, compliance time is primarily spent on the following tasks: policy and governance definition and a majority of organizations still rely on manual labor, email exchanges, and basic spreadsheets to conduct IT audit and compliance projects, and this can eat into schedules, he says.

By employing IT governance, risk, and compliance tools, data centers can centralize policy and governance maintenance, applying any changes immediately throughout the organization, and build a risk-aware asset database that maps to risk models for remediation prioritization.

Developing a repeatable, defensible process is the most critical element to crafting a time-efficient strategy, notes John Connell, managing consultant at the Electronically Stored Information Group at Kroll Ontrack (www.krollontrack.com). Once a process is in place and

functional, it's important to identify data sources and elements that may benefit from a technical or automated solution, he adds.

"Many organizations have implemented archives or searchable repositories for data that are subject to regulatory scrutiny," he says. "An archiving or discovery repository solution allows you to search for responsive material and quickly locate and extract it for production.

Staffing Needs

Monitoring tools can be helpful in controlling and centralizing compliance components, but it's equally important to put a comprehensive staff training program in place, notes Rick Wilson, product manager at Sherpa Software (www.sherpasoftware.com).

"Effectively communicating the importance of the compliance effort, for example, and maintaining records retention policies can boost efficiency," he says. "Reinforcing that message on a regular basis helps involve the entire organization in the compliance monitoring process."

Traditionally, regulatory compliance issues are primarily handled either with the use of internal resources – often special hires or redirection of existing staff – or with the help of a large audit firm, according to Joe Coyle, CTO for Capgemini North America (www.capgemini.com). "In both of these cases, there are massive impacts on the business in terms of time, distraction for operational duties, and the absolute man-hour cost of compliance support," he says. "More often than not, these costs far exceed budget."

A string outsourcing partner can help, and Coyle advises firms to make sure that the vendor can work with staff efforts in an efficient manner. A partner should possess domain-specific expertise and be able to understand the enterprise's business, risk, appetite, and existing processes, he notes.