

Sarbanes-Oxley: Lessons Learned

Organizations that need to be SOX-compliant are just now realizing they need to get serious about using technology to monitor and test their internal controls.

By Therese Rutkowski

Many publicly traded companies are in their third year of dealing with the Sarbanes-Oxley Act (SOX)--the law that makes corporate executives responsible for the accuracy of their financial statements and for the internal controls that minimize errors and reduce fraud.

After going through the rigorous process of documenting and testing those controls, such as the segregation of duties and appropriate access to financial systems, many of these companies--including insurers--spent far more on the effort than they ever imagined.

A full 70% of respondents to a 2005 Ernst & Young LLP cross-industry survey on trends in internal controls indicated SOX compliance costs were more than 50% higher than originally estimated. In fact, the average cost of SOX compliance was \$4.4 million, according to a March 2005 survey by the Financial Executives International, a professional association based in Florham Park, N.J.

One primary reason for such high costs was that companies jumped into documentation and testing without first conducting a risk analysis, says Steve Ferrer, an account manager with Strategic Business Solutions Inc. (SBS), a Baton Rouge, La.-based software development firm.

"There are a lot of horror stories out there about companies spending millions of dollars producing lots of paper documentation on mundane controls and job descriptions, but no one bothered to do a risk analysis," he says. Had they started with a risk analysis, they would have identified the controls that materially affect their financial statements, and spent far less money on those "big rocks" that an auditor is going to turn over.

Business Ownership Needed

Interestingly, however, is the large number of internal control problems companies did find while they were documenting and testing them. Seventy percent of firms surveyed by Ernst & Young conducted significant remediation of IT systems and controls. And, more than one-fourth of companies larger than \$5 billion in annual revenues found and fixed more than 500 control deficiencies, according to the New York-based accounting firm.

The vast majority of internal controls that companies have in place are manual rather than IT-based, notes Paul Hamerman, an analyst with Forrester Research Inc., in IT Compliance magazine.

In addition, he notes, most companies relied on existing in-house tools, such as spreadsheets, to document their controls. And those tools aren't designed to handle the variety of content that can be involved, including text, documents and diagrams.

"Nearly all organizations that need to be compliant are just now identifying that it's critical to become serious about applying technology to the controls monitoring and testing process," says John Verver, vice president of professional services at ACL Services Ltd., a Vancouver, B.C.-based provider of business assurance analytics to financial executives, compliance professionals and auditors.

What's more, these companies are only just beginning to understand that SOX compliance is a business management responsibility--not an auditing or IT responsibility, sources say.

Ninety-one percent of global audit executives recently surveyed by ACL Services said management and business process owners should "own" the monitoring of internal controls--and 33% said they have the technology in place or are planning to implement it in the coming year.

"One of the lessons learned so far with SOX compliance is that information security is not the same as IT," according to SBS' Ferrer, during a presentation at IASA 2006. "Most people look at information security as an IT function," he tells Insurance Networking News. "But actually, it's every employee's function. There are loads of examples where printed reports that contain sensitive information go out the door-and the IT person has nothing to do with that."

A Competitive Advantage

There are also many cases of basic control violations that occur even in large organizations, he notes. For instance, "we've seen companies where five or more employees are using the same password in the same system." That means auditors would have no way to determine who actually authorizes a transaction that may affect that company's financial statements.

Access controls and segregation of duties are fundamental business practices, Ferrer notes. If large organizations are allowing several people to use the same password, then small ones are likely negligent too.

"So we're talking about a tremendous opportunity for companies to improve their business practices," he says. "This is where the benefits of SOX compliance become evident. I see these improvements rippling into investment dollars. I see them being a competitive advantage."

In addition to lax controls, in most companies, financial management and ERP transactional systems are fragmented, and closing the books each financial period is complex, costly and time-consuming, notes Forrester's Hamerman.

Kansas City Life Insurance Co. (KCLI) executives knew about this problem all too well, according to Rob Fisher, director of financial systems at the Kansas City, Mo.-based insurance company.

In 2004, with Sarbanes-Oxley looming and the U.S. Securities and Exchange Commission (SEC) threatening to shorten deadlines for filing 10-Q and 10-K financial statements, KCLI began implementing business performance management software to consolidate financial data across three subsidiaries and assist with its regulatory filings in 48 states.

"Everything was spreadsheet-based and in PC-level applications and small databases," says Fisher. "So people were spending a ton of time downloading bits of data from the mainframe, and there were a lot of unnecessary bottlenecks and data handoffs."

Now, using a Web-based system from Hyperion Solutions Corp., Santa Clara, Calif., KCLI has a single data source, improved data quality, drill-down capabilities for data analysis, detailed audit logs, and streamlined financial and regulatory reporting.

"The SEC actually backed down from its shortened deadlines, but our CEO didn't," notes Fisher. "So we always file five days before the SEC requirement on 10-Qs and a full 15 days before required on 10-Ks." In addition, he notes, the company uses the system to create both GAAP statements as well as its state regulatory financial statements.

Quick Fixes

Similar to using technology to streamline financial reporting, insurance companies are beginning to understand the possibilities of using it for "continuous auditing," which includes detecting questionable transactions as they occur, as well as preventing errors or fraud by placing proper controls in ERP and financial accounting systems.

"The whole benefit of continuous auditing is: You know on a very timely basis when problems occur," says ACL Services' Verver. "So if a company's internal controls aren't working properly to prevent

duplicate payment to a vendor or payment of a fraudulent claim, for example, the company finds out quickly," he says.

Next on the agenda for SOX compliance: IT controls in the context of financial reporting. "Somebody has to sign off that this financial report is accurate," says SBS' Ferrer. "So if the company has software in place to collect and track and report information that winds up affecting the balance sheet, the company has to be able to prove that its software code is reliable."

Technology for Internal Controls

Stage 1: Informal: Ubiquitous desktop tools (Microsoft Office) and paper documents

Stage 2: Documented: Desktop tools, paper, content, or document management systems

Stage 3: Standardized: Purpose-built SOX compliance management software or in-house developed internal controls application using content and collaboration platforms

Stage 4: Managed: SOX compliance management software, controls analysis dashboards, and monitoring tools

Stage 5: Optimized: SOX compliance management software, dashboards and monitoring tools, application access control tools, and business process rules enforcement