



Sarbox: Year 2

The second time around promises more headaches, but some best practices are emerging.
[Bob Violino](#), CFO IT
September 15, 2005

First, the good news: Most companies have endured and survived their initial foray into Sarbanes-Oxley. And while it often proved a costly and occasionally frenzied experience, it has, many companies say, improved the controls that govern corporate operations. On the other side of the ledger, unfortunately, it appears that year two won't be the autopilot repeat that companies had hoped for. The first year taught many lessons that have yet to be embedded in most compliance programs, making the second year potentially more labor-intensive than the first.

One of the biggest lessons learned concerns the role that IT plays in supporting financial processes, which caught many companies off-guard. But some best practices are emerging, from both a technology and a management perspective, that can help companies address the compliance burden in year two and beyond without massive expense and perpetual panic.

Create a Formal Group to Oversee Compliance

In the first year, companies spent heavily on all manner of consultants and outside help to clear the Sarbox hurdle. Going forward, companies should establish a multidisciplinary governance council or steering committee to set the scope of compliance and resolve issues quickly. Such a council "is essential to making [compliance] go smoothly in year two," says John Hagerty, vice president and analyst at AMR Research Inc. in Boston. It puts IT, finance, and other business management on the same page and helps provide badly needed guidance. "IT people overprepared in 2004. They had little or no guidance and felt they did a lot of stuff they didn't need to do," says Hagerty. (Many would say the same about auditors, as we reported in the last issue. See "[Sarbox Surprises](#)" and "[Survey Says](#)," Summer 2005.)

The council or committee should ideally include the CFO or other high-level finance executive, someone from the internal audit department, the CIO or other IT executive, and a representative from business operations. The group should be designed to make rapid decisions so compliance issues don't linger for months. Hagerty says AMR recently ran a forum on Sarbox, and the half dozen or so companies that had implemented such a council reported that it was a key to their success in compliance efforts.

A formal Sarbox group helps foster cooperation between disciplines. Mark Lutchen, partner and practice leader for IT effectiveness and former CIO at PricewaterhouseCoopers, says that if CIOs haven't done so already, they should reach out to finance to obtain the skills they need to implement fundamental management disciplines — such as developing an IT management chart of accounts to collect IT spend and performance information. And, he says, CFOs should demand that CIOs embed those skills in their IT organizations.

At First Commonwealth Financial Corp. in Indiana, Pennsylvania, John M. Heise, vice president and operations audit manager, says that his company's Sarbanes-Oxley committee aims to foster a sense of accountability for compliance, and that requires a mix of skills. "Finance understands what controls need to be put in place," he says, "and IT offers advice on how to manage data resources."

Review Technology Controls from Year One to Eliminate Extra Work

Companies need to look closely at the IT controls they put in place during the first year of Sarbox to make sure they are actually necessary. "The first lesson we learned last year was that we overreacted and had too many key controls," says Mike Harreld, executive vice president of Southern Co. and CFO of Southern Co. Transmission, and head of the companies' Sarbox efforts. "If anything remotely looked like a control last year, we captured it. We stepped back when we were finished and said, 'We can be a lot more efficient and think about what the key controls are.' "

In year two, the Atlanta-based electric utility, with the help of a document-management application, is identifying key systems and ensuring that it has adequate controls in place where needed. And it is making sure those controls are tested — both internally and with its external auditor, Deloitte — once they are in place.

Harreld has assembled a team that is responsible for Sarbox compliance and has divided responsibilities into business cycles, such as financial reporting, and shared services, such as IT. Every key control throughout the organization has an "owner" and that owner is responsible for Sarbox compliance. "Our belief is that the way to wrestle this hog to the ground is to ingrain Sarbanes-Oxley into how we do business," Harreld says. "We always had a good control environment; we're just trying to make it more obvious and important."

Clarify IT's Role

As we noted in the last issue, there is often no clear delineation between what constitutes financial versus IT controls. Even if auditors and regulatory bodies continue to clarify the rules so as to keep an internal-controls audit from devolving into an assessment of every line of computer code a company relies on, there is no doubt that strong compliance will involve the IT department on many levels.

"This is an IT governance issue: how to align resources based on the priorities of the firm," says AMR's Hagerty. He recommends that companies use the risk-based approach outlined by the Securities and Exchange Commission in May of this year. "Figure out places where you have [the most] risk and focus your efforts there," he says.

Experts say organizations must also think more broadly than they have in the past when it comes to reviewing IT controls. "Everyone thinks the 'IT controls' job related to Sarbanes-Oxley is [complete] because they did what they had to do this past year concerning the tactical controls focused on the flow of financial information," says PricewaterhouseCoopers' Lutchen. But this tactical focus is preventing companies from seeing bigger, more strategic issues, such as the ability to address overall IT management and control of huge IT budgets. He argues that if Sarbox is, in a sense, ultimately about creating a "culture of accountability," then that culture must extend to IT, since IT failures can often be felt on the bottom line. "If you look back on many failed 'megasytem' implementations in the past and other failed critical IT initiatives in many companies, you will see that it is possible to correlate a [drop] in the stock price to a publicly announced failure," says Lutchen. Some companies may feel that it's a big leap from satisfying Sarbox requirements to embracing

best practices in IT governance, but for those looking to make year two as effective as possible, this may be a worthy goal.

Automate Controls and Compliance

Another lesson learned was that internal controls and Sarbox compliance are labor-intensive. But many vendors have introduced products — such as internal-control-management applications, process-management and workflow software, and business-performance-management systems — that help automate controls and manage the internal control and compliance process on an ongoing basis. And they say such products will ultimately reduce the costs of Sarbox compliance.

Lee Dittmar, a principal with Deloitte Consulting LLP who leads the enterprise governance consulting practice and also serves as co-leader of Deloitte's Sarbanes-Oxley practice, says automating controls has a number of benefits: "You can reduce risk, have better control, and reduce the cost of compliance."

AMR says key technologies that automate the testing of internal controls can reduce the cost of Sarbox compliance by more than 25 percent. But the outlay for such technology isn't necessarily cheap. To automate compliance, the firm says, companies should expect to spend between \$100,000 and \$1 million on technology.

Despite the potential benefits of automation, many companies have yet to invest in such products. A survey conducted and released in June by the Center for Continuous Auditing polled 247 senior audit professionals at companies with more than \$1 billion in annual revenue. The results showed that only 40 percent already automate — or plan to automate — the testing of their controls this year.

Telus Communications Inc. in Vancouver, British Columbia, which does not have to begin meeting Sarbox requirements until December 2006, is getting a jump on it now, in part by investing in specialized software. It uses a product from ACL Services Ltd. for two key business processes: its overall purchase-to-payment cycle and its purchasing-card program. The software helps the finance department monitor all corporate purchasing-card and accounts-payable transactions on a daily basis, allowing Telus to identify duplicate payments and other errors and boost its internal control process, says Gary Silsbe, director of operational excellence.

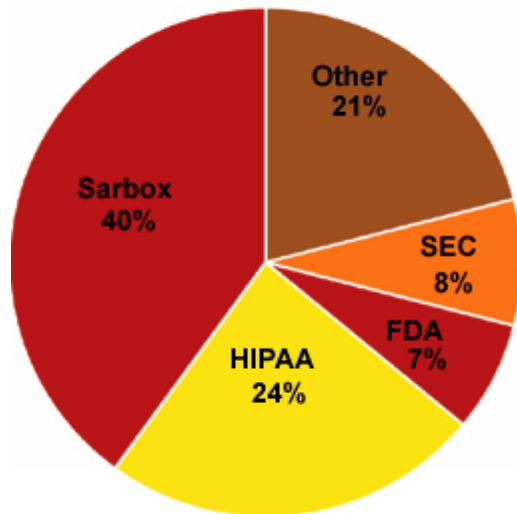
First Commonwealth, which used a manual process to gather risk data in its first year of Sarbox work, now uses a software product called Risk Navigator from Paisley Consulting. The software gathers data about corporate risk at the business-unit level; creates reports by business unit, process flow, and organizational objective; and identifies controls for each risk. Heise says First Commonwealth can gather far-more-detailed data using the software than it could using manual methods such as questionnaires, making compliance much easier.

Some companies manage to harness old and new technologies not generally associated with Sarbox requirements. At Viper Motorcycle Co., a Minneapolis-based manufacturer of luxury motorcycles, CFO Garry Lowenthal expects the company's SAP Business One application to aid in its compliance with Section 404 by providing detailed information on costs, revenue, and other financial data. He also believes that radio frequency identification technology may provide data relevant to Viper's business processes and internal controls.

Technology vendors are beating the Sarbox drum more loudly than ever, and almost every piece of software can be said to affect controls in some way, making it difficult to identify the most useful products. But experts say that should not deter companies from searching for automated solutions.

Not Just Sarbox

A survey of more than 255 companies finds them planning to spend an aggregate \$15.5 billion on the following compliance programs.



Source: AMR Research

© CFO Publishing Corporation 2005. All rights reserved.