



Small Public Companies Must Get SOX Religion

May 14, 2007

By Jennifer Zaino

Compliance won't be an option, and the longer you wait to get started, the harder and more costly it will be.

There's no more time to waste. Compliance with Sarbanes Oxley Section 404 is not going to become optional for public companies with market values under-\$700 million, given the Senate's recent move to set aside an amendment aimed at doing just that.

By June, the SEC is supposed to issue new guidance on tailoring internal controls over financial reporting, and the PCAOB (Public Company Accounting Oversight Board) is to issue a simplified standard for outside audits of companies' internal controls.

Assuming they meet those deadlines — and they expect to — smaller companies whose fiscal year ends in December have until next March to file management reports on their internal controls, and until March of 2009 to complete outside audits of these controls.

But even if there's a hold-up at the SEC or the PCAOB, it's time for smaller companies to get with the program, says Sumit Pal, Executive Vice President of WithumSmith+Brown Global Assurance, a division of WithumSmith+Brown Certified Public Accountants and Consultants.

"Giving a further extension really doesn't help the business community as such," says Pal. "Putting these controls in place is good business practice. There are many companies who don't have to comply with Sarbox, privately held or not profit companies, who are implementing Sarbox-like controls in order to be able to improve their business practices."

Sumit says that the accelerated filers who were the first to go through Sarbox compliance efforts have realized benefits in improving business processes, which continually morph and without controls in place rarely see their documentation updated.

"That will be an even stickier problem for small businesses because they don't allocate resources for these activities," he says.

Countless compliance challenges

Smaller companies have both advantages and disadvantages in preparing for Sarbox. For instance, they are likely to have fewer lines of business, fewer products, and less complex transaction processing systems, but they also have more limited resources in terms of smaller IT teams (which leads to gaps in process and controls documentation), limited personnel who then have to wear multiple hats (making segregation of duties a challenge), and lots of manual integration between different sets of applications.

A comparative lack of full-bore network security solutions and lack of IT awareness across the organization, from the CEO on down, also adds to the challenge. Smaller companies also are likely to wind up spending a greater percentage of annual revenue on compliance costs.

“That’s all the more reason for them to have started work earlier and spread costs over multiple years,” Pal says.

Pal’s perception is that most non-accelerated filers haven’t done any work in the area of Sarbox compliance, but if they start working on this now, they’ll still be in a better position than those who continue to delay. The first step is to form a cross-functional SOX compliance team that includes key people from each process, including IT, an internal audit function, and independent auditor, to identify resources, and get down to complete planning.

WithumSmith+Brown Global Assurance, whose business focuses primarily on small and mid-size companies, takes a five-phased approach to getting started on compliance efforts, beginning with scoping and project planning that involves identifying participants and looking at processes from a risk-rated point of view, so that organizations put attention on the IT systems that are connected with financial reporting. Following that, businesses must assess internal controls, evaluate them at the process, transaction and application levels, test their effectiveness, and remediate as necessary. That includes establishing a sustainable remediation process.

“Sarbox is not a one-time event, it’s a journey,” Pal says. “You have to make sure you build all this so you can sustain it over time.”

It’s too cost-prohibitive to treat compliance as an annual “reinvent the wheel” project rather than as a complete, sustainable and ongoing process.

Four “R’s” infuse the methodology. These are:

- Take a **risk-rated** approach, so that you look at key business processes in key locations, to streamline efforts and reduce the overall time and costs of the compliance process.

“With large accelerated filers, year one some companies tested well over 1000 controls, and in years 2 and 3 they brought that down to 250 or 300 controls,” Pal says. “SMBs have limited resources, so there’s all the more to take this approach to make the most efficient use of resource to complete this task.”

- Check for **redundancy**, and getting rid of duplicate key controls in favor of smart controls, choosing automated over manual to reduce testing.
- **Replace** higher frequency controls with lower frequency ones, to reduce the scope of work significantly, and
- Become **reliant** on preventative vs. detective controls.

A challenge for smaller companies is they have shorter timeframes in which to complete different aspects of compliance projects. But they can also take some very simple steps that take hardly any toll on resources and cost nothing but a willingness to move forward on improving access control and security.

Simple things like requiring passwords to have numeric and special characters, and to change them every couple of months, go a long way towards making it harder to crack into systems, and smaller companies can also do a better job segregating duties so that system administrators aren’t in end-to-end control of processes like user provisioning.

“All of these regulatory things, you will find they all make good business sense,” says Pal. “So they will help overall with all business processes with customers, suppliers or even employees.”