Box Their SOXes Off

Being proactive with
SAS 70 Type II audits
helps both parties in a
vendor relationship.

JOHN BOSTICK, dbaDIRECT

Data is a precious resource for any large organization. The larger the organization, the more likely it will rely to some degree on third-party vendors and partners to help it manage and monitor its mission-critical data. In the wake of new regulations for public companies, such as Section 404 of SOX (Sarbanes-Oxley Act of 2002), the folks who run IT departments for Fortune 1000 companies have an ever-increasing need to know that when it comes to the 24/7/365 monitoring of their critical data transactions, they have business partners with well-planned and well-documented procedures.

In response to a growing need to validate third-party controls and procedures, some companies are insisting that certain vendors undergo SAS (Statement on Auditing Standards) 70 Type II audits. These audits refer to an AICPA (American Institute of Certified Public Accountants) standard that sets forth the practice for evaluating the performance of outside service organizations. (A Type I audit describes the business's controls, noting if they are

suitably designed and in place; a Type II audit tests those controls and reports if they are working adequately.)

SAS 70 Type II audits have become increasingly important for major corporations because management has to assess the effectiveness of not only the company's internal controls over financial reporting, but also the critical outsourced services that might materially impact those controls—such as third-party monitoring and management of an organization's databases.

As a business partner or service provider to large corporations, you provide a valuable service to current and future clients by taking on an SAS 70 Type II audit yourself. You may be used to people coming in to look under every tile in your facility before signing on the dotted line, even if this is generally regarded as a hassle from both perspectives. Because of SOX, however, this checking is going to become more prevalent. Auditors from anyone and everyone you would consider doing business with are going to start showing up on your doorstep.

Completing an SAS 70 Type II audit says a company has processes that are accurate and robust and provides official federal paperwork to back up these claims. Simply being able to say you have completed such an audit may smooth the rest of the process a potential client company will put you through—and while today it could be a competitive advantage, it will soon be a competitive necessity.

HOW TO GO ABOUT IT (A FIRST-HAND ACCOUNT)

When you decide on an SAS 70 Type II audit, find a CPA firm with a robust audit practice built around SOX. A good firm will come in, tell you about what you are going to go through, and show you the roadmap for a Type II audit.

The first thing you'll do is create a "war room," where the documenting of your processes will be available in a central location and in a particular way. You will probably have to test your processes and continue to think them through. Traditionally, you may not have done a lot in the way of "buddy-checking," but the Type II preparation will force you to knuckle down on each other's work. Buddy-checking sometimes means stepping on delicate egos. Cerebral repositories won't work as a final product. It is important to make sure everything is organized and documented.

In our case, I had our chief technology officer, who is the top IT person at the company, assign his head of security and networking to take on the project and really get into the bowels of the audit process. We also had the operations leaders under him produce documentation on the event-processing systems.

In areas where we were light on documentation, we needed some all-nighters to develop the required robustness for the auditors. We had a guideline of what depth levels to reach. Those levels are significant to most companies, whether large or small, but most companies today don't have the resources internally to redocument while also performing their day-to-day activities.

At least, we didn't. So in preparing for the challenge, we had eight to 10 employees, not including those who

were interviewed, working with the auditors to demonstrate the documentation and the processes. With the exception of three or four employees, most were involved for a half-day or so. The other employees, especially those who deal with security and connectivity, were involved for a couple of weeks and captive for most of that time.

Again, however, I would say that by being proactive with the initial SAS 70 Type II and the renewals that followed, we have really helped mature our company from an operations standpoint. Frankly, as a CEO, given that a company's processes and controls are very difficult to measure on a balance sheet, knowing that your company has a certain level of preparedness and operational excellence in these areas is very comforting.

THE BENEFITS

The most obvious benefit for our company was that we learned about processes and controls cross-functionally within our organization. Our first SAS 70 Type II audit required us first to take a long look at what controls we had and where we might have some holes. Sometimes the C-level leadership believes controls are in place, but the reality is that they aren't, or they're not documented properly. The SAS 70 Type II audit showed where we could improve on the processes and controls we had, and it forced us to increase our cycle time for better processes moving forward.

I would recommend that everyone doing business with large companies get these audits. If the client does ask for it, and you say no, then you may have just disqualified yourself as a business partner. ☐

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

JOHN BOSTICK is president and CEO of dbaDIRECT, which provides data infrastructure management services to Fortune 1000 and Private 500 firms, including large utilities such as Cynergy and Kerr McGee.

© 2006 ACM 1542-7730/06/0900 \$5.00