

COMPLIANCE WEEK

II Getting Through A SAS 70 Audit: First-Hand Experience

By Matt Kelly — August 30, 2005

In the wake of Section 404 of Sarbanes-Oxley, Compliance Week has written extensively about SAS 70 Type II audits. (see coverage below, right.) The audits have become increasingly important for some public companies; management has to assess the effectiveness of the company's internal control over financial reporting, and critical outsourced services that might materially impact those controls—like payroll, for example—are included. As a result, many companies are insisting that certain vendors undergo "SAS 70 Type IIs." The audits refer to an AICPA standard that sets forth the practice for evaluating the performance of outside service organizations (a "Type I" audit describes the business' controls, noting if they are suitably designed and in place; a "Type II" audit tests those controls and reports if they are working adequately). This week we speak with the CEO of a database company that has recently undergone such an audit.

You began SAS 70 Level II audits annually in 2004. Why?

Well, as a seven-year-old company working as a service provider for Fortune 1500 shops, and providing a slice of their services within data infrastructure management, we're used to working with large financial institutions. We've had people look under every tile in our facility and do background checks, including deep personnel checks on our people. So we'd been in this environment for a while when one of our valued clients called us and said, "PwC is going to show up on your doorstep and do a full audit."

We knew that meant we'd have all our customers bring their auditors and show up at our doorstep. That was certainly OK with us, but we wondered about this SAS 70 Level II audit—would that be sufficient? A lot of this was new; we had a lot of phone calls and emails and so forth, and everyone decided it was acceptable. So we went out to an audit firm to do this.

So the initial, "We gotta get this done" was instigated by one client. And, quite frankly, thank God we acted aggressively, because everyone started asking for it.

How did you get started?

First, we're a very process-oriented culture; we're in the 'event processing' business and happen to be doing databases. Because of that, and because these audits constantly happen from customers of ours, we were used to outsiders showing up and asking a whole bunch of questions that were very personal about our business.

When we decided we needed an audit, I contacted my CPA firm. They have a robust audit practice around SOX, and they directed us to a separate firm that specializes in this. That firm came in, told us what they were going to go through, showed us the roadmap for a Level II audit, and we started getting prepared for it.

What did you do to prepare?

The documenting of processes we had already done. We didn't have them documented in a central location available to outsiders in a way they wanted, so we had to create a "war room" if you will, to collect them there.

Secondly, we had to test our processes and continue to think them through. Because of the size of the company, and the number of veteran professionals we have in the company, we traditionally hadn't done a lot of "buddy-checking" where we

BIO



Bostick

John Bostick is president and CEO of dbaDIRECT, which provides data infrastructure management services

to companies like Best Buy, Procter & Gamble, Warner Brothers, and others.

Prior to dbaDIRECT, Bostick was CEO of LÜCRUM, a Cincinnati-based strategic consultancy that he founded in 1994.

Previously, Bostick was general manager for Pomeroy Computer Resources, an IT solutions provider that went public in April 1992. Before joining Pomeroy, Bostick spent 10 years at IBM in Chicago and Cincinnati.

COMPANY BASICS

Company	dbaDirect
HQ	Cincinnati, OH
Employees	70
Industry	IT Services
'04 Rev.	Private

So the Level II preparation got us to knuckle down on each other's work ... and when you get down to buddy-checking, you had to have a delicate ego and you had to make sure it was all organized so you're not a cerebral repository but also have things down well on paper.

Your company has only 70 employees. Who was involved in the audit?

Our chief technology officer, who is the top IT person at the firm, assigned 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.

Where we had light documentation, we did some all-nighters to continue to develop the documentation robustly enough for the auditors in those areas. We had pretty much a guideline of what depth levels to reach, and those levels are significant to most firms whether large or small. I think most firms today don't have the resources internally to re-document things and do your daily job at hand.

You don't have an internal audit department, we presume.

We do not. So in preparing for the challenge, we probably had eight to 10 employees, not including those who were interviewed, involved with the auditors to show 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 security and connectivity, were involved for a couple of weeks and captive for most of their days.

But again, I'd say that the proactive steps that we took in the initial audit in 2004, and then the renewal in 2005, have really helped mature our company from an operations standpoint. And frankly, as a CEO, I can better sleep at night without that particular headache of how well our processes are documented and how accurate and truly robust they are.

Did you find any room for improvement when you examined your processes?



The obvious benefit was that we learned about our controls and processes cross-functionally. Before the first SAS 70 audit was done, it required us to take a long look at what controls we had and where we might have had some holes. As I said earlier, sometimes the C-level leadership believes we have controls in place but the reality is they really aren't, or they're not documented as much as they should be. And they also showed where we could improve on controls and processes we had, and it forced us to increase our cycle time for better processes.

How much did the audit cost?

It roughly cost \$20,000. You hear about big companies spending millions of dollars for all of Sarbanes, which has a tremendous amount of business-transaction analysis. We didn't have that.

How long did it take to conduct these audits?

The first one took, including preparation, eight weeks. On the one we just finished, people were on site for three weeks. We spent time up front getting ready, but the processes weren't months-long. They were weeks-long.

What's the return on investment here? It must be a useful thing to give customers these audit reports.

Absolutely. I also think that this kind of audit is tremendously helpful for management team operational excellence, knowing your company has a certain level of preparedness. That's a very difficult thing to measure on a balance sheet.

I'd say that everyone should get these audits. When the client does ask for it, if you say "no," then you've just disqualified yourself.

Thanks, John.

