

Assuring security

Frequently asked questions about the SAS 70 audit **Interviewed by Matt McClellan**

When companies receive a request for a SAS 70 audit, their first question is often, “What is this, and why am I being asked for it?”

A SAS 70 audit (statement of auditing standards no. 70) is one function of auditing that assesses the internal controls of a service organization. When a service organization has access to important information, such as employee banking information, social security numbers, etc., it needs to be determined that the manner in which this information is stored and shared is safe and secure.

“Imagine you are a big company and another company handles your payroll,” says Robert B. Brenis, CGEIT, CISA, MCP, PMP, a principal with Skoda Minotti Technology Services. “The payroll company has your employee names, Social Security numbers and access to your money, so it would need a SAS 70 because they are a service provider for your organization. A SAS 70 audit will ensure that the information shared is secure.”

Smart Business learned more from Brenis about SAS 70 audits.

How does a SAS 70 audit benefit a service company?

Being compliant opens doors for more work. A lot of companies are getting inquiries from prospective clients asking, ‘Are you SAS 70 compliant?’ If they say no, that’s the end of the conversation. It’s a great marketing tool for a lot of organizations, and it helps you identify areas where you have weak controls.

What differentiates SAS 70 from other audits?

A financial audit is the same procedure over and over again, it stays the same, every time. A SAS 70 is not a financial audit, so there is no boilerplate procedure; each audit is different.

If you have access to client data, such as employee or customer information, or financial transaction information, or if you are controlling any of your customers’ information, odds are you are going to need a SAS 70.

An example would be any company that houses other companies’ servers. They need a SAS 70 because they are controlling the backbone of your company.

Because they are different every time, does that make SAS 70 audits more difficult to prepare for than regular financial audits?

No, that’s one area in which your accounting firm can help you. They sit down with



Robert B. Brenis, CGEIT, CISA, MCP, PMP
Principal
Skoda Minotti Technology Services

clients and prospective clients and help them figure out what it is that they need to be concerned about. They then help them identify what controls need to be tested.

What about the companies whose data is in question, do they need to worry?

No, and the reason they are asking for the SAS 70 audit of their service providers is that they want to prove that data is secure. The SAS 70 audit proves that data is under control and everything is good. It gives them a level of assurance. Going back to the original example, the payroll company having a SAS 70 audit tells you that the dollars and social security numbers you have trusted them with are safe, that everything is under control.

Are there different types of SAS 70 audits?

There are two different types. Type I is simply a report on controls placed in operation. All it really says is the service company says controls are in place, and the auditor has looked and agrees with them that controls are in place, but no testing has been done.

A perfect example is if someone says they have a lock on their server room door. For a SAS 70 Type I audit, the auditor would go over, take a look and say, ‘Yep, there’s a lock on that door.’ The auditor doesn’t try to open

the door or come back unescorted to see if the door is open. The auditor just makes sure that there is a lock on the door.

How does that differ from a Type II?

Type I is as of today. A Type II audit is done over a period of time. The auditor will come in and test to see if things are in place and have been in place during that period of time. So, the auditor would try to open the door and would go back unescorted to see if that door was open.

Or, to look at another example, say you have visitor logs. The auditor will go through them and see if the people signing in or out have appropriate badge ID numbers. If you have visitor badge numbers one through five and somebody signs in with badge three at 9 a.m., then somebody else signs in with badge three at 9:15 a.m., there’s a problem.

How would a company determine which kind of audit they should have?

A Type I audit is enough to be SAS 70 compliant. Many customers often request a Type II audit from their service provider, though, to show greater evidence that controls are in place. A Type I is done when a company wants a SAS 70 audit because their customers are asking for one. Once the proper policies and procedures are put in place, a Type I audit is conducted.

Six months later, they have built up a history of following those policies and procedures. Then you do a Type II.

How often should a SAS 70 audit be done?

Minimally, they should be done once per year. It’s more common to have them done once every six months.

Are there any predefined controls that are required to be in a SAS 70?

No, as each SAS 70 is different. First, the auditor identifies the controls in place, and then identifies the tests that need to be done to prove those controls. A payroll company will be concerned about dollars and employees and all the data they have while a company that houses servers will be worried about people tampering with the servers or coming in off-hours — completely different things. <<

ROBERT B. BRENIS, CGEIT, CISA, MCP, PMP, is a principal with Skoda Minotti Technology Services. Reach him at (440) 449-6800 or rbrenis@skodaminotti.com.

Insights Accounting & Consulting is brought to you by Skoda Minotti