TECH INSIGHTS

weaver IT advisory services

SMALL PAIN, BIG GAIN

How third-party service providers and their customers benefit from the SSAE 16 transition

It's no wonder executives seemed less than enthusiastic about the new auditing standards and controls for service organizations instituted by the AICPA. In fact, most companies had already suffered through a decade of new internal controls and financial reporting requirements that managed to increase costs while offering nominal benefits.

This time, the reports that are part of the AICPA's new Service Organization Controls (SOC) reporting suite actually benefit outsourced service providers and their customers by providing additional transparency at a time when companies are looking to outsource rudimentary tasks or move data and applications to the cloud.

Companies previously felt like they had no option but to report under Statement on Auditing Standards 70 (SAS 70), even though it was often misused and did little to ensure the performance of service providers. However, the new SOC reporting options are better focused on the current needs of outsourced service providers and their customers.

Brian Thomas, advisory services partner, answers a few key questions about the benefits of the SOC reporting options for service organizations and their clients.

Why did the AICPA change the reporting options for service organizations?

Some of it was housekeeping. The AICPA is updating certain U.S. audit standards to harmonize them with international standards, resulting in the replacement of SAS 70 with SSAE 16 (also called SOC 1). Secondly, the SAS 70 and SysTrust reports weren't meeting the broader needs of outsourced service providers or their customers. SAS 70 (now SSAE 16 or SOC 1) addresses only internal controls over financial reporting, and SysTrust (now SOC 3) did not provide enough detail to customers — especially at a time when companies are increasingly contracting with Software as a Service (SaaS) and cloud providers, which is raising a host of different concerns. So, while doing its housekeeping, the AICPA addressed this gap with a new option called SOC 2.

What are the new SOC reporting options?

The new SOC reporting suite features three reports called SOC 1, 2 and 3. Best of all, the reporting formats are customizable, so customers can get information tailored toward their specific needs.

- ***SOC 1*** — This report is intended to fulfill the requirements of SAS 70 (now SSAE 16). It has been updated to match international standards and is focused on internal controls over financial reporting relevant to the service provider's customers.

CUSTOMERS CAN SIMPLY REVIEW THE REPORTS AND MAY BE ABLE TO AVOID THE COST OF AUDITING THE SERVICE PROVIDER THEMSELVES.

- ***SOC 2*** — This report is valuable because it addresses a service provider's controls as they relate to the security, availability, processing integrity, confidentiality and privacy of a system. All of these are important aspects of the non-financial performance of service providers. SOC 2 is more relevant for IT-based services and contains detailed results similar to a SOC 1.
- ***SOC 3*** (also SysTrust) — Its scope is the same as SOC 2; however, less information is provided about the results. A seal is issued that the service provider can post on its website. The accompanying report confirms only that a SOC 3 engagement was performed and the overall result without any details.

How do these new reports benefit service providers and their customers?

Alleviating the concerns of prospects and customers is one of the primary benefits for service providers. The reports may also reduce the need to accommodate auditors from client organizations because providers have to meet a fairly high audit threshold, instead of self-accrediting and validating their performance using a universal set of standards.

Customers can simply review the reports and may be able to avoid the cost of auditing the service provider themselves. Also, the new reports engender trust by providing greater transparency into a service provider's day-to-day operations, along with the assurance that a qualified auditor has examined its internal controls, compliance and performance.

How can service providers determine the best reporting format for each customer?

Certainly, the service providers should understand the needs and concerns of each customer and tailor the reports appropriately. They can also confer with the client's auditor to determine the exact scope of their reporting concerns. The format to choose really comes down to the information and transactions handled by the outsourcer and the concerns of its customers. For example, a client may be concerned about data confidentiality and privacy if they use any SaaS applications to manage customers and prospects, but they'll have different concerns if they are hosting their core financial application with a service provider. It makes sense for auditors from both organizations to confer when the parties are ready to negotiate the contract and reporting requirements.

How can customers and prospects use the reports to mitigate risk and select a best-in-class service provider?

Customers must read the reports and should not assume that everything's okay just because an auditor has ventured onto the service provider's premises. Customers need to understand the scope of the SOC report and its relevance to the services they purchase from the service provider. Look for trends over time with the issues that are identified in their reports and request additional information from the service provider, as necessary. Although service providers may not share the SOC reports with prospective customers, procurement specialists can develop screening criteria and RFP questions for service providers regarding the scope and issues identified in the report. Finally, don't let the pain of implementing the new standards keep you from enjoying the gains. Thanks to the new SOC reports, customers can finally have the assurances they need to outsource with confidence.

CONTACT US

BRIAN THOMAS, CISA, CISSP
Partner, IT Advisory Services

Brian.Thomas@weaverllp.com
713.800.1050

Weaver has offices throughout Texas.
More at weaverllp.com