What you need to know about the new SSAE-16 standard for technology and banking

It is hard to keep up, particularly when it pertains to technology and the never-ending and changing scenario of compliance. What has caught me by surprise recently is how often I encounter financial institution executives and IT managers that are not aware of a very significant AICPA change last year regarding technology reviews.

If you have relied on a vendor to provide a service in an outsourced or distributed manner, the SAS-70 report has played an important role. This report was the Statement of Auditing Standards # 70 for Service Organization's, and it was an AICPA (American Institute of Certified Public Accountants) requirement. The report was used as an auditing template for independent auditors to review the financial and internal controls of the service organization. It was a useful report, albeit difficult to read, and it has been in place for quite a while. Financial institutions that employed the above-mentioned technology are required to conduct an annual review of vendor relationships and document the review for the board of directors.

Times have changed and there is a new report in town. The SAS-70 has been replaced with the SSAE-16, also known as the Statement of Standards for Attestation Engagements #16. More importantly, the SSAE-16 became effective on 6-15-11. The AICPA has provided a website to help the industry with understanding the changes and the benefits.

What is important to note is that the previous SAS-70 report focused on the financial statement reliability aspect of the vendor being reviewed, in addition to a review of some control objectives. With technology expanding and becoming more complex, not to mention the growing challenges associated with risk management, the AICPA decided to update the auditing template. Understanding the changes is crucial to your organization in technology planning, compliance, and even your hiring practices. It is imperative that your management team and technology staff have a firm grasp on the new standard. Below are three excerpts from the AICPA that describe each type of report covered.

SOC 1 Report - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

These reports, prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, are specifically intended to meet the needs of the of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user' auditors), in evaluating the effect of the controls at the service organization on the user entities' financial statements. Use of these reports is restricted to the management of the service organization, user entities, and user auditors.

SOC 2 Report - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

These reports are intended to meet the needs of a broad range of users that need information and assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems the service

organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

Use of these reports is generally restricted.

Another document, Understanding How Users of Service Organizations Would Make Use of a SOC 2 Report, provides guidance to users entities on the factors they should consider when evaluating the relationship of the controls being reported on in the SOC 2 report to their environment. Examples of outsourced services include cloud computing, managed security, customer support etc.

SOC 3 Report - Trust Services Report for Service Organizations

These reports are designed to meet the needs of users who need assurance about the controls at a service organization that affect the security, availability, and processing integrity of the systems used by a service organization to process users' information, and the confidentiality, or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 reports can be freely distributed or posted on a website as a SysTrust for Service Organizations seal.

Industry regulators and the AICPA concur that the use of technology in almost every aspect of an institution is growing exponentially. Attached to this growth is risk, no matter how you look at it, and the challenge of containing, managing, and mitigating the increasing threat profile.

The SSAE-16 Statement of Controls template is a move in the right direction in regard to updating your understanding of the need to adapt to a constantly changing technological risk environment.

Change is good, particularly when you consider the benefits of new technology, but it is not without risks. It is important to understand both before you have to ask yourself: how did that happen?

The Wombat!

About the Author

Dan Fisher is president and CEO of The Copper River Group, a consulting firm headquartered in Fargo, N. D., that focuses on technology and payment systems research and consulting for community financial institutions. For nearly 30 years, Fisher has worked in the financial industry using technology to improve the bottom line. He was CIO of Community First Bankshares (now part of Bank of the West), has served as a director of the Federal Reserve Board of Minneapolis, the chairman of the American Bankers Association Payment Systems Committee, and was a member of the Independent Community Bankers of America Payments Committee. Fisher has written numerous articles on banking technology and the payments system. He has authored or co-authored six books and recently published a book titled, "Capturing Your Customer! The New Technology of Remote Deposit." You can contact Fisher at dan@copperrivergroup.com.

P.S. To understand Dan's nickname, check out "About the Wombat" on his website, www.copperrivergroup.com