AuditOne LLC

Risk-Managed Internal Audit and Credit Review Expertise

NEWS

AuditOne Advisory – SOC 1 Changes with the new SSAE 18 Standard

AuditOne, LLC June 2, 2017

AuditOne Advisory

From Bud Genovese, Chairman

Your financial institution should be receiving from your major service provider's annual SOC 1 controls reports (formerly called "SAS 70"). These reports are based on reviews called SOC – Service Organization Controls. The AICPA has just modified the SSAE 16 attestation standard for performing a SOC 1 review. Effective May 1, 2017, the SSAE 16 has been replaced by SSAE 18. The major changes that the SSAE 18 present are reviewed in this advisory written by Robert Kluba, our Technology Practice Co-Director. Please forward this to appropriate personnel in your firm, such as IT management or the person responsible for vendor management compliance. We hope you enjoy this technical update, thank you! – Bud

SOC 1 Summary of Changes from the SSAE 16 Standard to the SSAE 18 Standard

Services providers that store or process information for third parties should be able to provide an annual SOC (Service Organization Controls) report to customers when requested. A SOC 1 report focuses on the controls over financial reporting. If the information handled by the service provider relates to financial statements, then a SOC 1 review and report should be completed. The SOC 1, SSAE 16 format was created originally under the SSAE 16 standard which replaced the SAS 70 standard. Effective May 1, 2017, a SOC 1 report is now completed under the SSAE 18 AICPA attestation standard. The standard requires that the SOC 1 report only note "SOC 1" and should not reference or use "SSAE 18" as part of the report or title. This advisory presents the major changes that apply to SOC 1.

SOC 2 and SOC 3 reports are completed according to the AICPA Trust Service Principles. SOC 2 and SOC 3 reports are focused on the controls related to compliance and operation of the service provider. A SOC 2 or SOC 3 report provides documented assurances that operational safeguards are in place that relate to one, or all, of the following trust service principles: security, availability, processing integrity,

confidentiality, or privacy. The following changes do not affect the SOC 2 and SOC 3 reports, as the SSAE 18 does not apply to them.

SSAE 18 Changes That Apply to SOC 1

Subservice Organizations:

SSAE 18 is requiring that service organizations implement processes that monitor the controls at subservice organizations. This new requirement requires service organizations to state the vendor management controls they have in place for subservice providers (for example, colocation facility).

Complementary Subservice Organization Controls:

The SSAE 18 introduces the concept of “Complementary Subservice Organization” controls which will be included in the service provider’s system description. This concept establishes and defines the controls for which customers must now assume in the design of the system description. This addition to the system description is similar to the Complementary User Entity Controls section.

Signed Written Assertion Requirement:

The written assertion is the statement found within the SOC report where the service organization asserts that the system description provided is true and complete. This statement has always been contained within the SOC 1 reporting document but the requirement that the service organization signs the document was optional. Like many firms, AuditOne, Inc. has already been requiring this section to be signed by service providers as a way to strengthen the credibility of the report.

Service Auditor Risk Understanding:

The SSAE 18 requires service auditors to obtain a more in-depth understanding of the development of the subject matter than currently required, in order to better identify the risks of material misstatement in an examination engagement. This enhancement should lead to an improved understanding between assessed risks and the nature, timing, and extent of attestation procedures performed in response to those risks.

AuditOne Inc. Delivers Effective and Efficient SOC Audits

AuditOne Inc.’s skilled audit, technical and security experts deliver the highest quality, cost-effective, responsive SOC services in the industry. Please contact myself or Bud Genovese to review how we can make the SOC audit an effective and efficient experience for your firm. I will be more than happy to help you understand why

AuditOne Inc.'s user-friendly process and focus, makes it the market-leading smart choice.

Robert Kluba is the Technology Practice Co-Director of **AuditOne LLC**, the Nation's leading firm with the sole focus on financial institution internal audit and consulting services. AuditOne LLC affiliates with **AuditOne Inc**., a PCAOB registered CPA firm that specializes in SOC audits for service providers. Under Managing Director Bud Genovese, AuditOne Inc. has positioned itself to deliver affordable SOC reviews utilizing hands-on technical staff. The AuditOne group of technical experts also can assist in SOC related risk assessments and penetration testing requirements. Contact Robert Kluba or Bud Genovese (Contact Us) for more information.

AuditOne has been audited for compliance with the QAR requirements of the Institute for Internal Auditors (IIA).

AuditOne, LLC | LinkedIn

Address:
6131 Orangethorpe Avenue, Suite 470
Buena Park, CA 90620

Phone: 562.802.3581