



SERVICE ORGANIZATION CONTROL REPORTS

Overview of SAS 70 and SSAE 16

Effective June 15, 2011, Statement on Auditing Standards No. 70, Service Organizations (SAS 70), will be replaced by Statement on Standards for Attestation Engagements 16 (SSAE 16). This change aligns the U.S. with international standards for evaluating internal controls of service organizations.

Service Organization Controls

Today, it is common for entities to outsource certain tasks or functions to a service organization. When users of a service organization's services (user entities) outsource these tasks and functions, many of the risks of the service organization become risks of the user entities. In light of several prominent internal-control breakdowns, (e.g., security and privacy breaches, and frauds) and increasing regulatory focus on internal control (e.g., Sarbanes-Oxley Act, Basel II, HITECH and HIPAA), user-entity management is increasing its due diligence for prospective service organizations and governance oversight of current service organizations. Technological, regulatory and other changes have heightened the need for information and assurance that enable management to demonstrate it has addressed stakeholder concerns related to the security, availability and processing integrity of the systems a service organization uses to process user entities' data, and the confidentiality and privacy of the information these systems process.

By engaging an independent CPA to examine and report on a service organization's controls, service organizations can respond to meet the needs of their user entities and obtain an objective evaluation of the effectiveness of controls that address operations and compliance, as well as financial reporting at those user entities. To provide the framework for CPAs to examine controls and to help management understand the related risks, the AICPA established three **Service Organization Control (SOC)** reporting options (SOC 1, SOC 2 and SOC 3 reports).

SOC 1 engagements are performed in accordance with Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization. **SOC 1 reports focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements.** SOC 2 and SOC 3 engagements address controls at the service organization that relate to operations and compliance.

SOC 1 Report: What is it?

Reports on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting: SOC 1 engagements are performed under SSAE 16, *Reporting on Controls at a Service Organization*. SOC 1 reports are examination engagements undertaken by a service auditor to report on controls at an organization that provides services to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting.



There are two types of SOC 1 reports:

- **Type 1** – A report on management’s description of the service organization’s system and the suitability of the design of the controls to achieve the related control objectives included in the description as of a specified date.
- **Type 2** – A report on management’s description of the service organization’s system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

Use of a SOC 1 report is restricted to existing user entities (not potential customers). Updated guidance for SOC 1 reports (SSAE 16) is effective for service auditors’ reports for periods ending on or after June 15, 2011 (although early adoption is acceptable).

SOC 2 Report: What is it?

Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy: Many entities outsource tasks or entire functions to service organizations that operate, collect, process, transmit, store, organize, maintain and dispose of information for user entities. SOC 2 engagements use the predefined criteria in *Trust Services Principles, Criteria and Illustrations*, as well as the requirements and guidance in AT Section 101, *Attest Engagements*, of SSAEs (AICPA, *Professional Standards*, vol. 1). A SOC 2 report is similar to a SOC 1 report. Either a type 1 or type 2 report may be issued and the report provides a description of the service organization’s system. For a type 2 report, it also includes a description of the tests performed by the service auditor and the results of those tests. SOC 2 reports specifically address one or more of the following five key system attributes:

- **Security** – The system is protected against unauthorized access (both physical and logical).
- **Availability** – The system is available for operation and use as committed or agreed.
- **Processing integrity** – System processing is complete, accurate, timely and authorized.
- **Confidentiality** – Information designated as confidential is protected as committed or agreed.
- **Privacy** – Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity’s privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.



SOC 3 Report: What is it?

Trust Services Report for Service Organization: SOC 3 engagements use the predefined criteria in *Trust Services Principles, Criteria and Illustrations* that also are used in SOC 2 engagements. The key difference between a SOC 2 report and a SOC 3 report is that a SOC 2 report, which is generally a restricted-use report, contains a detailed description of the service auditor's tests of controls and results of those tests as well as the service auditor's opinion on the description of the service organization's system. A SOC 3 report is a general-use report that provides only the auditor's report on whether the system achieved the trust services criteria (no description of tests and results or opinion on the description of the system). It also permits the service organization to use the SOC 3 seal on its website. SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity, confidentiality and privacy).

The K Financial Advantage

K Financial is a licensed Certified Public Accounting firm, registered with the American Institute of Certified Public Accountants. Our CPAs who focus on examinations of service organization controls are also trained and experienced IT auditors. We have developed and follow an efficient and effective control assessment and testing methodology that enables us to deliver SOC reports at significantly lower rates than our competitors. In accordance with professional standards, we maintain our independence throughout our examinations, but we pride ourselves on taking a much more consultative approach than our competitors. We recognize that the AICPA standards may be confusing to our clients and the examination process may be intimidating. Therefore, all of our engagements are staffed with seasoned professionals who are able to help our clients define their control objectives and document their control activities in order to stream-line the examination process. Our services also generally include valuable recommendations to improve the overall internal control structure.