A New Series of Reporting Options for Service Organizations

By AICPA
Published on Mar 12, 2012

Many service organizations and other entities are familiar with SAS 70 reports — reports prepared following the CPA profession's Statement on Auditing Standards No. 70, Service Organizations. Innovations in technology and the increasing use of outsourcing have led to these reports being used in ways that were never intended. Specifically, SAS 70 engagements were not designed to examine compliance and operational issues, such as security, availability, processing integrity, confidentiality or privacy. Moreover, "SAS 70 Certified" and "SAS 70 Compliant" were terms that gained traction in the marketplace, but in actuality were not part of a SAS 70 report.

However, the American Institute of CPAs recently released a new series of reporting options, called Service Organization Control Reports, that enables CPAs to provide assurance on internal controls over subject matter other than financial reporting while filling the marketplace's need to demonstrate reliability and mitigation of risk. They are called SOC 1, SOC 2 and SOC 3 reports.

Here are brief descriptions of the three new SOC reports:

- A SOC 1 report results from an engagement under a new Statement on Standards for Attestation Engagements, SSAE 16 – Reporting on Controls at a Service Organization. SSAE 16 examines internal controls at a service organization that impact a user entity's controls over financial reporting. This report is to be used only by auditors of user organizations and the management of user entities. SSAE 16 requires the same level of evidence and assurance expected under the former SAS 70 service auditor engagement. It essentially fills the role of a SAS 70 report as it was originally intended.
- SOC 2 reports provide detail on controls at a service organization covering security, availability, processing integrity, confidentiality or privacy. Its use is generally restricted to certain identified users who, among other things, have some knowledge of the nature of the services that the service organization provides. The SOC 2 report can offer greater assurance to customers and stakeholders about internal controls in areas that were not meant to be covered by a SAS 70 report.
- SOC 3 reports are Trust Service examination reports. They address the same subject areas as a SOC 2 report, but in a shortened version (about one page, in fact) that can be used in a service organization's promotional efforts and on its website. SOC 3 reports can serve as a marketing tool, with potential customers for instance, to show the organization has appropriate controls in place to mitigate risks on the nonfinancial subject matters.

Since SSAE 16 is now effective, CPAs will no longer be performing service auditor engagements under SAS 70. That also means that your CPA firm is now offering all three reporting options for service organizations, including those covering controls over security, availability, processing integrity, confidentiality or privacy. Contact your Hein for more information.

Comparison of SOC 1, SOC 2 and SOC 3 Reports

	SOC 1 Reports	SOC 2 Reports	SOC 3 Reports
Under what professional standard is the engagement performed?	SSAE No. 16, Reporting on Controls at a Service Organization AICPA Guide, Applying SSAE No. 16, Reporting on Controls at a Service Organization	AT 101, Attestation Engagements, AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy	AT 101, Attestation Engagements, AICPA Technical Practice Aid, Trust Services Principles, Criteria, and Illustrations
What is the subject matter of the engagement?	Controls at a service organization relevant to user entities internal control over financial reporting.	Controls at a service organization relevant to security, availability, processing integrity confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices.
What is the purpose of the report?	To provide information to the auditor of a user entity's financial statements about controls at a service organization that may be relevant to a user entity's internal control over financial reporting. It enables the user auditor to perform risk assessment procedures, and if a type 2 report is provided, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing.	To provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality or privacy .A type 2 report that addresses the privacy principle, also provides a CPA's opinion about the service organization's compliance with the commitments in its statement of privacy practices.	To provide interested parties with a CPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality, or privacy. A report that addresses the privacy principle, also provides a CPA's opinion about the service organization's compliance with the commitments in its privacy notice.
What are the components of the report?	A description of the service organization's system. A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a type 2 report, the operating effectiveness of the controls.	A description of the service organization's system. A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a type 2 report, the operating effectiveness of the controls. If the report addresses the privacy principle, the service	A service auditor's report on whether the entity maintained effective controls over its system as it relates to the principle being reported on i.e., security, availability, processing integrity, confidentiality, or privacy, based on the applicable trust services criteria. If the report addresses the privacy

	In a type 2 report, a description of the service auditor's tests of the controls and the results of the tests.	auditor's opinion on whether the service organization complied with the commitments in its statement of privacy practices. In a type 2 report, a description of the service auditor's tests of controls and the results of the tests. In a type 2 report that addresses the privacy principle, a description of the service auditor's tests of the service organization's compliance with the commitments in its statement of privacy practices and the results of those tests.	principle the service auditor's opinion on whether the service organization complied with the commitments in its statement of privacy practices.
Who are the intended users of the report?	Auditors of the user entity's financial statements, management of the user entities, and management of the service organization.	Parties that are knowledgeable about: • The nature of the service provided by the service organization • How the service organization's system interacts with user entities, subservice organizations, and other parties • Internal control and its limitations • The criteria and how controls address those criteria	Anyone