Deloitte.

Service organization controls reporting framework: SOC1, SOC2 and SOC3

Which SOC report is appropriate for your service organization?

As part of the American Institute of Certified Public Accountants (AICPA)'s development of the Statement on Standards for Attestation Engagements (SSAE) 16, the AICPA also created the Service Organization Control (SOC) reporting framework – SOC 1, SOC 2, and SOC 3 – covering controls over services provided by organizations with the intent to: (1) address various needs and reporting requirements by service organizations, and (2) provide valuable information to address user needs, including risk assessment related to outsourcing. Each SOC report is summarized below for further information and how each addresses specific user needs:

- SOC 1 report – Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting
- SOC 2 report – Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy
- SOC 3 report – Trust Services Report for Service Organizations

	SOC 1	SOC 2	SOC 3
Subject matter and applicable professional standards	Report on controls relating financial reporting of user entities. Performed under AICPA's SSAE 16 standards.	Report on controls related to compliance or operations related to security, availability, processing integrity confidentiality, or privacy performed under AICPA's Trust Services Principles and Criteria and AT 101, Attest Engagements, standards.	
Report layout	Service auditor's opinion on fairness of presentation of the description of the system suitability of design and implementation of controls (for Type 1); and operating effectiveness of controls (for Type 2), including test of controls and related test results for Type II Reports.		No report other than a summary statement that can be distributed to anyone.
Management assertion	Management is required to provide a written assertion that is included in the report. Management should have a reasonable basis to provide the assertion, which includes considering the risks that threaten the achievement of the control objectives.		Management will be required to provide written assertion on effectiveness of controls over security, availability, processing integrity, confidentiality, and/or privacy.
Subservice organizations	The descriptions of the service organization's system may either (a) include the subservice organization's services, and related controls using the inclusive method, or (b) provide information on the nature of the subservice organization's services, but exclude the controls, using the carve-out method.		All significant subservice providers need to be included in order to receive an unqualified opinion. Also, there cannot be any significant user control considerations to receive an unqualified opinion.
Intended users	Management of the service organization, its user entities and their financial statement auditors.	Entities with knowledge about: 1) nature of services covered; 2) controls and its limitations; and 3) the criteria covered and how management's controls addresses the criteria.	Anyone
Restriction on report distribution	Restricted Use.	Restricted Use. However it is less restrictive than SOC 1 (see intended users above).	General Use: no restriction on distribution and can be posted on a website as a seal.

Demand Drivers for SOC 1, SOC 2 and SOC 3

As part of many companies' continual pursuit for efficiency and profitability, **outsourcing of non-core functions or activities to service organizations** with specialized expertise, personnel and/or equipment plays a vital role to help companies achieve their goals. As a result, service organizations are becoming more integrated with many aspects of the user's day-to-day operations and related internal control framework ranging from financial reporting to compliance with requirements of laws, regulations, rules, contracts, etc.

Additionally, there has been a spike in market demand for an increasingly popular service offered by certain service organizations related to **cloud computing**, which involves providing user entities with on-demand network access to a shared pool of computing resources, such as networks, servers, storage, applications, and services. The increasing use of these services has resulted in a demand by user entities for assurance regarding controls over the systems underlying those services.

To assist user entities in understanding the controls at service organizations, service organizations have historically relied heavily on SAS 70 examinations to report. With the introduction of the SOC framework, there are additional alternatives for service organizations to provide a useable and useful report. Service organizations can now determine the most effective reporting options to help meet market demand, the needs of their user base, and assist in developing new business.

Answers to FAQs related to the SOC Framework

Given the similarities between SOC 1 and SOC 2 reports, how can the SOC 2 report help service organizations?

Customer/user needs – We often see service organizations being asked by their users for assurance related to areas/controls not directly related to user's financial statements. SOC 2 was created with the intent that it would enable organizations, such as cloud computing vendors or call center operations, to demonstrate that their controls are sound and they are meeting a third party standard.

Potentially decrease the number of individual audits that your organization undergoes – Even with a SSAE 16 (SOC 1), many organizations still needed to accommodate individual audits for significant customers. This is particularly true in certain industries such as health care claims processing, credit and payments transaction processing, data center hosting services and for providers of "cloud" based computing solutions. SOC 2 offers the potential to rationalize the number and extent of these individual audits by providing a more in-depth report around areas of critical concern.

Meeting regulatory and other industry requirements – With the evolution of businesses today, including the drive for greater technology sophistication, regulators, industry groups and users are demanding more transparency from their service providers. A SOC 2 report can assist with meeting several regulatory requirements, while also demonstrating competitiveness within the industry and satisfying customer demand.

Can I combine an existing SOC 1 report with a SOC 2 report?

Combining SOC 1 and SOC 2 in a single report is often not a good option because the reports are aimed at two different audiences:

- SOC 1—intended for those current users with a financially significant stake in services performed – primarily users' financial executives and their auditors
- SOC 2—intended for user entity management, specifically those charged with overseeing the delivery of your services

However, combining efforts can create testing efficiencies related to common controls and is often contemplated as the service auditors get started.

What are benefits of a SOC 3 report over a SOC 2 report?

SOC 3 reports are designed to meet the needs of users who want assurance on controls at a service organization related to the AICPA's Trust Services Principles and Criteria, but where the detailed report is not needed. However, there can't be any carved out subservice providers, nor can there be any significant user control considerations in order to receive an unqualified opinion.

Which SOC report is appropriate for you?

Service organizations should understand the needs of their clients and select the reporting option that best suits client needs. Management should consider the following:

- **What is the intended use of report?**
  - Are users focused on internal control over financial reporting?
  - Are key compliance and operational controls such as those related to security, availability, processing integrity, confidentiality or privacy of primary interest?
- **Level of information related to your systems and processes?**
  - Are users in need of details related to systems, processes and controls?
  - Will the posting of a summary report or seal suffice?

It is important for service organizations to evaluate the unique aspects of each SOC report and match those aspects to client needs. The right combination will allow service organizations to provide value to clients and build trust and confidence in their outsourcing partnerships.

Contacts

Francois Lamontagne
Partner
Audit
+1 (345) 743 6232
flamontagne@deloitte.com

Lise Baril
Director
Risk Advisory
+1 (345) 743 6262
lbaril@deloitte.com