AICPA & CIMA

Together as the Association of International Certified Professional Accountants

SOC for Service Organizations Engagements

AICPA SOC

aicpa.org/soc4so

SOC for Service Organizations | Service Organizations™

AICPA SOC for Service Organizations Engagements

Overview

Today, more and more organizations are outsourcing certain functions or activities to third parties so that they can provide services or products more efficiently and cost-effectively to customers and business partners. Along with the benefits of doing business with these third parties (referred to as service organizations), however, come risks that the outsourcing organization needs to identify, assess, and manage. To help organizations manage these third-party risks, organizations and other interested parties are increasingly requesting more information about the effectiveness of controls at the service organizations with which they do business. The AICPA has developed several services, referred to as System and Organization Control (SOC) for Service Organization engagements, to assist organizations with their third-party risk management efforts.

In a SOC engagement, a licensed, independent CPA examines a service organization's controls in accordance with the AICPA's attestation standards. A SOC engagement culminates in a report on the internal controls at a service organization related to the system used to provide outsourced services. SOC reports include valuable information that can add credibility and trust to the information users need to manage the risks associated with outsourced service providers. A SOC examination is not a "certification"; instead, it is akin to an audit of historical financial statements. Similar to a financial statement audit where a CPA obtains evidence to support an opinion about the fair presentation of the financial statements, a service auditor performing a SOC examination obtains evidence to support an opinion about the suitability of design and operating effectiveness of controls at the service organization.

There are three types of SOC for Service Organization engagements:

1. SOC 1®— SOC for Service Organizations: ICFR (Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting)

   These reports are specifically designed to address controls at the service organization that are relevant to the user entities' financial statements. They enable user auditors to perform risk assessment procedures and obtain audit evidence about whether controls at the service organization are operating effectively. Use of these reports is restricted to management of the service organization, user entities, and user auditors.

   Examples of service organizations that provide services that directly tie to user entities' internal control over financial reporting include payroll processors, medical claims processors, loan servicing companies, and data centers.

2. SOC 2® — for Service Organizations: Trust Services Criteria (Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy)

   These reports address controls relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information these systems process. They provide a level of detail sufficient to address the user's vendor risk management needs and are restricted to specified parties with sufficient knowledge and understanding of the service organization's system and the nature of services it provides.

[1] In the attestation standards, a CPA performing an attestation engagement is ordinarily referred to as a practitioner. However, SOC 1, SOC 2, and SOC 3 engagements use the term *service auditor* rather than practitioner to refer to a CPA reporting on controls at a service organization.

[2] All SOC examinations are performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Assertion-Based Examination Engagements*. In addition, SOC 1 examinations are performed in accordance with AT-C section 320, Reporting on an *Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Financial Reporting.*

Examples of service organizations that routinely obtain, process, and transmit customer data include those that provide customer support, health care claims management and processing, enterprise IT outsourcing, e-commerce SaaS applications, managed security, financial technology services, and ESG metric services.

3. SOC 3® — SOC for Service Organizations: Trust Services Criteria for General Use Report

Like SOC 2, these reports address controls relevant to security, availability, processing integrity, confidentiality, and privacy. However, they do not provide the same level of detail. Therefore, they are considered general-use reports and can be freely distributed. Although SOC 3 reports are generally not required to be restricted, some report users may not have a sufficient understanding of the service organization's system to understand how controls within the system operate. Before agreeing on a SOC 3 examination, management and the service auditor need to consider whether a SOC 3 report, which includes only management's assertion and the service auditor's opinion about the effectiveness of controls at the service organization, is likely to meet the information needs of intended report users or whether a SOC 3 report will likely be misunderstood by potential report users. In some instances, management and the service auditor may agree to restrict the use of a SOC 3 report to the subset of potential report users whose informational needs are likely to be met by the SOC 3 report.

Because the informational needs of users vary, there are two types of examinations and related reports for both a SOC 1 and SOC 2 engagement:

SOC 1:

Type 1 — Examination on the fairness of the presentation of 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 — Examination on the fairness of the presentation of management's description of the service organization's system and the suitability of the designed and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period.

SOC 2:

Type 1 — An examination of whether (1) a service organization's description presents the system that was designed and implemented at a point in time in accordance with the description criteria and controls were suitably designed at a point in time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria if controls operated effectively.

Type 2 — an examination that also addresses the description of the system and the suitability of design of controls, but it includes an additional subject matter: whether controls operated effectively throughout the period of time to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

SOC 1 and SOC 2 reports include the following elements:

SOC 1 Examination	SOC 2 Examination
Components of a Type 1	
Management's description of the service organization	The description of the service organization's system
A written assertion by management of the service organization about whether, based on the criteria in management's assertion, i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date and ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed to achieve those control objectives as of the specified date	A written assertion by management of the service organization about whether i. the description of the service organization's system presents the service organization's system that was designed and implemented as of a specified date in accordance with the description criteria and ii. the controls stated in the description of the service organization's system were suitably designed as of the specified date to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria as of the specified date
A service auditor's report that expresses an opinion on the matters in (i) – (ii) above	A service auditor's report that expresses an opinion on the matters in (i) –(ii) above
Components of a Type 2	
Management's description of the service organization's system	The description of the service organization's system
A written assertion by management of the service organization about whether, based on the criteria, i. management's description of the service organization's system fairly presents the service organization's system that was designed and implemented throughout the specified period, ii. the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives, and iii. the controls related to the control objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives	A written assertion by management of the service organization about whether i. the description of the service organization's system presents the service organization's system that was designed and implemented throughout the specified period in accordance with the description criteria, ii. the controls stated in the description of the service organization's system were suitably designed throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and iii. the controls stated in the description of the service organization's system operated effectively throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria
A service auditor's report that i. expresses an opinion on the matters in (i) - (iii) above and ii. includes a description of the service auditor's tests of the controls and the results of those tests	A service auditor's report that i. expresses an opinion on the matters in (i)–(iii) and ii. includes a description of the service auditor's tests of controls and the results of those tests

Per the above, a SOC 3 report does not contain the same level of detail as a SOC 1 or SOC 2 report. A SOC 3 report will only include a written assertion by management of the service organization and a service auditor's report on whether management's assertion is fairly stated based on the applicable trust services criteria.

Licensed CPAs (or CPA firms) who perform any of the SOC for Service Organization engagements mentioned above (i.e., SOC 1, SOC 2 or SOC 3) may use or display the AICPA's official SOC for Service Organizations logo for use by CPAs (the "SOC Logo for CPAs") to market and promote their SOC service offerings.

To download and use the SOC Logo for CPAs, CPAs must register and agree to comply with the logo terms, conditions, and guidelines. The AICPA has established these guidelines to govern the use and display of the SOC Logo for CPAs.

The AICPA has developed a logo ("SOC Logo for Service Organizations") that may be used or displayed by Service Organizations that have undergone any of the SOC for Service Organization examinations mentioned above (i.e., SOC 1, SOC 2 or SOC 3) and have received a SOC report from a licensed CPA or non-U.S. CPA (or equivalent such as a Chartered Accountant).

To download and use the SOC Logo for Service Organizations, service organizations are required to register and agree to comply with the logo terms, conditions, and guidelines. The AICPA has established these guidelines to govern the use and display of the SOC Logo for Service Organizations.

The AICPA has developed a second logo ("SOC 2 Logo for Service Organizations") that may be used or displayed by Service Organizations that have undergone a SOC 2 examination and have received a SOC 2 report from a licensed CPA or non-U.S. CPA (or equivalent such as a Chartered Accountant). Service organizations that have received a SOC 2 report are eligible to use either the SOC 2 Logo for Service Organizations or the SOC Logo for Service Organizations.

To download and use the SOC 2 Logo for Service Organizations, service organizations are required to register and agree to comply with the logo terms, conditions, and guidelines. The AICPA has established these guidelines to govern the use and display of the SOC Logo for Service Organizations.

It is important to understand that display of a SOC Logo for Service Organizations indicates only that a service organization has undergone a SOC 1, SOC 2 or SOC 3 examination of the system or systems used to provide services to customers and business partners. Therefore, instead of relying on the displayed logo, interested parties are encouraged to obtain and read the service organization's SOC report and the independent CPA's opinion.

Additional SOC Resources:

Please visit the SOC Suite of Services page for additional SOC resources.

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.

aicpa.org
aicpa-cima.com
cgma.org
cimaglobal.com

2303-125810