tcp™

SSAE 16/18:
Service Organization Control (SOC)

What is a SOC Report?

There are actually three types of SOC reports; SOC 1, SOC 2, and SOC 3. The first of the SOC reports, SOC 1, provides a formal audit of a company's self-imposed controls for financial transactions. The shortfall with SOC 1 is that the relevance of the audit solely depends on the controls formulated and included by the service provider and the credibility of the auditor. With the emergence of new technology services and cloud computing entities, the need was recognized to protect against the over-application of SOC 1 by standardizing the adherence to the industry standard Trust Services Principles; Security, Availability, Processing Integrity, Confidentiality and Privacy. In recent years SOC 2 Type 2 has become the industry best practice for ensuring security of highly sensitive cloud-hosted data. SOC 2 significantly expands on SOC 1, but may not be cost effective for smaller organizations who are unable to readily meet the demands of the five Trust Services Principles and an in-depth audit of their security protocols.

Why the need for a SOC report?

The biggest reason for a SOC 2 report is to ensure the security of highly sensitive transactions, as mentioned above. Customers need to trust their service providers with confidential information, and a clean SOC 2 report means companies can depend on their service provider for secure, compliant hosting. That in turn means less worry for the customer, and less investment on their part in controls.

Which report should I require?

The choice of requiring SOC 1 or SOC 2 is based on the needs of the customer. In short, while SOC 1 is designed for transaction controls, SOC 2 is designed to ensure the security of those transactions. The table below lists questions a customer should ask when determining if they should require SOC 1 or SOC 2. Also keep in mind that because a SOC 2 often contains sensitivity security protocol data (requires NDA), the SOC 2 report is often summarized in a customer-facing SOC 3.

Question	Response	SOC Report Type Required
Will the report be used by you and your auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1 Report financial statements
Will the report be used by you or your stakeholders to gain confidence and place trust in a service organization's systems?	Yes	SOC 2 Report financial statements

Source: American Institute of CPAs (AICPA)

SOC Reports: Myths vs. Facts

Myth

All operational areas can be included in SOC 1 reports. Organizations can scope in operational, marketing, and regulatory areas that do not have a direct/indirect impact on financial reporting.

Fact

AICPA guidelines specify that the SOC 1 report is applicable only to internal controls over financial reporting. In cases where organizations need to include other areas such as confidentiality and security, they should adopt SOC2 reports.

Myth

Application software can be made to comply with SSAE 16 SOC 1 requirements.

Fact

SOC 1 reports are assurances provided for internal controls over financial reporting and not product evaluations.

SOC 2 audits are conducted on an annual basis and can be provided by your certified cloud service vendors with signed Non-Disclosure Agreement. Request our SOC 2 Type II report at dpo@timeclockplus.com

SOC 3 Type II audit report is also available without a signed Non-Disclosure Agreement.

Source: American Institute of CPAs (AICPA)

Under what professional standard is the engagement performed?	**SOC 1** SSAE No. 16, Reporting on Controls at a Service Organization AICPA Guide, Applying SSAE No 16, Reporting on Controls at a Service Organization.	**SOC 2** AT 101, Attestation Engagements AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.	**SOC 3** 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.	Controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.
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.	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.	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.
What are the components ofthe 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. In a type 2 report, also a description auditor's tests of controls and the tests results.	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.	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.
Who are the intended users of the report?	Auditor's 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.

Source: American Institute of CPAs (AICPA)