Understanding the Differences Between a Vendor SOC 1 2 3

SSAE 18

Effective May 1, 2017, SSAE 18 superseded SSAE 16. SSAE 18 is the guideline that sets the standard and dictates all SOC reporting. With the SSAE 18 update, you'll better understand your fourth-party's operations and procedures. And, on December 15, 2020, SSAE 20 took effect. SSAE 20 did not replace the SSAE 18, but it amended it.

The purpose of this minor change is to align the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board (ASB) description of materiality with the description of materiality used by the U.S. judicial system, the auditing standards of the Public Company Accounting Oversight Board (PCAOB), the U.S. Securities and Exchange Commission (SEC) and the Financial Accounting Standards Board (FASB).

Your third-party vendors who use vendors of their own to support the operations of their products/services are required to identify the functions and controls that your vendor assumes.

SOC 1

WHAT IT IS

A SOC 1 is designed to review a vendor's internal controls as they relate to financial reporting. SOC 1 audit reports are best for your non-information system-based products and services.

TWO TYPES

A SOC 1 Type 1 Report:
Audit controls as of a point in time (single date).

A SOC 1 Type 2 Report:
Covers controls that were in place and operating for a period of time. A Type 2 report includes a description of any significant changes. Type 2 assessments are more rigorous, and controls are reviewed for operational effectiveness over a period of time.

WHEN TO USE

The type of product does not have consumer private information being stored or hosted at the vendor. Examples may include:

- ✓ *Insurance products (where there is no consumer private info)*
- ✓ *Internal accounting software*
- ✓ *Back office administrative products*

BENEFITS

A SOC 1 report provides information about controls at a service organization that may be relevant to a user entity's internal control over financial reporting. This report helps user entities to determine if the control objectives are operating effectively.

SOC 2

WHAT IT IS

A SOC 2 report is an examination on the vendor's controls over one or more of the following **5 Trust Services Principles** (**TSP**):

Security:
The system is protected against unauthorized access, use or modification.

Processing Integrity:
System processing is complete, valid, accurate, timely and authorized.

Privacy: The system's collection, use, retention, disclosure and disposal of personal information are in conformity with the commitments in the service organization's privacy notice and with criteria set forth in the Generally Accepted Privacy Principles (GAPP) issued by the AICPA and CICA.

Availability:
The system is available for operation and use as committed or agreed.

Confidentiality: Information designated as confidential is protected as committed or agreed.

A SOC 2 is all about protecting private information (or in some cases, funds transfers) and making sure that the controls in place adequately protect information.

A SOC 2 report may cover one or all of these TSPs. TSPs determine the scope of what controls to monitor and what changes to make with the products or services offered. For example, if you're reviewing a data center or cloud service provider, at minimum you should be looking at Availability and Security TSPs.

Most of the time, this is probably the report you will want.

TWO TYPES

A SOC 2 Type 1 Report:
Audit controls as of a point in time (single date).

A SOC 2 Type 2 Report:
Covers controls that were in place and operating for a period of time. A Type 2 report includes a description of any significant changes. Type 2 assessments are more rigorous and controls are reviewed for operational effectiveness over a period of time.

BENEFITS

SOC 2 reports are specifically targeted towards information security and information system availability. Most of the principles covered in these reports are very closely related to an IT service, thus allowing the user entity to determine if proper controls are in place to protect their information.

WHEN TO USE

If you want a measure of how your vendor provides a secure, available, confidential and private solution, ask for a copy of their independently audited SOC 2 Report.

A SOC 2 report is an audit (and report) that defines a consistent set of criteria specifically around the product/services that an organization provides (to you). However, keep in mind as you review that the controls are created by the vendor and tested by an auditor or CPA firm.

Examples may include:

- ✓ *Internet banking*
- ✓ *Mobile banking*
- ✓ *Bill payment*
- ✓ *Any vendor that stores or accesses consumer private information*

SOC 3

WHAT IT IS

A SOC 3 is a high-level summary of the SOC 2 audit that comes with a seal of approval a vendor can publicly share.

While the SOC 3 has some of the components of the SOC 2, it's not as comprehensive as it's designed to be made available publicly without the requirement of an NDA. Therefore, it has less details, is less technical and will not contain the same level of otherwise critical information (to you) hat a SOC 2 contains.

WHEN TO USE

A SOC 3 can be used for the initial early upfront due diligence phase of a vendor until you have determined if they're a serious prospect.

BENEFITS

A SOC 3 is a good tool to use in the initial vetting period of new vendors. Keep in mind that it should not be used in place of a SOC 1 or SOC 2.

PRINTABLE VERSION