Building Trust by Obtaining a Service Auditor's Report

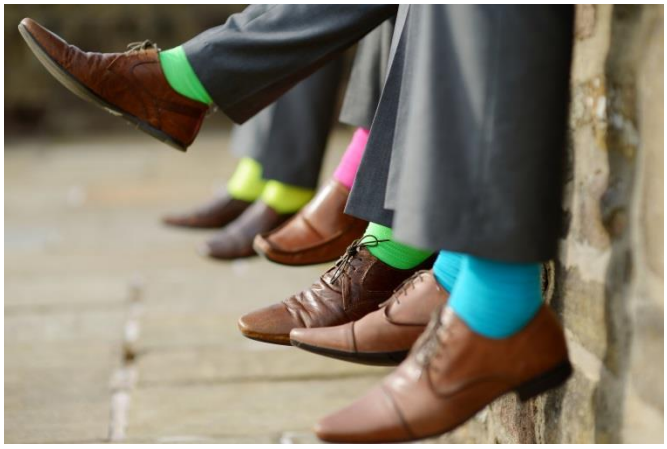
SOC 1, SOC 2, and SOC 3 Executive Summary

Updated October 2017

Larson

CERTIFIED PUBLIC ACCOUNTANTS

OVERVIEW



SOC 1, SOC 2, and SOC 3 audits are performed on service organizations, a third-party organization that provides services to a user entity, to help the service organization and the users of the service organization in assessing the service organization's internal control design and/or operating effectiveness. SOC 1, SOC 2, and SOC 3 reports differ in their targeted audiences, scope of the audits, and their control emphasis. A summary of such differences are included below:

	SOC 1	SOC 2	SOC 3
INTENDED USER	Financial Auditors	Users interest in service organization's compliance or Operations	Users interest in service organization's compliance or Operations **Specifically for Marketing**
FRAMEWORK AND GUIDANCE	SSAE18	AT 101 and AICPA Guide	AT 101 and AICPA Guide
OPINION FOR TYPE 1	• Fair description of controls • Controls were suitably designed.	• Fair description of controls and its implementation • Controls were suitably designed	N/A – Blanket Statement – report on whether service organization maintained effective controls over it system as it relates to the trust services principles being reported.
OPINION FOR TYPE 2	Controls are operating effectively during period in review	Controls are operating effectively during period in review	Same as above
USE	Restricted to users that already have an understanding of the service organization and its controls.	Restricted to users that already have an understanding of the service organization and its controls.	General user report. Can be distributed freely.
CONTROL OBJECTIVES	Defined by Client	Principles based on AT 101 (Security, Availability, Processing Integrity, Confidentiality , Privacy) Principles defined by Client	Principles based on AT 101 (Security, Availability, Processing Integrity, Confidentiality , Privacy) Principles defined by Client

INTRODUCTION

Larson CERTIFIED PUBLIC ACCOUNTANTS

In our business world today, businesses are becoming more and more interdependent on each other. For example, auto makers rely heavily on car dealerships to sell their cars, and insurance companies rely heavily on insurance agents or administrators to manage insurance policies. A third party organization that provides services for another entity is called a service organization. An entity that uses a service organization is called a user entity. A lack of a trusting, effective and efficient relationship between the service organization and a user entity could be detrimental to organization or any size. One of such incidents occurred in 2017 to Equifax, a consumer credit reporting agency, in which an estimated 145.5 million customer accounts were compromised when a software patch was not installed in a timely manner.

The American Institute of Certified Public Accountants (AICPA) has put forth a comprehensive framework, Service Organization Control (SOC) Reports, which helps built trust between service organizations and user entities. These reports are known as SOC 1, SOC 2, and SOC 3 Reports. The SOC Framework was established to help clarify and bring needed transparency in regards to reporting on controls at service organizations.

HISTORY

Statement on Auditing Standards No. 70 (SAS 70) was the predecessor of the SOC Framework. Issued in 1992, SAS 70 became the gold standard in performing audits of internal control on service organizations. With the momentum of the Sarbanes-Oxley regulation and the increase in internet driven applications, SAS 70 became widely popular to service organizations that now had increased accountability to their client partners (user organizations) and auditors (user auditors) alike to address control risks surrounding financial reporting. As organizations became more concerned about risk beyond financial reporting, SAS 70 often was misused to obtain assurance regarding compliance and operations. Additionally, new terms such as “SAS 70 Certified” and “SAS 70 Compliant” was used for business marketing purposes even though it was never the intent of SAS 70 reports to be used as a general stamp of approval. As such, the AICPA Auditing Standards Board (ASB) issued two standards, Statement on Standards for Attestation Engagements (SSAE) No. 16, which

was later revised into SSAE 18, and clarified SAS Audit Considerations Relating to an Entity Using a Service Organization (AU-C Section 402). This effectively split the old SAS No. 70 into two types of controls audit; control audit reports that are meant to report on an audit of financial statements (SSAE16), and control audit reports that are meant to report on other subject matter such as privacy, security, etc. (AU-C Section 402).

SOC 1 OVERVIEW

SOC 1 engagements are performed under SSAE 18. "SOC 1 reports are undertaken by a service auditor to report on controls at an organization that provides service to user entities when those controls are likely to be relevant to user entities' internal control over financial reporting.[i]" The control objectives are defined by the service organization. There are two types of SOC 1 reports:

TYPE 1

"A report on 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.[i]"

- Report on design of controls
- As of a specified date

TYPE 2

"A report on management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objective included in the description throughout a specified period.[i]"

- Report on design of controls
- Report on operating effectiveness
- Throughout a specified period

This can be illustrated in the figure below:

	SOC 1
INTENDED USER	Financial Auditors
FRAMEWORK AND GUIDANCE	SSAE18
OPINION FOR TYPE 1	• Fair description of controls • Controls were suitably designed.
OPINION FOR TYPE 2	• Controls are operating effectively during period in review
USE	Restricted to users that already have an understanding of the service organization and its controls.
CONTROL OBJECTIVES	Defined by Client

RESTRICTED USE AND TARGETED AUDIENCE

SOC 1 report is restricted to existing user entities (not potential customers). It is catered towards individuals that would be more interested in understanding controls surrounding transaction processing, reporting, and other controls surrounding the system related to financial reporting matters. Example of such individuals would be CFOs, controllers, etc.

SOC 2 OVERVIEW

"Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy: Many entities outsource tasks or entire functions to service organizations that operate, collect, process, transmit, store, organize, maintain and dispose of information for user entities.[i]" SOC 2 engagements address controls at the service organization that relate to operations and compliance. The biggest difference between a SOC 1 report and a SOC 2 report is that instead of having the control objectives defined by the service organization, the control objectives are prescribed by AT Section 101, Attest Engagements; and the AICPA Guide Reporting on *Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. The service organization may still be able to choose which of the Security, Availability, Processing Integrity, Confidentiality, or Privacy principles they will like addressed in the report. After the principles are determined, the service organization must then identify controls that address the prescribed criteria related to these principles. A list of these criteria and associated principles are included in Appendix A for your reference.

Once again there are two types of reports:

TYPE 1

- Report on design of controls
- As of a specified date

TYPE 2

- Report on design of controls
- Report on operating effectiveness
- Throughout a specified period
- Description of the tests performed and results
- Specially address one or more of the following five key system attributes:
    - Security
    - Availability
    - Processing integrity
    - Confidentiality
    - Privacy

This can be illustrated in the figure below:

	SOC 2
INTENDED USER	Users interest in service organization's compliance or Operations
FRAMEWORK AND GUIDANCE	AT 101 and AICPA Guide
OPINION FOR TYPE 1	• Fair description of controls and its implementation • Controls were suitably designed
OPINION FOR TYPE 2	• Controls are operating effectively during period in review
USE	Restricted to users that already have an understanding of the service organization and its controls.
CONTROL OBJECTIVES	Principles based on AT 101 (Security, Availability, Processing Integrity, Confidentiality , Privacy) Principles defined by Client

RESTRICTED USE AND TARGETED AUDIENCE

SOC 2 report is also restricted to existing user entities (not potential customers). However, unlike SOC 1 report, these reports are geared towards a broader range of users and addresses controls relevant to the user entity's system security, availability, processing integrity, confidentiality, and privacy.

SOC 3 OVERVIEW

Like SOC 2 reports, SOC 3 reports covers the same subject matter: security, availability, processing integrity, confidentiality, and privacy. SOC 3 reports can be issued on one or multiple Trust Services principles (security, availability, processing integrity, confidentiality and privacy). Unlike a SOC 2 report, a SOC 3 report is a general-use report that provides only the auditor's report on whether the system achieved the trust services criteria (no description of tests and results or opinion on the description of the system) and whether those controls are operating effectively for the period being audited. It also permits the service organization to use the SOC 3 seal on its website. Because of the general use nature of these reports, there are no differences between Type 1 or Type 2 reports, as illustrated below.

	SOC 3
INTENDED USER	Users interest in service organization's compliance or Operations **Specifically for Marketing**
FRAMEWORK AND GUIDANCE	AT 101 and AICPA Guide
OPINION FOR TYPE 1	N/A – Blanket Statement – report on whether service organization maintained effective controls over it system as it relates to the trust services principles being reported.
OPINION FOR TYPE 2	Same as above
USE	General user report. Can be distributed freely.
CONTROL OBJECTIVES	Principles based on AT 101 (Security, Availability, Processing Integrity, Confidentiality , Privacy) Principles defined by Client

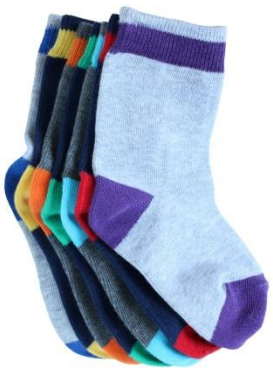
GENERAL USE REPORT

This report is a general use report; it allows you to place a SOC 3 seal on your website:

As such, SOC 3 reports are a great option for individuals that hope to broadly market the service organization's control effectiveness in the above areas to potential new user entity customers.

INCLUSIVE VS. CARVE-OUT METHOD

Service organizations often use other service organizations to perform certain transaction processing services. An example of these services may be a claims administrator using a third party for printing and mailing of claims checks. These second service organizations are known as subservice organizations. These sub-service organizations' controls may be within and out-side of the scope of the SOC reports depending on whether the inclusive or carve-out method is used.

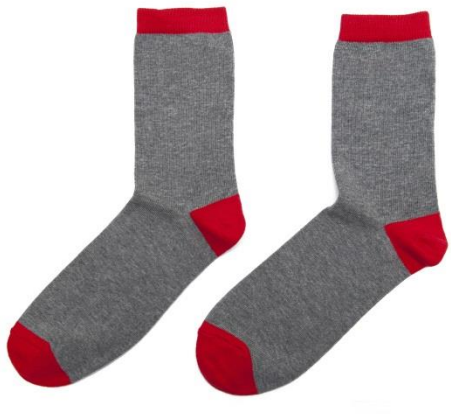


INCLUSIVE METHOD

If the inclusive method is selected, the SOC report will include a description of the nature of those services as well as the subservice organization's relevant control objectives and related controls in management's description of service organization's system. Although the inclusive method provides more information for users of the reports, it could be difficult to implement in practices because of the increased interaction between the service organization, the subservice organization, and the service auditor that is required. As such, the inclusive method is not commonly seen in the industry.

CARVE-OUT METHOD

As the name implies, the carve-out method specifies the limited scope of the report in regards to the subservice organization's controls. The scope of the subservice organization is essentially carved-out by including in management's description of the service organization's system the nature of the services performed by the subservice organization but excluding from the description, and from the scope of the service auditors engagement, the subservice organization's relevant control objectives and related controls. However, the service organization should still include in the report controls performed by the service organization that monitors the effectiveness of controls at the subservice organization. This carve-out method is commonly used in the industry today, especially when a Type 2 report is available from the subservice organization.



CONCLUSION

The differences between a SOC 1, SOC 2, and SOC 3 report are summarized as follows:

	SOC 1	SOC 2	SOC 3
INTENDED USER	Financial Auditors	Users interest in service organization's compliance or Operations	Users interest in service organization's compliance or Operations **Specifically for Marketing**
FRAMEWORK AND GUIDANCE	SSAE18	AT 101 and AICPA Guide	AT 101 and AICPA Guide
OPINION FOR TYPE 1	• Fair description of controls • Controls were suitably designed.	• Fair description of controls and its implementation • Controls were suitably designed	N/A – Blanket Statement – report on whether service organization maintained effective controls over it system as it relates to the trust services principles being reported.
OPINION FOR TYPE 2	Controls are operating effectively during period in review	Controls are operating effectively during period in review	Same as above
USE	Restricted to users that already have an understanding of the service organization and its controls.	Restricted to users that already have an understanding of the service organization and its controls.	General user report. Can be distributed freely.
CONTROL OBJECTIVES	Defined by Client	Principles based on AT 101 (Security, Availability, Processing Integrity, Confidentiality , Privacy) Principles defined by Client	Principles based on AT 101 (Security, Availability, Processing Integrity, Confidentiality , Privacy) Principles defined by Client

LARSON & COMPANY

The benefits of a SOC can include building trust with customers, increasing awareness of controls and their consistent application, and creating a better risk-assessment process which includes understanding the customer's perspective.[ii] Larson & Company can help you make the decision on which SOC is right for you. With our experience and expertise in auditing and IT consulting we have the knowledge that you need to perform the SOC audit as well as add value to your company's operations. For more information on SOC audits, please contact Geri Douglas or Andrew Wan at the information listed below.

Geri Douglas, CPA, Audit Partner – gdouglas@larsco.com 801-313-1900
Andrew Wan, CPA, CFE, Audit Partner – awan@larsco.com 801-984-1829

[i] Audrey Katcher, C. S., Janis Parthun, C. S., & Curtis Stewart, C. C. (2013). *Service Organization Controls.* AICPA.

[ii] Dan Steiner, IASA 2014 Educational Conference & Business Show

Larson & Company
9065 South 1300 East, Salt Lake City, Utah 84094
Main: (801) 313-1900 | Fax: (801) 313-1912
www.larsco.com

Larson CERTIFIED PUBLIC ACCOUNTANTS