2019 EDITION

The Vendor SOC Dictionary

A Glossary of Terminology for System and Organization Controls Reports

venminder

2019 EDITION

The Vendor SOC Dictionary

A Glossary of Terminology for System and Organization Controls Reports

This eBook is your vendor System and Organization Controls (SOC) dictionary that may be referenced to best understand the meaning of comprehensive concepts and gives you excellent insight into why each SOC definition is important to know. The next 7 pages are filled with a glossary of terminology for SOC reports.

Request a demo now to speak to one of our experts to learn how Venminder can help.

Request a Demo

CARVE OUT METHOD

The controls at your vendor's vendor (fourth party) have been excluded from the SOC audit. It's appropriate for a vendor to use the carve-out method for supporting services provided to the vendor that are required for normal operations. Your vendor should provide documentation supporting their own due diligence and vendor management practices. **Note:** It's still always encouraged to review your fourth party vendors regardless if the carve-out method is used or not.

CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)

A certification that is issued by the Information Systems Audit and Control Association and means the CISA has technical skills, knowledge and proficiency to face audit challenges.

COMPLEMENTARY USER ENTITY CONTROLS

SOC reports will usually include Complementary User Entity Controls. These are controls that the vendor has included within its system and rely on the user entity (you) to implement in order to achieve the vendor's control objectives. **Beware:** In these cases, the control objectives stated in the description can be achieved only if these complementary user entity controls are suitably designed and operating effectively (by you), along with the controls at the service organization.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

This is a newer addition with the advent of SSAE 18. These are controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system.

CONTROL OBJECTIVES

Control objectives as a whole represent the purpose of the specified control activities at the service organization. Control objectives address the risks that control activities intended to mitigate if implemented properly. Control objectives are accomplished by designing, implementing, maintaining and auditing an effective set of supporting control activities. The "meat" of a SOC report is in the Control Objectives, Control Activities, Test Procedures and Results section of the report.

EXCEPTIONS

Exceptions are discrepancies or deviations from the result an auditor would expect when testing one or more of the service organization's control activities. Each control within the service organization's description undergoes testing by an auditor. The auditor will verify and validate that

the provided manager's description is accurate and that controls have been suitably designed and are operating effectively to achieve all related control objectives or criteria. An exception is any finding that falls outside of the expected results of an audit after going through the defined steps.

FAIRNESS OF PRESENTATION

The auditor will determine if the vendor's system description is "fairly presented," if it accurately represents the system that was designed and implemented as of a specified date, Type I report or over a specified period of time, Type II report.

GAP (BRIDGE) LETTER

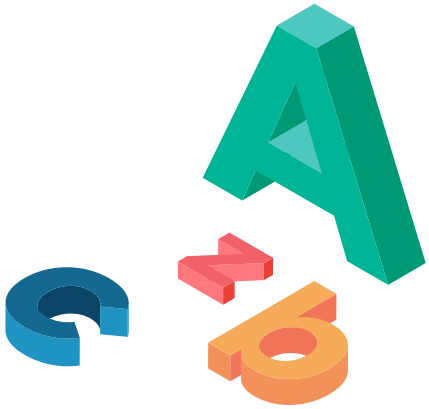
A letter issued by your vendor that covers the "gap" between the last SOC report period ending date and the date of the letter. It can be used by the user entity (you) as an interim assurance by management while waiting for the next audit report.

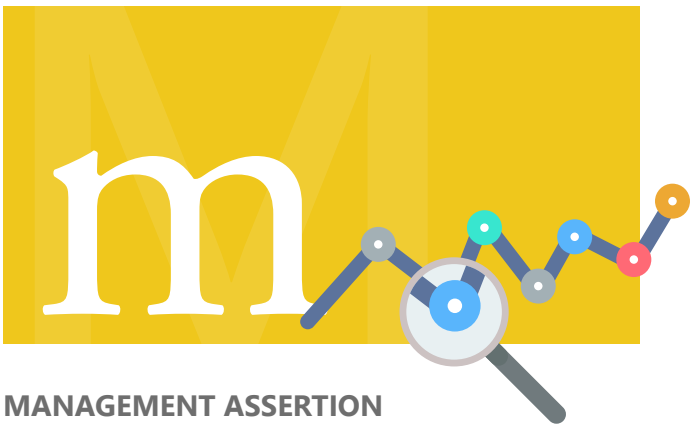
It should be noted that the CPA firm who performed the audit is not attesting to anything in the gap letter. Once the auditors have issued their report and left the site, they do not know if the internal control environment has changed or not.

Therefore, a gap letter is merely management's (management from your vendor) assertion that controls are still in place and operating effectively.

INCLUSIVE METHOD

If the Inclusive method was used, controls supporting normal operations provided by your vendor's vendor (fourth party) are included within the SOC report. Controls of the fourth party are presented separately from those of your vendor (third party) and their written assertions should also be included within the report.





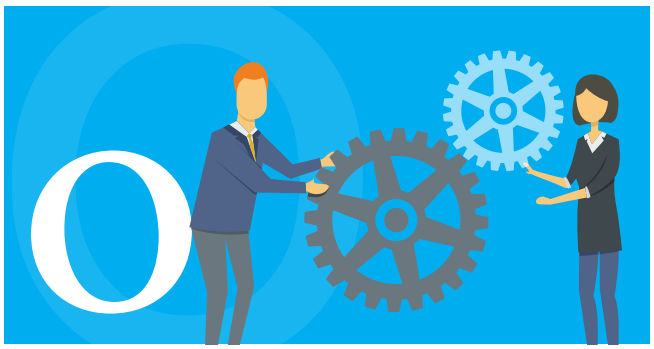
MANAGEMENT ASSERTION

Management at your vendor states what the system is at a high level and attests to what management has written in the System Description and Control Environment. This is required to be in the report. The auditor then expresses an opinion on whether management's assertion is accurate.

Look for "except for" or other exclusionary language that was added by management to the letter. It's not always about what is in the SOC audit. It can many times be about what is not included in the audit.

MONITORING ACTIVITIES

These are the processes used by management of your vendor to monitor the quality of internal control performance during the reporting period.



OPERATING EFFECTIVENESS

In the opinion of the auditor, a determination is made regarding whether a control is operating effectively and provides reasonable assurance that the control objectives stated in management's description of the vendor's system were achieved.

QUALIFIED OPINION

When an auditor performs test procedures and the results negatively impact the operating effectiveness of the control objective, they may issue a qualified report opinion. A qualified opinion means that you cannot place reliance on the controls supporting a particular area at the service organization based on the testing performed. Having a qualified opinion means that there is at least one control objective or criteria that the auditor believes the organization was not able to achieve. If a service auditor found exceptions such that a control objective was either not in place or was not effective,

the service auditor would issue a 'qualified opinion'. (This is a more significant finding than just an exception found for a single control objective. See "Exceptions" above).

Note that a single qualification does not mean that reliance may not be placed on other areas of the report free of qualifications.

RESTRICTED USE REPORT

SOC reports are required to include a statement restricting the use of the report to management (vendor), user entities (you) and your auditors.

RISK ASSESSMENT

These are the procedures used by management of your vendor to identify and analyze the risks that threaten successful achievement of the control objectives and ensure that controls described in the system description sufficiently mitigate those risks.

SSAE 18

In May 2017, SSAE 18 became the new standard for SOC reporting. The SSAE 18 causes the SSAE 16 to be retired as 16 is covered within 18. It's a simplified standard covering many others, the SSAE 16 was just one. SSAE 18 is a series of enhancements aimed to increase the usefulness and quality of SOC reports. The purpose for the creation of the SSAE 18 was to clarify the auditing standards and to reduce duplication within similar standards covering Examinations, Reviews and Agreed-Upon Procedure engagements, specifically SSAE Nos. 10-17. These now fall under SSAE 18.

SCOPE

The Scope of a SOC (control objectives and related controls) is defined by the service organization, not the auditor. Therefore, only findings identified in the failure to achieve a control objective included in the scope are disclosed in the auditor's opinion.

SERVICE AUDITOR

The SOC auditor should always be a properly licensed certified public accounting firm in order for you to rely on the audit of your vendor's controls. In a SOC report, the Service Auditor is the entity performing a SOC examination of the service organization's controls.

SERVICE AUDITOR'S REPORT
Commonly referred to as the "opinion letter," the Auditor will express an opinion on the fairness of the presentation of management's description of the system, on the suitability of the design and, if a Type II audit, on the effectiveness of the controls during the exam period.

SERVICE ORGANIZATION'S DESCRIPTION OF THE SYSTEM
An Organization's System is designed, implemented and documented by the management of your vendor to provide user entities (you) with the services covered by the auditor's report and is comprised of the personnel responsible for using and operating the system; the procedures that guide personnel in the delivery of services to clients, processes used to initiate, authorize, record and process transactions and the associated reporting system, as well as the overall Technical Infrastructure that supports, and is supported by, the organization's personnel, procedures and processes. Components of the technical infrastructure include physical hardware, software and data as well as the processes that monitor and report on non-transactional events within the System.

SERVICE ORGANIZATION OR SERVICE PROVIDER
The vendor providing the outsourced service to your organization.

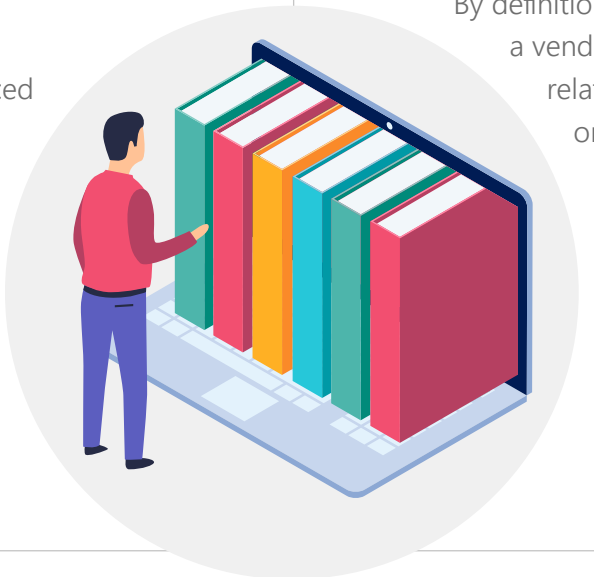
SOC
A SOC (System and Organization Controls) report is an independent audit report performed by a public accounting firm. The report will attest to the existence and effectiveness of controls specified by the company being audited (your vendor). Basically, the report should tell you if your vendor has the right controls in place to safeguard your data and if those safeguards are actually working, based on the scope of the audit determined by the vendor.

SOC 1 REPORT
A SOC 1 addresses internal controls that are relevant to a company's control environment over financial reporting. By definition, a SOC 1 is designed to review a vendor's financial and accounting controls and the systems that support them.

SOC 2 REPORT
A SOC 2 addresses internal controls that are relevant to a company's internal control environment over the following five Trust Services Criteria (TSC):

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

By definition, a SOC 2 is designed to review a vendor's control environment in relation to the selected TSC based on the vendor's defined scope.



SOC 3 REPORT
A high-level summary of the SOC 2 audit. It's not as detailed and often only requested during vendor vetting.

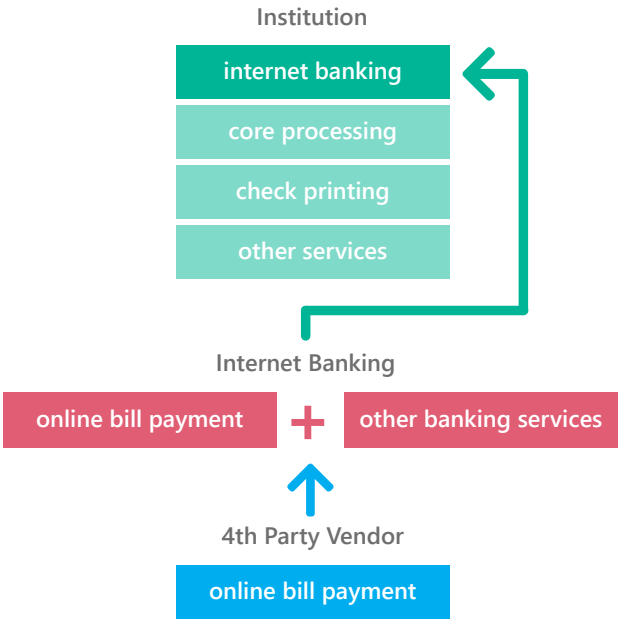
SOC FOR CYBERSECURITY

A report developed by the American Institute of Certified Public Accountants (AICPA) in 2017 that companies may provide upon request if someone is seeking to better understand how mature or effective their cybersecurity risk program is.

SUBSERVICE ORGANIZATION

Sometimes referred to as fourth parties or subservice providers, simply put, a subservice organization is your vendor's vendor. These subservice organizations perform some of the services provided to user entities that are likely to be relevant to controls over financial reporting.

A typical example would be the bill payment provider that is actually performing and delivering the bill payment service included as part of your internet banking contract.



SUITABILITY OF DESIGN

The Auditor will determine if controls are suitably designed and will provide reasonable assurance that the control objective(s) are achieved.

TEST OF CONTROLS

The procedure that evaluates the operating effectiveness of control activities necessary for achieving the control objectives stated in management's description of the service organization's system.

TRUST SERVICES CRITERIA

1. **Security.** The system is protected against unauthorized access (both physical and logical).
2. **Availability.** The system is available for operation and use as committed or agreed.
3. **Processing integrity.** System processing is complete, accurate, timely and authorized.
4. **Confidentiality.** Information designated as confidential is protected as committed or agreed.
5. **Privacy.** Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice and criteria set forth in *Generally Accepted Privacy Principles* issued jointly by the AICPA and the Canadian Institute of Chartered Accountants.

TYPE I REPORT

A Type I report includes the System Description and Management Attestation concerning the presentation and design of controls within the service organization. Type I reports audit controls as of a point in time.

TYPE II REPORT

It's only with a Type II report that the auditor validates that the stated controls are in place and reports on the effectiveness of the controls over a period of time (how well they're working). Generally speaking, controls must be in place for at least six months in order for a Type II report to be issued.

USER ENTITY

As the client of the service organization, you're the user entity.

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

(270) 506-5140 | venminder.com

About Venminder

Venminder is a leading third party risk management provider dedicated to helping the financial services industry mitigate vendor risk.

Venminder's team of due diligence experts offer a suite of services that can significantly reduce the workload by addressing the tactical challenges of vendor management tasks. Venminder's vendor management software can guide a user through critical processes such as risk assessments, due diligence requirements and task management.