Managing Outsourced Risk:

How to Read a SOC 1 or SOC 2 Report

By Audrey Katcher, Jennifer Zanone – ISSA member Denver Chapter**, and Christine Figge**

This article will help you better understand how a System and Organization Controls (SOC) report from a service organization can help you better manage the risk that your company outsources on a regular basis.

While your organization may outsource services or technology, risk is never completely outsourced. Your organization works in a ***shared risk responsibility environment*** with the entities you rely on. A System and Organization Controls (SOC) report is an audit report provided by independent, third-party auditors (service auditors) that looks at things like controls related to financial reporting or related to an organization's security, processing integrity, confidentiality, privacy, or cybersecurity. These audits are performed by certified public accountants (CPAs).

The following article will help you better understand how a SOC report from a service organization can help you better manage the risk that your company outsources on a regular basis. Entities you rely on are referred to as *subservice organizations*, and your organization as a user of the report is referred to as a *user entity*.

As a senior-level security leader, the table below is an overview of the article to allow you to reference your team to the sections that may be relevant to your organization during different situations. A good practice is to assign a team lead to obtain and monitor SOC report content for the key entities you rely on for security at least annually. Also, it is helpful to develop a consistent scorecard for SOC report monitoring.

Introduction to SOC reports

It is important for user entities to understand the basics of SOC reports before jumping into the details of the various sections of a report and how those sections might impact a user entity's risk analysis. A SOC report is the result of an independent CPA examination of a service organization's system. Use of SOC reports is restricted to specified parties, unless noted below. There are several types of SOC reports:

FOCUS AREA	RELEVANT SECTION
• My client/prospective client is requiring a SOC report – which one is necessary? • I'm relying on a SOC report; which one do I want to rely on? • If the service auditor's opinion has the words "In our opinion, except for …" included, it is a qualified opinion that indicates a failure of controls, which is broad and requires further investigation, if this is an area important to your business.	**Introduction to SOC Reports**
• Is there an issue with the service provider? • Did the report cover services I rely upon? • Does the report cover my areas of concerns/requirements	**How to Read a SOC Report** Section 1 - Independent Service Auditor's Report
• Does this report cover the system(s)/services our organization utilizes? • Did something change at the service provider that could put our organization at risk? • Are there other service providers involved and what is their control effectiveness? • What controls remain the responsibility of our organization?	**How to Read a SOC Report** Section 3 - Description of the System
• Are these the controls we actually rely upon for our requirements? • Did a control break that puts my organization at risk?	**How to Read a SOC Report** Section 4 - Test of Controls & Results

1. **SOC 1 – SOC for Service Organizations: ICFR** [1]. Service organizations may provide services that are relevant to their customers' internal controls over financial reporting and, therefore, to the audit of financial statements of the user entity.
   - Note that the control objectives of a SOC 1 report are defined by the service organization based upon the services they provide to customers.
2. **SOC 2 – SOC for Service Organizations: Trust Services Criteria** [2]. Service organizations may provide services that are relevant to the security of a system or to the privacy of information processed by a system for customers. This report covers controls over one or several of the trust services categories of security, availability, or processing integrity of a system or the confidentiality or privacy of the information processed by the system.
   - Note that the controls are defined by service organization management to meet their service commitments and system requirements based on the applicable trust services criteria. The common criteria constitutes the complete set of criteria for the security category and the other trust services categories include the common criteria plus additional category-specific criteria.
3. **SOC 3 – SOC for Service Organizations: Trust Services Criteria for General Use Report** [3]. Although the requirements and guidance for performing a SOC 3 examination are similar to a SOC 2 examination, the reporting requirements are different. Because of the different reporting requirements, a SOC 2 report is appropriate only for specified parties with sufficient knowledge and understanding of the service organization and the system, whereas a SOC 3 report is ordinarily appropriate for general use.
4. **SOC for Cybersecurity** [4]. As part of an entity's cybersecurity risk management program, an entity designs, implements, and operates cybersecurity controls. This is an engagement where a service auditor examines and reports on a description of the entity's cybersecurity risk management program and the effectiveness of controls within that program.
5. **SOC for Supply Chain** [5]. As part of an entity's system that produces, manufactures, or distributes products or provides an intangible product such as a commercial off-the-shelf application, the entity designs and operates relevant controls. This report provides information to identify, assess, and manage risks when an entity relies upon a producer, manufacturer, or distribution company as part of its supply chain.

The SOC 1 and SOC 2 reports listed above will be the focus of this article and can be performed as a Type 1 or a Type 2 report.

- A Type 1 report indicates that the scope of the report reflects a test of design, which may include a test of one sample/transaction to validate that the control has been implemented.
- A Type 2 report indicates that the scope of the report reflects a test of operating effectiveness over a period of time to validate that the controls were implemented and effective for the duration of the examination period.

How to read a SOC report

The structure of a SOC 1 or SOC 2 report (the most common reports), generally include the following sections:

Section 1: Independent service auditor's report

If the service auditor's opinion has the words "In our opinion, except for …" included, it is a qualified opinion that indicates a failure of controls that is broad and requires further investigation.

Section 2: Service organization's assertion

When reading a SOC report, it is helpful to know that the language presented in management's assertion is "standard" language your SOC auditor may help interpret. Should that wording be altered, it's important to understand the implications of that change.

Section 3: Description of the system

The description of the system is a narrative written by the service organization describing the information about the organization's system a) relevant to the user entities internal control over financial reporting (SOC 1) or b) including process overviews in accordance with the description criteria [6] (SOC 2). This section will also describe user entity and subservice organization control responsibilities.

Section 4: Test of controls and results

This section includes controls defined by the service organization and tests and results of tests defined by the service auditor. In this area you will need to identify the controls relevant for mitigating your risk and then identify if any of those controls have exceptions.

Section 5: Other information

Other information is an optional section of the SOC report that is presented by the service organization; the information contained in this section is not audited by the service auditor. The information contained in section 5 is information that the service organization believes to be relevant to user entities in general.

In the following section, we expand on common considerations when reading a SOC report. This information is not inclusive for every scenario. We highly recommend obtaining a SOC 1 or SOC 2 guide from the American Institute of Certified Public accountants (AICPA). Note that the SOC 2 guide has an appendix with information for service organization management, and both guides include sections for service organization management responsibilities.

The best place to start when reading a SOC report is section 1, paying attention to the audit opinion.

Section 1 – Independent service auditor's report

The service auditor's report will help the reader gain an understanding of the report scope, including the name of the system, the examination period covered by the report, the auditing firm, and service auditor conclusion (i.e., the opinion). It is the responsibility of the user entity to verify that the systems covered by this report (which is also clarified in section 3) are the same as the services utilized by the user entity (e.g., did you obtain the correct SOC report for the services you subscribe to from this service organization?) and that the examinations covered by this report are relevant for the period of time the user entity utilized the services of this service organization (e.g., were you a customer of this service organization during the period of this examination?).

The service auditor's report also discloses the auditing firm who performed the examination (e.g., is the audit firm that performed the examination reputable?) and the overall conclusion that the service auditor reached. An *unqualified* opinion is also known as a "clean" opinion with no "significant" findings and a *qualified* opinion (where the use of the term "except for" is present) is one where user entities may want to do more research (often looking to section 4 – Test of Controls and Results) to understand why the service auditor expressed concerns over certain areas of the examination and could not conclude that the all of the controls included in this report were operating effectively. When evaluating the opinion of a SOC report, a user entity can begin to understand risk impacts to its own organization utilizing the elements presented above.

SOC Report Consideration Section 1	Common Risk Response *(this may not be THE risk response for your organization)*
Confirm that the in-scope system matches the services provided to the user entity by the service organization.	If yes, **LOWER RISK** to the user entity
Confirm that the in-scope examination period matches the services provided to the user entity by the service organization.	If yes, **LOWER RISK** to the user entity
Is the report unqualified?	If yes, **LOWER RISK** to the user entity
Is the report qualified?	If yes, **HIGHER RISK** to the user entity
Is the report adverse or disclaimed?	If yes, **HIGHER RISK** to the user entity
If Type 2, is the report period shorter than three months?	If yes, **HIGHER RISK** to the user entity

Section 3 – Description of the system

The description of the system presented in section 3 of the report provides user entities with insight into the scope of services and control environments covered by this report, and in the case of a SOC 2, the system boundaries and other information required by the AICPA description criteria. As section 3 is written by the service organization and differs between SOC 1 and SOC 2, the order of these headers may change. Key areas to pay attention for risk evaluation include the following.

Significant changes

Significant changes described will give you an understanding of what has changed at the service organization during the examination period that could have had an impact on the scope of this report. It is important to evaluate whether these changes had/have an impact to the services your entity subscribes to. Generally speaking, the greater impact the changes disclosed have on the service organization and their control environment, the greater likelihood that there is a higher degree of risk for user entity consideration.

Subservice organizations

Subservice organizations are service providers to a service organization that are key in order to meet the control objectives in a SOC 1 report or to meet service commitments and system requirements in a SOC 2 report. Common subservice organizations can include data center hosting providers (e.g., colocation facilities) or software-as-a-service providers. The more subservice organizations that are presented in this section, the more the service provider has outsourced some of its operational risks to other entities. As such, user entities will want to understand whether subservice organizations have relevant SOC 1 or SOC 2 reports and whether the subservice organizations are treated under the inclusive method or the carve-out method for the purposes of the examination.

- Utilizing the inclusive method means that audit procedures performed by the service auditor include procedures specific to the subservice organization, meaning the service auditor is performing procedures for both the service organization and the subservice organization.
- Utilizing the carve-out method means that the procedures performed by the service auditor do not include the subservice organization, and the service auditor and the service organization are reliant upon monitoring procedures performed by the service organization to rely upon the controls of the subservice organization.

The fewer subservice organizations that are presented in this section means that the service organization has elected to perform most of the aspects of its business and/or controls independently. As a user entity, you may want to evaluate whether you feel it is appropriate for the services you have engaged.

Service organizations should include a narrative describing what processes and controls they have in place to monitor subservice organizations (e.g., risk assessments, audits, review of SOC or compliance reports, facility visits/walk-throughs). If your service organization has a large number of subservice organizations listed in their report without details of how

they monitor those subservice organizations, it is reasonable to request that they provide you additional control comfort if needed and/or include this information in future year SOC reports so that you, as a user entity, can evaluate whether the monitoring outlined in this section is in line with what you would expect for control reliance and/or in compliance with your service agreement.

Lastly, included as a sub-section of the report description are complementary subservice organization controls (CSOCs). CSOCs are relatively new in section 3 and are intended to communicate the specific control activities the service organization expects the subservice organization provider to have in place in order for the service organization to meet their control objectives or service commitments and system requirements. Please note that CSOCs have not been tested by the service auditor but are intended to communicate the nature of the controls that have been outsourced to a third party so if you, as a user entity, feel that the scope of services provided by the subservice organization is significant to your organization, you can reach out to your service provider or the subservice organization to obtain a copy of their SOC report or create appropriate alternative procedures.

Complementary user entity controls (CUECs)

This section of the description was written specifically for you, the user entity of the service organization. It outlines the controls that the service organization anticipates each of its user entities to have in place, such that the combined controls of the service organization and the user entity work together to meet the control objectives or trust services criteria. As the controls are designed to work together between the service organization and user entity, it is important for user entities to understand this section well. Each user entity should perform an exercise to map each of the controls listed in the CUECs to controls at your own organization to evaluate whether the controls in place at your own organization are in alignment with the CUECs. Further, user entities should evaluate whether their own controls are designed and operating effectively to understand whether the controls identified effectively address the responsibilities outlined in the report.

Relevant aspects of the control environment, risk assessment process, information and communication systems, and monitoring of controls

This section is included to provide an understanding of the governance and controls environment at the service organization. This narrative provides more detail and context as to how the service organization operates, its structure, etc. The following control components should be covered: information, communication, and monitoring activities, control environment, risk assessment, and control activities. Most often, control activities are sprinkled through these sections, so if you have questions pertaining to how the service organization handles certain operations or processes (e.g., risk assessment, organizational structure, employee training, security monitoring), come here to gain a more thorough understanding.

SOC Report Consideration Section 3	Common Risk Response *(this may not be THE risk response for your organization)*
Have there been significant changes to the report scope and/or service organization that impact the services provided to you as a user entity?	If yes, **MODERATE RISK** to the user entity
Are the subservice organizations presented in the report in line with what you would expect based upon the nature of services you receive from the service organization?	If yes, **MODERATE RISK** to the user entity
Are the subservice organization monitoring procedures presented in the description in line with what you would expect based upon the nature of services you receive from the service organization?	If yes, **LOWER RISK** to the user entity
Do the subservice organizations have SOC reports that are reviewed by the service organization?	If yes, **LOWER RISK** to the user entity
Can you map each of the CUECs presented in the description to one of the controls at your organization AND the mapped controls from your organization do not have exceptions?	If yes, **LOWER RISK** to the user entity
Are there exceptions noted in one of the controls mapped from your organization to the CUECs presented in the description?	If yes, **MODERATE RISK** to the user entity. Obtain an understanding of what caused the exception and evaluate the impact of that exception on your control environment
Are there control gaps when mapping controls from your organization to the CUECs presented in the description?	If yes, **MODERATE RISK** to the user entity. These gaps may be preventing you from control reliance.

Section 4 – Test of controls and results

Section 4 of the report presents the controls (defined by the service organization to meet control objectives or trust services criteria) that were tested as part of the SOC examination by the service auditor, how each control objective or trust services criteria was met by certain controls of the service organization, and the results of the service auditor's examination. Because section 4 is usually presented in a common table format, it is easy to identify exceptions noted in the results of test column on the right hand side of the page. If not presented in a tabular format, carefully look for any exception wording and what controls the exception relates to. As you've already read through the service auditor's report, keep in mind the service auditor's overall conclusions.

Section 3 of the report gives the reader a narrative of management's system; however, section 4 is where you as a user entity can evaluate the controls that were actually designed and operating effectively. It is important to consider as you read through the controls as written and testing results, whether the controls that are presented in the report are in line with what you expected of the service organization based upon the services they are providing to you: did the service auditor perform sufficient levels of sample-based testing to show that the control was operational throughout the examination period? Are there any instances when the service auditor only tested via inquiry? How quickly is access removed for terminated employees? Is administrative access at the service organization restricted to a pre-defined or pre-authorized group of individuals? Does the service organization have controls defined for monitoring of subservice organizations?

Exceptions do not automatically qualify a report. If the control objectives or trust services criteria were met by other controls in support of the control objectives or trust services criteria, the service auditor's opinion can still be "clean."

Section 5 – Other information

Management may elect to respond to control exceptions in the report to provide additional insight into what happened or what the service organization did to remediate the control exception. Such management responses are most often presented in section 5 of the report. If the responses are in section 5, they are not attested to by the service auditor. Lastly, if there are exceptions/deficiencies in the current year report, consider pulling out a copy of the prior year report to evaluate whether the control deficiencies that occurred in the current year also occurred in prior years.

Summary

SOC reports are intended to be a tool utilized by user entities to enable control reliance and can contain a lot of valuable information if you know where to look. Note that the primary users of a SOC 1 report will be the accounting and finance department; for a SOC 2, the IT security management group.

To obtain a copy of a SOC report for a service organization you work with, you must request it from the service organization; they control the distribution of the report. You may request a report from a service organization before signing up for their service, to help evaluate the vendor. As an ongoing service organization client, you typically request the report annually as long as you are utilizing their services.

But remember, just because a service organization has a SOC report does not mean that you can rely on the controls of that service organization blindly, you still need to:

- Evaluate the service organization's services
- Evaluate the state of controls disclosed in the SOC report
- Perform your own risk analysis.

Common risk factors are summarized below:

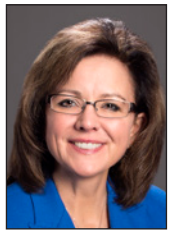
SOC Report Consideration Sections 4 and 5	Common Risk Response *(this may not be THE risk response for your organization)*
Were there exceptions disclosed in the test of controls?	If yes, **MODERATE RISK** to the user entity. Perform an evaluation of the impact of the exception to your organization.
Did the exceptions occur in prior years?	If yes, **MODERATE RISK** to the user entity
Did management remediate control exceptions and were the actions taken in line with what you would expect?	If yes, **LOWER RISK** to the user entity

Common LOWER Risk Factors *(this may not be THE risk response for your organization)*	**Common MODERATE/HIGHER Risk Factors** *(this may not be THE risk response for your organization)*
Unqualified opinion	Qualified/disclaimed/adverse opinion
Type 2 report (operating effectiveness of controls is tested)	Type 1 report (operating effectiveness of controls is NOT tested)
Period covered by the report closely aligns to the period relevant to you OR Period covered by the report does not necessarily align with your time frame, but the service organization has provided a bridge letter	Period is a point in time OR Period is short OR Period ends more than three months sooner than your relevant period
Fewer significant changes	Many significant changes disclosed in report
Established monitoring procedures in place over subservice organizations	Control environment described in section 3 does not seem to align with what you would expect for the services provided to you as a user entity
Your organization can map controls to each of the CUECs	Your organization does NOT have controls to map to CUECs
Controls tested align with controls you expected to mitigate risk as per agreements with the service organization	You expected certain controls to be tested, per agreements with the service organization, and they are not tested OR Controls are mostly carved out to subservice organizations and those entity's SOC reports have not been evaluated
Testing includes inspection, observation and/or re-performance	Testing is primarily inquiry
Management responses to control exceptions aligned with your expectations for the nature of services provided to you as a user entity	Exceptions noted with no management response or remediation plan
No exceptions or few exceptions identified with a documented management response/remediation plan	Recurring exceptions year over year

References

1. AICPA, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1) Guide*, Wiley (2017).
2. AICPA, *SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, Wiley (2018).
3. AICPA, "Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy" (2017) – https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf.
4. AICPA, "SOC for Cybersecurity"– https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html.
5. AICPA, "SOC for Supply Chain"- https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/soc-for-supplychain.html.

About the Authors



Audrey Katcher, CPA, CISA, CITP, has more than 25 years of experience, currently serving as a partner in RubinBrown's Business Advisory Services Group. Innovative services she leads include third-party assurance, cyber attest, System and Organization Controls (SOC and SOC1, SOC2, SOC3) services, and automation such as robotic process analysis. She may be reached at audrey.katcher@rubinbrown.com.

Jennifer Zanone, CISA, PMP, is a manager in RubinBrown's Business Advisory Services Group. She is an experienced compliance professional with a focus on IT risk, audit and general controls. She has managed SOC readiness assessments and IT controls testing for various clients. Jennifer has over 13 years of experience in IT consulting and may be reached at jennifer.zanone@rubinbrown.com.

Christine Figge, CPA, CGMA, is a partner in RubinBrown's Assurance and Business Advisory Services Groups. She has over 15 years of public accounting and consulting experience. She serves clients with her extensive System and Organization Controls (SOC) experience, knowledge of audit and compliance matters related to the mortgage banking industry, and by analyzing internal controls for public and private companies. She may be reached at christine.figge@rubinbrown.com.

The Open Forum

The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. Articles should be around 850 words and include a short bio and photo. Please submit to editor@issa.org.