venminder

HOW TO GUIDE
ANALYZING A SOC REPORT

WHAT IS A SOC REPORT?

In general, Service Organization Control (SOC) reports come from external audits of internal control environments for the services provided by a company. These reports provide information that your organization uses to assess and evaluate the risks associated with the outsourced service.

SOC reports are designed to help service organizations in compliance and due diligence efforts, promoting trust and confidence in their service delivery processes and controls.

WHAT A SOC REPORT IS DESIGNED TO ACCOMPLISH

SOC reports are designed to provide information to user entities (in this case, your organization) on three main things:

1. Controls a vendor has in place to protect their system
2. Controls that the user entity needs to implement to assist the vendor in accomplishing some of the controls
3. Independent testing of those stated controls providing assurance that the control environment is as presented

WHAT IS THE DIFFERENCE BETWEEN THE OLD SAS 70 VS SSAE 16?

For all intents and purposes, they are the same report. The framework which introduced the SSAE 18 in 2011 superseded the SAS 70 and added in more guidance to auditors and organizations.

THE DIFFERENT TYPES OF SOC REPORTS

	SOC 1	SOC 2	SOC 3
Type I	Audits controls as of a **specific point in time**. Covers internal controls surrounding financial reporting. Often used for newly established companies or companies with little history of operations to assess.	Affirms controls are in place for a **specific point in time**. Covers an organization's controls over one or more of the 5 Trust Service Principles: Security, Confidentiality, Availability, Processing Integrity and Privacy Often used by internet banking, mobile banking, bill payment and any vendor that stores or accesses consumer private information.	High level summary of a SOC 2 Type II. Publicly available and does not contain detail. Overview of the implementation of one or more of the 5 Trust Principles. Used for initial verification of due diligence. Not recommended as a report to assess vendor's security. Publicly attainable.
Type II	Audits controls over a period of time (usually 6-12 months). Includes a description of any significant changes. Often used by companies when there is little or no private consumer information shared.	Covers controls that were in place and evaluates whether they were operating effectively for a period of time (usually 6-12 months). Covers an organization's controls over one or more of the 5 Trust Service Principles: Security, Confidentiality, Availability, Processing Integrity and Privacy Often used by internet banking, mobile banking, bill payment and any vendor that stores or accesses consumer private information.	N/A

In general, you'll want to focus on a SOC 1 Type II report when your vendor is involved with the actual financial aspects of your organization. For example, if the vendor is providing a transactions processing service, a SOC 1 would be ideal. However, If that same vendor (processing transactions) uses a data center to house their equipment, you would want a SOC 2 Type II report as that is a service that is information systems centric versus financial systems centric. If both a SOC 1 Type II and SOC 2 Type II (we see this often) is provided by the vendor, then by all means, review both! There's no such thing as overkill when it comes to data security and processing integrity.

WHAT IS THE SCOPE OF THE REPORT?

Normally, there are two places where you can find the scope of the report you are reviewing. First, you'll find it within the "Independent Service Auditor's Report" section at the beginning of the report. Look for statements like, "We have examined [Vendor Name]'s accompanying Description of [Service Name]..." which will inform you of the primary focus of the audit. Another statement to look for here is, "Our examination did not extend to controls of the aforementioned (subservice organization/products/services)," meaning that those products or services were not included within the audit scope. You'll find similar wording within the vendor's "Management Assertion."

The second place to look for the audit scope is within Section 3 of the report. Search for a heading called "Scope of Report." This will give you a more in-depth explanation of the scope.

SIGNIFICANT SUBSERVICE ORGANIZATIONS

Just like you need a vendor to provide critical services, most of your vendors also need a vendor to provide critical services. In SOC reports, those third and fourth parties are called subservice organizations.

So why are they so important that they get their own section? Let's take the example of an online banking provider. In order to offer their products and services to you, they make some customizations to the interface for you and make it look like you want, but that entire environment you're working within is physically somewhere else. Many times this occurs with a subservice provider like a data center company. Now your customers are accessing your new online banking and the service goes down. Whose due diligence did you look at? Just the online banking provider? Or did you also review and assess the online banking provider's data center vendor? If you only looked at the online banking provider, you wouldn't know what protections are in place for your data, or the recovery time objective or recovery point objective, meaning how long are we likely going to be offline for and how much data did we lose, respectively. That's just one reason why significant subservice organizations are important.

WHAT TIME PERIOD DID THEY ANALYZE IN THE SOC REPORT?

Typical periods are January 1 through June 30 for a six-month audit period or October 1 through September 30 for a twelve-month audit period. This offset from January through December is because it takes two to three months to get the final report issued. One important disclaimer – any changes since then are not covered within the audit. A Gap or Bridge letter may be requested for additional comfort from management whether they know of any control changes, deviations or exceptions.

REVIEWING THE REPORT'S NARRATIVE

The narrative tells you about the vendor and products within scope of the audit. It should help answer concerns such as:

- Are the products and services you receive from this vendor covered in the SOC audit report you have in hand? Many vendors produce multiple SOC reports, just be sure you have the right one.

- Do they outline ways that they protect information, ensure transactions are accurate and ensure operations continue through a potential data or hardware loss?

In addition, while reviewing the narrative, you should determine the answers to a couple of crucial questions:

1. Do they have the right data protections in place?
2. How do they maintain operational control in the event of a data breach?

REVIEW THE CONTROL SECTION

Towards the bottom of SOC 1 and SOC 2 reports you'll normally find a list of controls called "Complementary User Entity Controls." These controls may be easy to scroll past, but these are some of the most important controls in the report. These controls are being passed to you from the vendor. In other words, inside the Complementary User Entity Controls section, the vendor is telling you that in order for their controls to be effective, you have to do your job to support those controls. Not doing so will absolutely have a negative impact and increase the risk to your organization. We've seen SOC reports with as few as 0 to 5 Complementary User Entity Controls but we've also reviewed many reports with over 30.

Tip: Complementary User Entity Controls are not required to be disclosed, but when that is the case, the vendor is stating that their controls are self-sustaining.

In regards to these specific controls, expect your regulator to:

- Ask to see a list of vendors where complementary user entity controls are identified in a vendor(s) SOC report, especially for critical and/or high risk products. This is your chance to demonstrate you read the audit and know where these special controls exist.

- Ask to see evidence of processes and/or procedures you have put in place to ensure you are executing internally on those controls.

- Be ready. We know this commonly happens during client exams.

ARE THERE ANY FINDINGS OR EXCEPTIONS ON ANY OF THE CONTROLS?

A significant finding is one that could have or could still pose a risk to the vendor to the point of internal systems being compromised by malicious outsiders. A common finding we see in our reviews concerns user management, specifically user terminations. We're reporting on findings showing months went by without administrative accounts being disabled or deleted. If that user were terminated and was malicious, you've just given extended access to someone with potential for malicious intent that has intimate knowledge of how your system works.

Exceptions are noted deviations from the documented control environment as discovered by the auditing entity. In other words, the vendor stated they have a control in place, the auditor tested it and "found" an exception.

You should review exceptions and determine if additional action is required. If the noted exceptions are severe enough the vendor may need to have increased monitoring in your vendor management program. Other actions may include reviewing previous reports to determine if a negative or positive trend is occurring within the vendor's environment.

OVERALL, HOW WELL DO THEY COVER THESE ITEMS?

Were there critical or high risk exceptions? You should develop a rating system for consistent reviews for all your vendors. This rating system should inform your overall risk assessment on the vendor and carefully identify any remaining risk associated with doing business with the vendor. The SOC report is only one element, although a very important one, in your overall risk assessment process.

ABOUT VENMINDER

Venminder has a team of due diligence experts who can significantly reduce your vendor management workload. The firm addresses the tactical challenges of vendor management tasks such as collecting compliance documentation, analyzing a vendor's financial health, deploying paralegals to assist with vendor contracts, reviewing a vendor's SSAE 18, monitoring a vendor's cybersecurity posture and much more. Venminder also has a software solution to organize, track and report findings to Senior Management, the Board of Directors and, ultimately, the examining bodies.

While you cannot outsource ownership of vendor risk, you can outsource the tactical work of assessing the risk.

Visit www.venminder.com for more information. If you would like to schedule a demo of Venminder software and services, click here or call (270) 506-5140. For vendor management resources visit Venminder's Resource Library.

Venminder has a team of CISSPs available to do a qualified review and analysis of your vendor SOC reports so that you can focus on the strategic decisions.

Download a free sample of our SOC Report Analysis now