Financial Institution Vendor Management

What you need to know about SOC Reports

2017 Edition

venminder

www.venminder.com

Contents

Introduction

The FFIEC IT Examination Handbook is very clear on examiner expectations regarding the due diligence and on-going oversight for your third-party providers.

> **Excerpt from FFIEC IT Examination Handbook, page 23 (updated November 2015)**
>
> **Third-party management program:** Due diligence and monitoring present valuable information on the third-party provider's control environment. This information is necessary to identify the risks in an institution's IT environment.

SOC audit reports are the best representation you can get from your vendor regarding the controls they have in place and how they are performing against those controls. But if you are not a subject matter expert on IT control environments, audit report formats or the auditor/tech language used for descriptions in the related documentation… well, it can be a bit daunting to read a SOC report and walk away with confidence that you understand the answer to the underlying question: Is my vendor handling my data in a safe, secure and responsible manner?

This e-book will assist you with enhancing your education level on SOC reports in a simple, easy to read and plain English (non-technical) approach.

And, remember, no question is a dumb question so don't hesitate to reach out to the staff at Venminder if we can offer any assistance. We'll be happy to answer your questions or even take the burden of the workload off of you if that's the right answer.

SOC 1, 2, 3 Understanding the Differences

As a financial institution you likely already understand that you should be asking many of your vendors for a SOC report, **especially your critical or high risk vendors**. Have you noticed that some vendors give you a SOC 1, others give you a SOC 2 and sometimes a vendor will give you both? A few may even give you a SOC 3. **There are big differences between the various types of SOC reports and the differences are not obvious to the uninitiated.**

First, let's go back a few years. You used to ask your vendors for a SAS 70 (Statement on Auditing Standards No. 70) report. Originally, the SAS 70 was intended to be an audit conducted over "internal controls over financial reporting." But, because the SAS 70 strayed far away from its intended use, the Auditing Standards Board of the American Institute of Certified Public Accountants created the SOC framework.

A SOC 1

The SAS 70 was replaced by an SSAE 16 (Statement on Standards for Attestation Engagements (SSAE) No. 16). Let's be clear. We're talking about the original definition of a SAS 70, not what it evolved into over the approximate 20 years it was in place in the market. The old SAS 70 and an SSAE 16 are very similar but the SSAE 16 has a few upgrades, like an attestation by a company's management confirming the described controls are in place and functional.

Oh, and by the way, a SOC 1 and an SSAE 16 are the exact same thing. Same book, different title – either one works.

So what does a SOC 1 cover?

A SOC 1 addresses internal controls that are relevant to a company's internal control **over financial reporting.** By definition, a SOC 1 (aka

SSAE 16) is designed to review a vendor's controls which could impact your financial reporting. These controls may include topics such as policies and procedures governing the vendor's delivery of products and services, logical security such as the use of strong authentication, physical security such as the layers of access controls surrounding Information Systems, and processing integrity such as transaction processing.

Additionally, there are 2 different types of SOC 1 reports - a SOC 1 Type I and a SOC 1 Type II. The difference? A Type I report audits controls as of a point in time (a specific date) by reviewing a single piece of evidence. A Type I report also includes a review of the suitability of those controls for the Vendor at that time. A Type II report covers controls that were in place and operating for a period of time, typically six to twelve months. A Type II report is always better than a Type I because it takes a sampling of evidence over the period of the audit for each control activity tested, providing a more thorough look into the Vendor's operations.

A SOC 2

Most of the time, this is probably the report you really want. It's most definitely the report you want from an IT type vendor. Unfortunately, because of the evolution of the old SAS 70 over the years, many folks erroneously believe that a SOC 2 report is the next level up from a SOC 1, and this couldn't be further from the truth. One is apples the other is oranges.

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

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

A SOC 2 is the only audit (and report) that defines a consistent set of criteria specifically around the products/services that a company provides (to you). If you want a measure of how your vendor provides a secure, available, confidential and private solution, there is only one way to get that assurance: ask for a copy of their independently audited SOC 2 report.

And just like the SOC 1, SOC 2 reports come in two different flavors. A Type I affirms controls are in place. A Type II confirms the controls are in place and are actually working. So, yes, SOC 2 Type II is the best representation of how well a vendor is doing when it comes to managing and safe-guarding your data. **However, keep in mind as you review that the controls are created by the vendor and tested by an auditor or CPA firm.**

A SOC 3

Once again, do not be fooled into believing that if a SOC 2 Type II is highly valuable that a SOC 3 must be the Grand Poobah of all SOC reports. It's not.

A lot of our clients would much rather have a SOC 2 Type II any day of the week over a SOC 3. While the SOC 3 is likely to have some of the components of a SOC 2, it's not going to be as comprehensive. Why? It's designed to be made available publicly (without the requirement of an NDA) so by nature it is less detailed/less technical and, therefore, will not contain the same level of otherwise critical information (to you) that a SOC 2 Type II contains. Basically, it's a high level summary of the SOC 2 audit that comes with a seal of approval that a vendor can post on their website.

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

Understanding a SOC 1 Report a Bit More in Detail

Let's re-look at a basic description of a SOC 1 report. **A SOC 1 describes the system of internal controls in place at a service organization which may affect your internal controls over financial reporting.**

If you are looking for a report that covers the service organization's systems and processes used to deliver the product/service you purchased from them, you have the wrong report. That is a SOC 2 report.

If you are looking for a report that is relevant to a vendor that processes financial transactions or you need assurance regarding the accuracy of finances (payment processors, payroll processors, etc.) then a SOC 1 would be appropriate.

Now that you have determined a SOC 1 is the right report for you, here are a few tips on how to read the report and draw conclusions.

1. IS THE REPORT A TYPE I OR TYPE II?

While both a Type I and a Type II will include a description of the system and the suitability of the controls defined in the control objectives in the description, there's a big difference between a Type I and Type II. Remember, a Type I covers a point in time and a Type II covers a period of time. The big difference between the two? Only a Type II will adequately test the controls.

2. WHAT IS THE SCOPE OF THE REPORT?

Look for the auditor's opinion section of the report. This will describe the scope of the audit and include the auditor's opinion of the result. Important stuff.

In this section you'll find a description of the products, services and locations covered in the report. Are these relevant to what the vendor is providing to your organization? More importantly, has anything important to you been excluded from the report? If the answer is no to the first question and yes to the second question, then the report is useless to you.

Also important to understand in this section is whether your vendor's vendor's (subservice organization) description and controls have been included. In most cases, they are not. In that case, look for the words "subservice organization" and review the surrounding content which will state whether controls were or were not included. If by chance they are covered, you'll likely find the words "inclusive." You'll care about this depending on what critical activities your vendor may have outsourced to another vendor. You may need to obtain a SOC 1 (or SOC 2) from your vendor's vendor(s).

3. WHAT DID MANAGEMENT INCLUDE OR EXCLUDE FROM THE REPORT?

Your vendor decides what will be audited and what will not be audited. It's entirely possible that if management is aware of issues or exceptions that they will elect to omit criteria from the audit. Look for language such as "except for" in the management assertion section of the report. Control objectives are defined by the vendor, not the auditor.

4. LOOK FOR THE COMPLEMENTARY USER ENTITY CONTROLS!

What's that you say? These are controls that support your vendor's control objectives that must be performed by you. In other words, your vendor is saying that the effectiveness of their controls rely on you doing your part by managing the controls they passed to you. You'll want to be aware of the complementary user entity controls and ensure you have implemented processes to cover them.

5. WHAT TYPE OF TESTING WAS USED?

Common testing types are inquiry, inspection, observation and re-performance. Be leery of reports where the only testing type was "inquiry." Inquiry should never be the only kind of testing performed, especially when the report covers a period of time.

6. UNDERSTAND THE TEST RESULTS

Look for a table. The control objectives, the description of the test and the test results are all included. Most importantly, look for management responses to the exceptions. Read the response and decide if you are satisfied with the answer. Did management include a remediation plan for the exception? Is it realistic and how much confidence do you have in their ability to correct? Remember, at this point the auditor is merely reporting. They will not issue an opinion on any management response.

The SOC 2 in More Detail

Do you need information about the products and services your vendor provides to you? For example, if you are hiring an Internet banking provider, shouldn't you care more how they control the privacy, security, availability, integrity and confidentiality of their data center facilities and server hosting? The answer is yes and that means you should be asking for a SOC 2 report. And remember, a SOC 2 is not the next level up from a SOC 1. They are two totally different animals.

A SOC 2 was designed for technology companies who are classified as service organizations. Examples would be data centers, IT managed services, Software as a Service (SaaS) vendors or other technology or cloud computing providers.

A SOC 2 REPORT COVERS THE 5 TRUST SERVICES PRINCIPLES:

1. **Security** – Is the service provider's system protected against unauthorized access?
2. **Availability** – Is the service provider's system available for operation as promised? (contractually or otherwise)
3. **Processing Integrity** – Is the service provider's system accurate and trustworthy?
4. **Confidentiality** – Is customer information protected?
5. **Privacy** – Is NPI used, retained, disclosed and destroyed in accordance with the provider's privacy policy?

Remember, SOC 2 reports also have two different types. A Type I merely says the controls are in place. But a Type II tells you if the controls are in place and if they're working!

Expect to sign an NDA to receive a copy of the SOC 2 report. SOC 2 reports are intended solely for the information and use of the specified parties –generally, the user entities and their auditors. They are not made public and your distribution of the report should be tightly managed on a need-to-know basis. After all, a SOC 2 is exposing detailed information about the very heart of how a vendor operates their business.

THERE ARE 3 MAIN SECTIONS IN EVERY SOC 2 REPORT:

1. Service Auditor's Report
2. Management's Assertion
3. Description of Systems

WHAT TO LOOK FOR:

In the Management Assertion section look for language that details what the report covers. You should be able to spot the products and services you receive from the vendor in this section. If not, the report is useless to you.

Look to see what Trust Services Principles (see above) are covered in the Service Auditor's Report section. It is not required that all five are covered. Management of the vendor is allowed to specify which criteria they want included in the report. It's not always indicative of a problem if all five are not covered, you should just be sure all your areas of concern are addressed.

Are your vendor's vendors (subservice organizations) covered? If you see language such as "inclusive," then at least one subservice organization is covered. If you see the words "carve-out," or "subservice organization" along with a statement that the subservice organization's controls are not included, then the audit did not include your vendor's third-party providers. If your vendor's vendors store or process customer data, then you'll need separate assurance from your vendor that their vendors are held to the same standard to which you hold your vendor.

Are there material exceptions that cause you concern? In the Service Auditor's Report section, look for words like "inadequate" or "misrepresentation." Big. Red. Flag. Also review any exceptions within the control testing section of the report.

Don't forget to pay particular attention to the "User-Entity" (that's you!) Controls. Often missed, this section is very important. The rest of the audit is about what the vendor will do to ensure safety, security, etc., but in this section the vendor is saying it's only good if you are doing your part by establishing processes and procedures to hold up your end of the bargain.

Finally, if you are looking for the best independent audit on a technology vendor, a SOC 2 is the only audit report that uses a pre-defined set of criteria regarding the services a vendor provides to you. Therefore, for critical or high risk technology vendors that either process, transmit or store customer data, a SOC 2 Type II is really the only answer.

CARVE-OUT METHOD

The controls at your vendor’s vendor (4th party) have been excluded from the SOC audit.

It is 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.

COMPLEMENTARY USER ENTITY CONTROLS

Every SOC report will 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:** 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.

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.

CRITERIA

The criteria defines whether the audit is a "Type I" or "Type II" examination.

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 (4th party) are included within the SOC report. Controls of the 4th party are presented separately from those of your vendor (3rd 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 or not management's assertion is accurate.

You should expect that issues or exceptions that have come to management's attention can result in management's assertion letter being modified. Look for "except for" or other exclusionary language that was added by management to the letter. It's not always about <u>what is</u> in the SOC audit. It can many times be about <u>what is not included</u> 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.

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. You should know that when you are a "potential" client of a vendor, this statement relieves the auditor of responsibility of the suitability of the report for the product or services that are being contemplated.

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.

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 financial institution.

SOC

A SOC (Service 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 (aka SSAE 16) 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 Principles (TSP).

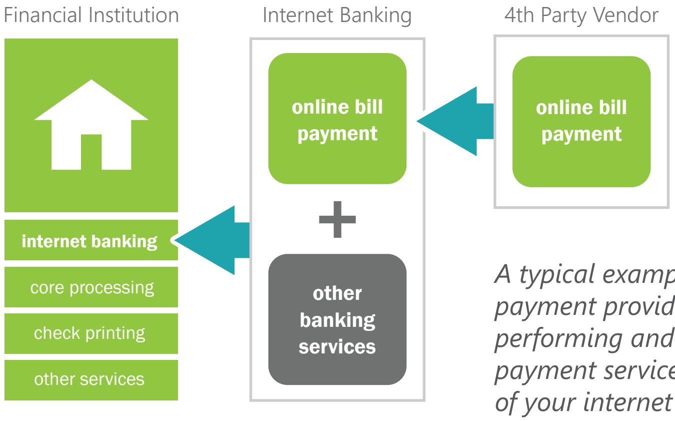
- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

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

If you are looking for a SOC report that covers IT controls, you need to ask for a SOC 2 report.

SUBSERVICE ORGANIZATION

Sometimes referred to as 4th parties, simply put, a subservice organization is your vendor's vendor.



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 PRINCIPLES

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. A public accounting firm obtains one sample per control activity and expresses the results of their testing.

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 are they 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 are the user entity.

About Venminder

venminder

Venminder provides a comprehensive suite of credit union and bank vendor management software and services to assess, monitor and manage third party vendor risks. With powerful, easy to use software and integrated/additional services, you can outsource some or all of the tactical side of your vendor management. Venminder's software and services are unique as they are broken down into modules, so you buy what you need, when you need it. In today's heavily regulated environment, the Venminder team, which consists of certified vendor management specialists (including in-house CPAs, paralegals, coaches and more), prides itself in solving the many challenges of meeting vendor management regulations. 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.