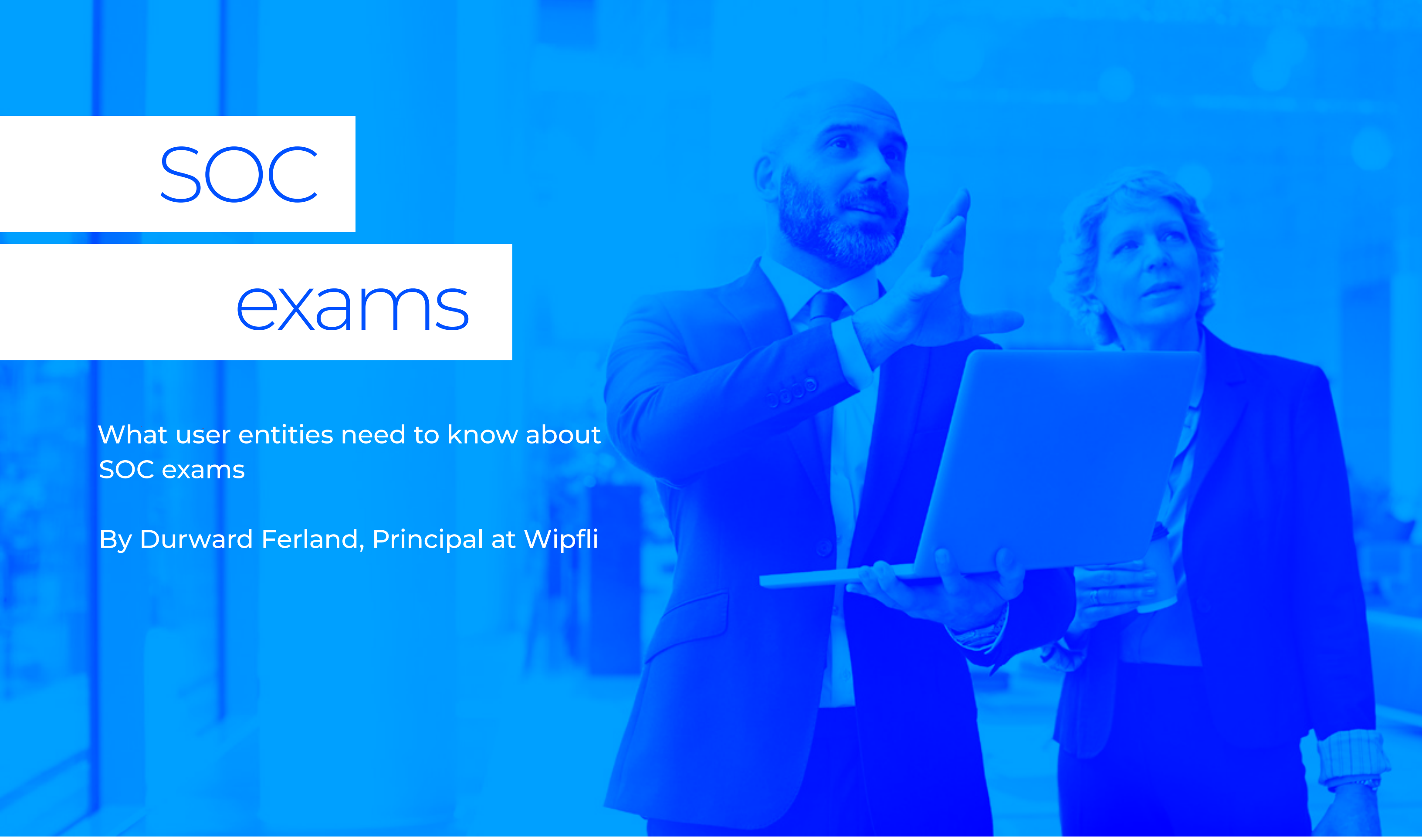


SOC exams

What user entities need to know about SOC exams

By Durward Ferland, Principal at Wipfli

Gain confidence in vendor controls

As the customer of a service organization, you rely on this vendor to provide valuable services. But you also rely on them to protect the system information they have access to.

You might have wondered before, does this vendor have strong internal controls in place? Are their employees following those controls? You also may have considered asking the vendor for proof that their controls are sound.

In fact, many companies conduct annual vendor due diligence activities, and they typically review the vendor's System and Organization Controls (SOC) exam report as part of that due diligence.

SOC for service organizations examinations allow service providers to give their customers a higher level of confidence in their processes and controls. But it's also on you, the user entity, to understand what a SOC exam is and how to read one.

In this white paper, we're going to cover what user entities need to know about SOC exams (also called SOC audits) — including what the different types of SOC exams are, when user entities should ask a service provider for a SOC exam, how to read a SOC exam opinion, what to do if a service provider doesn't have a SOC exam to review, and much more.

WIPFLI

Table of contents

Introducing the SOC exam

Introducing the SOC exam

The history of the SOC exam

SOC examinations are designed to help service organizations build trust in their service delivery processes and controls. A SOC exam does so through a report by an independent Certified Public Accountant (CPA) firm and by adhering to the standards of the American Institute of Certified Public Accountants (AICPA).

But they weren't always called SOC exams.

Back in April of 1992, the AICPA issued the Statement on Auditing Standards (SAS) No. 70, Service Organizations. The SAS 70 standard was designed to report on a service organization's internal controls related to its clients' financial reporting.

The SAS 70 standard was developed to be a communication between the auditor of a service organization and the auditor of a user entity. The user auditor could then rely on the SAS 70 exam to help plan and execute the user entity's financial audit. However, over the years, the SAS 70 standard became increasingly leveraged by user entities as part of their third-party due diligence of service organizations.

In January 2010, the AICPA issued the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. It was based on the International Standard on Assurance Engagements (ISAE) No. 3402 standard that was issued the month prior by the International Auditing and Assurance Standards Board (IAASB) — and it essentially updated SAS 70. Of note is how the SSAE 16 standard placed additional emphasis on the service organization's management description of its internal controls.

The term Service Organization Controls (which was later changed to System and Organization Controls) was introduced by the AICPA in May 2011, with the SOC 1 exam mapping to the SSAE 16 standard. The AICPA made this change because of the rise in how many businesses were outsourcing various functions to service organizations. The SOC 2 and SOC 3 exams were also introduced at this time.

According to the AICPA, cloud computing really spurred on this change. Because user entities provide service organizations with personal customer information to process or store, there is the potential for a breach in privacy practices. But the user entity is the one responsible for protecting that information even while it's in the service organization's hands — thus the demand for assurance that service organizations have the controls in place to keep this information confidential.

The old SAS 70 standard was designed around financial statement controls — not for reporting on controls that affect customer data and privacy. But because there was no better option, companies were using SAS 70 as a framework for doing so, and then calling themselves "SAS 70 certified." The AICPA's introduction of the SSAE 16 standard and the different types of SOC exams helped solved this problem by providing the necessary framework, as well as separating the distinct needs of organizations into the different SOC exam types.

In the past few years, there have been other notable changes. In 2017, the AICPA launched the SOC for Cybersecurity framework to standardize reporting on the effectiveness of cyber risk management controls.

In 2018, SSAE 18 replaced SSAE 16. The biggest change between the two is that SSAE 18 requires service organizations to implement controls that monitor the effectiveness of controls at subservice organizations they utilize.

Important definitions

Now that we've covered the history of SOC exams, let's move into defining the major players. This will set the stage for the next section, where we explain the differences between the types of reports and opinions.

Service organization: An organization (or segment of an organization) that provides services to user entities.

Subservice organization: A service organization used by another service organization to perform some of the services provided to user entities.

User entity: An entity that has engaged a service organization to perform services or transactions that are subjected to controls that may be physically and operationally removed from the user organization.

User auditor: An auditor who audits and reports on the financial statements of a user entity.

Service auditor: A CPA firm that reports on the controls of a service organization. This is the firm that performs the SOC exam.

This same year, changes were also made to SOC 2 reporting requirements. One big change was to restructure and align the Trust Services Criteria with the COSO framework.

In 2020, the AICPA released SOC for Supply Chain for entities that produce or distribute products to identify, assess and address supply chain risks.

Types of reports: SOC 1, SOC 2, SOC 3, SOC for Cybersecurity and SOC for Supply Chain

Depending on the type of assurance your organization needs, one of four different SOC exams will apply.

As the user entity, you will be asking the service organization for their SOC exam report, so it's important to familiarize yourself with what each exam type covers and thus know which one to ask for.

SOC 1

A SOC 1 examination is a report on a service organization's controls as they relate to a user entity's internal control over financial reporting. Essentially, it's what the old SAS 70 standard was used for.

SOC 1 reports are now prepared in accordance with the SSAE 18 standard. They are specifically intended to meet the needs of user entities and the CPAs who audit the user entities' financial statements, helping them understand the effect of the service organization's controls on the user entity's financial statements.

SOC 2

The AICPA developed SOC 2 Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Confidentiality, Processing Integrity, or Privacy to address the need for reports on controls other than those covering financial reporting.

Thus, a SOC 2 examination is a report on a service organization's controls that are relevant to any combination of the following: 1) security, 2) availability and 3) processing integrity of the systems the service organization uses to process users' data, and the 4) confidentiality and 5) privacy of the information processed by these systems.

Let's dive into these five Trust Services Criteria:

Security: The security criterion states that the service organization's system is protected against unauthorized access. It applies to all outsourced environments, particularly when enterprise users require assurance regarding the service organization's security controls for any system — financial or nonfinancial.

The security criterion is incorporated into the common criteria required for all SOC 2 exams because security controls provide a foundation for the other domains.

Availability: The availability criterion states that the service organization's system is available for operation and use as committed or agreed to by the user entity. It applies when user entities require assurance that the system will be available when they need it, including in a disaster. In fact, this criterion is most commonly requested when disaster recovery is provided as part of the standard service offering.

Confidentiality: The confidentiality criterion states that information designated as confidential is protected as committed or agreed to. This criterion applies when the user entity requires additional assurance regarding the service organization's practices for protecting sensitive business information and when a service organization is entrusted to maintain confidentiality of a customer's data.

Processing integrity: The processing integrity criterion states that the service organization's system processing is complete, accurate, timely and authorized and applies when such assurance is required.

Privacy: The privacy criterion states that personal information is collected, used, retained and destroyed in a way that conforms to the user entity's privacy notice and with criteria stated in generally accepted accounting principles (GAAP). This criterion applies when the service organization interacts directly with end users and gathers their personal information.

Examples of outsourced services relevant to a SOC 2 exam include cloud computing, data centers, managed security, hosted services and customer support.

Specifically, SOC 2 reports are often used for:

- Oversight of the service organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

SOC 3

A SOC 3 exam is foundationally similar to the SOC 2 exam. Like the SOC 2 exam, it's designed to meet the needs of users who require assurance about a service organization's controls that affect the security, availability and processing integrity of the systems used to process user information, and the confidentiality and privacy of that information.

However, a SOC 3 exam is used in place of a SOC 2 exam when the organization does not have the need for or the knowledge necessary to use a SOC 2 report. Notably, SOC 3 reports do not include a description of the system or the detailed description of the tests or test results that SOC 2 reports do. Note that a service organization must have a SOC 2 exam to get a SOC 3 exam.

Because these are general-use reports, SOC 3 reports can be widely distributed or posted on the service organization's website.

SOC for Cybersecurity

As mentioned in the history section, the AICPA created the SOC for Cybersecurity framework in 2017 to standardize reporting on the effectiveness of an organization's cyber risk management controls. The SOC for Cybersecurity report provides information to you as the user entity about the performance of the service organization's cybersecurity risk management program as assurance that your data is being protected by adequate controls.

SOC for Supply Chain

The AICPA released SOC for Supply Chain in 2020 as a voluntary reporting framework for entities that produce or distribute products. The report provides a common framework for these organizations to describe their supply chain risk management efforts.

Types of reports: Type 1 vs. Type 2

SOC exams deliver one of two types of reports: Type 1 and Type 2.

In a Type 1 report, the auditor reports on the fairness of the description of a service organization's system and on the ability of the design of its controls to achieve the related control objectives (SOC 1) or criteria (SOC 2 or SOC 3) included as of a specified date.

In a Type 2 report, the auditor reports on everything in a Type 1 report and also includes an opinion on the operating effectiveness of the controls to achieve the related control objectives (SOC 1) or criteria (SOC 2 or SOC 3) included throughout a specified period.

Type 2 exams can be more intensive for the service organization. However, they may provide a user entity with greater assurance on the effectiveness of the service organization's internal controls.

It's most common for service organizations to undergo a Type 1 exam for their first SOC exam. Control exceptions that are identified can then be used to strengthen the controls in place prior to undergoing the more extensive Type 2 exam.

A Type 2 exam covers a period of time, usually ranging from 6-12 months. The service organization typically has the exam cover a 12-month period, unless:

- There have been significant changes in controls during the last 12 months.
- It is a new company.
- The exam covers a new product or service that has not been offered for 12 months.
- A new customer has initiated a change in procedures.
- There is a new location or there are changes to the facility.
- There have been changes or turnover in senior management.

Service organizations are required to identify the time period the exam will cover. They typically use the following considerations to determine the time period to select:

- Whether the service organization wants the exam performed on or near major user entities' financial year-end
- Whether the service organization wants the exam performed on their own financial year-end date
- Whether the service organization wants the exam performed on or near the completion of a significant annual control
- Whether the service organization wants the exam to have a quarterly period end date (e.g., March 31, June 30, September 30 or December 31)

Types of opinions: carve-out vs. inclusive

If a service organization uses a subservice organization to perform services that would be covered under a SOC examination, management's description also needs to describe the subservice organization's involvement and its significance in providing those services.

There are two approaches to describing the nature and function of a subservice organization:

The carve-out method

Under this method, the subservice organization's relevant controls are excluded from the service organization's description of the system and from the scope of the SOC exam. However, controls at the service organization to monitor the effectiveness of the subservice organization's controls are included.

The carve-out method is typically used: 1) when the services provided by the subservice organization are not extensive or 2) when a service auditors' report on the subservice organization is available to user entities of the service organization.

If the vendor you're asking for assurance from is using the carve-out method of reporting, you should ask them for the subservice organization's SOC examination report as well.

The inclusive method

Under this method, the subservice organization's relevant controls are included in, but differentiated from, the service organization's description of the system and within the scope of the engagement. In other words, the SOC exam considers the controls at both the service organization and the subservice organization.

The inclusive method is typically used 1) when the services provided by the subservice organization are extensive and 2) when a service auditors' report on the subservice organization is not available to user entities of the service organization.

If the inclusive method of reporting is used, the service auditor must also obtain a written assertion from the subservice organization's management about: 1) the fairness of the presentation of the description of the subservice organization's system and 2) the suitability of the design and, in a Type 2 examination, the operating effectiveness of the controls.

Types of opinions: unmodified, qualified and limited scope

We covered above how Type 1 and Type 2 exams both involve an opinion from the service auditor on the fairness of the description's presentation. There are many types of opinions, but we'll dive into the three most common: unmodified, qualified and limited scope.

Unmodified

An unmodified opinion, commonly referred to as a clean opinion, states that the description of controls is presented fairly, the controls are reasonably designed and the controls are in place as of a certain date.

If it is a Type 2 exam, an unmodified opinion also states that the controls were tested by the service auditor and the controls were operating effectively over a certain period of time.

Qualified

A qualified opinion indicates that certain controls that were identified by the service organization were not reasonably designed, not in place as of the period end date or not operating effectively over a certain period of time.

A qualified opinion does not necessarily apply to all the control objectives (SOC 1) or criteria (SOC 2 or SOC 3) in the examination — only those identified in the qualification.

Limited scope

A limited-scope opinion indicates that the service organization chose not to have certain aspects of their control environment evaluated, and the service auditor believed that these aspects of the control environment are relevant to user entities. The opinion identifies those aspects the service auditor believed should have been included.

Helping user entities understand their SOC responsibilities

When you need to ask a service provider for a SOC exam

If your organization outsources business responsibilities, you remain accountable for managing the risk related to the services performed by the third party. Essentially, the security of your customer information and the integrity of the information processed remain your responsibility.

This makes reviewing a service organization's SOC exam report one significant way to help manage the potential risks that come from outsourcing services and gain assurance that the service organization's processes can be relied on.

If a service organization processes, handles or stores any of your data, you should ask them for their SOC exam report.

How to determine whether the scope is adequate and covers the services you use

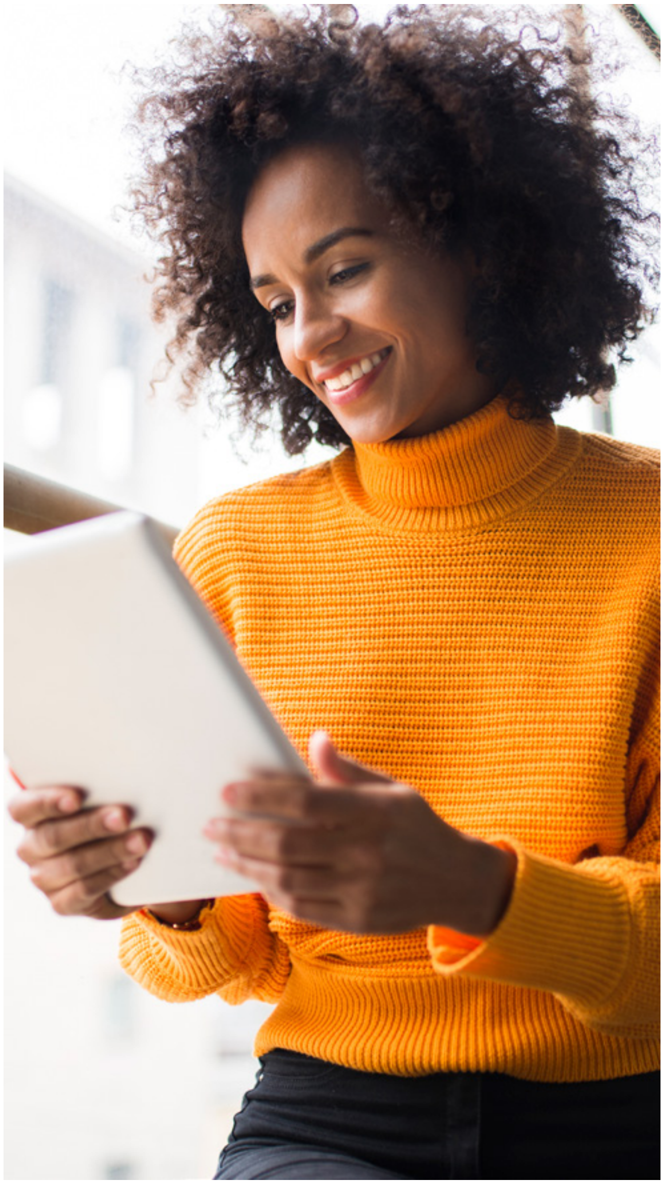
The scope of a SOC exam may vary depending on the control objectives or criteria, as well as the existence of any key subservice providers. Your organization should determine whether the scope of the report appears adequate to meet your assurance needs.

The scope of a SOC 1 exam is based on the control objectives selected by the service organization. Most SOC 1 reports cover their organization and administration, customer servicing, computer operations, software change management, logical security and physical security.

The scope of the SOC 2 and SOC 3 exams is determined by the criteria selected by the service organization. Refer back to the Types of reports: SOC 2 section in this white paper to review the five Trust Services Criteria that service organizations can select from.

To make sure the SOC exam report is relevant to your organization and adequately covers the vendor's services you use, it's important to review the products and services addressed by the exam. If your vendor uses a subservice organization to provide services that are relevant to internal controls, it's also important to understand whether the report uses the carve-out method or the inclusive method.

If you're reviewing a carve-out report, make sure to evaluate the impact of the services carved out to determine whether additional due diligence procedures are needed at your vendor.



How to read the SOC exam opinion

There is not a passing or failing score for a SOC exam. The results of the exam consist of several components, a few of which are shared with user entities. These are the opinion, the exceptions, the complementary user entity considerations and the complementary subservice organization controls.

The opinion

Earlier in this white paper, we covered the different types of opinions: unmodified, qualified and limited scope. An unmodified opinion is the ideal result you're looking for.

In the event of a qualified opinion, you are responsible for evaluating the qualified control objective(s) and determining the impact to your organization. You or the service organization may also have mitigating controls to limit the risk from the qualified control objective(s).

In the event of a limited-scope opinion, you are responsible for evaluating the scope limitations and determining the impact to your organization. You or the service organization may also introduce mitigating controls to limit the risk from the areas that were not covered in the SOC examination.

Exceptions

For each control identified in the SOC exam, the results of testing are presented in the report. The results of testing for that control will state, "No exceptions noted," or will state the identified exceptions.

When exceptions are identified, the details of the exception are presented for you to identify the impact of the exception on your organization. Individual exceptions may or may not impact the overall opinion — depending on the severity of the exception(s), the number of exceptions, whether the cause of the exception was an isolated problem or a systematic problem, and the impact of the exception on your organization.

When you review the SOC report for any exceptions, determine not only the impact of any you identify but also how the vendor plans to mitigate them (or if they already have since the SOC exam was performed).

Exceptions do not necessarily mean you should change vendors, so long as your vendor has detailed sufficient plans or responses to the exceptions. The key thing is that the exceptions were identified and can now be dealt with.

Complementary user entity considerations (CUECs)

CUECs are controls that your vendor has included within their system that they're relying on you to implement in order to achieve their control objectives. During the SOC report review, determine whether the CUECs are applicable to you and whether you have implemented them or need to do so to minimize your risk.

Complementary subservice organization controls

Complementary subservice organization controls are controls that your vendor has assumed are in place at their subservice organization and are necessary to achieve the control objectives or trust services criteria.

What a bridge letter is

Bridge letters (also called gap letters) are used by service organizations to bridge the time between their last SOC exam and your fiscal year-end, so you don't have to wait until the service organization's next SOC exam.

The bridge letter lists the SOC report end date, any changes the service organization has seen in their internal control environment since that date, a statement that management is not aware of any other material changes outside of those listed, and a disclaimer that the bridge letter relates only to that organization and does not replace the actual SOC report.

The letter is signed only by the service organization, not the service auditor who performed the SOC exam. The letter should also include the actual SOC report with it.

What else you should ask the service organization for besides their SOC exam

Reviewing the SOC exam is only one part of the overall vendor due diligence activities you need to perform when working with a service organization.

These vendor due diligence activities will vary based on the complexity of the services performed by the service organization and your experience with them. They often include activities such as obtaining an understanding of the service organization's financial stability, disaster recovery and business continuity planning activities and insurance coverage.

What to do if the service organization does not have a SOC exam

If your vendor does not have a SOC exam, or if the SOC exam does not cover the services you are using the service organization for, you should identify other methods to evaluate their internal control environment.

At a minimum, your evaluation should include the vendor's organization and management activities to ensure operational competency, computer controls over the daily processing and logical security of the systems related to your services, software change management and programming activities, physical security of the premises, and controls over the services the vendor is performing on your behalf.

You may choose to perform inquiries, observations and inspections of the policies, procedures and security safeguards at the service provider. You could also ask them for alternative audits, such as HITRUST or ISO 27001, or you could engage an auditor to perform an evaluation of the vendor's internal control environment on your behalf.

The benefits of a SOC exam

Since you're responsible for managing the risk of outsourcing services and giving vendors access to system information, it's critical to help manage potential risks.

By knowing how to read a SOC exam report and determine what information is relevant to your organization, you can help ensure you get the most value and assurance out of reviewing the report — and know you're in good hands with your vendor.

If you have questions about SOC exams and how they relate to user entities, Wipfli's SOC specialists are ready to answer them. Our professionals have extensive experience in performing SOC exams for service organizations of all types and can help you move forward with requesting a SOC exam from a vendor and analyzing the results.

wipfli.com/SOC