360ADVANCED

YOUR GUIDE TO

SOC EXAMINATION REPORTS

INFO@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

Table of Contents

What Is a SOC Examination?

A **System and Organization Controls (SOC)** examination is an independent, third-party assessment of a service organization's commitment to service and trustworthiness. For any company that intends to outsource a part of its business, such as payroll, record-keeping, or IT, it's a way to vet and gain reasonable assurance that potential service providers are operating under effective and safe controls.

SOC reports utilize independent, third-party auditors to examine various aspects of a company, such as:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy
- Controls related to financial reporting
- Controls related to Cybersecurity

The examination produces incredibly detailed and robust internal control reports that bring with them a number of benefits, including investor and shareholder confidence and the ability to minimize both potential security breaches and process waste.

The need for SOC reporting

The idea of controls auditing is not a new one. The SOC reporting process was created by the American Institute of Certified Public Accountants (AICPA) to keep standards on pace with the quick and prolific growth of outsourcing. According to the AICPA, the trend has been fueled by several factors[1], including the pressure to improve operational costs, a growing virtual workforce, and a lack of internal resources. Alongside outsourcing, there's a parallel trend toward cloud-based services that use the internet to send, receive, and store information. The model is cost-effective and simple for companies that outsource, but it also involves an inherent risk – transmitting potentially sensitive data to service organizations via the web. Because of the heightened risk of security breaches, and the liability that comes with it, the industry has demanded a higher level of scrutiny. Adherence to the SOC framework gives them the assurance they seek from their partners.

Who benefits from SOC examination reports?

For any company with a business model based on providing a service to another company, a SOC examination is a way to show that necessary controls are in place to handle sensitive data securely and accurately. A company that initiates a SOC assessment also gains the confidence that their data is more secure from a potential breach.

A number of service organizations are typically required to undergo a SOC assessment:

- Financial and payroll third-party providers
- Medical claims processors
- Data center companies
- Collection companies
- Customer support companies
- Prescription Benefit Management Service Providers (PBMs)
- Loan servicers
- Software as a Service (SaaS) providers that touch or impact financials or sensitive data of clients

However, any service-based company can benefit from SOC assessment. Industries such as tax-service providers, banks, investment firms, healthcare practices, and co-location services are most likely to demonstrate their commitment to security, availability, processing integrity, confidentiality, and privacy through SOC assessments. Any company that can't afford a data breach may require their service providers to demonstrate they have completed a SOC assessment.

The 3 Types of SOC Examination Reports and More

There are three main types: SOC 1, SOC 2, and SOC 3. There is also SOC for Cybersecurity, which we will cover later in this section. The correct one for your organization depends on its type, size, and the kind of services it intends to provide. **The biggest difference between a SOC 1 vs. SOC 2 report is the focus of examination.**

SOC 1

A SOC 1 report, also known as a Statement on Standards for Attestation Engagements (SSAE) 18, is an assessment which focuses on an organization's internal controls relevant to financial reporting. It is used to demonstrate the effectiveness of their internal controls over financial reporting, particularly for entities handling financial transactions. SOC 1 reports are typically requested by user entities, such as auditors and regulators, to gain assurance about the integrity and reliability of financial information processed by service organizations.

SOC 1 Report: Type 1, Type 2

The SOC 1 report can be either Type 1 or Type 2. Generally speaking, a Type 1 examination is an inquiry and observation of an organization's controls as of a single date in time – no testing matrices are included, rather a listing of controls. A Type 2 examination consists of the inquiry and observation *as well as testing* the operating effectiveness of the controls over a period of time, and therefore provides a more thorough validation.

Specific to the SOC 1 report, a Type 1 examination presents an assessment of whether an organization's internal controls have been effectively designed to meet certain control objectives over financial reporting as they relate to its provided services. It establishes the design of the system of controls and assists the organization's management in improving the capability maturity of its core processes so that it can be prepared for a SOC 1 Type 2 examination.

The SOC 1 Type 2 examination includes all the objectives of the Type 1 examination, as well as an opinion about whether the controls were operating effectively to meet the specified control objectives over a specific period of time. The results of testing are included within matrices which detail each relevant control. It's conducted in a manner that promotes management to focus on continuous process improvement and adaptation to changing industry circumstances and the client company expectations.

A real-world example of a SOC 1 Type 2 assessment

There are many situations that can initiate a SOC assessment. The service provider may proactively strive to meet their control objectives, or the "user entity", or company hiring the service provider, may request one before confirming a partnership.

If a major healthcare organization decides to outsource its payroll, for example, it would request a SOC assessment of the third-party service provider.

SOC 2

A SOC 2 examination report is for service organizations whose user entities do not necessarily rely on controls for financial reporting purposes, but do **require a maintained controlled environment** for things like storing third-party data, IT systems management, or data co-location. It offers an assessment of the design and operating effectiveness of an organization's controls to protect the business partners' intellectual property. SOC 2 reports are based on the Trust Services Criteria and include one or more of the 5 categories outlined below:

Security

According to the AICPA, Security includes protection against "unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives."

Privacy

Personal information is collected, used, retained, disclosed, and disposed of in conformity with both the user entity's privacy notice and the Generally Accepted Privacy Principles used by both the AICPA and the Canadian Institute of Chartered Accountants (CICA)

Availability

The system is available for its agreed-upon use

Processing Integrity

Processing is complete, accurate, timely and authorized

Confidentiality

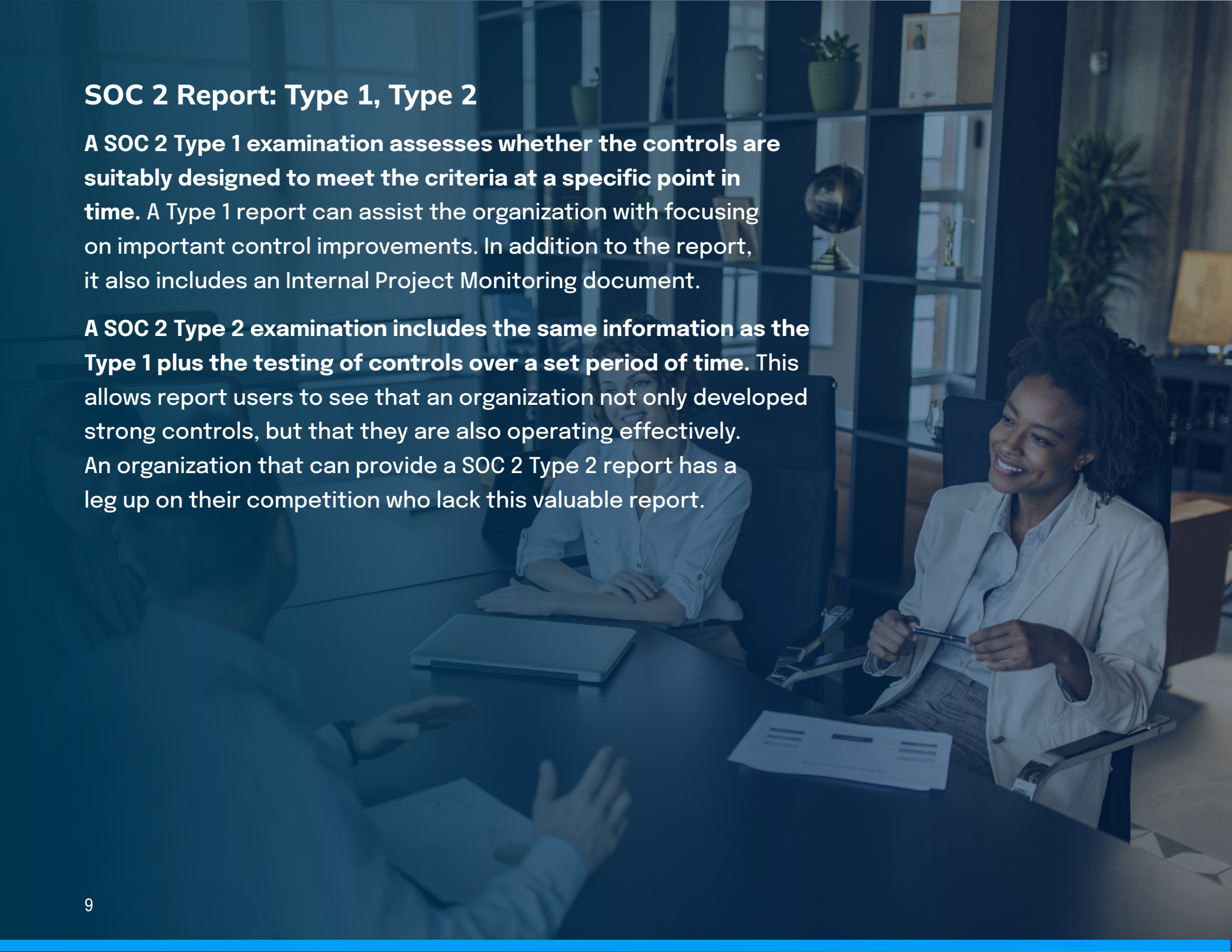
Confidential information is protected to the agreed-upon level

A SOC 2 report must include the Security category, also referred to as the common criteria, as a minimum requirement. However, it has the flexibility to incorporate any other combination of relevant categories listed above, as determined by management, to align with their industry standards and business needs.

SOC 2 Report: Type 1, Type 2

A SOC 2 Type 1 examination assesses whether the controls are suitably designed to meet the criteria at a specific point in time. A Type 1 report can assist the organization with focusing on important control improvements. In addition to the report, it also includes an Internal Project Monitoring document.

A SOC 2 Type 2 examination includes the same information as the Type 1 plus the testing of controls over a set period of time. This allows report users to see that an organization not only developed strong controls, but that they are also operating effectively. An organization that can provide a SOC 2 Type 2 report has a leg up on their competition who lack this valuable report.



What's the difference between SOC 1 and SOC 2?

Trust a compliance and assurance company to help you define which SOC report is right for your company.

SOC 1	SOC 2
Report Purpose Provides service providers with information and a service auditor's opinion about controls at said provider organization that are likely to be relevant to user entities' internal control over financial reporting.	**Report Purpose** Provides users with information and a service auditor's opinion about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy.
Intended Users Management of the service organization, user entities during some or all of the period covered by the report (for type 2 reports) and user entities as of a specified date (for type 1 reports), and auditors of the user entities' financial statements.	**Intended Users** Management of the service organization and specified parties who have sufficient knowledge and understanding of the service organization and its system.
Report Components a) Management's description of the service organization's system b) A written assertion by management of the service organization about whether, based on the defined control objectives, (i) management's description of the service organization's system is an accurate representation that was designed and implemented throughout the specified period (ii) the controls related to the control objectives stated in management's description of the service organization's system were suitably designed throughout the specified period to achieve those control objectives, and (iii) the controls related to the objectives stated in management's description of the service organization's system operated effectively throughout the specified period to achieve those control objectives.	**Report Components** a) Management's description of the service organization's system b) A written assertion by management of the service organization about whether, based on the defined categories (i) the description of the service organization's system that was designed and implemented throughout the specified period in accordance with the description criteria, and the controls stated in the description of the service organization's system And that the controls stated in the description of the service organization's system: (ii)were suitably designed throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria, and (iii) operated effectively throughout the specified period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable Trust Services Criteria.

Other SOC reports

Additional, more specialized versions of SOC reports are also available for user entities who have different needs.

A **SOC 3 Report** – formerly known as a SysTrust or WebTrust – like a SOC 2, is a highly specialized examination designed to evaluate system reliability through several areas of an organization, including security, availability, processing integrity, confidentiality, and/or privacy. The primary difference from a SOC 2 is that SOC 3 excludes the results of testing and certain other specific information within the description in order to make it available for general use, e.g., an organization can share this report on their website and generally distribute it freely.

A **SOC for Cybersecurity** is an engagement that reports on an organization's cybersecurity risk-management programs across the enterprise. In an age of ever-increasing reports of cyber attacks, it provides objective assurance that controls are in place to manage a cyber attack.

Initiating a SOC Examination

AICPA rules stipulate that the user entity – the company hiring the service provider – is responsible for assessing and addressing the risks they face related to financial reporting, compliance with laws and regulations, and operational efficiency and effectiveness, regardless of who performs them. When an organization contracts with a third-party service provider for any key processes or functions, it doesn't dissolve the company of the compliance responsibility.

This makes it essential for companies who intend to do any type of outsourcing to obtain reassurance that they can trust their partners – especially those in high-risk, volatile areas. SOC reports can provide this, but the process of requesting, obtaining, reviewing, and validating the reports is also the obligation of the user entity.

In summary, if your organization outsources its financial processes, record-keeping, or IT, you should inquire with a compliance vendor if a SOC assessment is necessary.

To request a SOC examination report from your vendors

First, determine which type of report you'll need (you may need different types from different vendors). For established partners, the request should be sent to the vendor via phone or email from your organization's day-to-day contact. You also may consider outsourcing requests to a third party specializing in SOC assessments, who will handle everything from the first request through the documentation on your behalf.

For new and potential vendors, consider being proactive by making mandatory SOC compliance a part of your contract.

Proactive SOC examinations

A third-party service provider can initiate a SOC assessment to show compliance in advance of winning a new contract. A SOC report can demonstrate that you company has the necessary controls in place to handle sensitive data securely and accurately. In a crowded marketplace, it can also help a company rise above the competition.

Choosing Your SOC Examination Report Provider

As the number of SOC reports grows, so does the list of providers who conduct them. Several factors are important when choosing the right provider for you, and the most important is this:

> The company who completes your SOC 1 or SOC 2 assessment **MUST be a licensed CPA firm.** SOC reports are governed by the AICPA (American Institute of Certified Public Accountants) and are not allowed to be issued by anyone other than a licensed CPA firm.

Why? Because your provider must include the Auditor's Opinion for your report to be complete:

- Management's Assertion
- Auditor's Opinion
- Description of Services
- Testing Results (for Type 2 reports)

Only certified CPA firms can provide legitimate opinions on the contents of the two latter sections. In fact, even CPA firms can't conduct SOC assessments unless they are verified to be independent.

In addition, non-CPA organizations are not allowed to partner with CPA firms to perform the assessments. That's not to say the auditing organization can't enlist the help of subject-matter experts, but strict requirements must be met.

All of this is to hold the examination process itself to the same stringent standards as the assessments themselves. As your company is responsible for assuring compliance, it pays to do your due diligence when researching a SOC assessment and report provider.

Preparing for Your SOC Examination

Whether an assessment begins as a request from a client or a proactive measure, the **first step is usually to undergo a SOC Readiness Assessment.** For the SOC 1, SOC 2, and SOC for Cybersecurity reports, this preliminary assessment identifies specific controls and any gaps that could hinder the achievement of objectives/criteria during the assessment. It also provides specific, actionable guidance for management to make decisions about improving weaknesses and maintaining your system of controls.

During the assessment, you'll lay out a thorough explanation of exactly what your business is and what services it offers. It will help narrow your focus and get to answers more quickly during evaluation and testing.

Next, you'll delve into the details of your services – processes, support systems, and areas that are most critical to your clients' reassurance. It also will help weed out extraneous information that isn't applicable to your relevant services.

Finally, you'll get into the nitty-gritty of pinpointing key controls and gaps, such as controls that are ineffective or missing completely. This is a critical step because those deficiencies are what will keep you from achieving compliance.

A Different Kind of SOC Examination Report Experience

A Type 2 examination can last up to a year, causing a strain on a company's time and resources. **Hiring an audit firm that focuses on SOC assessments to manage every step of the way can ease the burden** of having to manage such a large undertaking solo, especially for small businesses.

Discover what our clients already know: 360 Advanced solutions strengthen your compliance strategy and offer peace of mind to your clients.

Sources:
(1) https://www.aicpastore.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2012/CPA/Jun/Easy123.jsp