WINDHAM BRANNON
offering more

SOC FAQs

Introduction: What are SOC® Examinations?

An Independent Systems and Organization Controls (SOC) report provides independent verification on third-party vendors' systems and controls. There are three main categories of SOC reports: SOC for Service Organizations, SOC for Cybersecurity and SOC for Supply Chain.

Leaders of service organizations have an opportunity to demonstrate trust and transparency with customers with SOC examinations. Committing to strong control systems is a safeguard for the organization as well as the businesses it works with. And with cybersecurity as an ever-increasing threat, now is the time to proactively address and manage risks before a breach occurs. Because data security is a key component of SOC examinations, they give organizations a competitive advantage in attracting and retaining customers.

What is a SOC 1® examination and what are the different types?

A SOC 1® examination is designed to assess whether the internal controls of service organizations are suitably designed and effectively operating to address financial reporting risks. SOC 1 reports are typically performed for payroll, medical claims processing, loan servicers, and SaaS companies that provide a service with a financial reporting impact. SOC 1 reports are "restricted use" reports commonly used by service organization customers, management and auditors.

There are two types of SOC 1 reports. Type 1 documents and describes controls as of a specific date. It tests the design of controls but does not seek to evaluate their effectiveness. Type 2 reports cover a specified period, usually at least six months, and not only describes internal controls, but also evaluates how well they're working.

What is a SOC 2® examination and what are the different types?

SOC 2® examinations are broader and are designed to address a service organization's controls as they relate to the American Institute of Certified Public Accountant's (AICPA) Trust Services Criteria. The Trust Services Criteria includes availability, security, processing integrity, confidentiality and privacy. SOC 2 reports are important to ensure organizational and regulatory oversight, vendor management, internal corporate governance and risk management. SOC 2 reports are used by external stakeholders and those charged with governance.

Like SOC 1 examinations, there are two types of SOC 2 reports. Type I assesses whether the system design and presentation are fair at a specific point in time. Type II also evaluates fairness but also attests to how well the controls are operating. Type II reports are performed for a reporting period versus a specific point in time.

What is a SOC 3® examination?

SOC 3® examinations are less comprehensive and easier to read than SOC 2 examinations but still focus on the Trust Services Principles; specifically, controls associated with one or more Principles are evaluated. SOC 3 examinations are often used in marketing efforts and are ideal when external users don't need to understand the details or results of specific tests.

What are the Trust Services Principle categories of a SOC 2® examination (i.e. Security, Confidentiality, Processing Integrity, Availability and Privacy) and what do they cover?

SOC 2® examinations are customized and fit the unique service controls that an organization wants to better manage. The five Trust Services Principles encompass the following controls and protections:

- Security: How system resources are protected against unauthorized access, like malware, theft, data misuse and more.
  - For example: two-factor authentication and firewalls
- Confidentiality: How secure a system's data is and who has access to it.
  - For example: Financial and other personally identifiable information is restricted to certain users and only accessible with access controls.
- Processing Integrity: Whether and to what extent a system meets its purpose in terms of data processing.
  - For example: Data is not unintentionally manipulated and delivered on time
- Availability: How accessible systems, products or services are as determined by a contract or agreement. Both parties determine the minimum level of accessibility.
  - For example: Network performance in the event of a data breach or site downtime
- Privacy: How well a system complies with privacy rules and principles set forth by the AICPA, privacy notices and other regulatory guidelines.
  - For example: Preventing unauthorized access to names, addresses and bank account numbers

What are the main sections of a SOC® report?

Service organization leaders should note the difference between examination and report. SOC examinations are the practice of evaluating controls whereas reports are issued by the auditor.

The main sections of a SOC 1 or SOC 2 report are: a description of the system at a point in time, management assertion, auditor's opinion, and in the case of a Type 2 report, a description of the auditor's tests of controls and test results. Management assertions and auditor's opinions vary in depth and scope according to whether it is a Type 1 or Type 2 report.

What is a SOC® for Cybersecurity examination?

SOC® for Cybersecurity examinations were introduced in 2017 to proactively monitor and assess an organization's cybersecurity risk management processes.

What is a SOC® for Vendor Supply Chain examination?

SOC® for Vendor Supply Chain examinations, which were introduced in 2020, are performed for organizations that produce, manufacture or distribute products to allow suppliers or service providers to better understand the interconnected risks of supply chain relationships.

How is SOC® for Cybersecurity and a SOC® 2 examination different?

The two examinations have different purposes, and while there are several differences, the two most notable ones are which organizations the examinations apply to and the examinations' scope. While SOC® 2 examinations are intended for service organizations, SOC for Cybersecurity examinations can be performed on any type of organization, including not-for-profits. Cybersecurity examinations also

Preparing for a SOC® Examination

How can organizations prepare for a SOC® examination?

Service organization management can take several steps to prepare for a SOC® examination, including:

- Defining the examination scope, which consists of several sub-steps like identifying services to users, the system to deliver services, potential risks, the type of SOC® examination to be performed, and much more
- Describing primary service commitments to user entities and related system requirements
- Defining primary system requirements related to the above commitments
- Identifying and analyzing potential risks that could prevent the organization from accomplishing service commitments and system requirements
- Designing, implementing, operating, monitoring and documenting appropriate controls
    - In a Type 2 examination, also assess whether the controls are operating effectively

What is a SOC "Readiness Assessment"?

Generally, a readiness assessment is simply management's identification of gaps in controls and suggestions for fixing them. The complexity of the upcoming SOC® examination and current state of control processes will dictate how intensive (or not) the readiness process will be; for example, the organization may need to first identify which of the Trust Services Principles will be included in the examination, draft control descriptions, conduct process walk-throughs, map existing controls, attempt to fix gaps in controls, test the results and more.

SOC® Examination Details

What are the different types of opinions rendered in a SOC® examination?

There are four types of auditor opinions: qualified, unqualified, disclaimer and adverse.

A qualified opinion indicates that controls were not designed and/or operating effectively (Type 2 reports only); in other words, there are significant control deficiencies.

An unqualified opinion is the opposite and indicates that controls appeared to be designed and/or operating effectively (Type 2 reports only). There can still be issues; however, an unqualified opinion with issues means that the deficiency appeared to be immaterial.

A disclaimer means that the auditor was unable to issue an opinion, usually because information or procedures were limited.

An adverse opinion indicates that SOC® report users cannot rely on the organization's systems at all.

Why do companies undergo SOC® examinations?

Leaders of service organizations undergo SOC® 1, SOC® 2 or SOC® 3 examinations for different reasons.

SOC® 1 examinations are relevant to financial reporting and are thus part of financial statement audits.

SOC® 2 examinations may be requested by a third-party, like customers or regulatory authorities, to provide oversight or conduct due diligence on security, privacy and more.

SOC® 3 examinations are often requested by management to demonstrate assurance and confidence in one or more of the organization's service controls.

How often should a SOC® examination performed?

Typically, SOC® examinations cover a one-year period. There are situations where a SOC® examination may be valid for slightly more or less time depending on the circumstances and scope.

Conducting a SOC® Examination

Who can perform a SOC® examination?

SOC® examinations can only be performed by licensed CPAs. SOC® examinations for public entities can only be performed by CPA firms registered with the Public Company Accounting Oversight Board.

Why are CPAs, CISAs and CIAs best suited to perform SOC® examinations?

CPAs, CISAs and CIAs bring a unique combination of experience, expertise and knowledge of various systems, processes, and controls. They understand how to evaluate and improve controls to help ensure data, system security and efficiency. They also adhere to stringent professional standards and ethics and offer complete objectivity and independence. Plus, they are well-positioned to advise on industry best practices and unique risks.

What is the inclusive versus carve-out method of SOC® examinations?

Both methods address the services of certain vendors, called subservice organizations, but differ in their level of detail.

The inclusive method for SOC® examinations includes a description of the subservice organization's services, its components used to deliver services to the main service organization, and the relevant controls. Thus, the subservice organization's relevant controls and services description are included in the scope of the organization's SOC® examination.

This method is helpful when the subservice organization's services are extensive, information isn't readily accessible or it doesn't issue its own report.

The carve-out method for SOC® examinations evaluates services at a subservice organization that are not included in the scope of the main service organization's SOC® examination. A description of these services and expected controls is still included as well as how the organization monitors and provides reasonable assurance that the subservice organization's controls are operating effectively.

What is the timeline and approach by which a SOC® auditor performs a SOC examination?

A potential timeline that adheres to most SOC® examinations is almost impossible to state as every situation is different. However, any SOC examination will involve three phases – 1) Planning; 2) Fieldwork; and 3) Reporting. In most cases, an auditor will begin with the preparation of a "document request listing" followed by interview sessions, evaluation and reporting procedures.

Use of SOC® Reports

Who can review a SOC® examination report once it is issued?

SOC® 1 reports are "restricted use" and usually limited for use by Company management, auditors, customers (both current and prospective) and regulators.

SOC® 2 reports can be made available to external stakeholders, but management and the auditor must agree on specified parties, or intended users, in the scope of the examination. Specified users should have an appropriate level of knowledge and understanding about the report's contents and can include organizational personnel, business partners, regulators, and others.

SOC® 3 reports can be made public.

SOC® for Cybersecurity reports are intended for management, governance officials, business partners, investors, and other stakeholders.

SOC® for Vendor Supply Chain reports are intended for customers, business partners, and non-regulatory bodies (such as industry associations).

Can SOC® examination reports be used for marketing purposes?

Yes, in some cases. SOC® 1 reports are only intended for internal use and cannot be publicly distributed. Otherwise, due to most reports' usual level of complexity, SOC® 3 reports are most often used for marketing purposes, especially as they contain less detail and illustrative examples.

Transitioning SOC® Auditors

What are the benefits of replacing an incumbent SOC® auditor?

Like engaging a new CPA or auditor for other types of work, replacing an incumbent SOC® auditor can provide a service organization with a different perspective, approach and capabilities. Some of the same triggers as other types of audits apply, such as issues with communication, timeliness or expertise.

Additionally, replacing an incumbent SOC auditor prior to beginning a different type of SOC examination, like Cybersecurity or Vendor Supply Chain, with an auditor that specializes in these areas can help to ensure a smooth process that management can feel comfortable and confident with the auditor's expertise in the subject area.

How difficult is it to transition a new SOC® auditor to perform a SOC examination?

In most cases, not difficult at all. It's best to transition to a new SOC auditor before the examination begins to ensure a seamless process.

Look for an auditor that is AICPA-affiliated, experienced in the industry, has had a peer review within the past three years, and whose approach and communication style match the organization's.

What are the benefits and considerations of using an audit firm to perform both the financial statement audit and SOC® examination?

Financial statement auditors already act as independent, objective advisors for an organization. One of the benefits of working with the same auditor is their knowledge of the organization and industry is already proven. Also, there is one point of contact for both engagements and better coordination for complex requirements. Plus, a SOC examination tends to reduce the amount of time an auditor spends on a financial statement audit. The auditor can advise on stronger controls to benefit the organization financially as well as with data security.

However, there are three important considerations:

- The SOC auditor must hold an active CPA license;
- The auditing firm must be a member of the AICPA to perform SOC examinations; and
- The CPA and firm must be independent and hold no material interests in the organization (like shareholders, investors, etc.).

How can a SOC® examination impact other attestation agreements, like financial statement audits?

SOC examinations help to reduce financial statement audit timelines and cost by proactively assessing and reducing risk. The two engagements are separate, but some testing done for SOC examinations could provide evidence for financial statement audits. Additionally, having access to financial and data security controls allows the auditor to seamlessly link organization-wide controls to similar objectives.

COVID-19

What are the implications of COVID-19 on SOC® examinations?

COVID-19 will impact organizations differently depending on the nature of the business and industry, among other factors. There are several considerations related to SOC® examinations, including:

- The impact of the organization's systems that are used to provide services to customers, and those systems' controls;
- Whether and to what extent the organization laid off or furloughed staff responsible for maintaining controls;
- If new controls had to be implemented in response to COVID-19;
- If existing controls had to be modified;
- And more.

If a SOC examination was performed prior to COVID-19, depending on the business, an updated examination may be needed to re-assess procedures and ensure the organization can respond to post-pandemic risks appropriately.

Can SOC® tests be performed remotely?

Yes, although it depends on the organization and type of tests. The auditor's need to access appropriate personnel and evidence does not change regardless of whether the organization is operating remotely.

Relevant documentation can be uploaded to a secure portal and shared remotely, and secure video conferencing can be used as a substitute for in-person observations. Some tests, like physical inspections, walk-throughs or observations may need to be adjusted temporarily. The auditor may need to revise his or her opinion to note the limited scope of an examination.

If the auditor cannot access relevant documentation in a remote environment, the SOC examination may need to be delayed. If this is the case, management should speak with customers and other stakeholders as soon as possible.

Are organizations required to disclose COVID-19 effects or going concern issues in the SOC® examination?

It depends. SOC® 2 examinations require management to disclose any significant changes to the organization's operations, system, or system controls. This may include disclosures related to COVID-19.

The auditor is not responsible for determining whether there is going concern in a SOC examination. If there is such a concern, management may consider whether to include this disclosure in their description of the system.

The auditor is permitted to ask management about the effects of COVID-19, related to operations, services, and technologies; customer communication about service changes or agreements; any change to systems or controls; new risks; or other concerns.

PRACTICE LEADERS

Dean Flores, CISA
dflores@windhambrannon.com
678-510-2820

Al Tanju, CPA, CISA, CGMA
atanju@windhambrannon.com
678-510-2722

windhambrannon.com