WINDHAM BRANNON
offering more

SOC EXAMINATION FAQ

What are SOC Examinations?

A System and Organization Controls (SOC) report provides independent verification on third-party vendor, or service organization, systems and controls.

Leaders of service organizations have an opportunity to demonstrate trust and transparency with customers through SOC examinations. Committing to strong control systems is a safeguard for the organization as well as the businesses with which it works. Data security is a key component of SOC examinations and allows service organizations to not only address compliance but also show that they are vigilant over their customer's data management.

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 companies that provide a service (e.g., payroll, medical claims processing, loan servicers and SaaS companies) 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 three 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 designed to address a service organization's controls as they relate to the American Institute of Certified Public Accountants' (AICPA) Trust Services Criteria. The Trust Services Criteria includes security, confidentiality, processing integrity, availability, 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 also used by external stakeholders and those charged with governance.

Like SOC 1 examinations, there are two types of SOC 2 reports. Type 1 assesses whether the system design and presentation are fair at a specific point in time. Type 2 also evaluates fairness but also attests to how well the controls are operating over a period of time. A detailed chart is available here.

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 Criteria; specifically, controls associated with one or more Criteria are evaluated. SOC 3 examinations are considered general use reports, usually accessible on a company's website, 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 Criteria categories of a SOC 2 examination 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 Criteria 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?

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?

A SOC for Cybersecurity examination is a reporting framework developed by the AICPA to help organizations communicate to their stakeholders regarding the effectiveness of their cybersecurity risk management programs. It is not a compliance requirement but rather a voluntary assessment that provides assurance about an entity's cybersecurity controls.

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. These examinations provide independent assurance on the effectiveness of controls over a company's production, manufacturing, or distribution processes. By identifying and mitigating risks related to cybersecurity, fraud, quality control and regulatory compliance, businesses can enhance trust with stakeholders, demonstrate strong risk management and boost operational integrity.

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.

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 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.
    - 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 first need to identify which of the Trust Services Criteria 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 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 be performed?

Typically, SOC examinations cover at least a three-month period and usually up to 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 (PCAOB).

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

While CPAs are required to perform the examinations, those who carry the additional credentials of CISA or CIA (or those CPAs who have credentialed team members) 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 and SOC 2 reports are restricted use reports but can be marketed as such by the use of the AICPA’s SOC seal / logo (SOC Logo for Service Organizations - Registration and Guidelines | Resources | AICPA & CIMA). SOC 3 reports are most often used for marketing purposes, and the report itself is usually posted on company websites.

WINDHAM BRANNON
offering more

WHY CHOOSE WINDHAM BRANNON

Windham Brannon is a recognized leader in providing advisory, assurance and tax services to clients both nationally and globally. Serving clients in 75+ countries all over the world, our mission is to create exceptional outcomes for our clients and our people, offering more than just technical insight you would expect – we offer more proactivity, more attention and more investment into goals and priorities. Our best-in-class professionals are responsive and diligent as your trusted advisors, getting ahead of your needs so you can be well-positioned within the middle marketplace.

Dedicated Client Focus

We act as your trusted advisor, providing legendary client service that is attentive, collaborative and personalized to meet your needs.

Industry Expertise

Our professionals possess premier knowledge and technical skill in a variety of industries, including national and global resources.

Results-Driven Approach

As a trademark of our client service, we are motivated to deliver beyond the results you expect to help you succeed.

DEAN FLORES, CISA
Principal, Risk Advisory
Services Leader

678.510.2820
dflores@windhambrannon.com

Dean leads our Risk Advisory Services Practice with more than 20 years experience in governance, risk and compliance services. His primary focus includes SOC examinations, security and privacy compliance, internal control evaluations and internal audit support.

ATLANTA OFFICE
3630 Peachtree Road NE, Suite 600
Atlanta, GA 30326
404.898.2000

CHATTANOOGA OFFICE
605 Chestnut St., Ste 1260
Chattanooga, TN 37450
423.708.3423