Serious security professionals invest in SOC 2 to protect their people, & secure their business.

ebook

Understanding SOC 2 Audits

OSTENDIO

Introduction

Many service organizations today are getting asked to demonstrate that they are operating in a secure and compliant manner. With the increased reliance on third-party service providers to conduct business functions, organizations don't want to do business with vendors who they believe are at-risk Service providers can build and maintain stakeholder trust and provide transparency through a Service Organization Controls (SOC) report, which is certified by an independent third-party auditor. A SOC 2 attestation report is designed to help service organizations build confidence in the service performed and controls related to the services.

SOC 2 is emerging as a leading standard across industries that can be used for regulatory or non-regulatory purposes to cover business areas outside of financial reporting. These reports play an important role in regulatory oversight, internal corporate governance and risk management processes, and can lose their integrity if rushed. Only serious security professionals know what it takes to get SOC 2 done right to ensure their people are compliant and secure.

This eBook aims to provide insight into SOC 2 compliance, the overview of an audit, and how you can leverage your people to get prepared for SOC 2.

We'll Cover

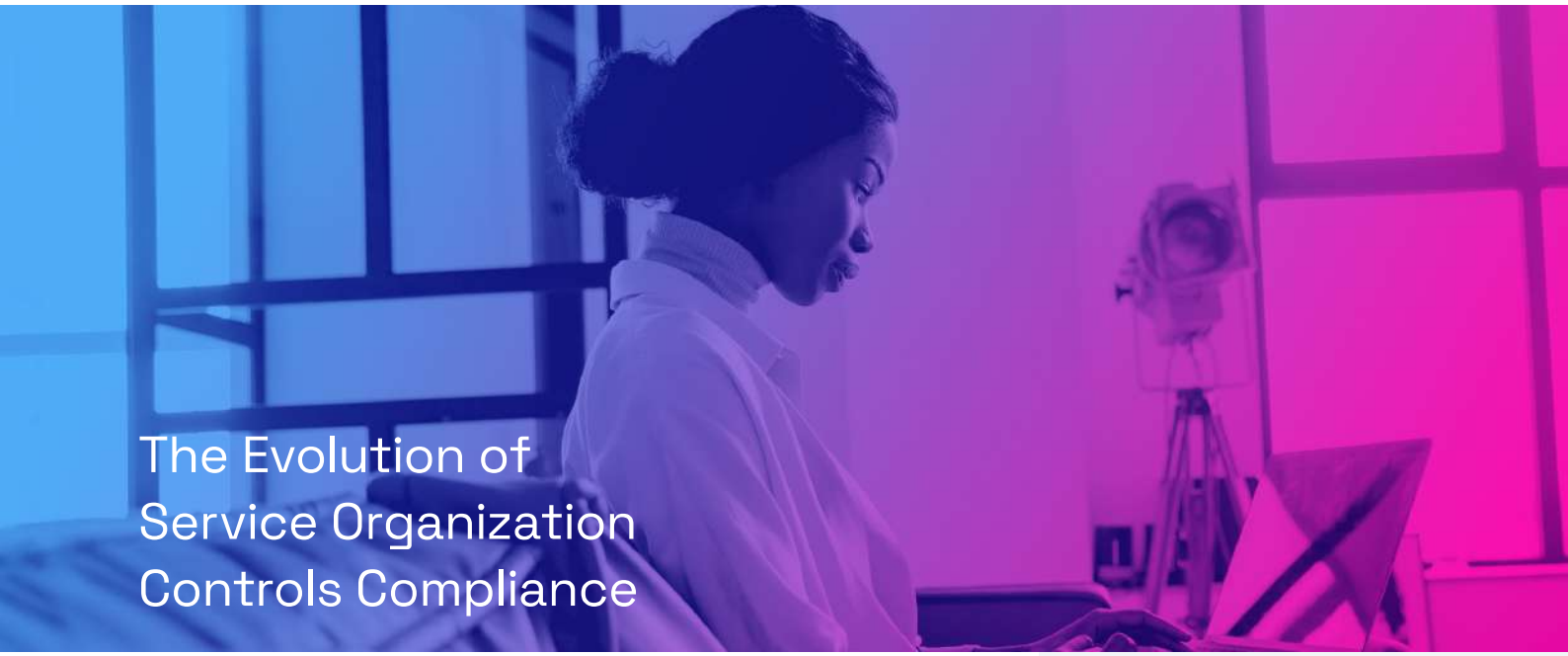
1. The evolution of SOC compliance
2. Differences between SOC 1, 2 and 3 reports
3. SOC 2 Type I and Type II
4. Trust Services Criteria
5. An overview of a SOC 2 audit
6. Challenges and success tips
7. Timing and costs

"

SOC 2 and SOC 3 reports are proving to be a popular option for security professionals. They offer a comprehensive set of controls across multiple domains while maintaining the flexibility to manage the scope and the scale of coverage in line with an organization's maturity. This ebook will help you better understand if SOC reports are the right choice for your business

GRANT ELLIOTT

CEO, Ostendio



The Evolution of Service Organization Controls Compliance

It's not uncommon today for business' to outsource certain services to third-parties. However, with outsourcing, the risks of the service organization are inherited by the company who hired them.

Up until June 2011, the Statement on Auditing Standards No. 70 (SAS 70) was used by auditors to report on financial reporting controls of their clients. The American Institute of Certified Public Accountants (AICPA) then moved to Statement on Standards for Attestation Engagements (SSAE) No. 16 to account for limitations within SAS 70. However, organizations wanted reporting that provided assurance on controls over operations and compliance as well – not just financial controls. The adoption of new technologies such as SaaS, PaaS and IaaS also drove the demand for an expanded report.

The AICPA created the SOC framework to cater to the growing trend of outsourcing business operations.

This framework provides guidance on standards that should be used for reports covering operational and technological business risks – not just financial controls as was the case before the SOC framework. SOC reports can be applied to virtually any industry or business sector.

There are 3 types of reporting options: SOC 1, SOC 2 and SOC 3. For the purposes of this guide, we will focus on SOC 2, but we will outline the main differences and similarities between the 3 reports for context.

3 types of reporting options:

SOC 1

SOC 2

- For the purposes of this guide, we will focus on SOC 2, but we will outline the main differences and similarities between the 3 reports for context.

SOC 3

The Differences Between SOC 1, 2 and 3 Reports

SOC 1

A Service Organization Controls 1 report, or SOC 1, is an audit of the internal controls at a service organization that are relevant to internal control over financial reporting (ICFR). If you handle any financial data that may affect your clients financial reporting, you may be asked for a SOC 1 report. SOC 1 reports are limited in scope – they only relate to an entities financial reporting.

These reports are intended for auditor to auditor communication. SOC 1 report distribution is restricted to 'current customers'. It can be shared with prospective customers if a third-party NDA Non-Disclosure Agreement letter is obtained.

Examples of organizations who may be asked for a SOC 1 report include payroll processors and lending services.

SOC 2

A SOC 2 report is similar to a SOC 1 report in that it also reports on the internal controls, policies and procedures of an organization. The difference is that SOC 2 reports are specifically designed to report on the controls that make up the Trust Services Criteria. The Trust Services Criteria are classified into the following categories: Security, Availability, Processing Integrity, Confidentiality and Privacy.

SOC 2 reports have less restricted distribution than SOC 1 reports. They can be shared with customers, management,

Examples

SOC 1

- Payroll processors
- Lending services

SOC 2

- Cloud providers
- Saas provicers

SOC 3

- General use

SOC 1 and SOC 2 reports cannot be combined as they are issued under different standards.

regulators and third-parties. As they can contain sensitive information about how your organization operates, you may want to consider having a Non-Disclosure Agreement in place before you share it. If you can't get access to a SOC 1 or SOC 2 report, look for a SOC compliant seal on a company's website or other marketing material.

Examples of organizations who may be asked for a SOC 2 report include cloud and SaaS providers.

SOC 3

Similar to SOC 2 reports, SOC 3 reports also focus on the Trust Services Criteria controls. However, unlike a SOC 2 report, SOC 3 reports are certified and can be widely shared. As they are 'General Use' reports they can be a valuable marketing tool for demonstrating the effectiveness of your control environment.

SOC 2 and 3 reports can be combined. The work performed by an auditor may be able to be used to report on a SOC 3 engagement as well.

Report Type	Focus	Certification	Intended Users	Distribution
SOC 1	Internal controls for financial reporting	No	Your management, auditors, CFO, CIO, controllers and compliance officers	Restricted to current customers and auditors
SOC 2	Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality and Privacy controls	No	Your management, CFO, CIO, controllers, compliance officers, vendor management, regulators and other specified/relevant parties	Restricted to current customers, auditors, regulators and specified parties
SOC 3	Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality and Privacy controls	Yes	Any interested party	General use

SOC 2 Report Types

There are two types of SOC 2 reports: SOC 2 Type I and SOC 2 Type II.

Most organizations eventually undergo a SOC 2 Type II, however, it is often recommended to start with Type I before moving onto Type II.

Both Type I and Type II reports are Service Organization Control reports, which means that they report on the controls and processes at a service organization.

- **SOC 2 Type I**
  Type I reports center around a 'point in time'. It focuses on the description of the system, controls, and the ability of these controls to obtain their objectives at a certain point in time, e.g. June 23rd 2018.

- **SOC 2 Type II**
  A SOC 2 Type II report has the same focus as Type I, plus additional information about whether the controls are operating effectively over a specified period of time – typically over a 12-month period. Type II provides more assurance as the auditor tests the operating effectiveness of the controls. SOC 2 Type I does not show tests of controls or reports.

Trust Services Criteria[1]

SOC 2 reports are specifically designed to report on the controls that make up the Trust Services Criteria.

An audit may report on one or more of the Trust Services Categories, as decided by your management team. A company can choose to report on any category, but the audit must include Security as it is part of the Common Criteria.

Common Criteria (includes Security)

- Organizational Controls
- Availability
- Risk Assessment
- Change Management

Availability

- Disaster Recovery
- Environmental Controls

Processing Integrity

- End to end Completeness and Accuracy
- Processing Monitoring

Confidentiality

- Encryption
- Data Disposal

Privacy

- Privacy Agreements
- Encrypti9on

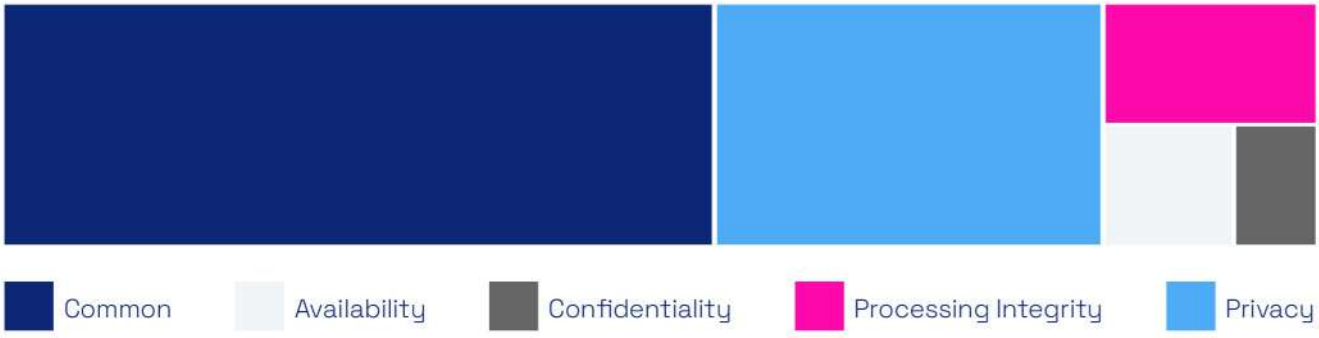
[1] As defined by AICPA Assurance Services Executive Committee (ASEC)

Proportionate Level of Effort

- **SECURITY**
  The system is protected against unauthorized access (both physical and logical).
- **AVAILABILITY**
  The system is available for operation and use as committed or agreed.
- **PROCESSING INTEGRITY**
  System processing is complete, accurate, timely and authorized.
- **CONFIDENTIALITY**
  Information that is designated "confidential" is protected as committed or agreed.
- **PRIVACY**
  Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (GAPP) issued by the AICPA and CICA.

Adding additional categories increases the scope of the criteria which makes the reports more expensive and more time and resource intensive. Privacy uses an additional set of 18 criteria. Unless your organization is processing or housing PII it is usually not necessary to include it as a Trust Category.

Choosing which Trust Categories are in scope is extremely important. For help getting started with and going through the SOC 2 report process, contact Ostendio for a no cost consultation with one of our security and compliance experts.



Overview of a SOC 2 Audit

Define Scope

Determining the SOC 2 reporting period is crucial when scoping your report. If you've decided to undergo a Type II audit, some common time-frames are 6, 9 or 12 months. Make sure to narrow down systems you want in scope. We recommend choosing systems that contain sensitive data such as Protected Health Information (PHI). Your service organization should only report on what is relevant to your user entities. Many organizations do not report on all 5 Trust Services Categories at once. You can build on to your report each year. It's important to note that your organization decides what is in scope. You can get recommendations from SOC 2 preparers or auditors, but the ultimate decision is made by your management team.

Separating Preparation Support from the Audit

When seeking help, it is important to differentiate between help with audit preparation and execution of the actual audit. Auditors must remain independent and so the same organization should not be involved with both audit preparation and the actual audit assessment. Choosing your SOC 2 vendors is a very important step.

Your auditor must be a licensed CPA firm. You should review who is on the audit team, whether they have been peer reviewed (happens every 3 years), and if they retain their independence from SOC 2 preparers. A CPA firm should not perform both the audit and the audit preparation. AICPA has a guide for hiring a high-quality auditor which can be found on their website.

Readiness Assessment

A Readiness Assessment is not necessary but is highly recommended as it can save a lot of time when completing your SOC 2 audit. If you choose to complete a Readiness Assessment, remediation is crucial. Allow yourself enough time to correct gaps before moving forward with your audit. An auditor can perform the readiness assessment and make recommendations but cannot design or execute controls – there needs to be clear independence.

OVERVIEW OF A SOC 2 AUDIT CONTINUED

The Audit Process: It typically takes anywhere from 1 – 2 months to prepare for the audit. The audit process usually follows an approach of planning, fieldwork, and reporting.

- **Planning**
  The System Description should be provided to the auditor first as this defines the scope of systems and controls.
- **Fieldwork**
  The auditor will mak e requests for evidence, follow-ups, select sam-ples, etc. When it comes to SOC 2, if you didn't document it, it didn't happen. Examples of evidence include organizational charts, asset inventories, evidence of on-boarding and off-boarding processes and change management. When reviewing the evidence, the auditor may choose to conduct on-site interviews or complete them by phone.
- **Reporting**
  Your management team will receive the draft report for review. Manage-ment will have to sign an Assertion Letter and Management Representation Letter. The auditor will issue the report on an agreed upon date. Always review this report carefully as you will be giving it to internal and external stakeholders.

Structure of a SOC 3 Report

Section 1: Independent Service Auditor's Report

- Outlines the scope of the report
- Test Period
- Auditors opinion on operating effectiveness to meet controls

Section 2: Assertion of Client

- Management's statement that the description of controls is complete and accurate
- Signed by executive leader(s)

Section 3: Description of the System

- Written by the management, it provides details of the sytems being reported on
- Description includes the supporting processes, policies, procedures, personnel and operational activities that constitute the service organization's services

Section 4: Description of Criteria, Controls, and Results of Tests

- Control objective (related to the applicable trust service categories)
- Controls in place at the service organization to meet the objectives
- Auditor's tests of the controls
- Results of the tests

Aiming for Success: Challenges and Tips

In order for a SOC 2 audit to be successful, there needs to be adequate planning and preparation.

SOC 2 reports require annual reassessment. You can't rest on your laurels after you've successfully completed a SOC 2 report. You also need to think about the resources you'll need – financial and employee time.

And don't forget to budget for annual reassessment!

Another important aspect of a successful audit is organizational buy-in. Some processes will need to change in order to ensure controls are being met efficiently and this may take some time. Leadership buy-in is extremely important.

Selecting your Trust Categories can be a difficult decision as it depends on a number of factors. Remember, your auditor can suggest and make recommendations about which ones to choose but ultimately it is the decision of your management team. There is always the option to only report on one the first year and then build on your report each year.

Document, document, document.

We can't stress this enough

- Everything needs to be documented. If you didn't document it, it didn't happen in the eyes of an auditor. Ostendio significantly eases the collection, management and mapping of evidence across all required controls. Evidence is kept current ensuring it is always up to date, and all communications, changes and mitigations are fully tracked and stored within the Ostendio platform.

Cost and Timing

A question we often get asked is 'how much will this cost'? Unfortunately, the answer is, it depends.

Cost

A number of factors influence the price including:

- The type & number of Trust Categories you want in scope
- The size of the environment
- The type of report (SOC 2 Type I or Type II)
- The number of applications
- The number of employees yur organization has

Remember, this is an annual recurring report, so the upfront cost is always higher. Expect costs to lower by 10 - 20% in subsequent years.

Our second most common question is 'how quickly can we get this done'? And again, unfortunately, the answer is it depends.

Timing

It can take anywhere from 6 – 8 weeks to several months. It's contingent on a number of factors including:

- Current readiness
- Number of Trust Categories
- Available resources
- Company size
- Current level of security maturity

As an experienced SOC 2 preparer, we can provide a better estimate about cost and timing after a scoping discussion.