LAIKA

heylaika.com

SOC 2 UNIVERSITY

Expert guidance and resources for growth-minded individuals

LAIKA

heylaika.com

Table of Contents

CH.01 SOC 2 INTRODUCTION

Your customers want it. Your customers (might) have it. What is SOC 2 and why does your startup need it?

BY MARY LISTER

What is SOC 2?

SOC 2, which stands for System and Organization Controls report, is an auditing standard maintained by the American Institute of Certified Public Accountants (**AICPA**) to test an organization's internal controls for information security and privacy. It's an objective, third-party system that tells customers that they can trust your startup to handle their information with the utmost care.

This is the compliance audit most commonly sought by startups, particularly SaaS, as it's relevant for any business that uses the cloud to store data. To become compliant, a startup must choose at least one or more trust services criteria and a type to test against.

What's the difference between SOC 1, SOC 2, and SOC 3?

There are three types of SOC reports, but each covers a separate industry and type of service organization. We've outlined the three options below:

SOC 1

Service Organization Control 1 evaluates the effect of service organization controls on financial statements. For example, say your SaaS startup provides billing services to large companies. Chances are your customers will require the startup to become SOC 1 compliant because the startup's billing process impacts their financial reporting. **(See Chapter 2 on SOC 1 vs SOC 2 for more details)**

SOC 2

Service Organization Control 2 is a procedure that examines service providers. The audit determines if they are securely managing 3rd party data, like personal information, to protect information and ensure privacy. Compliance with SOC 2 is usually a requirement when considering SaaS providers.

SOC 3

Service Organization Control 3 is a public report of internal controls over security, availability, processing integrity, and confidentiality. Like all other SOC certifications, it was established by the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) Trust Service Criteria (TSC).

What is SSAE 16 and SSAE 18?

You might hear the term 'SSAE' when referring to SOC audits. This refers to the AICPA's Statement of Standards of Attestation Engagements: the regulations auditors use to evaluate companies and more specifically evaluate compliance controls.

SSAE 16

In 2011 the AICPA revealed SSAE 16, formerly known as SAS 70, which required auditors to evaluate a startup's internal controls and the impact the organization can have on the control environment. This was particularly important for auditors to accurately assess a company's financial statements (SOC 1).

SSAE 18

In 2017 the AICPA replaced SSAE 16 with SSAE 18, an assessment standard covering both SOC 1 and SOC 2. The main purpose of the update was to demand companies to take more control and accountability over third-party vendors. The new standard requires businesses to apply the same risk assessment standards to vendors they work with directly and indirectly.

What is the Trust Services Criteria?

Issued by the AICPA, the Trust Services Criteria evaluates how companies process information and manage customer data. This covers five components, which include security, privacy, availability, processing integrity, and confidentiality. In order to define the scope of the audit and the necessary controls, SOC 2 reports must address one or more of the criteria.

What is the COSO framework?

In 2013, the AICPA combined the TSC framework with the COSO framework, which is used to access the design, implementation, and maintenance of a startup's controls. Complementary to the TSC, COSO's five components include:

1. Risk assessments
2. Information and communication
3. Existing control activities
4. Monitoring activities
5. Control environments

The TSC and COSO frameworks help businesses work towards a clear set of guidelines when achieving their SOC 2. Get more details on TSC and COSO in **Chapter 4**.

What are the types of SOC 2 reports?

There are two types of SOC 2 reports companies can obtain: Type 1 and Type 2. The difference between Type 1 and Type 2 is design versus operating effectiveness.

A Type 1 tests design by looking at your description of controls at a particular point in time. A Type 2 tests operating effectiveness by collecting evidence of your controls in operation over a 6 to 12-month period. **Check out our section on types here**.

Which types of companies need SOC 2?

If your business does anything with data and software, or uses cloud computing, chances are you will need a SOC 2 audit at some point soon or in the future. Specifically designed for businesses that store data in the cloud, SOC 2 applies to almost every SaaS business.

A SOC 2 report is particularly important for growth-focused B2B startups that are looking to move upmarket and attract bigger customers. Today, enterprise buyers now **require** businesses to become SOC 2 compliant.

While most startups seek out a SOC 2 audit once reaching their Series A or B, it may be beneficial to do so beforehand if you've already begun selling to enterprise customers.

Why is SOC 2 compliance important for startups?

SOC 2 compliance:

1. Helps businesses move through enterprise procurement
2. Establishes credibility between you and your competitors
3. Protects sensitive data from hacks or threats

Enterprise companies expect startups to meet the same procurement cycles and compliance requirements as other vendors. In many cases, bigger customers will ask you to become SOC 2 compliant before working with them.

SOC 2 as a competitive edge

Savvy startups also use SOC 2 compliance as a competitive differentiator. Compliance doesn't just tell enterprise buyers that you are open for business. It's a powerful brand and marketing message that signals to the world that your startup is more **established, credible, and attuned to your customer's needs.**

Compliance protects your startup against devastating financial and reputation losses. It ensures your company is built on solid processes that remain strong and secure as your team grows, your product becomes more complex, and you take on bigger clients. Without it, you put yourself, your startup, and your customers at risk of losing it all.

CH.02 SOC 2 VS SOC 1

Confusing SOC 2 and SOC 1 reports can be easy. Both frameworks can report over the same controls, but are different in focus.

What is SOC 1?

What does it test? Unlike SOC 2, SOC 1 hones in on internal controls that impact customer financial reporting and is tested based on objectives the auditor and the business agree to. These objects depend on what your customers need for their own financial reporting. For example, how effective are auditors in evaluating tax statements?

Who needs it? Any large public, or non-public, company will require their service providers to get a SOC 1 if they impact their financial reporting, even indirectly.

What is SOC 2?

What does it test? Service Organization Control 2 is a procedure that examines service providers. The audit determines if they are securely managing 3rd party data to protect and ensure privacy. SOC 2 uses the COSO framework to test your internal controls against five **Trust Services Criteria: security, availability, confidentiality, privacy, and processing integrity.**

Who needs it? SOC 2 has become the gold standard for SaaS solutions. In many cases, enterprise buyers require all vendors to get SOC 2 compliance. This makes the audit particularly **important for growth-focused B2B startups** that are starting to attract enterprise customers in order to move upmarket. Today, more SaaS startups than ever choose to pursue SOC 2 in order to satisfy enterprise customers' needs.

How similar are SOC 1 vs SOC 2 reports?

Both SOC 1 and SOC 2 reports come in different flavors. A Type 1 audit tests the design of your compliance program at one point in time. A Type 2 audit, on the other hand, tests not only your compliance program but also the operating effectiveness of controls over time. Generally most businesses should start with a Type 1 and build towards a Type 2, unless a specific client requires a Type 2 immediately. **(More on SOC 2 types here)**

When do you need a SOC report?

Increased regulations, security threats, and data protection standards are pushing compliance requirements downstream. If it is **not blocking a deal now,** it will if you plan to grow. The longer you wait, the more complex, time consuming, and costly it will be. Technical and operational debt will accrue and complicate changing organizational behaviors.

CH.03 SOC 2 TYPE 1 VS TYPE 2

To become SOC 2 compliant, businesses need to choose a type of audit that test against certain trust services criteria: SOC 2 Type 1 vs Type 2. Be careful not to mistake Type 1 for SOC 2 and Type 2 for SOC 2. They all mean something different.

What is the difference between SOC 2 Type 1 and SOC 2 Type 2?

There are two different types of SOC reports:

A SOC 2 Type 1 (Type I report) audit tests the design of your compliance program.

It assesses your compliance at one point in time. Typically, this involves checking to see that you've identified and documented the controls you have in place, as well as provide sufficient evidence that your controls are functional at that point in time.

A SOC 2 Type 2 (Type II report), on the other hand, tests not only your compliance program but also the operating effectiveness of controls over time. Usually, a Type 2 audit assesses your compliance over a six to 12-month review period, with your first audit typically lasting up to six months. **(Check out our detailed blog on SOC 2 Type 2 here)**

What are the similarities between SOC 2 Type 1 and SOC 2 Type 2?

Both **audited by a licensed CPA firm**, SOC 2 Type 1 and Type 2 provide customers and third-party vendors with reasonable assurance that the service provider meets controls objectives against the chosen trust services criteria-- availability, confidentiality, security, privacy, and processing integrity.

Not only can you trust that the business you are working with complies with industry standards, but also that the business is appropriately protecting sensitive, personal information.

How does a service organization decide what type of report they need?

Businesses should start with a Type 1 then build to a Type 2, unless a specific client requires a Type 2 immediately. However, the type of report can depend on how urgently businesses need compliance, and if they will eventually need a Type 2 report.

If an organization needs a SOC 2 report as soon as possible, it might be enough to begin with a Type 1 audit. Type 1 audits are faster and can set realistic expectations for a Type 2 audit report. Keep in mind that

A Type 2 audit is more comprehensive and shows a greater level of audit assurance. Although it covers the same controls as a Type 1, Type 2 audits go further in-depth on the operating effectiveness of the controls with evidence. The results of SOC 2 Type 2 are more indicative of how securely the organization operates.

Which is better for startups selling into the enterprise, SOC 2 Type 1 or SOC 2 Type 2?

Each type comes with its own benefits and challenges. Type 1 is faster and cheaper than Type 2. The requirements aren't as strict as Type 2, since Type 1 tests the suitability of the design of controls and does not require evidence. Type 2, however, points to a higher level of compliance.

Type 1 is enough for some enterprise customers, making it a sufficient option for some startups. That is until SaaS startups want to work with enterprise customers that require a more complete picture of their compliance. In that case, you'll want to pursue SOC 2 Type 2.

When should you obtain a Type 1 vs Type 2 SOC report?

Generally, businesses should explore both SOC 2 reports as soon as possible. The attestations can be customized to the current stage of your business (pre-seed, seed, series A, etc), and made to change as the business evolves. **(See: Why Stage-Appropriate Compliance Matters for Startup Growth)**. As your company grows, so will the need for information security to protect against unauthorized access.

At the minimum, we recommend seed companies upgrade their internal controls and series A companies implement SOC 2 Type 1, tighten people management controls, and prepare business continuity plans. You might even need to start a SOC 2 Type 1 earlier if you sell to financial institutions or healthcare organizations.

Which SOC report can you get faster and cheaper?

As with many important and complicated things, the answer is — it depends.

The deciding factor here is complexity. How many employees work for your startup? How many systems do you run? Do you have multiple locations? What's your startup's revenue like? How sensitive is your customer data?

In a best-case scenario, a SOC 2 Type 1 audit can cost anywhere from $10k to $30k and can take as quickly as 2-4 weeks to draft, and then another 2-4 weeks for the audit. A SOC 2 Type 2 audit can cost roughly $30k, and take anywhere from 2-6 weeks to draft, 6 to 12 months to collect evidence, and 4 to 6 weeks for the audit.

However, in both scenarios, businesses usually spend much more time preparing for the audit.

CH.04 SOC 2 TRUST SERVICES CRITERIA

What are the SOC 2 trust services criteria, and how should you decide what applies to your business?

What are the SOC 2 trust services criteria?

To become SOC 2 compliant, your startup needs to undergo an audit and receive a clean report testifying the quality of your controls. This is determined by the Trust Services Criteria, formerly known as Trust Services Principles, and audit type.

A SOC 2 report can test against five Trust Services Criteria: security, availability, confidentiality, privacy, and processing integrity. When you engage an auditor, you decide which of the five you'd like tested, if not all. These decisions are often influenced by what enterprise buyers request.

What are the importance of each SOC 2 trust services criteria?

Let's break down the five components together.

Security

Also known as the "common criteria," security is the foundational criteria required in a SOC 2 assessment. Security focuses on the protection of information and systems against unauthorized access. It tests if your customers' information is protected at all times (collection, creation, use, processing, transmission, and storage) along with the systems that handle it.

Security is required in any SOC audit because it not only sets overarching security standards for your company, but also overlaps with the others: setting security controls for availability, confidentiality, privacy, and processing integrity.

Availability

Availability addresses network performance, downtime, security event handling, etc. This criterion makes sure your systems are secure and available for customers to use when they expect to. This is important for startups that promise customers access to their data and your services at key times.

For example, your team worked hard to get your platform's uptime to 99.31%. By validating your uptime and other availability considerations with the availability criteria, you're further demonstrating your reliability to your customers.

Confidentiality

Confidentiality addresses the handling and protection of information, personal or not, that you've agreed to designate confidential and secure for your customers (think of proprietary information like business plans, financial or transaction details, legal documents, etc.)

In addition to the protections outlined in the security criteria, the confidentiality criteria provide guidance for identifying, protecting, and destroying confidential information.

For example, your platform manages a customer's documentation about their trade secrets and intellectual property. For obvious reasons, they only want people within the company (and only some of them) to have access to this sensitive information. The confidentiality criteria signal that you're set up to protect that information and secure access as desired. It also shows that you're set up to appropriately destroy confidential information if, say, the customer decides to stop using your platform.

Privacy

Privacy addresses the secure collecting, storing, and handling of personal information, like name, address, email, Social Security number, or other identification info, purchase history, criminal history, etc.

Similar to confidentiality, the privacy criteria test whether you effectively protect your customers' personal information. Confidentiality, on the other hand, applies to any information you agreed to keep confidential.

Processing Integrity

Processing integrity addresses processing errors and how long it takes to detect and fix them, as well as the incident-free storage and maintenance of data. It also makes sure that any system inputs and outputs are free from unauthorized assessor manipulation. This criterion helps businesses make sure their services are delivered in an accurate, authorized, and timely manner.

For example, the processing integrity criteria demonstrate to customers that your data, processes, and system work as intended, so they don't have to worry about inaccuracies, delays, errors and whether only authorized people can use your product.

Which trust services criteria should I include in my SOC 2 audit?

Even though the security criteria is the only necessary TSC for a SOC 2 audit, you may choose to test the other criteria that are relevant to your startup and how you serve your customers.

In our experience, most enterprise customers want to work with startups that are SOC 2 compliant in security and confidentiality. If you're struggling to decide which criteria to tackle in your first audit, security and confidentiality make a good starting point. Otherwise, add on the criteria your target customers want and are asking for.

How is the COSO framework different from Trust Services Criteria?

In 2013, the Committee of Sponsoring Organizations of the Treadway Commission, also known as COSO, created tighter controls that all businesses must implement in order to achieve a SOC 2 report.

While the Trust Services Criteria assess internal controls over the security, availability, processing integrity, confidentiality, and privacy of a system, the COSO framework addresses the following components:

1. **Risk assessments:** How does an organization assess all types of risk?
2. **Information and communication:** How do businesses internally and externally communicate what is expected?
3. **Existing control activities:** What existing controls does a business currently have in place? How effective were the controls over a period of time?

4. **Monitoring activities:** How do businesses oversee the entire organization? How do they identify and fix processes that aren't working?
5. **Control environments:** How does a business create procedures that guide the company? How do they make sure that all controls are operating effectively?

Both the TSC and COSO framework provides a way for businesses to assess internal controls. However, not all TSC's need to be met, and organizations must meet the five COSO components and their relevant controls to achieve a SOC 2 report.

SOC 2 has a long list of controls that each business pursuing a SOC 2 report needs to implement. But first, let's talk about where this controls list comes from.

SOC 2 controls are based on the **Trust Services Criteria deemed applicable to your organization**. A SOC 2 report focuses on non-financial criteria related to security, availability, confidentiality, processing integrity, and privacy.

Modeled around policies, communications, procedures, and monitoring, Trust Services Criteria each have corresponding controls.

Get more information on SOC 2 Trust Services Criteria.

What are SOC 2 requirements?

SOC 2 requirements change according to the type of information a business needs to secure.

An organization should select the Trust Services Criteria requirements relevant to their business and the commitments they make to their customers. However, security is required and referred to as "Common Criteria."

The SOC 2 controls we list here are an overview of those you may need to implement for your SOC 2 report. The ones that are relevant to your business should be selected by your CISO and management team.

SOC 2 Controls List

While there are many controls associated with each of the five TSCs, controls associated with the common criteria include common IT general controls.

Control Environment

These SOC 2 controls relate to a commitment to integrity and ethical values.

Involvement of the board of directors and senior management's oversight relating to the development and performance of internal control.

Hold individuals accountable for their internal control responsibilities in the pursuit of objectives.

Communication and Information

This includes SOC 2 controls related to the internal and external use of quality information to support the functioning of internal control.

Risk Assessment
This requests the identification and assessment of risk relating to objectives, including fraud.

Monitoring Activities
Place controls related to the performance of ongoing and separate evaluations to determine deficiencies of controls and communicate those to the correct parties.

Control Activities
These relate to the control activities contributing to risk mitigation and policy and procedure establishment.

Logical and Physical Access Controls
Related to the implementation of logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet its objectives.

- Issuing of credentials to new internal and external users
- Authorization, modification, or removal of access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design
- Restriction of physical access to facilities and protected information assets to authorized personnel to meet its objectives
- Implementation of controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet its objectives.

System Operations
SOC 2 controls related to the use of detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities and (2) susceptibilities to newly-discovered vulnerabilities.

- Response to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
- Monitoring of system components and the operation of those components for anomalies indicative of malicious acts, natural disasters, and errors

Change Management
Controls related to the authorization, design, development, testing, approval, and implementation of changes to infrastructure, data, software, and procedures to meet its objectives.

Risk Mitigation
Identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Additional SOC 2 Criteria for Privacy, Processing Integrity, Confidentiality, Availability

In addition to the requirements attached to Security, businesses should fulfill the controls for other relevant categories based on the commitments they make to their customers.

Find examples of additional SOC 2 control categories and control types that satisfy these categories below.

Privacy: Provides notice of privacy practices to relevant parties.
The notice is updated and communicated in a timely manner, including changes in the use of personal information.

Processing Integrity: Obtains or generates, uses, and communicates relevant, quality information regarding the SOC 2 objectives related to processing.
This includes definitions of processed data, and product and service specifications, to support the use of products and services.

Confidentiality: Identifies and maintains confidential information to meet SOC 2 objectives related to confidentiality.

- Retention and Classification
- Disposal of Information

Availability: Maintains, monitors, and evaluates current processing capacity and use of system components like infrastructure, data, and software.

- System Capacity

Maintaining processing capacity and use of system components (infrastructure, data, and software) to manage demand and enable the implementation of additional capacity to help meet objectives.

- Backups and evironmental controls
- Recovery controls

How does my business fulfill SOC 2 controls?

There isn't one path to fulfilling SOC 2 controls and prepping for audit. The process should include policy implementation and technical and operational procedures.

Policies

For SOC 2 Type 1, auditors ask to examine authored policies, who they've been distributed to, and the procedures put in place to execute the policy.

In a Type 2 audit, auditors examine the functionality of controls over a 6-12 month time period. A comprehensive report is written based on the evidence provided.

Technical Procedures

SOC 2 controls primarily focus on policies and procedures instead of technical tasks; however, the implementation of technical procedures typically involves building or managing new tools, like endpoint security. These procedures are monitored over time for effectiveness and relayed to audit teams while pursuing a SOC 2 report.

Operational Procedures

Just as important as technical processes, operational procedures involve managing vendors and due diligence, creating uniform onboarding and termination procedures, and collecting evidence on their effectiveness.

These procedures are crucial to creating a risk assessment for auditors and understanding the business' risk appetite.

CH.05 SOC 2 COST

Considering SOC 2 compliance and curious about how much it will cost? Learn how to save time and money on your SOC 2 audit.

There are plenty of factors that can shift the cost including internal hires and infrastructure, vendor selection and management, and law firms and auditors. See below for a better understanding of each.

Getting a SOC 2 report is more manageable for small businesses, particularly if they get started early. The sooner best practices are implemented, the easier it will be to maintain SOC 2 compliance and move upmarket.

How much do startups spend on SOC 2?

Companies that wait to get a SOC 2 report until a Series C will spend more than a seed startup. However, the cost of implementation and audit alone for SOC 2 Type 1 and Type 2 typically costs 50-person businesses about $80k.

TDLR; without managing your SOC 2 process with experts and a software platform, it could cost upwards of $70k and last over 18 months.

How can I save money on a SOC 2 report for my startup?

The best way to save money on a **SOC 2 report** is to start early and maintain controls and best practices. The scope of your SOC 2 can determine the price; larger organizations will need to pay more for a larger scope and more extensive controls.

Gap Analysis and Scope

$5k - $10k

Before getting into the execution of your SOC 2, a compliance expert will need to evaluate the information security practices already in place. Whether you're looking to renew your SOC 2 certification or starting from scratch, this is an important step to understanding the scope of work needed.

To get an inside look into the process, **check out our blog post on our own SOC 2 gap analysis**.

Control Implementation

$5k - $10k

After establishing the gaps that need to be addressed and a remediation plan, your compliance team will dive into implementing SOC 2 controls. While you may think the audit is the most important part of SOC 2, implementation is really the main event. **You can learn more about implementation from Laika's SOC 2 certification here.**

This cost varies based on the controls needed, how much you outsource versus build internally, and your timeline. If you handle it internally, you'll need to make a full-time hire or reallocate other employees' work, losing some organizational efficiency and productivity.

This cost as something can be absorbed internally if you have specific hires to manage the process. Otherwise, you'll likely be losing around 60-100 hours of work from your current employees.

Risk Assessment

$10k - $17k

After all your controls have been implemented, a compliance task force will need to review the evidence you collected, test the operational effectiveness of your controls, and assess your risk. These steps address audit readiness and involve accepting the amount of risk your organization has deemed acceptable.

SOC 2 Audit

The cost of a SOC 2 audit depends on the time spent evaluating controls, answering questions from auditors, the size of the organization, and the type of audit.

Most businesses pursue a SOC 2 Type 1 report first, followed by a SOC 2 Type 2.

For more information on **SOC 2 Type 1 vs. SOC 2 Type 2, check out our run-down here.**

SOC 2 Type 1 audit

$12k - $27k

This is the first, one-time audit involved in SOC 2 compliance. Auditors will examine a snapshot of your SOC 2 controls at a single point in time to determine the design is correct.

SOC 2 Type 2 audit

$15k - $100k

These audits need to be performed annually. Depending on the scope of your SOC 2 and the size of your organization, this audit could take up to 9 months to complete.

Hidden Costs

SOC 2 isn't just a one-and-done task. Many of the costs listed below are recurring or constant tasks that will need to be performed as part of your new security posture.

Consultants

CISO $550/hr
CISA $200/hr

Control implementation, a risk assessment, and managing an audit requires at least foundational knowledge of SOC 2 compliance. If you opt for a software-only solution to assist on your SOC 2 journey, it's likely you'll need to hire a compliance expert consultant to help the process along.

Depending on the complexity of your controls and the necessary experience level of your consultant, the cost will vary.

Policy Templates and Writing

$5k - $10k
Time: 2 weeks

If you don't have in-house counsel or compliance experts, you'll need to outsource some paperwork to a legal firm. This includes any new policies you'll need to author, like risk mitigation, privacy policies, formal business continuity plans, etc.

Depending on which external party handles your audit, you may be able to outsource review of the documents to them as well.

Internal Training

$1k / 50 employees

Time: 2 weeks

A requirement for SOC 2 is security awareness training for employees. You'll need to develop the training yourself or outsource; either way, it'll likely cost time and money to create and execute the training.

The average associated cost depends on the size and maturity of your business, as well as the type of data you handle.

On-going SOC 2 Requirements

A major component for SOC 2 compliance is choosing your vendors, executing due diligence to ensure they are also SOC 2 compliant, or building your own solution to be compliant as needed.

Some of these vendors include endpoint security, logging and monitoring tools, password management, hiring and termination tools and processes, and security awareness training. The cost below is broken down into estimates for each vendor:

Endpoint security

$190 for 5 licenses

Employee background checks

$20-$100/per hire

Vulnerability scanning

$2k - $2.5k

SOC 2 compliance can quickly get very expensive. And it can be difficult to calculate your budget when considering multiple factors, from internal productivity loss to audit firms and vendors. However, SOC 2 is only becoming more imperative to do business.

CH.06 SOC 2 AUDIT

A SOC 2 audit is an examination of a service organization's compliance with SOC 2, according to the Trust Service Criteria defined by the AICPA.

A SOC 2 Type 1 report covers:

- Management's description of the system
- **Control objectives design**

Because a Type 1 report is framed around a specific date, it does not show tests of controls or the results of tests. Generally, the CPA that executes the audit will issue an opinion, which addresses the suitability of control architecture.

Type 2 audit

During a Type 2 audit, the auditors will look over the description of controls to **better understand how to test and judge the effectiveness.**

In a SOC 2 Type 2 report, **the auditor will issue a similar opinion** as a Type 1 with the addition of operating effectiveness. Controls are evaluated over a period of time, typically a 12 month period. The report shows descriptions of control tests and results by the auditor.

Who can audit my SOC 2 compliance?

Any certified public accountant (CPA) affiliated with the AICPA can perform a SOC 2 audit.

Realistically, technology-forward businesses should hire an auditor that is familiar with the SOC 2 framework. They can quickly and easily evaluate a security posture. While that does include big-name firms, there are plenty of accounting firms that specialize in security audits that cost much less.

How long does a SOC 2 audit take?

A couple of weeks to several months.

Unfortunately, the **length of the audit is variable**. It can last anywhere from a week to multiple months. This is based on preparation, organization of evidence, and communication with auditors.

CH.07 SOC 2 REPORT

A SOC 2 audit report is a 30-40 page document that describes a service organization's controls and whether it stands up to scrutiny.

An organization can choose a SOC 2 report that focuses on any of the five trust services criteria and either a Type 1 or Type 2.

Written by an AICPA (American institute of certified public accountants) accredited firm, a SOC 2 report serves mainly as auditor-to-auditor communication. It's meant to be read, understood, and evaluated by other compliance and information security professionals. The use of this report is generally restricted.

How do you determine what SOC report you need?

A strong understanding of SOC 1, SOC 2, and SOC 3 are required to decide which SOC audit a business needs.

- SOC 1: evaluates the effect of a service organization's controls on a customer's financial reporting
- SOC 2: evaluates if service providers are securely managing customer data, like personal information, to protect and ensure privacy; the most common framework for SaaS providers
- SOC 3: a public report of internal controls over security, availability, processing integrity, and confidentiality

Once a business has determined which SOC attestation best fits their goals, they'll want to pick between the two SOC 2 Types: SOC 2 Type 1 and SOC 2 Type 2. **(See Chapter 2)**

- **Type 1:** tests design by looking at your description of controls at a particular point in time
- **Type 2:** tests operating effectiveness by collecting evidence of your controls in operation over a 6 to 12-month period

All SOC reports are verified by the AICPA and tested against one or more of the trust services criteria. **(Learn more about TSC's)**

- **Security:** focuses on the protection of information and systems against unauthorized access
- **Availability:** addresses network performance, downtime, security event handling, etc
- **Processing Integrity:** addresses processing errors and how long it takes to detect and fix them, as well as the incident-free storage and maintenance of data
- **Confidentiality:** addresses the handling and protection of information (personal or not) that you've agreed to designate confidential and secure for your customers
- **Privacy:** addresses the secure collecting, storing, and handling of personal information

How much does a SOC 2 report cost?

We've seen SOC 2 audits start around $20k for startups and cost hundreds of thousands for larger companies. Your cost will depend on a number of factors:

1. Team size and distribution
2. Lack or abundance of control documentation
3. Complexity of services as well as the number and complexity of processes
4. Scope of your audit (Trust Services Criteria and Type 1 or 2)
5. Reputation of your auditor

For the audit and report alone, expect to pay $10k to $30k for a SOC 2 Type 1 audit and around $30k for a SOC 2 Type 2 audit.

Who can perform a SOC 2 Audit?

Only an AICPA accredited CPA firm can conduct your SOC 2 audit. However, that doesn't mean that every CPA firm is a good fit for your startup's SOC 2 audit. **(See audit section)**

Certain auditors are more startup-friendly than others. Find a CPA that understands the specific needs of tech-focused startups over more traditional companies. For example, you'll want to work with an auditor who understands the impact cloud-based information storage, co-working spaces, and other unique considerations have on compliance.

How are SOC 2 reports used in the sales process?

As mentioned previously, a SOC 2 report is particularly important for growth-focused B2B startups that are looking to move upmarket and attract bigger customers. Today, enterprise buyers now require businesses to become SOC 2 compliant.

Enterprise companies may love your product or service, but can't accept proposals until businesses answer 100-question security questionnaires. In order to fill those out, businesses need to have a SOC 2 program in place.

A SOC 2 report not only shows enterprises that your business is established, credible, and attuned to customers' needs, but also ready to answer their due diligence questions quickly and efficiently.

What is the structure of a SOC 2 report?

A SOC 2 report is broken down into four sections: Independent Auditors Report, Management Assertions, Description of the System, and Auditor's Tests of Controls and Results of Test. Let's break down the four:

What is the independent auditor's report?

The report from the auditor provides the service auditor's opinion on the system description, design, and operating effectiveness to meet the control objectives. Your auditor will provide an opinion of how the business tests against the Trust Services Principles in scope.

If the auditors' opinion agrees with the management assertions, a business will receive a clean bill of health, meaning a service organization's system can be trusted.

What are management assertions?

Management assertions provide facts and assertions made by the service organization that relates to the systems under audit. The business is responsible to provide complete, accurate, and reliable information for the assessment.

What is the description of the system?

The description of the system section provides an overview of the business services/offerings, and structure. This section will cover what the business is used for, what kind of data the system holds and transmits, and an overview of the types of users. Moreover, this section includes information on the internal business information like where employees are located, the types of teams the company leverages, and more.

What are the auditor's tests of controls and results of tests?

The auditor's tests of controls and results of tests section will typically be displayed in a matrix:

Objectives related to the criteria of the report

1. Controls in place at the service organization to meet the objectives
2. Auditor's tests of the controls
3. Results of the tests

What is a bridge letter?

Between SOC reports, audit firms sometimes issue 'Bridge Letters' to serve as intermediate validation that can be useful for your sales and security diligence conversations.

How often do you need to get a new report?

Your SOC 2 report lasts for one year. That means, once a year passes from your completed audit, you will need to undergo the process again.

This is because startups grow, processes and systems become more complex, and teams change. It doesn't take long for an ambitious startup to outgrow its audit. This means the evidence you gather and the controls your auditor tests in your subsequent annual SOC 2 audits will likely look different from your first.

While there's no obligation to pursue compliance to begin with, much less every year, you run the risk of upsetting customers and blocking sales, particularly bigger enterprise deals, by operating on a stale SOC 2 report.

Remember, many enterprise customers won't consider working with a startup without SOC 2 in place (See, Introduction for More Information)

CH.08 SOC 2 CHECKLIST

It can be challenging to understand the first steps when starting the SOC 2 process. Businesses implement and maintain SOC 2 in a variety of ways.

We broke down the basic process to tackle SOC 2 compliance into a checklist below.

1. **Choose objectives and TSCs**
   The first action item on your SOC 2 checklist involves the purpose of your SOC 2. Before diving into controls, an organization needs to determine the objective of their SOC 2 report and choose relevant TSCs.

   There are two types of SOC 2 reports, Type 1 and Type 2. Businesses typically start with a Type 1 and build up to a Type 2. We recommend this order for our own clients.

How do you determine which trust services principles to test for?

The type of information and data stored or transmitted by a business should determine the applicable TSCs.

SOC 2 encompasses 5 TSCs:

- Security
- Privacy
- Processing Integrity
- Confidentiality
- Availability

The only required criteria is security.

For more information on Trust Service Criteria, click here.

2. **Perform a gap analysis and develop a remediation plan**
   A compliance team examines the practices and procedures a business has in place and compares the security posture to SOC 2 best practices to identify gaps. Based on the gaps found, a strategic remediation plan is set to tackle SOC 2 in the most efficient way possible.

   Take a look behind the curtain at our own SOC 2 gap analysis and remediation plan here.

3. **Implement stage-appropriate controls**
   Enterprises need drastically different controls to demonstrate SOC 2 compared to startups. From logging and monitoring to HR tasks and vendor management, a compliance team can identify ways to save time and money by implementing the correct tools and processes.

4. **Perform a risk assessment**
   When control implementation is about 80% complete, the compliance team performs a risk assessment. As a crucial part of the audit, the risk assessment understands any potential risks an organization incurs through growth, geography, or outside information security best practices.

5. **Preparing for audit**
   After the risk assessment mitigation and acceptance process, the business needs to prepare for an audit.

   ### How do you prepare for a SOC 2 audit?

   While this means gathering evidence of implemented controls, it also means preparing an internal team to answer questions and work with auditors throughout the audit process.

   ### How do you determine your company's readiness for a SOC 2 audit?

   After your team collects and compiles evidence for auditors and assesses and accepts risk, the organization is ready for audit.

6. **Execute the audit**
   SOC 2 audits last between 2 weeks and a couple of months. This depends on the number of questions or corrections from the auditors. Though businesses cannot technically fail a SOC 2 report, many will want to correct discrepancies to avoid a poor report.

7. **Maintain and monitor compliance over a 12-month period**
   SOC 2 audits need to be performed on an annual basis. We recommend that our clients set up integrations to automatically collect evidence and monitor practices over time. This helps avoid heavy time commitments from team members and continues to secure information.

Thank you for reading Laika's SOC 2 University.

If you have any questions, or need information regarding SOC 2 or Laika, please feel free to contact us at **info@heylaika.com.**