

secureframe

The Ultimate Guide to SOC 2



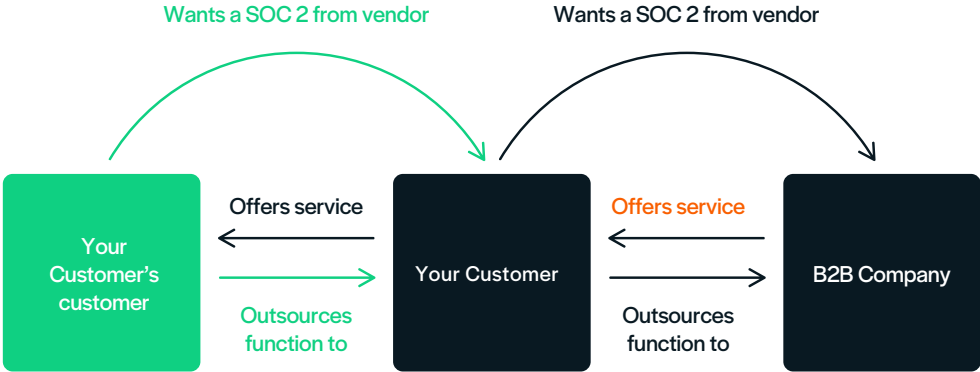
Part I: Introduction to SOC 2

Who Needs SOC 2?

Any organization offering a B2B service/product, along with any B2C organization handling sensitive customer information, should think about obtaining a SOC 2 (Service and Organizational Controls 2) report.

Why is SOC 2 Becoming More Important?

Increasingly, companies are outsourcing certain operations or departments to external service organizations. Think payroll (e.g., ADP Workforce Now, Gusto, Rippling), team communications (e.g., Slack, Microsoft Teams), and project management (e.g., Asana, Monday, Smartsheet). Many of the security and compliance risks of the service organization providing these operations become the risks of the companies using these external services. Understandably, a company outsourcing a function wants the service organization to provide a third party- generated report assuring appropriate compliance and security measures are met.



Does My Company Need a SOC 2?

The report applies to any organization providing a service for outsourcing the collection, processing, transmission, storing, organizing, maintenance, or disposal of customer information.

Relevant examples:

- Software companies providing operational services:
 - 🕒 Project management
 - 📅 Issue tracking systems
 - ✉️ Team communications
 - 🔒 Asset management and cybersecurity
 - 🔊 Salesforce automation
 - 🔗 Deployment automation
 - ☁️ Cloud hosting, compute, and/or storage
- Software companies collecting, processing, or otherwise handling sensitive customer data (SOC 2 can apply to any industry; however, more sensitive industries are noted below):
 - 🏦 Fintech
 - 🏥 Healthcare providers and payers
 - 💰 Payroll processors

Geographically, if you're targeting U.S. based businesses, SOC 2 has become the most commonly requested security and compliance standard for procurement and vendor security teams.

Lastly, your organization could technically not maintain any customer data but still be requested to obtain a SOC 2 by a customer to validate your organization's security controls and processes.

Why is SOC 2 Becoming More Important?

Increasingly, companies are outsourcing certain operations or departments to external service organizations. Think payroll (e.g., ADP Workforce Now, Gusto, Rippling), team communications (e.g., Slack, Microsoft Teams), and project management (e.g., Asana, Monday, Smartsheet). Many of the security and compliance risks of the service organization providing these operations become the risks of the companies using these external services. Understandably, a company outsourcing a function wants the service organization to provide a third party- generated report assuring appropriate compliance and security measures are met.

What Is SOC 2?

A SOC 2 report attests to the processes and controls a company has put into place to safely manage data in order to protect customer interests and data.






SOC 2 is one of the Service Organization Control (SOC) Frameworks developed by the American Institute of CPAs (AICPA). It is technically not a certification; it is a report based on a framework developed by the AICPA to be used by a certified accounting firm to audit, assess, and attest to a company’s compliance and security practices.



Specifically, a SOC 2 attestation report is the results from the CPA firm’s assessment using the agreed upon controls between the company and assessor against the company’s environment related to the security, availability, confidentiality, processing integrity, and privacy and the effectiveness of those controls. Security, availability, confidentiality, processing integrity, and privacy are Trust Service Criteria (TSC) developed by AICPA in order to help companies set criteria for managing customer data.

SOC 2 Trust Service Principles



Trust Service Criteria	Explanation
 Security	Information and systems are protected against unauthorized access and unauthorized disclosure, including potentially compromising damage to systems. Information (or data) should be protected during its collection or creation, use, processing, transmission, and storage.
 Availability	Data and systems are available for operation and use. Systems include controls to support accessibility for operation, monitoring, and maintenance.
 Confidentiality	The organization should protect information designated as confidential (i.e. any sensitive information).
 Processing Integrity	System processing (particularly of customer data) is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
 Privacy	Personal information is collected, used, retained, disclosed, and disposed of in accordance with relevant regulations and policies.

Security is the only required principle, but organizations typically include Availability and Confidentiality within the scope of an audit. Processing Integrity and Privacy are usually only included by larger organizations, stemming from internal requests or external customer requests.

Companies work with auditors and Secureframe to determine which of the five criteria should be in scope of the report.

I've Heard About SOC 1 and 3 - What are Those?

SOC 1, 2, and 3 are all Service Organization Control (SOC) Frameworks developed by American Institute of CPAs (AICPA) to attest to company internal controls and their compliance.

SOC 1 focuses on controls for financial reporting, whereas SOC 2 emphasizes controls for information security. SOC 2 targets companies providing a B2B service or B2C service (depending on the nature of the customer information). SOC 1 targets companies providing services that could affect clients' financial statements or internal controls over financial reporting.

The following companies could benefit from a SOC 1:

- FinTech companies
- SaaS companies focused on financial statements or accounting
- Payroll or payment processors
- Loan servicers
- Claims processors

SOC 3 is a more concise and high level version of the SOC 2 meant to be released publicly as marketing material (bragging rights). You cannot get a SOC 3 without first getting a SOC 2, but a SOC 3 can be issued in conjunction with a SOC 2 (at an additional cost).

What Is the Difference Between a SOC 2 Type 1 and a Type II?

A SOC 2 Type 1 report are the results of an assessment against the trust service criteria framework for a point in time. An auditor examines the design of the SOC 2 framework and creates a set of agreed upon controls to assess against by (1) examining the description of security and compliance controls and (2) reviewing evidence around controls.

A SOC 2 Type II report provides greater assurance to customers and partners than a SOC 2 Type 1 report because the auditor attests to the continued effectiveness of internal governance, controls, and processes over a period of time (rather than a point in time). For clarification, in a SOC 2 Type II audit, an auditor will request populations and samples as evidence stemming from the entire assessment window.

In summary, a SOC 2 Type 1 tests security control and process design for a point in time, whereas a SOC 2 Type II tests actual security controls and processes operating effectiveness over a period of time. During this period of time, the customer must operate without deviation from the required SOC 2 controls and processes - evidence collection does not start to occur until the end of this assessment period.

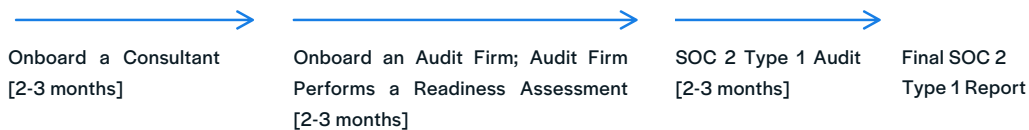
How Long Does It Take to Get a SOC 2 Report?

Historically, SOC 2 is a large and time-consuming process. Most companies target a Type 1 initially, followed by a Type II, because of the quicker turnaround time and it shows customers your commitment to getting a Type II.

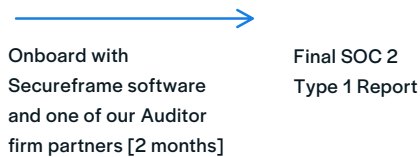
SOC 2 Type 1

There is a substantial difference between the time it takes to get a SOC 2 Type 1 Report the traditional way versus with Secureframe.

SOC 2 Type 1 : Traditional Way



SOC 2 Type 1 : With Secureframe



Type 1 - Timeline and Costs (Traditional Way)

- For organizations without internal security teams, the first step is to commonly hire an information security consultant to develop policies and processes for the company to follow and put into practice. This takes approximately 2 - 3 months. If the company is a larger enterprise company, the next step would be to bring in an audit firm and have them perform a readiness assessment that takes approximately 2 - 3 months.
- After those two steps, a company would move to undertake a SOC 2 Type 1 audit and, assuming everything is properly in place, the final report is delivered about 3 months after kicking off the audit.
- Approximate time for Type 1 report: 6 - 9 months
- Approximate cost for Type 1 report: \$60,000

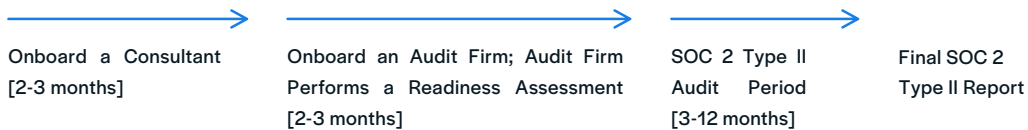
Type 1 - Timeline and Costs (With Secureframe)

- From onboarding to SOC 2 Type 1 Report in hand, it takes Secureframe 2 months
- Approximate time for Type 1 report: 2 months
- Approximate cost for Type 1 report: <\$40,000

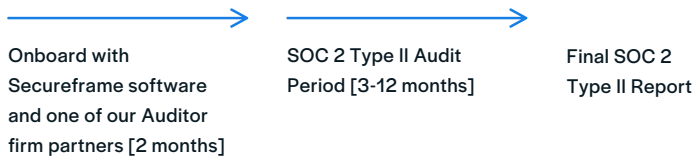
SOC 2 Type II

Similar to SOC 2 Type I, Secureframe can greatly speed up the process of obtaining a SOC 2 Type II report.

SOC 2 Type II: Traditional Way



SOC 2 Type II: With Secureframe



Type II - Timeline and Costs (Traditional Way)

- Similar to Type I, if a company doesn't have an internal security team, the first step is to hire an information security consultant to develop policies and processes for the company to follow and implement. This takes approximately 2 - 3 months.
- Similar to Type I, if the company is a larger enterprise, they'd bring in an audit firm to perform a readiness assessment that takes approximately 2 - 3 months.
- After those two steps, a company would undergo a SOC 2 Type II audit which can last anywhere from 3 to 12 months. The typical window is 6 or 12 months.
- Some companies opt for a 3 month window for their first SOC 2 Type II audit to complete the process quicker, but would typically do a 6 or 12 month window for subsequent audits.
- Approximate time for Type II report: 7-18 months
- Approximate cost for Type II report: \$100,000+





Type II - Timeline and Costs (With Secureframe)

- Onboarding with Secureframe's software and auditor firm partner takes 2 months
- After onboarding, a company would undergo a SOC 2 Type II audit which can last anywhere between 3 to 12 months. The typical window is 6 or 12 months.
- Approximate time for Type II report: 5-14 months
- Approximate cost for Type II report: <\$50,000

	With Secureframe	Without Secureframe
SOC 2 Type 1 Report	2 months	6-9 months
SOC 2 Type II Report	5-14 months (depending on audit assessment window)	7-18 months (depending on audit assessment window)

* Timelines can vary depending on number of security policies and processes in place as well as overall readiness

What Will Getting a SOC 2 Report Help With?

-  Speed up the sales cycle by eliminating security and compliance as a sales objection
 - In the process of preparing for SOC 2, Secureframe can help you prepare a compliance package for sales discussions
 - Easier to sell upmarket by gaining the trust of larger companies
-  Build new and existing customer confidence and satisfy their SOC 2 requests
 - A third party opinion that your security controls are in place and are effective, which helps in winning deals against your competition as well as retaining customers in the long run
 - The report assures legal and risk departments that your service is secure
-  Build a strong compliance and security foundation to avoid surprises later on
 - Creates a culture of cybersecurity and compliance
 - Creates a framework for managing security risks across the company
-  Improve enterprise cybersecurity
 - Builds security into your company's operations as important, clearly defined processes
 - Improves company-wide security awareness with defined responsibilities and practices

- 👤 Gain a competitive go-to-market advantage
 - Win deals against non-SOC 2 audited competition
- 👛 Increase investor, partner, and customer confidence
- ✅ Accelerate technical due diligence by a potential buyer or investor
- 🕒 Increase staff productivity by reducing time spent on vendor questionnaires
- 🔧 Satisfy regulatory needs
 - Although SOC 2 itself is not a regulatory requirement, it does overlap with several regulation-based frameworks such as PCI DSS and HITRUST
 - Pursuing SOC 2 compliance can expedite enterprise compliance efforts as a whole

Part II: Getting Audit Ready

Generally speaking, audit readiness action items fall into (9) categories:

-  Assemble Security Team
-  Organization and Management
-  Communications
-  Risk Management
-  Design and Implementation of Controls
-  Monitoring of Internal Controls
-  Infrastructure and Access Controls
-  Change Management
-  Assessing Audit Readiness

Our audit readiness items focus on the SOC 2's Common Criteria, Security, which applies to all SOC 2 audits. As we mentioned previously, larger companies or companies with a particular scope will add on Confidentiality and Availability in addition to Security, but for the purposes of our guide, we'll focus on Security.

Because the actions needed for a SOC 2 are numerous, we'll cover the first few action items for each category.

Assemble Security Leader and Team

- Fulfills Common Criteria 1 (CC1 - Control Environment) by ensuring that management and the board of directors emphasize security and integrity.
- Choose the appropriate team member to lead the information security program. This team member will be responsible for overall compliance and will assign responsibilities and oversee the collection of evidence required to complete your company's SOC 2.
- For smaller organizations, this is typically a CEO, CTO or VP of Engineering. At the very least, a member of senior management should take on the lead role for management of the information security program.

Organization and Management

- Fulfills Common Criteria 1 (CC1 - Control Environment) by ensuring that management and the board of directors emphasize security and integrity.
- Create a company organization chart with reporting lines and job titles.
- You'll need to keep your organization chart updated throughout the audit period.
- Create documented job descriptions for every role/title at the company.
- Require documented 1:1s or yearly performance reviews.

Communications

- Fulfills Common Criteria 2 (CC2 - Communications and Information) by ensuring clear procedures for the company team to communicate with one another and with partners, vendors, and other external parties.
- Put into place a change management process that uses a ticketing tool to ensure changes are properly authorized, documented, and communicated.
- Provide customers with a public email or contact form to report incidents, failures or other concerns.

Risk Management and Design and Implementation of Controls

- Fulfills Common Criteria 3 (CC3 - Risk Assessment) by emphasizing the importance of routine company "check ups" to identify new risks, analyze existing risks, and continue monitoring how changes could affect different risks.
- Create a Risk Management Program.
- Perform a Risk Assessment at least annually.

Monitoring of Internal Controls

- Fulfills Common Criteria 4 (CC 4 - Monitoring Activities) by continually observing and assessing the effectiveness of practices.
- Conduct penetration tests and internal/external vulnerability scans for your in-scope networks and systems.

- Fulfills Common Criteria 9 (CC 9 - Risk Mitigation) by formalizing vendor management and other business processes for responding to and improving upon risks.
- Create a vendor management program to manage vendor risk.
 - Often, vendor management is one of the most time consuming parts of the SOC 2 process. You'll need to assess the security posture of your highest risk vendors by creating a vendor security questionnaire specific to your company and manually follow up with each vendor until they fill out the questionnaire.

Infrastructure and Access Controls

- Fulfills Common Criteria 5 (CC 5 - Control Activities) by building procedures for processes and technology to decrease security risks and strengthen compliance.
- Fulfills Common Criteria 6 (CC 6 - Logical and Physical Access) by strengthening technical and data security.
- Fulfills Common Criteria 7 (CC 7 - System Operations) by creating processes for monitoring the company systems, including incident response and post-mortems.
- Requests for access to applications and systems must be documented and approved by the appropriate manager using least privilege and role-based access controls principles.
- Deploy and configure a log management system to identify events and trends that could impact the company's security objectives.

Change Management

- Fulfills Common Criteria 8 (CC 8 - Logical and Physical Access) by ensuring that any technical changes impacting system infrastructure are rigorously reviewed.
- Create a Change Management policy, including Version Control.
- Document your formal software development lifecycle methodology that governs the authorization, design development, configuration, testing, implementation, maintenance, and modification of software, systems, and infrastructure.

(SOC 2 Type 1 Only) Assess Audit Readiness

- During the audit readiness assessment, the auditor will make sure that you have the correct policies and controls in place. This includes setting up evidence collection processes so that there is a paper trail for the auditor to study.

Part III: The SOC 2 Attestation Report

What Goes Into a SOC 2 Attestation Report?

Your SOC 2 report consists of (1) a narrative and (2) a controls grid.

What Is a Narrative?

Your auditor will write a description of your company and its security and compliance practices, known as a “narrative”.

The Narrative consists of:

- A description of your company (legal jurisdiction, corporate structure, and established independence between the board of directors and executive team)
- A system and services description
- Control environment
 - The cadence of your established controls (which is usually annual), as well how you’ve gathered evidence to verify these controls
- System architecture
 - Will typically show diagrams of data flow and your security / system architecture

What Is the Controls Grid?

All of your controls will be examined against what was provided to the auditor as evidence to meet the framework requirements.

The auditor will list all controls and provide commentary on provided evidence as well. If evidence is insufficient, the auditor will note an “exception”.

Part IV: Getting a SOC 2 with Secureframe

The SOC 2 Process

The SOC 2 Process can be divided into the following stages:

1. Learn More About SOC 2
2. Survey Your Organization's Needs
3. Identify an Auditor
4. Establish Appropriate Policies and Controls
5. Implement Controls Using Processes and Tools
6. (SOC 2 Type II only) Collect Evidence that Controls Are Implemented
7. Receive Your SOC 2 Report






1. Learning More About SOC 2




You'll need to understand all of the smaller projects (specific to your company) that may arise as a result of the SOC 2 audit readiness process and build a formal SOC 2 roadmap. Examples of common tasks include:

- Implementing a ticketing system for access control and change management
- Configuring system logging, monitoring, and alerting mechanisms
- Conducting dynamic and static vulnerability scans for applications and code
- Creating a robust set of policies that's in alignment with SOC 2 requirements

Most companies completing a SOC 2 engage a consultant or advisor to help them understand and implement the processes required to undertake a SOC 2 audit.

With Secureframe, you won't need a consultant; our software does the heavy lifting.

	With Secureframe	With Consultant
 <p>Your Team's Time Commitment</p>	<p>~20 Hours *</p> <p>* Time commitment dependent upon initial readiness, environment complexity, and other key factors.</p>	<p>100-150+ Hours.</p> <p>A SOC 2 is a large undertaking with many moving pieces. It normally requires executive buy-in and regular meetings to ensure preparation stays on schedule.</p>
 <p>Audit Project Management and Evidence Collection</p>	<p>Integrated security compliance and audit readiness, including continuous, automated evidence collection via numerous system connections (e.g. AWS, GCP, Azure, Gusto, Gitlab, Zenefits, etc).</p>	<p>Need to project manage and assign individual evidence collection tasks to team members and a consultant, typically across project management software, spreadsheets, and ticketing systems. Manual evidence collection includes screenshots and cron jobs.</p>
 <p>Controls and Policies</p>	<p>Leverage Secureframe controls, policies and templates to meet SOC 2 requirements and streamline audit readiness.</p>	<p>Work with a consultant to build policies and reporting documentation for a variety of different controls.</p>
 <p>Vendor Management</p>	<p>Track and monitor vendor environments, risks, and compliance reports.</p>	<p>Manual and time consuming vendor management process. May take weeks or months to get a security questionnaire response from a vendor.</p>
 <p>Risk Management</p>	<p>Conduct risk assessments and track risks seamlessly and with support within the Secureframe platform.</p>	<p>Spend additional time trying to define and organize assets, threats, and vulnerabilities. Then perform risk calculations manually.</p>

 Access Monitoring	<p>Monitor who has access to what systems at all times based on connected integrations.</p>	<p>Maintain an internal access matrix which has to be manually updated every time access is changed within any in-scope system.</p>
 Asset Tracking	<p>Gain visibility into cloud assets, user devices, and code repositories and their respective owners through integrations in Secureframe platform.</p>	<p>Either manually track each in- scope asset within a spreadsheet or require ongoing spot checks of each individual system.</p>
 Proprietary Readiness Report	<p>Generate an audit readiness report to track framework-specific compliance progress which you can use to minimize security blockers during a sales cycle.</p>	<p>Pay an additional fee to your consultant or dedicated internal resource to perform a gap analysis and track progress to becoming audit ready on an ongoing basis.</p>

2. Survey Your Organization’s Needs

Define the Scope of Your Audit

You’ll want to define the scope of your audit up front. Rather than relying on an auditor to do this for you, it is important to be proactive about determining which systems, products, and/or business units are involved in the scope of the audit. The processes of determining the scope is a collaborative process between Secureframe, the auditor, and the customer.

Additionally, you’ll want to define which Trust Services Criteria you want to address within the scope of your audit (note: Secureframe can assist with this). The Trust Services Criteria are essentially categories of rules for managing customer data defined by the AICPA.

3. Identify an Auditor

Audits typically range from \$60k to \$100k or more, depending on factors such as the number of employees, physical offices, and overall size of the in-scope environment. At Secureframe, we will make introductions to our auditing partners and help bring your audit cost to as low as \$15k for a SOC 2 Type II report.

Once you've selected your auditor, Secureframe will facilitate communications with the auditor, streamline the evidence collection process, and advise on technical and audit related nuances.

4. Establish Appropriate Policies and Controls

Policies are written documents describing what best practice security and compliance processes your company implements while the procedures describe how those processes are implemented.

Major policies include:

- Encryption
- Data Classes
- Access Control
- Internal Control
- Acceptable Use
- Code of Conduct
- Risk Assessment
- Key Management
- Disaster Recovery
- Business Continuity
- Information Security
- Change Management
- Incident Response Plan
- And more

Controls are security practices aligned to a compliance framework to satisfy requirements provided by an auditor.

With Secureframe, we do the heavy lifting and help you build both your SOC 2 compliant policies and help establish your required controls. Not only do we work with you to customize our pre-created policy templates to your specific business needs, but we also work with your auditor to customize controls that best suit your environment.

5. Implement Processes and Tools

Working with Secureframe will save you significant time and effort since we'll make sure controls are correctly interpreted and any required process changes are implemented successfully across your organization. Additionally, we work with you to collect the evidence necessary to fulfill controls. In most cases, our platform collects audit evidence automatically through integrations, saving manual effort!

6. (SOC 2 Type II only) Collect Evidence that Controls Are Implemented over a Period of Time (the “audit period”)

You'll need to retrieve evidence to verify that your controls are implemented and effective during your entire audit period (usually 6 or 12 months). Typically, your auditors will want specific evidence uploaded for every single control - a process that can be daunting!

With Secureframe, we streamline the process by providing a Data Room where you can store all of your evidence in one location.

It is important to bridge the gap between the policies and controls you have on paper, and the processes and operations you have in practice to ensure your policies are actually implemented.

** At this point in the audit process, Secureframe can help you package your audit readiness materials into a compliance package for prospects that you can use to accelerate your sales process even if your SOC 2 audit is not complete yet.

7. Receive Your SOC 2 Report

Once your auditor is satisfied that your controls have been implemented effectively, you'll receive your SOC 2 Report which you can begin to share with prospects during the sales cycle.

How Secureframe can help you save time and costs when getting your SOC 2

The traditional SOC 2 process can take hundreds of hours of your company's time. It may also require you to hire a consultant to provide custom guidance for an extended period of time.

But Secureframe's software will take only a few hours of your company's time. We offer:

- Transparent Audit Pricing
- Customizable Policies
- Continuous Control Monitoring
- Turnkey Employee Onboarding
- Automatic Evidence Collection
- Simple, Real-time Dashboard for Audit Progress
- Industry Standard Risk Management Program
- Extensive Vendor Management
- Expert Audit and Compliance Guidance
- And More

Additionally, Secureframe can help you compile materials into a shareable compliance package for customers, allowing you to accelerate the sales cycle and security reviews even before you complete your SOC 2.

More Questions?

Reach out to support@secureframe.com to learn more!