SPRINTO

The only ‘SOC 2 for Startups’ Guide you will ever need.

Sometimes, you can do everything and still come up short.

Here's a SOC 2 for Startups Guide that ensures you stand tall.

Always.

Table of content

08 How much does SOC 2 Compliance Cost?

- How Much Does a SOC 2 Type 1 Compliance Cost?
- How Much Does a SOC 2 Type 2 Compliance Cost?
- SOC 2 Compliance Costs – why do they vary?
- Is There Any Other Cost of SOC 2 Certification?
  - Cost of Lost Productivity
  - Staff Training
  - Security tools
  - Readiness assessment
  - Legal fees
- What are the total SOC 2 Compliance Costs?

---

09 SOC 2 with Sprinto

- Why do you need SOC 2 automation?
- SOC 2: Manual vs Automation - What's the difference?
  - The opportunity cost of time and employee productivity
  - A faster and more confident approach to SOC 2
  - Cost of compliance
  - The evidence collection
  - Continuous monitoring
  - Vendor risk management
- How much does SOC 2 compliance cost with Sprinto?

01

What is SOC 2?

Service Organization Control 2, popularly known as SOC 2, is a voluntary security framework that defines how organizations must design their internal controls and other security-related operations to preserve customer data and privacy.

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 is a set of requirements designed for businesses that store customer data in the cloud.

SOC 2 attestations are based on the five Trust Services Criteria (TSC) of Security, Availability, Confidentiality, Processing Integrity, and Privacy (more on that later). The audits are conducted by third-party AICPA-certified auditors chosen by the organizations.

02

Who needs SOC 2?

SOC 2 is designed for businesses that store customer data in the cloud, making it relevant for all SaaS businesses and those that use the cloud to store customer information. Typically, businesses with a presence in the US or targeting growth in the region can consider getting SOC 2 attested.

03

Why do you need SOC 2?

More often than not, SOC 2 can be a critical decision-making component for enterprise customers. Startups with SOC 2 attestations stand a better chance at landing enterprise deals as against those that don't have SOC 2.

If your startup handles sensitive customer information, SOC 2 is a given eventuality. So, instead of waiting for a prospective customer to ask, it pays to get SOC 2 compliant sooner than later.

From our experience of working with hundreds of SaaS businesses, here's a quick overview of why you need a SOC 2:

1. **Customer Demand.**
   Necessary to win enterprise deals

2. **Cost-Effective.**
   A single data breach could cost you millions of dollars.

3. **Competitive Edge.**
   You compare favorably over competitors who aren't compliant.

4. **Securing your Business.**
   It shows your systems & networks are secure.

5. **Regulatory Journey.**
   SOC 2 dovetails other compliance frameworks too.

6 **Best Practices.**

It provides deep insights into your internal controls, governance, and more.

7 **Answer security questionnaires with ease.**

Use your time & resources for business functions.

Benefits of SOC 2

Customer Demand
Essential to winning enterprise deals.

Cost Effective
A single data breach could cost you millions of dollars

Best Practices
Get insights into your internal controls, governance & more

Competitive Edge
Your compare favoranly over competitors

Regulatory Journey
SOC 2 dovetails other compliance frameworks too.

Securing your business
You compare favorably over competitors

Answering security questionnaires with ease
Use your time & resources for business functions

04

What is a SOC 2 report?

A SOC 2 report is a detailed description of your SOC 2 audit. It is an evaluation by an independent certified auditor who checks if your business provides a secure, confidential, and private solution to your customers. The auditor releases the report after examining your organization's control over one or more of the Trust Services Criteria you have chosen.

The SOC 2 report contains the auditor's detailed opinion on your internal controls' design and operating effectiveness. It serves as a testimony of your infosec practices and enables your customers and customers' customers to assess and address the risks that arise from their relationship with your organization

Every SOC 2 report has five sections.

Section 1	Management of Example Cloud Service Organization's Assertion Regarding its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1
Section 2	Independent Service Auditor's Report
Section 3	**Example Cloud Service Organization's Description of its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1** **System Overview and Background** • Infrastructure •Software •People •Procedures • Data **Customer Responsibilities** - Relevant Aspects of the Control Environment, Risk Assessment Process,Information and Communication Systems, and Monitoring - Policies and Procedures - Physical Security - Logical Security - Monitoring - Relationship between CCM Criteria, Description Sections, and Trust Services Criteria
Section 4	Applicable Trust Services Principles, Criteria, and CCM Criteria and Related Controls, Tests of Controls, and Results of Tests
Section 5	Other Information Provided by Example Cloud Service Organization Not Covered by the Service Auditor's Report

How to read an auditor's opinion in a SOC 2 report?

Unqualified – You pass with flying colors!

The auditor's unqualified opinion indicates that the auditor found no issues during the audit. All the controls tested were designed appropriately (Type 1 report) and operated effectively (Type 2 report).

Qualified – Close, but not quite

This means that some areas need attention. What is the worst thing about a qualified report? It depends on the failed controls and how they affect the report's users.

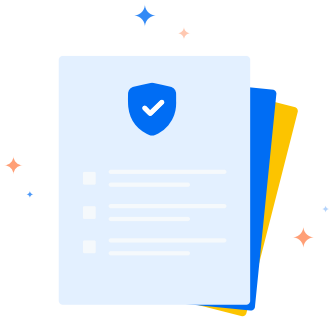
Adverse – You failed

An adverse opinion means the organization materially failed one or more standards, and its controls and system aren't reliable.

Disclaimer of Opinion – No comments!

This isn't really an opinion. Essentially, the auditor could not form an opinion based on the information provided. It occurs when auditors do not have access to the required information or cannot complete it neutrally.

05



What are the types of SOC 2 report?

A SOC 2 report comes in two types – Type 1 and Type 2. You can decide which one you want depending on what your customers require of you and the timelines you are ready to work with.

A SOC 2 Type 1 report affirms that the internal controls are in place at that point in time.

A SOC2 Type 2 confirms that the implemented controls are actually working too over a period of time;

SOC 2 Type 1 report attests that your internal controls have been effectively designed to meet SOC 2 requirements at a particular point in time; it's like a snapshot. Therefore, the SOC 2 Type 1 audit reviews the design of your organization's internal controls at a point in time.

SOC 2 Type 2 report (the one we think you will eventually need) confirms that the controls in place are working effectively too over a period of time. During a Type 2 audit, your auditor will test both the design and operating effectiveness of your internal controls over a period of time (typically three-six months).

SOC 2	Type 1	Type 2
What?	Attests that your internal controls have been effectively designed to meet SOC 2 requirements at a particular point in time	Tests both the design and operating effectiveness of your internal controls over a period of time (typically 3–12 months)
Why?	Starting your SOC 2 journey; are in a rush	Completed Type 1; not in a hurry
Monitoring Perios	Point in time	3–12 months

If you decide to go for Type 1, here's what it

- It shows you're committed to data security
- It indicates you plan on eventually becoming fully SOC 2 compliant
- It'll give you a ringside view of which organizational controls to include in the Type 2report
- It'll give you a practical understanding of the criteria auditors will want to test against in a Type 2 report

The audit for Type 1 doesn’t require a monitoring period, is less intrusive, and requires you to give a snapshot (with evidence) of the various checks and systems (read as controls) you have put in place to meet the SOC compliance requirements.

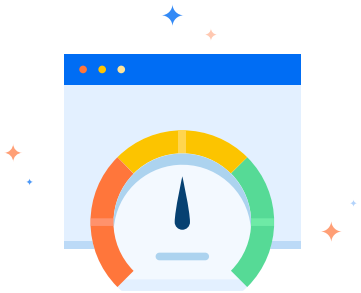
Even though a Type 1 report takes less time and makes for a great starting point, as your business grows, there's a high likelihood that your vendors and prospects will ask for the more comprehensive Type 2 compliance before working with you.

Here again, you ought to be aware that to obtain your Type 2 report, you must operate the controls over a period of time, about three-six months for the first audit and one year for subsequent audits.

Pro Tip:

- Know your customers' requirements to decide which type of SOC 2 report you need
- Allocate the budget for audit prep and the subsequent audit

06



What are SOC 2 Trust Services Criteria?

Formerly known as the Trust Principles, there are five Trust Services Criteria that businesses are evaluated on during a SOC 2 audit. Think of each criterion as a focus area for your infosec compliance program; each defines a set of compliance objectives your business must adhere to with your defined controls

Here's a quick overview of the five TSCs.

Security

It must be in scope for every SOC 2 audit and is, therefore, referred to as the common criteria. It requires you to enable access control, entity-level controls, firewalls, and other operational/governance controls to protect your data and applications. This TSC takes substantial effort and will require participation from your IT Development, IT Infrastructure, HR, senior management, and operations teams.

Availability

The Availability criteria in SOC 2 focuses on minimizing downtime and require you to demonstrate that your systems meet operational uptime and performance standards. It includes network performance monitoring, disaster recovery processes, and procedures for handlingsecurity incidents, among others. Business continuity, data recovery and backup plans are critical pieces here.

SOC 2 Certification

Security
- Network/application firewalls
- Two-factor authentication
- Intrusion detection

Confidentiality
- Encryption
- Access control
- Network/Application firewalls

Availability
- Performance monitoring
- Disaster recovery
- Security incident handling

Privacy
- Access control
- Two-factor authentication
- Encryption

Processing integrity
- Quality assurance
- Processing monitoring

Confidentiality

This principle requires you to demonstrate the ability to identify and safeguard confidential information throughout its lifecycle by establishing access control and proper privileges (to ensure that data can be viewed/used only by the authorized set of people or organizations). Confidential data includes financial information, intellectual property, and other business-sensitive details specific to your contractual commitments with your customer.

Processing Integrity

This principle assesses whether your cloud data is processed accurately, reliably and on time and if your systems achieve their purpose. It includes quality assurance procedures and SOC tools to monitor data processing. This is relevant for businesses that execute critical customer operations such as financial processing, payroll services, and tax processing, to name a few.

Privacy

It requires you to protect Personally Identifiable Information (PII) from breaches and unauthorized access through rigorous access controls, two-factor authentication, and encryption. Privacy is relevant to you if your business stores customers' PII data, such as healthcare data, birthdays, and social security numbers.

Everything you need to know about becoming SOC 2 compliant

07

A Step-by-step guide to becoming SOC 2 compliant?

Step 1 Choose your objectives for SOC 2 compliance

The first action item of the SOC compliance checklist is to determine the purpose of the SOC 2 report. The specific answers to why SOC 2 compliance is important to you would serve as the end goals and objectives to be achieved in your compliance journey

Here are some examples

- Your customers have asked for it
- You are entering a new geography, and SOC 2 compliance will add to your strength
- You want to bolster your organization's security posture to avoid data breaches and the financial and reputation damage that comes with it
- You are catching up with competitors who are SOC 2 compliant

That said, not wanting a SOC 2 compliance because customers aren't asking for it or because none of your competitors has it isn't advisable. It's never too early to get compliant. It's always an advantage to be proactive about your information security.

Step 2 Identify the type of SOC 2 report you need: SOC 2 Type I or SOC 2 Type II

As we mentioned earlier, a SOC 2 report comes in Type 1 and Type 2. You can decide which one you want depending on what your customers require of you and the timelines you are ready to work with.
For instance, choose SOC 2 Type 1 if you are starting your compliance journey or are pressured for time and need to show compliance intent to prospects or customers

Choose SOC 2 Type 2 if you are already compliant with other frameworks, have completed your SOC 2 Type 1 and the three-six months observation period or your customers have specifically asked for it. The level of detail required regarding your controls over information security (by your customers) will also determine the type of report you need. The Type 2 report is more insightful than Type 1.

Here's how you can identify which SOC2 report better fits your requirement. insightful than Type 1.

- [ ] We have undergone a SOC 2 audit before
- [ ] Our SOC2 report requirement isn't urgent (within 3–6 months)
- [ ] We have dedicated resources to develop and implement security policies
- [ ] Our workforce understands their roles and responsibilities when implementing controls
- [ ] We have a system in place to communicate system changes

If most of your answers are a no, it perhaps make better sense to start with a SOC 2 Type I audit. You can get to the SOC 2 Type II audit once security controls and processes are in place.

Step 3 Define the scope of compliance based on the Trust Service Criteria (TSC)

Defining the scope of your audit is crucial as it will demonstrate to the auditor that you have a good understanding of your data security requirements as per the SOC 2 compliance checklist. It will also help streamline the process by eliminating the criteria that don't apply to you.

You must define the scope of your audit by selecting the TSC that applies to your business based on the type of data you store or transmit. Note that Security as a TSC is a must. Regulatory requirements will also have a bearing on your criteria selection. That said, in our experience, most SaaS businesses typically only need Security, Availability and Confidentiality (or their combination) as TSC in their SOC 2 journey.

Select the TSC that applies to you

Security

- [ ] Do you review and document your security procedures?
- [ ] Do you have backup and recovery procedures in place?
- [ ] Do you have specific procedures to handle cyber safety incidents?

Availability

- [ ] What is your service uptime?
- [ ] Do you have processes to address service issues that affect your availability?
- [ ] Do you have access controls in place for your Who all can access your service?
- [ ] Are there any restrictions?

Confidentiality

- [ ] How do you handle and process confidential data?
- [ ] Do you have access management incorporated into your organization?
- [ ] How do you avoid unauthorized access? Do you have processes in place?

Processing Integrity

- [ ] Are your processing systems providing timely and accurate data to users?
- [ ] How do you ensure the integrity of data?
- [ ] Do you have specific procedures in place to correct errors quickly?

Privacy

- [ ] Do you have a data retention policy that's documented and communicated to customers?
- [ ] Do you store personally identifiable information (PII)? If yes, where and how do youstore it?
- [ ] Do you protect PII on your system?

A SOC 2 audit looks at your infrastructure, data, people, risk management policies, and software, to name a few items. So, at this stage, you must also determine who and what within categories will be subject to the audit. For instance, you can keep some of your non-production assets from the scope of the audit

Step 4 Conduct internal risk-assessment

Risk assessment and risk mitigation are crucial in your SOC 2 compliance journey. You must identify any risks associated with growth, location, or infosec best practices and document the scope of those risks from identified threats and vulnerabilities. You should assign a likelihood and impact to each identified risk and then deploy measures (controls) to mitigate them per the SOC 2 checklist

Here are some questions to help you in this process:

- [ ] Have you identified the potential threats and associated risks to your business?
- [ ] Have you estimated the potential impact of these threats on your business?
- [ ] Have you tagged the critical systems based on the risks identified?
- [ ] Have you developed mitigation strategies for the risks?

Any lapses, oversights or misses in assessing risks at this stage could add significantly to your vulnerabilities. For instance, missing to identify the risks for a specific production entity (endpoint) in the case of an employee on extended leave or lapses in risk assessment of consultants/contract workers (not employees) could leave a gaping hole in your risk matrix.

To Dos

- Make an inventory of the critical systems and internal controls
- Draw a line between production and non-production systems
- Identify business risks, assign a likelihood and impact to each of them
- Deploy policies and procedures to mitigate them

Step 5 Perform gap analysis and remediation

You must examine your procedures and practices at this stage and compare their compliance posture with SOC compliance checklist requirements and best practices. Doing this will help you understand which policies, procedures, and controls your business already has in place and operationalized and how they measure against SOC 2 requirements

Here are some questions to point you in the direction:

- [ ] Do you have a defined organizational structure?
- [ ] Do you have authorized employees to develop and implement policies & procedures?
- [ ] What are your background screening procedures?
- [ ] Do your clients and employees understand their role in using your system or service?
- [ ] Are your software, hardware, and infrastructure updated regularly?

Remediate the gaps with improved or new controls, as applicable. These may include modifying workflows, introducing employee training modules, and creating new control documentation. The risk ratings (carried out earlier) will help you prioritize the remediation

Here are some common remediation practices to get you started

- [ ] Align and deploy controls based on the chosen TSCs
- [ ] Set up a clear organizational structure
- [ ] Have well-defined infosec policies & procedures
- [ ] Conduct background screening procedures for all new employees
- [ ] Ensure changes in the code repositories are peer-reviewed
- [ ] Conduct periodic security training of all employees
- [ ] Collect evidence of compliance

> Remember, SOC 2 audit requires you to produce evidence for the processes, policies and systems you have put in place. Evidence can be your information security processes and procedures, screenshots, log reports and signed memos, to name a few. Your inability to show demonstrable proof of SOC 2 compliance requirements can get flagged as **exceptions** by the auditor. And you don't want that!

Implement stage-appropriate controls

At this stage, you will align and implement internal controls to demonstrate how your organization meets the SOC 2. Each of the five TSCs in SOC 2 comes with a set of individual criteria (totalling 61). You will, therefore, need to deploy internal controls for each of the individual criteria (under your selected TSC) through policies that establish what is expected and procedures that put your policies into action.

Know that the controls you implement must be stage-appropriate, as the controls required for large enterprises such as Google differ starkly from those needed by startups. SOC 2 criteria, to that extent, are fairly broad and open to interpretation.

For instance, you may implement two-factor authentication to prevent unauthorized access to your network, while another organization may choose to implement firewalls, while others may deploy both!

Step 6 Undergo Readiness Assessment

A readiness assessment evaluates whether you meet the SOC 2 requirements to undergo a full audit. You can hire an independent auditor to perform it. Note this auditor is NOT the SOC 2 auditor you will hire for your SOC 2 attestation.

Here are the focus areas for the readiness assessment:

Gap analysis – The independent auditor will detect vulnerabilities and gaps and generate a list of specific recommendations and actions. It takes around 2–4 weeks from start to finish.

Controls matrix – They will also evaluate and help you build your controls matrix, detailing your objectives map, internal controls identification, and control characteristics.

Auditor documentation – The auditor will vet your documentation and suggest improvements.

Based on the auditor's findings, remediate the gaps by remapping some controls or implementing new ones. Even though technically, no business can 'fail' a SOC 2 audit, you must correct discrepancies to ensure you receive a good report.

Step 7 SOC 2 audit

Authorize an independent certified auditor to complete your SOC 2 audit and generate a report. While SOC 2 compliance costs can be a significant factor, choose an auditor with established credentials and experience auditing businesses like yours.

Expect a long-drawn to-and-fro with the auditor in your Type 2 audit as you answer their questions, provide evidence, and discover non-conformities. Typically, SOC 2 Type 2 audits may take between two weeks to six months, depending on the volume of corrections or questions the auditor raises. Type 2 has a mandatory monitoring period of three-six months. A Type 2 report offers more significant insights into your organization's controls and their effectiveness.

Here are some questions the auditor may ask:

- [ ] Can you share evidence to show that all your employees undergo background verification?
- [ ] Can you show proof of how you ensure that the changes in your code repositories are peer-reviewed before its merged?
- [ ] Can you demonstrate with evidence that you remove access to emails and databases once an employee resigns from your organization?
- [ ] Can you show proof that you run background checks on all your employees?
- [ ] Can you share proof of how you maintain the endpoint security of all systems?

> In comparison, the audit for Type 1 doesn't require a monitoring period, is less intrusive, and requires you to give a snapshot (with evidence) of the various checks and systems (read as controls) you have put in place to meet the SOC compliance checklist requirements. Note that after you clear your SOC 2 Type 1 audit, you must go through an observation period of three to six months before applying for Type 2.

Step 8 Establish Continuous Monitoring Practices

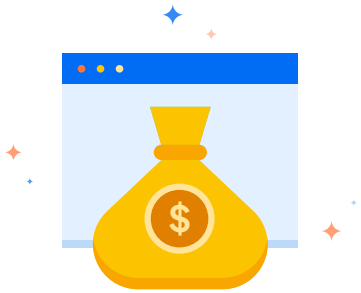
Getting your SOC 2 compliance report isn't just a one-time event. The report is just a start as security is a continuous process. It, therefore, pays to establish a robust continuous monitoring practice as SOC 2 audits happen annually. For instance, when an employee leaves your organization, a workflow should get initiated to remove access. If this doesn't happen, you should have a system to flag this failure so you can correct it. .

Here are some guidelines on what a robust continuous monitoring practice can achieve:

- It should be scalable; it should grow with your organization
- It should make evidence collection easy and streamlined
- It shouldn't get in the way of your employees' productivity
- It should alert you when a control isn't deployed or deployed incorrectly
- It should give you the big picture as well as an entity-level granular overview of your infosec health at any point in time.

These apart, you will need to undertake measures (at additional cost) such as mobile device management (MDM) software, vulnerability scanners, incident management systems, updation of security measures, and pen-testing, among others, all these measures should part of your SOC compliance checklist.

08



How much does SOC 2 Compliance Cost?

SOC 2 compliance costs aren't cheap. We won't pretend that it is!
But that doesn't make it any less worthwhile – in fact, you should view it as an investment that could bring you invaluable business in the future.

But exactly how much does a SOC 2 compliance cost? The answer depends on various factors; hence, the costs will vary accordingly.

SOC 2 compliance cost in 2023 averages between **$30000 – $150000**.
The actual costs of getting.

SOC 2 compliant would depend on the eight criteria below

1. **Type of Attestation Required**
   SOC 2 Type 1 or SOC 2 Type 2 or both

2. **Size of the Organization**
   Costs increase with the size of the company

3. **Audit Scope**
   Costs increase with the number of Trust Service Criteria chosen

4. **Maturity of your Security Controls**
   Costs increase if the current security practices aren't robust

5. **Complexity of Organization**
   Costs spiral up with the complexity of systems & controls

6 **Type of Auditor chosen**

CPAs (or firms) come with different price tags

7 **Security Tools**

Costs of SOC tools typically needed to ensure compliance add up too

8 **Readiness Assessment**

Costs vary based on the type of auditor chosen (optional)

Let's dig into some of these criteria to help you understand the costs better.

SOC 2 Type 1 vs SOC 2 Type 2 Compliance Cost

In SOC 2 Type 1 compliance, your organization will be assessed for the design of your internal controls, such as policies, procedures, and controls at a point in time.

We'd estimate the starting costs of a SOC 2 Type 1 audit alone to range between **$8000 to $30000**, while the cost of SOC 2 Type 2 with a more extended evaluation window of 3–12 months ranges between **$20000 – $50000**.

The final costs, as mentioned earlier, depend on your organization's size, complexity (of systems & controls), audit readiness and the type of auditor chosen.

These costs don't include the cost of readiness assessment (optional), additional security tools needed and the lost productivity costs of employees involved in the process. We have covered these cost overheads in the later part of the eBook.

Pro Tip:

As much as you want to keep a lid on the costs, choose an auditor with established credentials and experience in auditing businesses like yours. Remember, your SOC 2 report is only as good as the auditor who attests it.

The cost of continuous monitoring

Continuous monitoring also adds to your SOC 2 compliance cost. The cost of running continuous monitoring programs for your information security management systems depends on how you prefer to operate them on an ongoing basis.

You could:

- Use internal expertise and bandwidth to implement this manually
- Hire consultants/external help to run cyclical internal audits
- Purchase a continuous monitoring tool

Using internal resources adds to lost productivity costs and takes up hundreds of hours. A consultant to help run cyclical internal audits can cost about **$10000**.

Is There Any Other Cost of SOC 2 Certification?

There are many other potential SOC 2 compliance cost mines.
Here's how they stack up.

- Cost of Lost Productivity
- Staff Training
- Security Tools
- Readiness Assessment
- Legal Fees

Cost of Lost Productivity

SOC 2 compliance is extensive work and demands hours from multiple people within your business. These employees would be busy doing their important work in an ideal world.

The cost of lost productivity is challenging to quantify, but you will notice when you start losing hours of employee productivity to SOC 2 each week

Even if you have managed to prep for the audit with limited hands on-the-job (or with the help of a consultant), the actual audit will need help and support from most departments within your business.

People will almost certainly need to be removed from their day-to-day tasks to work on the audit.

For instance, some of your key hires (engineering leads, people ops, and senior management) will need to join meetings and calls with the auditor, liaise with the consultants, spend time on remediation of issues found in the report, and work on implementations, to name a few.

All these are exhaustive in scope and will require substantial time and effort. SOC 2 will likely take much time from the people within your teams with the best knowledge of the security controls under assessment.

💲 **Cost:** Can run into thousands of dollars

Staff Training

Your employees are the first line of defense in a security threat or data breach. SOC 2, therefore, emphasizes the security training of staff. Generally, staff awareness training costs $25 per user, but the costs can run up to **$15000** per training session (trainer costs) depending on the content, quality, and training company.

New security tools needed to become SOC 2 compliant could also require staff training.

- Background Checking Software
- Backup Software
- Encryption Tools
- Antivirus and Anti-phishing Solutions

Whether you carry out security awareness training in-house or via a third party, there'll be associated time and monetary costs.

💲 **Cost:** **$25** per user to **$15000** per session

Security Tools

Before requesting an audit, invest in softwares and tools to improve your security posture. You can base your choice of tools on the results of your gap analyses & assessments.

Here are a few technical security measures you may need:

- Monitoring the security of your staff's laptops with MDM
- Antivirus software
- Password manager for your employees
- Vulnerability scanning solutions for codebases or hosting infrastructures
- Incident response and management system for operational and security incidents

Depending on what you need, the costs will add up. MDM, for example, costs about **$48** per user annually, while vulnerability scanners range from **$6000** to **$25000**. Password managers and antivirus software, however, are available for free too.

Cost: can vary from **$7000** to **$25000+**

Readiness Assessment

Although readiness assessment is optional, it helps prepare you for the eventual SOC 2 audit. Here, an external consultant (whom you employ for the job) tests all your SOC 2 controls, highlights the gaps, and makes recommendations on how to remediate them before the SOC 2 audit.

If your organization does decide to carry one out, you'll get:

- A neutral opinion on your SOC 2 audit readiness
- Help to see weaknesses and points of failure in your existing internal controls
- Ideas on how to make your processes and procedures stronger

Estimates for a readiness assessment start at around the **$10000** mark. And, of course, if the evaluation throws up many issues that need fixing – those are further costs to be considered.

💲 **Cost: $10000**

Legal Fees

All the data protection policies you've signed up for can affect your SOC 2 readiness. Any legal document that has a bearing on how data gets handled within your organization must be reviewed ahead of the SOC 2 audit – as there's no use in security controls that put you in breach

You'll need to consider any legal fees associated with the review of your existing legal agreements.

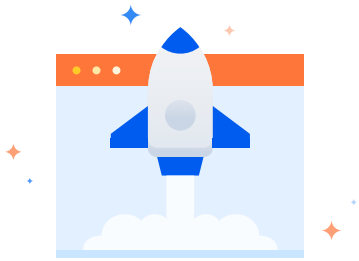
These could include:

- Contractor Agreements
- Employment Agreements
- Customer Agreements

Bear in mind that legal documents may also need to be revisited later.

💲 **Cost:** This can vary depending on the extent of legal work required

09



SOC 2 With Sprinto

Sprinto is tailored to suit the specific needs of cloud-hosted organizations. From 100+ integrations to 15+ frameworks, Sprinto's platform makes it easier for organizations to manage and demonstrate their information security compliance and certifications.

Sprinto automates repeatable compliance tasks and gives you a real-time, 24×7, continuousmonitoring overview of your SOC 2 security profile. It automates the evidence collection needed to demonstrate SOC 2 compliance and makes it easier and error-free to become and remain compliant.

And in the process, it saves your businesses a ton of time and money.

Why do you need SOC 2 automation?

As a cloud-hosted business, you have several information assets, such as servers, S3 buckets, load balancers, laptops, and more. And when you list all the assets where information is stored, including your vendors, the list could run into thousands! SOC 2 requires you to secure all your information assets per the risks identified for each of them.

For instance, if it's an S3 bucket, you must ensure it isn't publicly accessible. Or, if it's an EC2 instance, you need to protect its Secure Socket Shell (SSH) access and keep the database and hard disk encrypted

In essence, every asset type needs a different kind of security check. Now imagine running and monitoring these checks on thousands of assets every day. Trust us; it will soon snowball into a security nightmare!

With SOC 2 automation softwares, this is a solved problem. The SOC 2 compliance automation software lists all your information assets, defines and maps controls for different information assets, and continuously monitors them to ensure compliance status gets maintained always.

So, SOC 2 automation makes compliance faster, easier, and error-free.

SOC 2 Manual vs Automation: What's the Difference?

As cloud-hosted companies, you would have an intrinsic understanding of the benefits of automation. Aside from the generic advantages, here are the key factors that swing the deal in favor of automation.

The opportunity cost of time and employee productivity

The manual approach to SOC 2 requires your key engineering hires and the CTO to spend considerable time setting up the processes and documentation initially. And later, after a successful attestation, they will need to monitor and maintain compliance and repeat the entire process before the SOC 2 attestation expires (a year later).

Automation solves this problem smartly. It only needs an initial investment of time and effort during the implementation of SOC 2 compliance automation software. However, subsequent audits and monitoring are relatively simple.

Sprinto's SOC 2 automation software further reduces your team's investment in terms of time by allocating a dedicated compliance expert who walks you through the entire process. Having a dedicated compliance expert's support allows your infosec team to eliminate the time they would have otherwise spent attending self-learning tutorials on software implementation.

HackerRank

> *While the onus is still on the teams and employees to complete their tasks, since using Sprinto, our engineering teams are spending as much as 20% less time looking for problems. The platform automatically alerts us when something needs to be done, where we need to look, and what will take us to the 100% compliance mark.*

A faster and more confident approach to SOC 2

A manual approach to SOC 2 (whether you do it yourself or hire an external consultant) easily takes up 3–4 months in audit preparation. Much time gets spent understanding the SOC 2 requirements, implementing them, and undergoing rounds of SOC 2 self-assessments and SOC 2 readiness assessments. Even after all this, you wouldn't walk into an audit as confidently as when using automation software.

Sprinto offers a health dashboard that gives you an objective real-time overview of your compliance. Once you have plugged all the control gaps and hit the 100% audit readiness mark on your dashboard, rest assured that you can walk into the audit without worrying about the outcome.

What's more, when you automate SOC 2, your audit prep time reduces considerably. Depending on the type and size of your organization, the scope and type of SOC 2 report and your security readiness, it would roughly take you anywhere from a couple of weeks to a maximum of a month to get your SOC 2 ducks in a row if you work with Sprinto

PreSkale

> *For us, information security, code optimization, and product development all command the same priority. Indeed, to deliver value is to deliver it securely – this is the ethos we stand by and hope to cultivate in our culture.*

Cost of compliance

Aside from the auditor's fee, the SOC 2 compliance cost depends on the type of attestation needed, the size of your organization, the scope of the audit, and the cost of security tools needed. While adopting a DIY approach may seem like a low-cost option, the cost of lost productivity can add up significantly.

Sprinto's compliance automation platform is priced at a starting price of only **$8000** (depending on the organization's size).

The evidence collection

The manual route requires you to maintain pieces of evidence to demonstrate compliance, such as screenshots, policy documents, and whatnot. Therefore, the back-and-forth email threads with the auditor tend to be long and cumbersome. It also requires you to establish a secure way to share the required evidence with the auditor.

Sprinto integrates with your systems and infrastructure and simplifies evidence collection and audits. So, instead of sifting through folders looking for specific evidence, your auditor gets presented with pieces of evidence that are bagged, tagged, and neatly organized, just like how they like it.

Sprinto supports automatic and manual evidence collection to accommodate edge cases.

Continuous monitoring

Sprinto continuously monitors your compliance status and alerts you in cases of lapses, delays and non-compliance.

For instance, it automatically alerts you if an employee has yet to be offboarded (in terms of revoking access) or if a new employee still needs to undergo the staff security training program.

Real-time monitoring helps you know your compliance status at any point in time. And take quick remedial actions when needed. In contrast, the manual route isn't continuous and relies on spot checks to monitor your compliance status.

Vendor risk management

Sprinto offers robust vendor risk management features, allowing you to manage vendor agreements and certifications. The manual approach, in comparison, is long-winded and less robust.

How much does SOC 2 compliance cost with Sprinto?

When you use Sprinto's compliance automation platform, your entire SOC 2 experience is seamless, effortless and error-free. Sprinto automates all the manual, error-prone, repetitive busy work with minimal intervention and time from your staff.

Sprinto's compliance automation platform is priced at a starting price of only **$8000** (depending on the organization's size).

Here's all that you get access to with Sprinto as your compliance partner.

- Sprinto comes built with a continuous monitoring system that validates your compliance with proof and alerts you when something isn't done or done incorrectly.
- MDM, Security Awareness Training, and Incident Tracking Software (~$1000+) come bundled into the platform.
- You can access Sprinto's network of partners to assist you with pen etration tests and vulnerability assessments at discounted rates.
- Sprinto offers built-in support for free/open-source vulnerability scanners.
- Additionally, when you utilize Sprinto, you get access to a network of certified auditors who can perform SOC 2 audits for a reduced cost starting at $4999 (depending on the size of the organization).
- You can view your audit readiness anytime on the Sprinto dashboard.
- You get access to Sprinto's in-house compliance experts, who hand hold the entire audit prep process for you.
- Sprinto also offers out-of-the-box policies (pre-approved by our auditors) that can help you indirectly save on legal costs.
- Save on the opportunity cost of lost productivity by keeping SOC 2 from getting in the way of your employees' work.
- You save time as Sprinto can help you get audit-ready in weeks

Book a demo today to learn more about how Sprinto can help you breeze through your SOC2 journey

Get in touch:
sales@sprinto.com
www.sprinto.com

SPRINTO