Zero to SOC 2 Compliance Roadmap for SaaS Platforms

Nick Leghorn
Co-Founder, Secure Start Partners
info@securestartpartners.com

Secure Start Partners

SecureStartPartners.com
info@securestartpartners.com

Introduction

In today's fast-evolving cloud landscape, data security and privacy are paramount, especially for companies building Software as a Service (SaaS) applications. As businesses entrust more critical data and services to SaaS providers, the demand for verifiable security assurances grows. The SOC 2 audit has emerged as a leading standard for assessing the internal controls related to data protection, making it an essential consideration for SaaS organizations aiming to build trust with clients, partners, and regulators.

SOC 2 compliance has become particularly popular among SaaS companies due to increased customer scrutiny, competitive differentiation, and regulatory pressures. As more enterprise customers demand evidence of robust security controls before engaging with a SaaS provider, SOC 2 attestation often serves as a prerequisite for business. The audit provides a trusted, independent validation that a company adheres to stringent security standards—helping SaaS companies accelerate enterprise sales cycles and build lasting customer confidence.

The problem is that, for smaller companies, the expense and the complexity required to achieve a clean SOC 2 audit might actually not make it a profitable or realistic business objective. On the other hand, it could also be the key to unlocking significant additional customers that otherwise would be reluctant to sign up.

The goal of this whitepaper is to give companies an idea of what's required for a SOC 2 audit, some of the larger components that are involved, and a three-phased approach that has worked well in the past for implementing the controls required to successfully complete an audit.

Having A Guide May Be Useful

Before we dig in, take a quick look at the page count on this document. This is just a general overview of the process of getting a SOC 2 audit completed and does not go into detail about how specific controls need to be implemented or give advice about what kinds of strategies will pass scrutiny with auditors.

If you've never gone through an audit before or don't have much experience working directly with auditors you may find yourself at a disadvantage that results in an unsuccessful audit, one that costs significantly more than expected, or has an unnecessarily large negative impact on the ability for the business to continue to innovate.

Having a trusted partner riding shotgun for the audit is an investment – allowing your employees and executives to focus on the business while the audit runs smoothly in the background, removing roadblocks that may appear along the way, and ensuring that the company can get the maximum value from the final report instead of being stuck with a report that doesn't actually meet your customer's needs.

That's exactly the support and assistance that Secure Start Partners can provide. If that is something you believe might be helpful, reach out and let's start a conversation. Our contact information is on the cover page.

Quick Overview of the SOC 2 Audit

The SOC 2 framework was developed by the American Institute of Certified Public Accountants (AICPA), a prestigious body overseeing standards for certified public accountants in the United States. SOC (or System and Organization Controls) reports originated from the need to provide independent validation of a service organization's internal controls. Unlike traditional financial audits, SOC 2 was designed specifically to address the controls relevant to protecting the privacy, security, and integrity of customer data, as outlined in the Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, and Privacy).

There are two main types of SOC 2 reports: Type 1 and Type 2. A SOC 2 Type 1 report evaluates the design and implementation of systems and controls at a specific point in time—essentially providing a snapshot of an organization's risk management posture. In contrast, a SOC 2 Type 2 report not only assesses the design but also examines the operational effectiveness of these controls over a defined period, typically spanning several months. The Type 2 report provides a higher level of assurance, showing that safeguards are not just in place but are consistently followed.

Typically, companies will prefer a SOC 2 Type 2 report due to the improved assurance that it provides, but will accept a SOC 2 Type 1 report for some lower risk activities or for companies that don't have sufficient corporate history to support a Type 2 report. It may be possible for some companies to simply continue getting a Type 1 report year after year rather than progressing to a Type 2 report depending on customer requirements and expectations, but this may also open the door to some questions that the company would prefer not to answer.

Technically the SOC 2 and its associated Trust Services Criteria (TSCs) are not prescriptive – they do not have a checklist for specific controls that are required to be implemented in every organization. Instead, auditors and companies are expected to work together to define a set of controls that are appropriate to properly secure the company and its systems that align with the Trust Services Criteria. While there can be some differences from one SaaS platform to the next, typically for most SaaS platforms the controls recommended by auditors are consistent and predictable, and can be broken down into three broad phases as described below.

The one thing to keep in mind about the SOC 2 is that this isn't simply an audit of the product or the technical infrastructure of a company – **this is an audit of the maturity of the company as a whole**. That includes the hiring process, performance management for employees, financial controls, and a whole lot more. A successful SOC 2 audit requires cooperation from all areas of a business, and starts by taking stock of what's going well and what needs improvement.

Phase One: Risk Assessment and Penetration Testing

Most people reading this paper will simply see a SOC 2 audit as a means to an end. It's a piece of paper they need to be able to sell their service and gain new customers. But the reality is that a SOC 2 audit is an opportunity to improve and mature the business, ensuring that the right structures are in place to keep the business healthy and growing no matter what comes down the road.

Both for the SOC 2 and generally for the business, the right place to start is with a **Risk Assessment**. This is a process where an expert comes into the business, reviews existing documentation, conducts interviews with company leaders, and returns a document that describes the current risks that the business is facing and some recommended improvements that can be made to reduce those risks. It also reviews any existing controls and determines whether they are operating effectively, or if there is anything that needs to be adjusted.

One important piece of information that is required to perform a good risk assessment is a recent **penetration test**. Typically SOC 2 auditors will require a penetration test to happen once every 12 months, no matter whether the company is trying to achieve a Type 1 or a Type 2 audit.

Something to be aware of is that there is a difference between "penetration testing" and "vulnerability scan". Most auditors will require a manual penetration test, which is an engagement from an independent third party where a team of security experts assess the platform and look for any vulnerabilities. This is different from a vulnerability scan, where an automated system will programmatically test for known vulnerabilities. The manual penetration test provides a higher quality signal for issues that might exist in the SaaS platform, and the results are typically something that customers will also ask to see during the sales process.

For newer companies, the risk assessment process is typically best performed by a third party vendor who is experienced in this kind of assessment. They likely have seen similar companies in similar states of maturity and can make recommendations that will maximize the risk reduction for the business with the minimal cost of investments.

Important to remember is that, throughout this process, the business is in charge of its own destiny. A good risk assessment isn't a pass or fail scenario but instead the start of a conversation, one where the business is able to understand what level of risk they currently experience, identify what kind of appetite for risk they have, and what they need to do to make reality match their appetite.

Phase Two: Paperwork, Process, and Tooling

As a result of the risk assessment process, it is likely that there will be specific controls identified that should be implemented or adjusted. These controls are codified within companies as written policies, which neatly brings us to the next phase of the process.

Auditors for SOC 2 expect written policies to exist, be approved by management, and be reviewed every year by company leadership. They also expect that these policies are acknowledged by employees at the start of their employment and again every year or whenever policies change significantly.

The content of these policies starts with the risk assessment that was just performed and addresses identified risks, but also includes a standard set of controls that are expected for mature organizations. Generally speaking, the list of policies is as follows:

- Information Security Policy
- Acceptable Use Policy
- Access Control Policy
- Password Policy
- User Account Management Policy
- Asset Management Policy
- Data Classification and Handling Policy
- Change Management Policy
- Configuration Management Policy
- Vendor Management / Third-Party Risk Management Policy
- Incident Response Policy
- Business Continuity and Disaster Recovery Policy
- Data Backup and Retention Policy
- Cryptography and Encryption Policy
- Mobile Device and Remote Access Policy
- Network Security Policy
- Physical Security Policy
- Personnel Security Policy (including onboarding and offboarding procedures)
- Security Awareness and Training Policy
- Vulnerability and Patch Management Policy
- Monitoring and Logging Policy
- Privacy Policy (especially if Confidentiality and Privacy TSCs are in-scope)
- Risk Management Policy
- Software Development / Secure Development Policy
- Email, Communication, and Social Media Policy

The longest part of this phase isn't writing the policies – those are available as templates and easily approved. The longest part of this phase is implementing the policies and making sure that they are truly operating correctly.

Phase Three: Testing, Reviews, and Remediation

Now that there are defined policies and requirements, the company actually needs to implement them. And not only do they need to be implemented, but the company needs to ensure that the controls are working correctly and procedures are being followed. Every company should develop their own list of reviews that need to be performed on a regular basis, but generally companies going for their first audit will need to do the following internal reviews and tests and remediate any issues prior to starting the audit:

- **Access Control Reviews**

  The typical controls in a SOC 2 audit require that access is granted to employees based on their roles, and based on documented requirements. Any deviation from those parameters, or any additional access, should be documented and approved. Auditors prefer to see companies review their access control configuration on a quarterly basis and document the results.

- **Vendor Management Reviews**

  As part of ensuring that the company is trustworthy and reliable, companies should be ensuring that the vendors they rely on are also reliable and secure. That means reviewing those vendors prior to starting business relationships with them and re-reviewing those vendors every year. Most small companies want to move quickly and onboard vendors without much review process, which means performing a “sweep” of existing vendors prior to the first audit is a requirement.

- **Employee Offboarding Reviews**

  When an employee is terminated, their access needs to be removed “promptly” from all systems. The definition of how long that time frame is for removal is up for debate, but generally 24 hours is the accepted benchmark for what is expected. A review should be performed to ensure that this is happening within that time frame, and if not, new processes might be needed.

- **Change Management Reviews**

  This is the first actual technical control that needs to be tested and reviewed, which is further proof that the SOC 2 is about the whole company and not just the technical environment.

  Auditors expect that every change to the company’s product is properly considered, reviewed, tested, and communicated to customers. As part of preparing for the audit, the company should make sure that this is happening.

- **Incident Response Testing**

  Hopefully companies never need to implement their incident response plan, but the reality is that companies that are moving fast and innovating will likely need that plan on a monthly basis. Once documented, engineering teams should practice the incident response process at least once per year and make sure it provides an effective mechanism for remediating issues.

- **Disaster Recovery Testing**

  The technical term is “disaster recovery testing” but in reality it’s just a test that the backups work. Production systems should be backed up on a regular basis, but just because backups exist doesn’t mean that they actually work. Once per year the backups should be tested to make sure they will actually provide a reliable mechanism to restore systems to operation.

- **Security Awareness Training**

  The most “check the box” of the testing and controls that need to be implemented, but also likely the most impactful, is security awareness training. Immediately upon hire and again annually, all employees need to be trained on security topics relevant to their jobs and any new technologies that are emerging. This is also the perfect opportunity to remind employees about the company policies and expectations.

Once these audits and reviews have been performed, it is likely that you are in a good position to understand whether or not you are ready for a SOC 2 Type 1 or a SOC 2 Type 2 audit.

In the event that some things are still a little half-baked and need time to be completely implemented, it is likely that the company will still be able to successfully achieve a clean SOC 2 Type 1 report. This is just a point-in-time audit that the controls exist within the company and something is being done to try and implement them, not necessarily that the controls are consistently operating and effective.

That’s what the SOC 2 Type 2 report is designed to provide, assurance that the controls are consistently implemented and working correctly. If all of your internal testing is complete and did not uncover any issues, it might be time to move to a Type 2 report.

Audit

Once all of the risk assessment, policy development, and internal testing is completed, now is the time to get the auditors lined up.

There are a number of accredited auditing firms available to do the work, and likely you have a group of colleagues and other companies you work with who can recommend an appropriate

auditor. Our recommendation is that you work with an information security professional who has gone through this process before to be able to provide input and guidance on what auditor to choose and how to engage them.

Something to note is that auditors cannot provide consultation services during the audit, and some (good) auditors will refuse to perform both consultation and audit services to the same customer. It presents a conflict of interest that they are trained to avoid. What that means for companies is that it's best to start with a trusted consultant to guide them through the process and then obtain a separate auditing firm to perform the audit work itself.

Typically, auditors will want to start with a **readiness assessment** – this is a one-time consultation to determine what controls are appropriate for the company to implement to achieve SOC 2 compliance, and whether any gaps exist between those controls and the current environment. These assessments and the relevant evidence can be converted into a SOC 2 Type 1 assessment if successful.

Once the controls are defined, that's when the proper audit can begin for a SOC 2 Type 2 audit.

A Type 2 audit covers a period of time, typically 12 months (but can be shorter, such as 6 months). Audits start with a **request for populations**, which is where the company is expected to list all instances where specific things happen. For example, all changes to the production environment, all access control changes, or all vendors that the company uses. From those, the auditors will select **samples** which are specific instances that the auditors will want to investigate to ensure that the controls are properly followed. This process of determining populations and obtaining evidence for the samples is the longest part of the audit by far.

In addition to the samples of activities during the audit period, the auditors will also want to interview some company employees and see relevant evidence to ensure that the controls are operating properly. Typically this is somewhere between 100 and 150 discrete requests for information for a small SaaS based company, some of which are simpler to fulfill than others.

In the end, once the evidence is provided, the auditors will return their opinion and report. The company is able to edit and provide back the **system description** section of the audit, which describes the company and the product specifically. Auditors will identify any deficiencies or issues found during the audit, and the company can then provide a **management response** to those issues at the end of the report that acknowledges the findings and discusses any remediation that is being put in place.

Once all of that has been completed, the report is reviewed by the auditors and signed by an agent of the company.

Conclusion and Timeline

This process is not quick, and it is not easy. A SOC 2 audit report is intended to be proof positive that a company has a mature organizational structure and properly implemented controls, and any issues will likely be discovered during the audit. That's a near guarantee – if there's something you are unsure about or wanting to hide, the auditors are likely to sniff it out.

Typically, from start to finish, this is a six month process from the moment a company decides to start down this path. It can be much faster if the company employs or works with an expert who has gone through the process before, but some processes cannot be rushed.

The audit itself will take about six to eight weeks from start to finish to complete, no matter whether you are going for a Type 1 or a Type 2 audit. The biggest factor in getting the report back quicker is simply how quick the company can provide the requested information. The auditors themselves will take about a month to write, review, and issue the report if everything is immediately available.

Companies should consider what level of SOC 2 audit they need, and what they can afford. Sometimes getting a Type 1 audit is enough. Sometimes an audit is overkill depending on the intended customers. Each company should do that math themselves, and a competent and experienced consultant can help them make that determination.