Security Program Development:

A No-Nonsense Guide to SOC2 Compliance

TRUE NORTH

• PSR

Table of Contents

Table of Contents **2**
Introduction: **3**
What Does the Process Look Like? **3**
What's in it for You? **3**
The Trust Services Criteria **4**
Creating a SOC2 Project Plan **4**
- Form Your Team 4
- Define Your Scope 5
- Gap Assessment & Evidence Collection 5
- Address (Closing) Your Gaps 5

Key Resouces to Pursue SOC2 Alignment **6**
- Executive Sponsor 6
- Your Internal Team 6
- Project Manager 6
- Primary Author 6
- Legal 6
- IT/Security 7
- Employee Security Training 7
- External Consultants (Optional) 7

The Cost of a Formal SOC2 Audit Engagement **7**
- The Auditor Engagement 8

What Now? 8

Introduction:

Much of the information available online about the SOC2 framework is vague and filled with industry jargon. We at True North PSR wanted to create something clear, uncomplicated, and pragmatic for our clients (present clients and future clients). So, here it is.

SOC2 is filled with plenty of jargon but at its core, it's about what resources (e.g. files, applications, permissions) the users of your systems have access to, and whether there are any time-based or location-based restrictions placed on their access.

SOC2 compliance is an audit framework designed to help service organizations (e.g., software services, and service agencies) demonstrate how they keep customers' data secure. Commonly adopted by software vendors, it establishes enforceable policies to secure companies' systems and protect the privacy of their customer data. SOC2 must not be confused with the SOC 1 framework, which reports on financial reporting controls at service organizations, nor the SOC 3, which reports on the same information as SOC2 but in a format intended for a more general audience.

What Does the Process Look Like?

The process to become SOC2 compliant typically takes six months.

To begin the process, first form a team to own the project. That team will be responsible for conducting a readiness assessment and defining the audit scope. They will write information security policies and procedures and develop an implementation plan to close any identified gaps.

Next, they engage with a third-party assessor to complete a SOC2 Type I audit, which is designed to be a **point-in-time** snapshot of your organization's controls. When the SOC2 Type I audit is complete, you will receive a SOC2 Type I report. This report will guide you in closing the identified gaps over a six-month period.

Finally, once that work is done and your controls have been in place for at least six months, the SOC2 Type II audit can begin. With the Type II audit, an assessor will verify the operating effectiveness of your internal controls over time.

What's in it for You?

Your decision to become SOC2 certified is voluntary and, despite what some self-interested or otherwise inexperienced consultants may tell you, is not necessary to achieve HIPAA compliance or other regulations and standards such as PCI-DSS.

However, your investors or your customers may insist that your company become SOC2 certified. They may express concerns about security to their business partners, and seek verifiable evidence that you are processing and storing their information securely. Alternatively, your prospective or existing customers may request detailed technical information about your controls environment so frequently that you and your

company's leadership team realize that the most efficient way to respond to these requests at scale is with an independently issued SOC2 certification.
In any event, SOC2 demonstrates to your investors and customers that you have the proper people, policies and procedures in place to not only effectively handle security incidents but also to respond adeptly.

The Trust Services Criteria

The six principles within the SOC2 framework against which you'll be assessed - security, availability, processing integrity, confidentiality, and privacy - are defined by the AICPA (American Institute of CPAs). Importantly, you are not necessarily required to address all the Trust Service Principles. Instead, you will select the ones that are relevant to the services you provide to your customers. Briefly,

Security
Gives customers reasonable assurance that their data is safe and secure. Further, it demonstrates that the company's systems are protected against unauthorized access (both logical and physical).

Availability
Focuses on validating that your systems are available for operation and use, with minimal disruption or 'downtime'.

Processing integrity
Focuses on ensuring that the information processing activities carried out by your systems yield accurate, complete, and up-to-date data.

Confidentiality
Ensures that information classified as 'confidential' (or a similar term) is protected as committed to or agreed to by the company and the parties with whom it contracts.

Privacy
This refers to how personal information—such as a person's first name, last name, or phone number—is collected, used, retained, disclosed, and disposed of. It ensures that your data handling practices align with your privacy notice and use the criteria defined in the relevant AICPA privacy principles.

Creating a SOC2 Project Plan

Form Your Team

You will need an executive sponsor who will lead the project and help navigate your company's political landscape, a senior person to help drive the project, and IT/security leaders to ensure project adoption. Given your company's jurisdictional and industrial context, you will also want an HR resource and a legal resource to help your company navigate its legal obligations and employee rights.

Define Your Scope

SOC2 reports are based on the Trust Services Criteria (TSC) relevant to security, availability, processing integrity, confidentiality and privacy.

Depending on what you need the scope of the assessment to be, you will apply some combination of these principles to guide and limit the scope of your audit.

Gap Assessment & Evidence Collection

This assessment is designed to educate your team on the audit scope and conduct preliminary investigative and prep work, such as: (i) taking account of all relevant administrative procedures and controls, (ii) creating an inventory of your technical systems and data processing workflows, and (iii) identifying your data repositories.

This is a likely task for a consulting engagement. Expect some areas to have obvious deficiencies.

The complete list of evidence requests is, essentially, a complete manifest of everything your auditor expects you to deliver to substantiate any claims of adherence to the SOC2 framework. Your company's ability - or inability - to provide the requested documentation (evidence) will reveal what is missing.

The order in which you address those gaps should be determined by the level of risk each of those deficiencies presents to your business. In most cases, for example, you'll want to address poor access management controls before you address any common issues related to password cycling.

Address (Closing) Your Gaps

This process could be as short as three months or as long as 12+ months, depending on what issues are revealed during your gap analysis and your company's available personnel and financial resources.

Don't be surprised or dismayed by those gaps. Give yourself enough time to address them. This is the meat of the process. Fixing these findings could mean hiring people, shoring up your documented policies and procedures, or even making improvements to your software development process.

In those cases where you must create new documentation (e.g., policies, procedures, guidelines), delegate those tasks to as many people as is reasonable within the context of your organizational structure. You will rely on other teams to create these documents in accordance with their respective areas of expertise. If you are serving (even if only informally) as your company's SOC2 program chair, it will be your role to assign tasks, track status, and ultimately store responses in a centralized evidence repository.

Key Resouces to Pursue SOC2 Alignment

Executive Sponsor

Ultimately, this person must be able to answer why the organization is pursuing SOC2. This person must also be able to understand and continuously explain why, for example, next year's revenue depends on completing SOC2.

It will also help if this individual has some experience with risk management. If you have a particularly complex organization, your executive sponsor will have a lot of work to do.

Your Internal Team

Establish and assign an internal team to own the SOC2 process from start to finish. Expect this to become a full-time focus for the duration of the project.

This responsibility cannot be delegated to your IT or security team or handled by junior staff. The initiative needs to be led by someone who is sufficiently familiar with technical systems to be efficient with the team’s time. That person will also need to be sufficiently senior to successfully cut through the company politics and get things done.

Project Manager

This person will help drive the SOC2 effort and manage the day-to-day responsibilities of gathering information, scheduling resources, etc.

Your project manager doesn't necessarily need to fully understand the requirements for SOC2 certification or have compliance expertise, but they should be skilled at completing tasks across the organization.

Primary Author

You need a senior primary author who can handle some quasi-legal technical writing.

This person also needs to understand the business and operations; otherwise, that person will be ineffective when interviewing other teams, slowing down your entire SOC2 progress.

Legal

As you begin creating and refining policies, ask your legal Counsel for input early in the process. They will also play an important part in working with your company’s stakeholders (e.g., investors, customers, vendors) when contracts need to be updated.

These agreements, in aggregate, represent the responsibility and accountability your company and its representatives bear with its stakeholders. These documents also determine what assertions you may make - or must make - in your policies regarding confidentiality, privacy and security. Barring the existence of other automated controls, it would be wise for appropriate personnel at your company to review this documentation annually, with each audit.

IT/Security

These teams will have a large volume of technical functionality that needs to be conceptualized, built, and proven during an audit. This is high-intensity work, and much of it revolves around ensuring your organization can detect and respond to a security incident.

Coming out of the audit, you will likely need to purchase additional tools, such as data loss prevention (DLP) software or security incident and event management (SIEM) software. You may also need to change the way your organization controls physical access to your office building or data centre. Your IT and Security teams will help to shoulder that workload. The cost that your company will incur for these resources will depend on several factors, including the volume of data your organization processes, and the number of employees who will, in some manner, use these solutions.

Employee Security Training

Many organizations falsely think they can delegate responsibilities solely to members of the IT and information security teams. Although members of those teams will play a big part in the process, your core SOC2 team will also include HR, legal, and other business units, as noted above.
Security Training

If you haven't already, you should start conducting annual security awareness training, either in-house or through a third party. Someone will need to make sure the entire company completes the training and that all employees sign up to receive it. Expect this to have a minor impact on team productivity and to incur minor logistical costs.

External Consultants (Optional)

if your organization or team is new to SOC2, it might make sense to also hire a third-party consultant to help guide you through the pro- cess. This consultant, likely a CPA (Certified Public Accountants) should have extensive knowledge of the Trust Services Criteria. The consultant will help you figure out which principles apply to the scope of your audit.

The Cost of a Formal SOC2 Audit Engagement

If your company is in the ‘start-up’ phase of its growth, your investors, customers, and leadership team may collectively determine that formally certifying against the SOC2 framework is not strictly necessary. In this case, completing the work outlined above will still considerably improve your information security and data privacy program, and will give you a body of documentation and other evidence to support your company’s claims of ‘alignment’ with the SOC2 framework.

However, if your company determines that it is ready to (or needs to) formally validate the maturity of its security program, it must now engage a qualified and licensed audit services firm to audit its controls against the SOC2 framework.

The Auditor Engagement

Expect the cost—for a small enterprise of 100-150 employees—to complete a SOC2 Type I (point in time) to be in the $20k-$40k CAD range and $70k-$90k for a SOC2 Type II. Keep in mind, however, that costs will vary considerably depending on factors such as the company headcount, the number of offices, and the complexity of your organization and its business activities.

However, the cost of the audit itself is just the beginning. You will, in almost all cases, need months of dedicated time from your existing staff or consultants. Once the audit is complete, the auditor's report will note that either:

- Your security program controls meet the requirements of the framework (you 'passed' the audit), or
- The auditor identified significant findings that must be addressed before your company meets the requirements of the framework (you 'failed' the audit)

If you find yourself in the latter position, take a breath - an optimised security program is something to which almost all companies aspire. Review the report, then update your security program roadmap.

The work of strengthening your company's security stance is iterative. Your company, your customers, and other interested parties will benefit most from these improvements if you look at security as a journey; not a destination

What Now?

As you've navigated through this guide, we hope you've gained a deeper understanding of the SOC2 compliance journey and the value it could add to your business. Embracing SOC2 is not just about meeting a regulatory requirement; it's about securing trust in your services and protecting your customers' personal or otherwise confidential — a fundamental aspect of data-driven business.

At True North PSR, we recognize that the path to SOC2 compliance can seem daunting. If you determine you don't have sufficient in-house resources to properly execute this project, this is where our expertise can make a crucial difference. Our team is ready to assist you at every step, ensuring that your compliance efforts are as seamless and efficient as possible. By partnering with us, you gain access to a wealth of knowledge and a partner who is as committed to securing your systems as you are.

Consider visiting our website at <www.TrueNorthPSR.com> to learn more about how we can help streamline your compliance program, ease the burden on your internal teams, and enhance your security posture. We would be happy to help you turn the complexities of SOC2 compliance into a strategic advantage for your business.