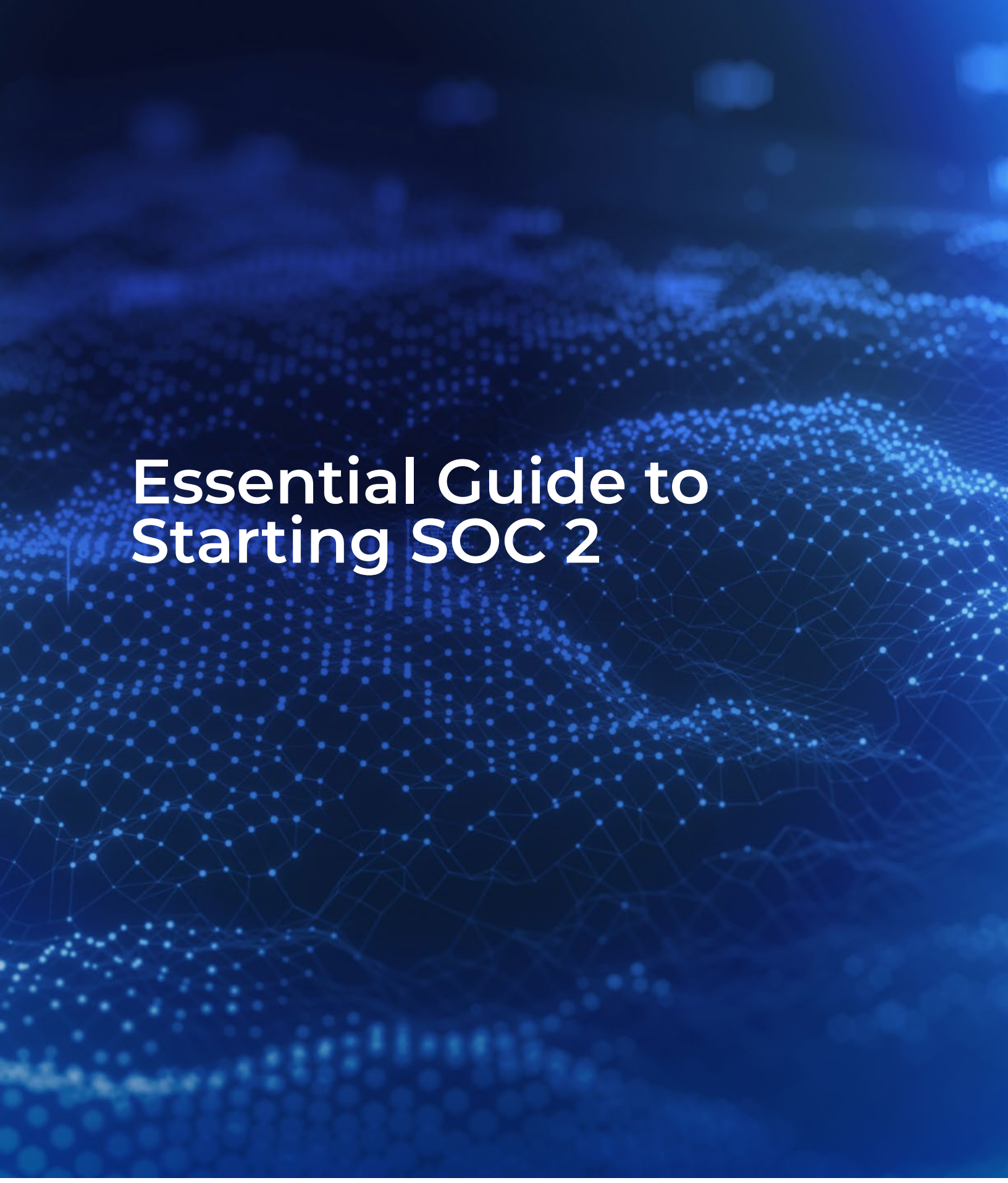


strongdm

# Table of Contents

01

# Are you starting your SOC 2 certification?

We wrote this because all the resources on the internet around **SOC 2 certification** were filled with acronyms and jargon and ultimately left us with more questions than answers.

**In this ebook we'll share a practical, tactical, step-by-step approach to SOC 2 so you get your certification efforts off to a great start.**

Specifically, you will learn:

- What is SOC 2 and the differences between a Type 1 and Type 2 audit
- How to scope your SOC 2 audit
- The time and financial investments required for a successful audit
- Staffing properly for the audit

02

# What is SOC 2?

SOC stands for **Service Organization Control**, which comes to us from the AICPA (American Institute of Certified Public Accountants). In a nutshell, SOC helps companies demonstrate they have implemented the proper controls to assure security, availability, processing integrity, confidentiality, and privacy of customer data.

Where things get a bit confusing is that SOC 2 comes in a few different flavors:

### Type 1

This report examines security controls at a specific point in time

### Type 2

This report assesses those same controls over a longer period of time (typically 6 months)

**For more information about the different SOC 2 types, see our posts called What is SOC 2 Type 1? and What is SOC 2 Type 2?**

To potentially confuse things further, there are SOC 1 and SOC 3 audits your company can pursue as well. SOC 1 examines a company's financial statements and reporting, and SOC 3 essentially takes the SOC 2 report and presents it in a format meant for a general audience.

**If you're interested in learning a bit more about the background of SOC 2, reference our post called What is SOC 2 Compliance?**

03

## How do I scope my SOC 2 audit?

A critical part of the SOC 2 process is understanding how to properly scope your audit — this is a step that's typically done with the help of an outside consultant. The consultant will help you figure out which of the **Trust Services Principles** (security, availability, processing integrity, confidentiality and privacy) apply to your company.

Regardless of which principles end up being applicable to your audit, a great first step is to take an inventory of the critical systems you use to deliver services to your customers. After all, you can't protect what you don't know you have, right? If there are systems you think should be excluded from scope, write up a justification as to why. You will need to "prove" these scope decisions when you go through your audit.

For more help on figuring out your SOC 2 scope, see our blog post called Defining Your SOC 2 Scope.

04

## What does a SOC 2 audit cost?

SOC 2 is a significant investment — not just in money, but in time as well. Here are some of the costs you'll incur during your audit:

- **SOC 2 Type 1 audit: $12-17k**
  This audit looks at your security controls at a point in time, and takes about 2 weeks to complete.
- **SOC 2 Project Manager: $50-75k**
  This individual oversees the audit from start to finish, which takes about 6 months.
- **Internal audit review: $10k annually**
  Your audit will require assistance from your legal and HR teams, as they will be best suited to review and update the various contracts you have with customers, vendors and contractors. Keep in mind this contract review will be a cost you incur annually.
- **Tools and technologies: $5-50k**
  Undoubtedly, your SOC 2 audit findings will require the purchase of tools — such as a SIEM (security information and event management) to log key events on your systems. Some tools may be quick to install and get up and running; others may take months to roll out.
- **Training: ~$5k annually**
  Part of SOC 2 compliance requires your staff to be trained on security topics. It doesn't matter if the training is conducted using your internal staff or an external consultant, but it's something you need to do every year.

For more information on SOC 2 costs, see our blog post called Budgeting for SOC 2.

05

## What internal/external staff do I need for a SOC 2 audit?

One of the most important things to remember when staffing for your audit is that you can not delegate this project solely to your IT and security teams. Yes, these teams will play an important role, but you're also going to need an executive sponsor, at least one project manager, an audit author who can do a large amount of writing and interviewing, and the aforementioned HR and legal resources. The IT and security teams will play a major role when the project is underway, as they will inherit a large number of technical projects to complete — both during and after the audit.

For more information on selecting the right team members for your audit, see our blog post titled How to Build Your SOC 2 Team.

06

## Conclusion

A SOC 2 audit, while time and cost-intensive, has many benefits — both to you and the clients you serve. These benefits include:

- Establishing a third party opinion on which — or all — of the Trust Services Principles apply to your organization.
- Identifying security gaps in your organization.
- Demonstrating to clients that you truly take the confidentiality, integrity, and availability of their information seriously.
- Differentiating yourself from competing companies who have not achieved SOC

You can alleviate a lot of SOC 2 audit and implementation struggles by using tools to automatically track who has access to your critical databases, servers, VPNs and Web applications.

strongdm

To learn more about how to centrally manage your environment, visit https://www.strongdm.com/product/

strongdm

strongDM's infrastructure access platform gives every business secure access controls in a way folks love to use. Trusted by the Fortune 500 to fast-growing businesses like Peloton, SoFi, Chime, Yext, and Better, strongDM gives businesses the control and visibility they need at the speed they want with one platform that works for every environment. strongDM is intentionally distributed. Head to **www.strongdm.com** to learn more.