



GUIDE

5 Things to Do Prior to a SOC 2 Audit



Introduction

Obtaining the AICPA SOC 2 Report has become a popular, and in some cases required, way for companies to demonstrate to their customers that they are addressing risk and have established controls across categories of security, availability, processing integrity, confidentiality and privacy.

If you are considering a SOC 2 audit, which is performed by a CPA (Certified Public Accounting) Firm, you will want to prepare for a successful examination by completing the following five tasks.

01 Create A Risk Management Plan

When approaching your initial SOC 2 audit you will need to consider how you will establish a risk management process. Formally identifying and addressing risk is a SOC 2 requirement, but is also a responsible exercise for your company to undertake.

On a recurring basis, yearly at minimum, Senior Management and the Board of Directors should evaluate customer obligations, threats to meeting obligations, and ways of mitigating identified threats. It's important to note that mitigation is not a one-time exercise: threats evolve, and so should your risk management plan.

02 Perform A Risk Assessment

When approaching your initial SOC 2 audit you will need to consider how you will establish a risk management process. Formally identifying and addressing risk is a SOC 2 requirement, but is also a responsible exercise for your company to undertake.

On a recurring basis, yearly at minimum, Senior Management and the Board of Directors should evaluate customer obligations, threats to meeting obligations, and ways of mitigating identified threats. It's important to note that mitigation is not a one-time exercise: threats evolve, and so should your risk management plan.

03 Develop Policies & Procedures

Many small or startup companies follow internal policies and procedures, but few are formally documented. Not only will formal documentation of control-related policies and procedures be necessary to give to the auditors, but they will guide your employees in understanding your organizational expectations, and the consequences for non-compliance.

There are some general written policies that most companies have, regardless of size, but for the purposes of the SOC 2 audit, your company's minimum policy set should include: Information Security and Privacy Policy; Employee Handbook with Code of Conduct; Risk Management policy; Incident Response policy; Change Management policy (for system and application changes); and a Vendor Management policy (particularly if you have outsourced critical functions of system operations, such as placing your infrastructure in a cloud environment).

04

Define The Scope Of The System

In a SOC 2 report, there is a system description section, which is the written narrative to the reader of the report, describing the in-scope system and the controls in place that supports the delivery of products, solutions or services to your customers. The description typically includes system components such as infrastructure, software, personnel, data and procedures.

The SOC 2 examination will require the auditors to evaluate the design of controls as they pertain to the AICPA's pre-defined Trust Services Criteria (TSC), which report on controls relevant to security, availability, processing integrity, confidential and privacy. Much of the initial design of control understanding for auditors will be accomplished by their reading of a well-defined system description, and you should be familiar with the TSC and their five categories to guide and limit the scope of your SOC 2 audit and to draft your system description.

05

Select The Right CPA Firm To Conduct The Audit

Choosing the right CPA firm for your SOC 2 audit can be challenging; there are multiple factors you should consider when evaluating firms.

Reputation

We recommend you ask the CPA firm for multiple SOC 2 audit client references so you can contact each and get first-hand information of how the audit project went for each client. Asking questions like, "How long did the process take?" "Were there any unexpected problems or delays?" "How easy was it to work with the auditors?" "Would you recommend this firm for our audit?" "Are you planning to stay with this firm for your subsequent report?" The answers to these questions can help you decide if the CPA firm is the right fit for you.

Industry

Does the CPA firm specialize in SOC 2 audits for companies in the same, or similar industry as your own? If you're a technology company, hosting your service in the cloud, but the CPA Firm's SOC 2 specialty is supply chain management, you may find that their auditors are not familiar with your type of service or controls, which can cause confusion and unwanted delays.

Cost

Is the audit a fixed-fee engagement, or does the CPA Firm charge by the hour? Most CPA Firms perform SOC 2 engagement on a fixed-fee basis, so be wary of those who are billing by the hour.

Audit Process

How will the audit be conducted? Is the CPA Firm setup for secure remote and online team collaboration? Will there be onsite requirements, and if so, for how long?

Timeframes

Is the CPA Firm flexible enough to work around your schedule, throughout the various phases of the project? How soon will you get the final report once the fieldwork has ended? Some national CPA Firms can take up to 90-days to deliver a report, while others can deliver in as little as 14 days, so keep that in mind if you make report delivery commitments to your customers.

“ If you want to sell software and set up the foundation for your security program, it's critical to get a SOC 2 audit. This will enable your business to align with the essential security expectations of your future customers.

James Condon
Director of Research



“ Having successfully gone through the audit, I wish now we would have started sooner. If I had one piece of advice to offer companies considering a SOC 2 audit, it's to make it a company priority and just get started. Sensiba helps demystify the process and will walk with you the entire way. If you drag your feet, then a year from now you'll be looking back knowing you could have been certified already.

Victor Nee
Director of IT





About Sensiba

We hope this white paper gives you a better understanding of the five tasks that can help you prepare for a successful audit. If you need help with SOC 2 readiness, or any of the steps outlined in this white paper, we encourage you to reach out. We understand that SOC reporting requirements can be confusing, so we are happy to answer any questions you have about the process.

Sensiba is a licensed, award-winning tax, audit, and advisory firm that has been in business for over 40 years in the heart of Silicon Valley. We have deep expertise serving the technology industry, and while we are proud to count some of the world's largest companies as our clients, we are passionate about start-ups because, like you, we are entrepreneurs at heart.

For more information on things to do prior to a SOC 2 Audit, contact our team:

Jeff Stark

Partner

jstark@sensiba.com

Brian Beal

Partner, Risk Assurance Services

bbeal@sensiba.com

