AKITRA

SOC 2 Basics:
FAQ on SOC 2 Compliance for SaaS Vendors

Revised March 7, 2022

What is SOC 2?

SOC 2 is a compliance framework used by service providers and their auditors in order to demonstrate the security and general trustworthiness of the providers' services. The "SOC" in SOC 2 stands for "System and Organization Controls." SOC 2 is governed by the American Institute of Certified Public Accountants (AICPA).

The framework consists of a set of criteria that specify what an organization needs to do in order to be certified as meeting the AICPA's SOC 2 criteria. The criteria cover five different categories: **security, privacy, confidentiality, availability and processing integrity**. These five categories of criteria are referred to as "**Trust Services Criteria**" (**TSC**). (They used to be called Trust Services Principles, until the AICPA revised its terminology in 2017).

The only one of these five TSC categories which is required for compliance is **security**, while the other four are optional. Many firms initially opt to be audited for security only – typically if they have never been through a SOC 2 examination before – and then widen the scope in subsequent years' audits.

SOC 2 is a compliance framework that is more "descriptive" than "prescriptive". This means that the TSC criteria are more similar to guidelines than they are rigid requirements. So, service organizations like yours have broad leeway in designing and implementing the "controls" to satisfy the criteria. Controls have to meet a test of reasonableness, have to make sense in terms of the unique aspects of your business and its environment, and have to pass being examined and approved by your SOC auditor. This means SOC 2 will not be interpreted the same way for a 10-person SaaS company as for a 1000-person global company.

What is a SOC 2 attestation report?

An attestation report is a document in which you (the client) and the auditor – whose work must be vetted by a CPA, if the hands-on auditor is not a CPA themselves – both *attest* that the content of the report fairly and accurately reflects that the organization is truly meeting the SOC 2 criteria. This document is usually called just a "SOC 2 report", and provides confirmation that the client is compliant with SOC 2.

The four main sections of a SOC 2 report are:

- Section 1: an attestation by your company's management
- Section 2: an attestation by the auditor
- Section 3: a narrative system description of your company's service and the system that supports it

- Section 4: a detailed description of the relevant criteria, the controls that address them, the tests applied by the auditor, and the test results

What are the advantages of Akitra's compliance automation service?

Andromeda Compliance transforms the time-consuming, expensive and non-repeatable manual compliance process into something far better and faster.

Akitra's platform offers these **TOP 10** benefits:

1. **Ease of Use:** An easy to use, well-structured and automated process guides you through the compliance process from initial setup all the way through to a completed audit report.
2. **Automation saves time and $$$:** Automation of the collection of evidence from workstations, servers and cloud platforms and services ensures continuous monitoring and continuous collection of evidence – far more efficiently and cost-effectively than trying to do so manually. Akitra achieves this through integration with the APIs of all the audit-relevant services, such as the HR service tracking employee onboarding and off-boarding, or the DevOps system, or the cloud services platform such as AWS / Azure / GCP.
3. **Support for multiple frameworks:** Akitra's compliance platform is built to support multiple frameworks, including SOC 1, SOC 2, ISO 27001, NIST 800-53, HIPAA and GDPR. Having one platform to support them all reduces learning time for customers and auditors alike. It also ensures consistent and sustainable compliance processes while saving enormous amounts of time and expense – for years to come!
4. **Policies and controls in a box:** Includes customizable templates for policies and controls. Enables companies without such documents and processes to quickly put the necessary framework in place for audit readiness.
5. **Collaboration:** Enables easy communication – within the Compliance service – between all the company team members involved in the audit, and between the auditor and the company's compliance coordinator. Shared comments and task notifications keep everyone on the same page.
6. **Single source of truth:** Acts as a single repository of all compliance-related policies, controls, evidence, and reports. Eliminates wasted time and having to start from scratch with every new audit.
7. **Efficient auditing:** An auditor portal allows the auditor to efficiently access all relevant documents and complete the review and approval process efficiently. Once complete, content for the final report can be downloaded in bulk. Almost all of the final SOC 2 report can be generated from within the Akitra service. This includes the critical Section 4 with details on how the company is satisfying the TSCs, what tests the auditor has performed, and what the results were. It also includes Section 3 with narrative explanations of the company structure, system architecture and processes. These efficiency gains mean smaller invoices from auditors!
8. **Broadest scope and flexibility for your evolving needs:** 95+ third party integrations, more than any other compliance vendor; seven compliance frameworks; product customizability to choose the UI color theme you prefer.
9. **Continuous monitoring for continuous compliance:** Becoming compliant with SOC 2 Type 1 at a point in time is a great first step. But, to move on to SOC 2 Type 2 requires showing continuous compliance over a period of months. Only automated monitoring and continuous evidence collection make that possible.

10. **Expert support and guidance:** Akitra provides more than just an automated compliance platform, critical as that is. Akitra's solution also includes regular access to compliance experts to guide you through the compliance process, from onboarding through crossing the compliance finish line – and beyond. We make sure you succeed.

Who is the audience for a SOC 2 report?

The AICPA states that SOC 2 reports are designed to "help service organizations that provide services to other entities, build trust and confidence in the service performed, and in the controls related to the services, through a report by an independent CPA." In short, it's designed to reassure your partners as well as the customers and prospective customers of your SaaS service that your company is secure and safe to do business with.

Why do I need a SOC 2 report?

You need a SOC 2 report because your customers want you to be SOC 2 compliant or else they may not buy from you. Or if they do buy from you, they'll first make you jump through more hoops – such as giving you lengthy security questionnaires to fill out – to demonstrate that you really are secure. (And of course, they may also care about the other categories of criteria than just security, which means even longer questionnaires to complete).

Instead of suffering the headaches of answering endless questionnaires from your prospects, just hand them the SOC 2 report and then the compliance conversation can be short and sweet. Then move on to closing more business, with shorter sales cycles and a higher percentage close rate.

If I have a SOC 2 attestation report, does it help me get other certifications such as HIPAA and ISO 27001?

All the compliance frameworks have different requirements, originating from different sponsoring bodies, such as the AICPA or the European Union's GDPR compliance agency.

That said, YES, having SOC 2 will get you much closer to being compliant with the other frameworks as well, because of the heavy overlap between them. With SOC 2, you will have already built your framework of policies, controls and procedures, and you will already have instilled in your organization the discipline of following the necessary processes for security, confidentiality, availability and so on.

Akitra's compliance automation platform offers a critical advantage: it uses a common architecture across all of the frameworks it supports, including SOC 1, SOC 2, ISO 27001, NIST 800-53, HIPAA and GDPR. This means that most policies and controls are common across these frameworks. It also means that if, for example, you collect evidence for one common control, then that evidence is updated across ALL frameworks. This ensures consistency and saves enormous amounts of time and expense.

What is a SOC 2 "control"? How is it evaluated by the auditor?

A control is a statement of how your company meets the requirements of one or more of the SOC 2 criteria. For example, if the criterion is "The entity evaluates security events … then the entity evaluates why and how it can be avoided in the future", and one of the controls that meets this criterion is that the company has ensured that "Identified security incidents are reviewed and investigated by an incident response team", the auditor will assess two things:

- Does the control (together with the other controls tied to a given criterion), meet the requirements of that criterion?

- Does the evidence presented by the company support that it is consistently following its own controls?

If yes to both questions, the auditor approves the control.

How is a SOC 2 report created?

You and your colleagues perform a gap analysis, customize your policies and controls and then collect supporting evidence (automated reports, policy documents, compliance reports from outside suppliers, etc). You can do all this starting from scratch: creating all your own policies and controls, and manually collecting all the evidence, and so forth. OR, far more easily, you can use a compliance automation platform such as Akitra's and complete the work more effectively in a fraction of the time, with much less work, at much lower cost, and in a way that is continuous and easily repeatable for future audits.

Next, a certified auditor must then audit all this content and all these processes. This means that the auditor goes through all the controls and a sampling of the evidence that the controls were applied, performs some tests to confirm that you've done what you say you've done, records the results, and provides the necessary attestation that all is good. You then have a SOC 2 report to share with your partners, customers and prospects!

What is a compliance automation service and why would I need to use one?

A compliance automation service such as Akitra's Andromeda Compliance replaces the labor-intensive, traditional approach to compliance. That old approach uses lengthy spreadsheet task lists, endless emailing of questions and comments, and a great deal of emailing and uploading of documents – policies, screenshots, reports, even Slack conversations! All of these become increasingly difficult to track, and the activities of the multiple players involved on both the client and the auditor sides become harder and harder to coordinate.

Most frustrating of all, this entire process then needs to be repeated on at least an annual basis, with a great deal of relearning and repetition of all the steps taken earlier. It's a terrible money and time sink.

In short, automated compliance is faster, less aggravating, more repeatable and lower cost than the traditional manual approach.

What are the different kinds of SOC 2 reports?

There are two kinds: Type 1 and Type 2.

- Type 1 is a point-in-time assessment of your controls and how diligently you're implementing them.
- Type 2 covers proof of compliance over a period of time, which is initially no less than three months. After that, once a year will suffice.

With a Type 2 report, the key is that the company must be able to show that it was in compliance *during the entire period* covered by the SOC 2 report. That's why SOC 2 Type 2 requires continuous monitoring and prompt remediation of any compliance problems as they arise – such as an AWS EC 2 instance that isn't protected by multi-factor authentication access or an employee workstation that is not protected by an antivirus program.

How long does the audit readiness process take?

It depends on several factors. For example, how mature are your organization's processes, such as having well-defined policies covering security, employee onboarding, disaster recovery and confidentiality? If your firm lacks these, and the associated controls and procedures to implement them, it's going to take you longer, even if you take advantage of the policy templates provided by a service such as Akitra's Compliance.

For SOC 2 Type 1, performing a basic risk assessment, defining policies and controls, and collecting evidence might take a younger company that has never been through the compliance process about six weeks, followed by one week of auditing and one week to draft the final report. A more experienced company that has been through the SOC 2 process before and is using Akitra's compliance automation **can easily cut that time in half**.

For SOC 2 Type 2, add in 3-6 months of monitoring, since evidence needs to be regularly collected over a period of time to demonstrate continuous compliance.

The single most important thing you can do to speed up the beginning-to-end compliance process is to use a **compliance automation platform**. Beyond that, some practices that can speed up the compliance process include having a dedicated compliance coordinator to manage the whole project, communicating to key players the importance of responding promptly to compliance information requests, and having an executive sponsor.

What is pen testing?

Pen testing (short for penetration testing) is conducted both for purposes of gap identification as well as for validating that the changes that have been made as part of the SOC 2 process have achieved their intended result. Both Akitra as well as independent firms such as Prescient Security offer this service, using a variety of tools, and probe the client's network and service looking for vulnerabilities such as missing user authentications, applications with known vulnerabilities, SQL injection flaws and system misconfigurations.

Almost all auditors insist on the use of pen testing as part of the audit. It is an excellent practice that will make your security more robust and build confidence among your customers that your service is truly secure.

What are the costs of a SOC 2 Type 2 audit, using a compliance automation service like Akitra's?

There are three main costs:

- **Audit:** The audit firm's charges will depend on the engagement's scope, such as which of the five TSC categories (security, privacy, confidentiality …) need to be supported, the number of employees and contractors in your organization, the number of entities involved (such as multiple international subsidiaries) and your level of preparation. Auditing additional frameworks at the same time, such as ISO 27001, increases the total cost but is cost-effective in the longer run.

- **Compliance automation service:** Akitra charges an annual subscription fee based on the number of employees/contractors in your company and the number of frameworks to be supported.
- **Your time:** The two items above are about hard dollar costs. The most important cost may actually be the "soft costs" of your time and your colleagues' time. It is this cost that a compliance automation service can drastically reduce, by enabling you to complete the process both faster and with less tedious, error-prone work. This is true not only for becoming compliant, but for *maintaining* continuous compliance over time.

If your firm opts for third party pen testing services, this would be an additional cost.

Is there a checklist of everything I need to do?

A compliance automation service like Akitra's will guide you through the process methodically and systematically, with many of the mundane tasks of evidence collection actually automated. But since SOC 2 is a flexible framework that allows a lot of freedom in how companies design and implement their controls, a simple checklist would never be adequate. Without automation, expect to be mired in lengthy spreadsheet task lists, tracking potentially hundreds of emails and text threads, and endlessly hounding your colleagues to meet their deadlines to provide needed evidence.

Why might the SOC 2 auditor decide that my firm's SOC 2 controls and evidence are not sufficient?

There are several potential areas where problems might arise. If the company's policies and its controls are not aligned, then one or both needs to be changed. If evidence that the controls were actually implemented is not available, then the audit period may need to be reset to a later time period. If the evidence is sloppy – for example, screenshots provided without context or dates – the auditor may reject it. Compliance automation can typically solve all these problems.

Auditors will give their clients a remediation period to fix problems that have been identified -- a week or two is typical. But, if the problems are severe enough and are not remedied in a timely way to the satisfaction of the auditor, she may issue a "qualified opinion", which points out some of these flaws. Your customers don't want to see that. So, a qualified opinion is to be avoided at almost any cost – and Akitra's compliance automation service will help you do so.

Am I good to go forever once the SOC 2 report is finalized?

Life should be so easy but alas, no. A SOC 2 Type 1 report covers only a point in time -- a specific date. A SOC 2 Type 2 report covers a specified period of time, such as one year. If another year passes by and you do not have your company re-audited, your customers are likely to worry that you may very well be no longer compliant. That's the business reason that SOC 2 audits need to be performed regularly, typically once a year. In between audits, you and your compliance automation service provider need to be continually monitoring your compliance and collecting evidence to prove it.

Does a SOC 2 report cover my entire company, including its subsidiaries?

It depends what you want the scope of the report to be. According to the AICPA, the report can cover (a) an entire company; (b) a subsidiary, division, or operating unit level; (c) a function relevant to the company's operational, reporting, or compliance objectives; or (d) a particular type of information used by the company.