SOC 2 Compliance

THE COMPLETE GUIDE

strongdm

Table of Contents

TL;DR

In this article, we'll take a comprehensive look at SOC 2 and the requirements for certification.

You'll learn what SOC 2 is, who it applies to, why it's important, and how it benefits an organization. By the end of this article, you'll have a clear understanding of the differences between Type 1 and Type 2 assessments, the SOC 2 Trust Principles underlying these assessments, and the criteria auditors use to evaluate and report on the associated controls.

01

What is SOC 2?

SOC 2 stands for “Systems and Organizations Controls 2” and is sometimes referred to as SOC II. It is a framework designed to help software vendors and other companies demonstrate the security controls they use to protect customer data in the cloud. These controls are called the Trust Services Principles and include security, availability, processing integrity, confidentiality, and privacy.

For organizations evaluating SaaS or cloud services providers, compliance with SOC 2 is a minimum requirement. This is because it confirms to the customer that you have a certain level of maturity around security best practices.

What SOC 2 is not

It’s important to note that SOC 2 compliance is neither a legal requirement nor a proxy for actual security best practices. While the assessment covers the core departments and processes that interact with sensitive data, it’s not driven by HIPAA compliance or other regulations and standards.

Certification is performed by external auditors and not by the government, and the resulting report merely confirms that the processes you self declare are actually being followed in practice.

Nevertheless, the significance of the role of SOC 2 in data security cannot be underestimated. Understanding its origins can help to explain why.

02

History of SOC 2

SOC 2 evolved from the Statement on Auditing Standards (SAS) 70, an old audit that Certified Public Accountants (CPAs) used to assess the effectiveness of an organization’s internal controls.

While security was included under the umbrella of internal controls, it came to the attention of the American Institute of Certified Public Accountants (AICPA) that some organizations were offering SAS 70 reports as proof they were safe to work with. In response, AICPA replaced SAS 70 with the Statement on Standards for Attestation Engagements (SSAE) 16 report, which was later renamed Systems and Organizations Controls 1 (SOC 1).

Then in 2009, AICPA introduced SOC 2 as an audit report with a strict security focus and issued the five Trust Services Principles. These principles were defined as “a set of professional attestation and advisory services based on a core set of principles and criteria that address the risks and opportunities of IT-enabled systems and privacy programs.”

Simply stated, the principles represent the criteria to be used to evaluate and report on an organization’s controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems.

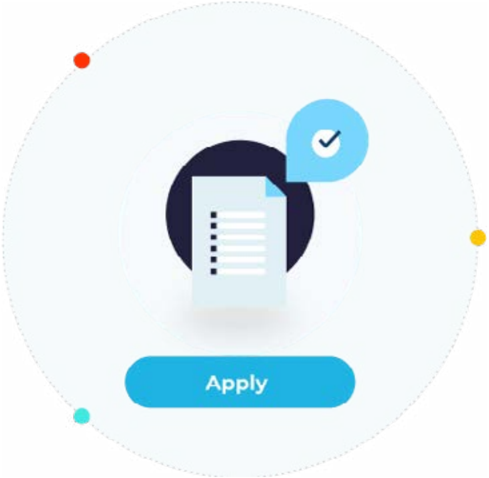
AICPA further stipulated that it was not necessary to address all the Trust Service Principles, and that an organization should select only those relevant to their own services.

03

Who Does SOC 2 Apply To?

SOC 2 is specifically designed for service providers that store customer data in the cloud, as a way to help them demonstrate the security controls they use to protect that data. As such, it applies to nearly every SaaS company and cloud vendor, as well as any company that uses the cloud to store customer information.

If you're reading this, there's a pretty good chance SOC 2 applies to you.



04

Importance of SOC 2 Compliance

From the point of view of a potential customer, working with a vendor that has fulfilled the SOC 2 requirements is a guarantee of sorts. It means you can provide the information and assurances they need regarding how you process users' data and keep it private.

But facilitating organizational oversight isn't the only point of SOC 2 compliance.

According to AICPA, the reports produced during the process of achieving compliance can also play an important role in:

- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

05

Benefits of SOC 2 Compliance

CREDIBILITY

At a fundamental level, SOC reports show potential customers that you're serious about integrity, ethics, and security throughout your operations. Being able to demonstrate that you have the proper people, policies, and procedures in place to handle a security incident and respond accordingly places you firmly on the candidate list—which is the first step towards being selected as the preferred provider.

FASTER SALES CYCLES

Showing compliance can also speed up your sales cycle. Pitching new business can be easier on your sales team because they will very likely be spared the burden of completing endless RFIs during the sales process. Instead, they can simply submit the company's SOC 2 reports.

LONG-TERM BUSINESS SUCCESS

Perhaps the most important benefit arises from the work required in terms of preparation for the SOC 2 Type 2 assessment. This is covered in more detail below, but it essentially requires you to install long-term, ongoing internal practices that will ensure the security of customer information. By their very nature, these practices will ensure the long-term success of your business.

06

SOC 2 Types

Becoming compliant typically takes six months and requires the completion of two audits by third-party assessors. The SOC 2 Type 1 audit is designed to assess the design of your security processes at a particular point in time, while the subsequent SOC 2 Type 2 audit involves verifying the operating effectiveness of your internal controls over the longer term. Completion of the Type 1 audit is a prerequisite for Type 2.

Type	Detail
SOC 2 Type 1 (Type I)	You'll begin by forming a multidisciplinary team, electing an executive sponsor, and identifying an author who can collaborate with each team lead and translate their business needs into policies. Using the AICPA Trust Services Principles as your base and selecting only those that apply to your services, you'll then define the scope of the audit and write and refine the appropriate policies. You can expect this to take around two months to implement, test, and fine tune the policies before you're ready to book a formal assessment. The assessment typically includes interviews with staff, walkthroughs of your physical space, and a thorough review of your documentation. Once the auditor has worked with you to clarify any necessary exceptions, the SOC 2 Type 1 report will be generated. To take a deeper dive, check out: SOC 2 Type 1 Guide: Everything You Need To Know
SOC 2 Type 2 (Type II)	You can't embark on the preparations for the Type 2 audit until you've been through the Type 1 process. This is because while the Type 1 audit assesses processes and policies, the Type 2 audit verifies the effectiveness over time of the controls you've instituted to ensure those processes and policies are followed. To walk through the complete path to a Type 2 audit, read: SOC 2 Type 2 Guide: Everything You Need To Know

07

SOC 2 Controls

The 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy documents the control criteria which have been established by the Assurance Services Executive Committee (ASEC) of the AICPA. These are the criteria your selected auditor will use to evaluate and report on the controls you have put in place to ensure the security, availability, processing integrity, confidentiality, or privacy of information and systems.

The Trust Services Criteria consist of:

- Criteria common to all five of the trust services categories (common criteria)
- Additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories

Common Criteria

Type	Detail
CC1 Organization	The CC1 series of controls forms the foundation of ethics and integrity on which all subsequent controls are built. It establishes how your organization has been incorporated and addresses how your Board of Directors was formed. It also includes HR topics such as recruitment and training practice.
CC2 Communication	The CC2 controls establish your obligation to collect information and describe how it will be disseminated internally and externally. While they may appear obvious, their purpose is essentially to eliminate ignorance as a valid excuse for a failure to investigate a control violation.
CC3 Risk	The CC3 control series is focused on financial risks, but many modern technology companies pivot implementation of these controls towards technical risk.
CC4 Monitoring	The CC4 series of controls deals with how you intend to monitor your adherence to the controls themselves. They establish the cadence for your audit and how you intend to communicate the results to internal and external stakeholders.
CC5 Control Activities	The CC5 series of controls deals with the control activities themselves. These control activities take place within the technology environment you've deployed, as well as within the policies and procedures you've adopted. The most important element of the CC5 controls is the establishment of the policies themselves and how these are distributed to personnel.

Specific Criteria

Type	Detail
CC6 Logical & Physical Access	The CC6 series of controls is by far the biggest section of controls within the Trust Services Criteria. It’s where the rubber meets the road between your policies and procedures and the actual implementation of your security architecture. Everything you have to say about access, data handling and disposal, and threat prevention is included somewhere in the CC6 series.
CC7 Operations	The CC7 series of controls sets forth the pillars of your security architecture and implies certain tool choices such as those regarding vulnerability detection and anomaly detection.
CC8 Changes	The CC8 series of controls is in fact a single control dealing with changes. It seeks to establish an approval hierarchy around significant elements of the control environment such as policies, procedures, or technologies. As long as your environment does not permit unilateral changes to these elements of the control environment, you should be in good shape.
CC9 Mitigations	The CC9 series of controls addresses risk mitigation. It’s related to the three series where risks are identified, but it goes a step further to prescribe the activities and steps that should be taken to mitigate those risks. For example, if database failure were identified as a risk, a mitigation action would be taking backups of that database.
P Series - Privacy	The P series of controls addresses Privacy. This is an enormous and relatively new addition to the Trust Services Criteria and incorporates 18 controls in total. Most of these controls are focused on businesses that have substantial privacy obligations and are already equipped with solid policy. So what’s needed is to map the existing controls to the P series controls.
PI Series - Processing Integrity	The PI series addresses situations where your organization is performing transactions on behalf of another organization. Just as with the privacy controls, it’s likely that your customer contract already contains many of the guarantees the PI controls seek to address. Your task will be to map your existing contracts, commitments, and policies back to the PI series controls.

08

SOC 2 Certification

To attain SOC 2 certification, you must ensure compliance across the Trust Services Criteria. Five main principles are used to measure and report upon this, which include: .

✓ **SECURITY:**
This principle gives a customer reasonable assurance that their data is safe and secure, and demonstrates that systems are protected against unauthorized access (both physical and logical).

✓ **AVAILABILITY:**
Besides the security principle, availability is the second most common principle chosen for the SOC 2 examination. It focuses on systems being available for operation and use.

✓ **PROCESSING INTEGRITY:**
This principle focuses on system processing being complete, accurate, timely, and valid.

✓ **CONFIDENTIALITY:**
The confidentiality principle ensures information deemed confidential is protected as committed or agreed.

✓ **PRIVACY:**
The privacy principle refers to how personal information (first name, last name, address, phone number, etc.) is collected, used, retained, disclosed, and disposed of. It ensures your data handling practices align with your privacy notice and use the criteria defined in privacy principles issued by the AICPA.

Not every SOC 2 report must include all five principles, so figuring out which Trust Services Principles apply is key to defining the system boundaries and the scope of the audit—and to maintaining your sanity.

For example, if you run a data center and offer data storage to customers, but your client does all the data processing on their own systems, then the security and availability principles—but not the processing integrity principle—would apply. If the stored data contains personal information, then the privacy principle would also be in scope for your service organization.

We promised to provide all the definitions, links, and resources you need to gain a solid understanding of SOC 2. Our aim is to be a single port of call for all things SOC 2 and our complete guide would not be complete unless we invited you to dig into the strongDM knowledge base for more information.

09

SOC 2 Resources

- SOC 2 Glossary
- SOC 2 Report: A Breakdown
- SOC 2 Dashboard
- SOC 2 Audits
  - Prepare For Your First SOC 2 Audit
  - How Long Does a SOC 2 Audit Take
  - SOC 2 Audit Scope
- SOC 2 Policies Guide
- SOC 2 Training Course
- SOC 2 Log Management
- Differences Between SOC 1 vs SOC 2
- How To Stay SOC 2 Compliant
- SOC 2 Team & Roles
- SOC 2 Certification Cost
- Free SOC 2 Policy Templates
- Comply - Open-source repo for SOC 2 resource management and pre-authored policies

strongdm

StrongDM is a Zero Trust access platform that centralizes and simplifies access management for all technical users across every resource in your infrastructure, whether on-premises or in the cloud. By embracing Zero Standing Privileges and implementing Just-in-Time (JIT) access across your full tech stack, StrongDM provides fine-grained, context-based policy enforcement in real time.

Security teams gain complete visibility and control over access and actions with advanced reporting and analytics, helping to identify unused access grants, inactive resources, and over-privileged roles to enhance security and compliance postures. End users enjoy fast, intuitive access to the resources they need when they need them, improving productivity and operational efficiency.

Connect with us on **LinkedIn** and **YouTube** or head to **www.strongdm.com**.