The SirviS Guide to SOC 2

Contents

Introduction

Developed to ensure the privacy and security of customer data, SOC 2 compliance is critical for all enterprises that process, store, or transmit this data.

Although SOC 2 attestation is completely voluntary, not having it can be a huge red flag, telling potential customers and clients that their secrets aren't safe with you or your vendors.

The good news is, the SOC 2 reporting framework is flexible. Using the framework requirements as a guide, your enterprise can write internal controls that fit your unique situation and needs. But how can you know if you're doing SOC 2 right?

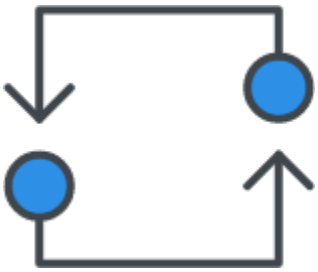
What is SOC 2?

System and Organization Controls for Service Organizations 2 (SOC 2) is a framework for determining whether a service organization's controls and practices are effective at safeguarding the privacy and security of its customer and client data.

The American Institute of Certified Public Accountants (AICPA) developed SOC 2 in response to growing concerns over data privacy and security.

The framework evolved from the 1992 Statement on Auditing Standards No. 70: Service Organizations (SAS 70), which guided the financial audits of third-party service providers such as insurance claims processors and hosted data centers.

Type 1 assesses the effectiveness of controls at a point in time.



Type 2 assesses controls over a period of time — in the case of SOC 2, typically one year.

Over time, IT services became more central to business, and more organizations opted to outsource their technology functions to third-party service providers such as Software-as-a-Service (SaaS) vendors.

But SAS 70 was designed for financial audits, not for assessing data security and privacy controls. So, in 2011 AICPA issued the Statement on Standards for Attestation Engagements No. 16 (SSAE 16). These standards—now updated to SSAE 18—are used in SOC 2 audits today and emphasize data security.

SOC 2 reports discuss five "Trust Services Categories" (formerly "Trust Services Principles"):

- "The **security, availability,** and **processing integrity** of the systems the service organization uses to process users' data," and
- "The **confidentiality** and **privacy** of the information processed by these systems."

Trust Service Categories

The AICPA defines these categories this way

1. **Security:** The effectiveness of policies and procedures governing the way organizations protect themselves against unauthorized access and respond to security breaches resulting in unauthorized disclosure of information will be periodically evaluated.

2. **Availability:** Information and systems must be available for operation and use to meet the entity's objectives.
3. **Confidentiality:** Information designated as confidential must be sufficiently protected from unauthorized access to meet organizational effectiveness.
4. **Processing Integrity:** System processing should be complete, valid, accurate, timely, and authorized to meet organizational objectives.
5. **Privacy:** Personally identifiable information must be collected, used, disclosed, and disposed of in a secure manner.

Who Needs a SOC 2 Report?

Put simply, if your enterprise is a service provider that handles customer data, you should have a SOC 2 report. If you outsource work, your sub-contractors should be SOC 2 compliant, as well.

Showing SOC 2 compliance helps demonstrate your organization's commitment to protecting the privacy and security of your customers' information—increasingly important in our connected digital age.

Industries needing SOC 2 include

- Cloud computing
- IT security management
- Software-as-a-Service (SaaS) vendors
- Financial processing
- Accounting and auditing
- Customer support
- Sales support
- Medical claims processing
- Legal
- Pharmaceutical
- Insurance claims processing
- Human resources
- Data analysis

- Document and records management
- Workflow management
- Customer relationship management (CRM)
- Technology consulting

Often, organizations will designate a team to oversee and coordinate SOC 2 compliance efforts. The job titles of these positions may include:

- Executive sponsor. This may be your:
  - Chief Technology Officer (CTO)
  - Chief Information Officer (CIO)
  - Chief Security Officer (CSO)
  - Chief Information Security Officer (CISO)
  - Chief Risk Officer (CRO)
- SOC 2 project manager
- Author
- Legal
- IT
- Information security
- Risk officer/risk manager
- Compliance officer/compliance manager
- IT auditor
- Consultant

Who has the role of SOC 2 manager varies from enterprise to enterprise, but stakeholders may include:

- Chief Technology Officer (CTO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Chief Information Security Officer (CISO)
- Chief Risk Officer (CRO)
- Risk manager
- Compliance officer/compliance manager
- IT auditor

Why You Need SOC 2 Compliance

1. Customer Demand

Protecting customer data from breaches and theft is top-of-mind for your clients, so without a SOC 2 attestation you could lose business.

2. Cost effectiveness

Think audit costs are high? In 2018, a single data breach cost, on average, $3.86 million—and that figure rises every year. An ounce of prevention is, in this case, worth many pounds of cure.

3. Competitive advantage

Having a SOC 2 report in hand will give you the edge over competitors who cannot show compliance and enhances your organization's reputation as trustworthy.

4. Peace of mind

Passing a SOC 2 audit provides assurance that your systems and networks are secure—not just to your clients and customers, but internally, as well.

5. Regulatory compliance

Because SOC 2's requirements dovetail with other frameworks including HIPAA and PCI DSS, attaining certification can speed your organization's overall compliance efforts.

6. Value

The benefits of a SOC 2 report go beyond the framework itself, providing valuable insights into your organization's risk and security posture, vendor management, internal governance, regulatory oversight, and more.

When to Become SOC 2 Compliant

How about now? Because, chances are, your competitors are already SOC 2 certified.

Every service organization that handles customer or client data, from scrappy startups to multinational corporations, should be compliant with this increasingly important framework. But SOC 2 certification is no quick-and-easy deal. It requires teamwork, advance planning, coordination, internal audits, and more.

In the meantime, your risk of data breaches is higher than it needs to be. Opportunities for business might be passing you by.

Even if you already have your SOC 1 attestation, you'll still need SOC 2. Because, while SOC 1 deals with financial reporting, SOC 2 generates internal control reports around those five trust principles: data security, privacy, processing integrity, confidentiality, and availability.

A SOC 2 report can take nine months or even a year to complete, especially if you're using spreadsheets to track your progress.

SOC 2 vs. SOC 1: What's the Difference?

Don't be fooled by the similar acronyms: SOC 1 and SOC 2 compliance is as different from each other as night and day.

In fact, they only have a few things in common:

- Both are based on SSAE-18, a set of auditing standards developed by the American Institute of Certified Public Accountants (AICPA).
- Both concern service organizations.
- Both can generate Type 1 and Type 2 reports.

A SOC 1 report will discuss organizational controls that affect the enterprise's financial statements. Are the controls well designed? Do they work, helping the organization to meet its financial goals?

A SOC 2 audit is not at all about financial reporting. A SOC 2 report discusses controls that affect the organization's information security, availability, and processing integrity, as well as data confidentiality and privacy.

SOC 2 has much more in common with SOC 3. In fact, these reports are pretty much the same—the difference lies in their intended audience.

- SOC 2 reports provide information about your organization for an informed, knowledgeable audience whose members often have a vested interest in the audit findings.
- SOC 3 reports address a more general audience and tend to be shorter and less detailed than SOC 2 audits.

SOC 2 Type 1 vs. Type 2 Reports

The difference between SOC 2 Type 1 and Type 2 reports lies in the amount of time each covers.

- SOC 2 Type 1, often an organization's first-ever SOC 2 report, looks at control governing data security and privacy at the time of the audit.
- SOC 2 Type 2 reports discuss the effectiveness of your organization's information security and privacy control since your last SOC audit, which typically means one year.

The two types of reports are used differently by organizations:

- SOC 2 Type 1 takes a "snapshot-in-time" approach, setting a baseline for future audits.
- SOC 2 Type 2 asks how well your data security and privacy controls have worked since your last SOC 2 audit.

So, the audit procedure some organizations follow is:

- Type 1 for the first SOC 2 audit
- Type 2 for subsequent SOC 2 audits

What Happens During a SOC 2 Audit?

A SOC 2 assessment works much like any other audit. The independent Certified Public Accountant or accounting firm you choose can help you:

- Determine your audit scope, a critical first step in which you determine:
  - Which of the 5 SOC principles, now called Trust Services Categories apply to your organization
  - Which SOC report you need: Type 1 or Type 2. Most organizations choose Type 1, which considers SOC 2 compliance at a point in time, for their first SOC 2 audit, and Type 2, which examines compliance over a period of time, for subsequent audits.
- For each applicable Trust Services Category, the auditor will examine your controls, a process that includes evidence collection, to evaluate whether they are working as they should. Documents the auditor may examine include:
  - Organizational charts
  - Asset inventories
  - Onboarding and off-boarding processes
  - Change management processes

If the auditor finds problems or gaps, no worries, you'll have an opportunity to remediate. Findings can drive up audit costs, however, so thorough preparation using a SOC 2 audit checklist is your best bet for efficiency and ease.

Next Steps

Preparing for a SOC 2 assessment can be a daunting task. SirviS will assist with the audit preparation, setting up the data collection tools and finding the Certified Public Accountant or accounting firm to perform the audit.