Security Ideals –
White Paper

1775 W State St. Suite 335 Boise, ID 83702 302-433-6222
www.securityideals.com

SOC 2 Compliance A Comprehensive Guide

2025 Edition

Intended Audience

This whitepaper's intended audience is those concerned with obtaining SOC 1, 2, or 3 compliance. That includes readers who are considering undergoing an audit, readers currently under audit, and anyone interested in learning more about SOC audits.

SOC 1 VS SOC 2 VS SOC 3

SOC 1

SOC 1 is a financial audit that reports on internal controls over financial reporting and is used by financial controllers, CFO's, and employees concerned with financial reporting. SOC 1 audits consist of Type 1 & Type 2 audits.

SOC 2

SOC 2 audits are designed to evaluate an organization's security, availability, processing integrity, confidentiality, or privacy controls. These reports are typically shared under NDA by management, regulators, and others. SOC 2 audits are either type 1 or type 2. SOC 2 Type 2 is the audit most companies are after. It's the audit prospective clients request, healthcare systems require before trading data, and is becoming the standard in the United States.

SOC3

SOC 3 audits report on the security, availability, processing integrity, confidentiality, or privacy controls of an organization. The big difference between SOC 2 and SOC 3 is that SOC 3 audits are designed to be publicly available. SOC 3 is sometimes seen as inferior due to the lack of details about the system or how it operates. Most clients interested in making their audit available on their website elect to add on a SOC 3 with a SOC 2 Type 1 & Type 2 for a incremental fee.

SOC Report Comparison

	WHAT IT REPORTS ON	WHO USES IT
SOC 1	Internal controls over financial reporting	User auditor and users' controller's office
SOC 2	Security, availability, processing integrity, confidentiality or privacy controls	Shared under NDA by management, regulators and others
SOC 3	Security, availability, processing integrity, confidentiality or privacy controls	Publicly available to anyone

A SOC 2 OVERVIEW:

SOC 2 isn't a rigid set of rules or a detailed standard. It's a framework that demonstrates the maturity of a company's information security functions, including security, availability, processing integrity, confidentiality, and privacy.

Completing a SOC 2 audit (with no major findings) isn't enough to prove that you're 100% secure, but it will demonstrate a level of confidence and help to build trust with your customers.

A Brief History of SOC 2

Before SOC 2 audits, the original AICPA standard for auditing service organizations was known as a "SAS 70" (Statement of Auditing Standards No. 70). The SAS 70 audits were originally performed by Certified Public Accountants (CPAs) to audit the effectiveness of internal financial controls. This began in April of 1992 and continued until April of 2010. SAS 70 audits began to be applied to an organization's internal controls around data and information security more broadly as time went on. In early 2010 AICPA introduced the Statement on Standards for Attestation Engagements no. 16 (SSAE16), which broke down into Service Organization Controls 1 (SOC 1) & Service Organization Controls 2 (SOC 2). These audits were introduced to provide confidence in an organization's security with added credibility that an independent third-party conducts the audit. They quickly became the defacto standard in the United States when larger companies conduct due diligence on potential service organizations.

In 2021, SOC 1 reports are designed to audit financial controls and reports, as the original SAS 70 was designed. SOC 2 Reports are written after conducting an audit against the Trust Service Criteria (TSC) standard, which we discuss later in this white paper. This standard is the best choice if you'd like to improve your company's information security maturity and business process stability.

SOC 2 Trust Service Criteria (Trust Principles)

SOC audits are conducted around five "Trust Service Criteria," which were previously referred to as the "Trust Service Principles." When you hire an auditing firm to conduct your audit, you will choose which criteria you want the auditor to attest to. Deciding which criteria to select for your audit is a decision best made by business stakeholders and what is most important to your customers.

The Trust Service Criteria are:

Security
All SOC 2 reports include at least the security trust service criteria, and it's often referred to as the "common criteria" because it's common to all SOC audits and reports.

Availability
Information and systems are available to meet the company's objectives. Service level agreements with customers are met and tracked.

Processing Integrity
System processing is complete, timely, valid, accurate, and authorized to meet the company's objectives.

Confidentiality
Information that is classified as confidential is adequately protected.

Privacy
Personal information is collected, used, disclosed, retained, and disposed of in accordance with the stated privacy policies. The privacy trust service criteria are only applied to personal information, and some audit firms treat SOC 2 privacy as a separate audit altogether.

SOC 2 Trust Service Criteria

All SOC 2 audits include the security trust service criteria sometimes referred to as the "Common Criteria." The Common Criteria is the largest section of the audit and contains elements of all an organization's information security controls. Some companies elect for a "common criteria audit" the first year, which is the equivalent of selecting only the "Security" trust service criteria. Keeping the scope small is an excellent way to ease into the SOC audit process. Still, many customers are picky about a SOC audit with specific criteria, so be mindful of your customers and their needs.

In addition to Common Criteria, most companies elect to add on Availability and Confidentiality. The Processing Integrity Criteria is typically added on by companies that process a large volume of transactions, as well as financial institutions. Privacy is rarely selected as part of a SOC 2 audit. Most companies who would choose the Privacy addon are choosing to focus on GDPR instead. While complying with GDPR, there is a significant focus on privacy, and GDPR is required to sell products and services to European Countries.

SOC 2 Common Criteria (Security TSC)

Control Environment – CC1
The entity demonstrates a commitment to integrity and ethical values.

Communications and Information – CC2
Policies and procedures are in place to ensure security, and the entity communicates well both internally and externally.

Risk Assessment – CC3
The entity conducts risk assessments and monitors business activities for changes that may impact risk.

Monitoring Activities – CC4
Internal controls are continually monitored, evaluated, and communicated to key stakeholders.

Control Activities – CC5
Precise controls have been developed to mitigate potential risks in processes and technology.

Logical and Physical Access – CC6
Access to data is protected both by logical access controls and physical access controls. Role-based access control is utilized to produce a need-to-know access strategy.

System Operations – CC7
The system is operational and robust, including ongoing monitoring, incident response, and disaster recovery.

Change Management – CC8
All changes that affect the function of the system are thoroughly tested and approved before implementation. Changes are tracked in a change management system.

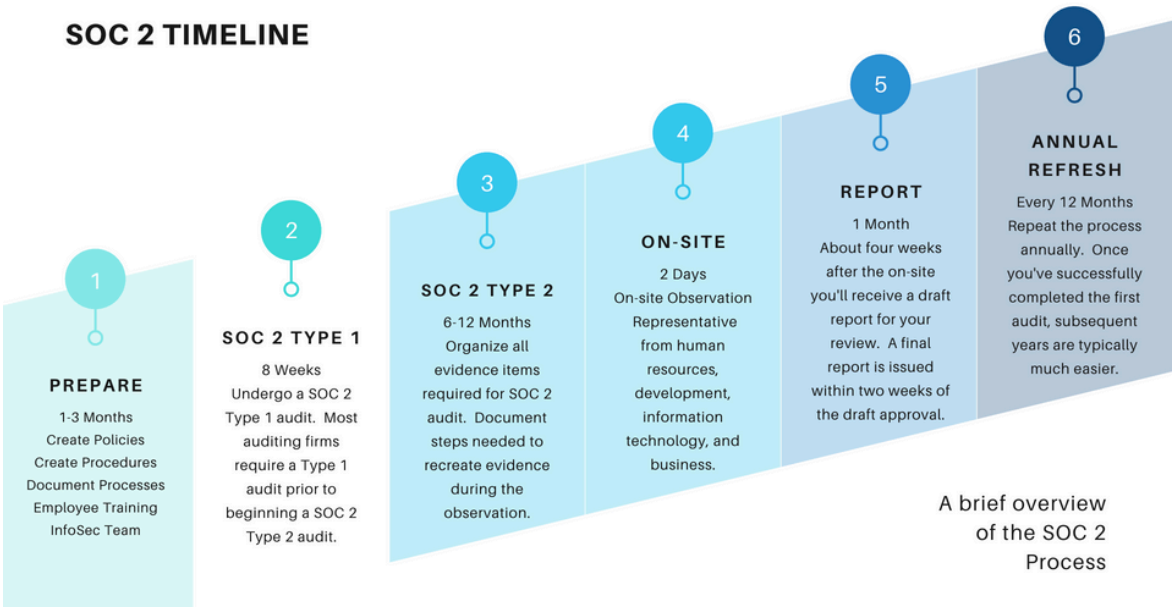
Risk Mitigation – CC9
Risks are mitigated through vendor management and appropriate business processes.

The SOC 2 Audit Process

The SOC 2 standard was created by the AICPA. A licensed, certified public accountant must sign all SOC 2 audits. To achieve SOC 2 compliance, most companies spend six months to one year preparing. This preparation includes deciding which systems will be included in the audit (in scope), developing policies and procedures, and implementing new security controls to minimize risk. The first time you complete a SOC 2 audit, you'll receive a SOC 2 Type 1. Most companies want a SOC 2 Type 2. This means to obtain a SOC 2 Type 2, you'll need to complete the SOC 2 Type 1 audit and then conduct a SOC 2 Type 2 audit after six to twelve months have elapsed. This distinction can be confusing but is very important.

Here's an easy way to remember: **S** = SCOPE, **T** = TIME

SOC 1 = Financial Scope
SOC 2 = Information Security Scope
Type 1 = At a single point in time
Type 2 = Over a period of time (usually 6-12 months)



A brief overview of the SOC 2 Process

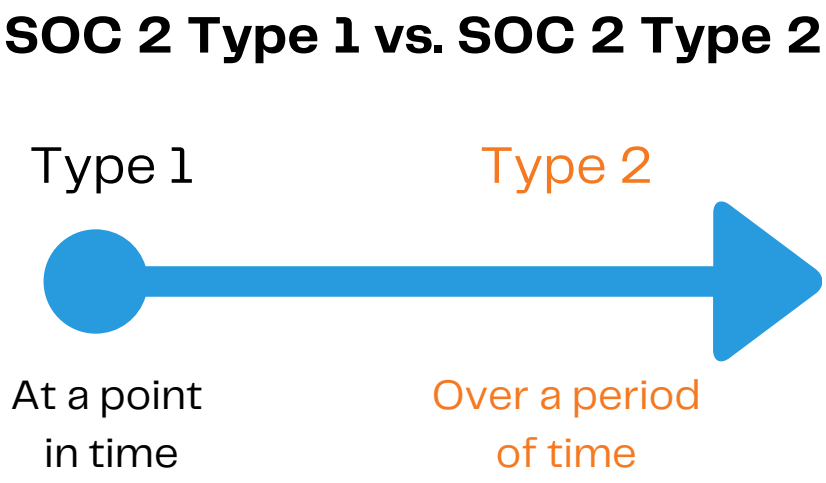
When an organization is ready to begin the audit, it will hire a licensed CPA auditing firm to conduct the audit. The actual process starts with a scoping discussion and selection of the Trust Service Criteria that will be evaluated by the auditor. The following six to eight weeks are used to collect and submit evidence to the auditing firm, usually through the use of a portal or document request spreadsheet. During the six to eight-week period, most auditing firms will hold weekly phone calls to evaluate the quality of evidence and the speed at which the organization is uploading evidence. After the evidence collection period has been finished, the auditors will schedule an onsite audit. This is typically a two-day in-person meeting at your office. Many audits conducted during 2020 and 2021 were "virtual onsite audits" due to Covid-19. These are conducted through video conferencing platforms but function in the same way as traditional onsite audits. While in your office, the auditor will conduct interviews and review evidence items.

SOC 2 Type 1 vs Type 2

SOC 2 Type 1
An audit is conducted against the selected Trust Service Criteria at a single point in time. This audit demonstrates: All the security controls in place today are properly designed.

SOC 2 Type 2
An audit is conducted against the selected Trust Service Criteria over a period of time. This audit demonstrates: All the security controls are properly designed, and there is sufficient proof that the controls were adequate during the last six months. This "period of performance" is typically six months for the first year a company is audited and becomes every twelve months after the first audit is successfully completed.

Type 1 reports are easier to prepare for since they don't require six months or more of historical data to support the security controls. However, while Type 2 reports require more time to prepare for, they are also much more valuable in the hands of a potential client, board member, investor, partner, etc. In our experience, companies that conduct due diligence through information security questionnaires will not accept a SOC 2 Type 1 and are only interested in a SOC 2 Type 2. Most auditing firms provide a discount for companies going through SOC 2 Type 1 & Type 2 audits in the same year. We strongly recommend selecting a SOC 2 Type 2 audit as your goal and using the SOC 2 Type 1 as a required milestone in the overall project.



SOC 2 Competitive Advantage

Organizations of all sizes can benefit from building deeper trust with customers, prospects, and partners. If you process or store customer data, you should be concerned with how your organization protects it.

Data breaches are becoming more common every year. The news is full of stories about how large companies recently lost 150 million user records or millions of breached credit card numbers. The aftermath of these security breaches can cost tens of millions of dollars, and the reputational harm can last years.

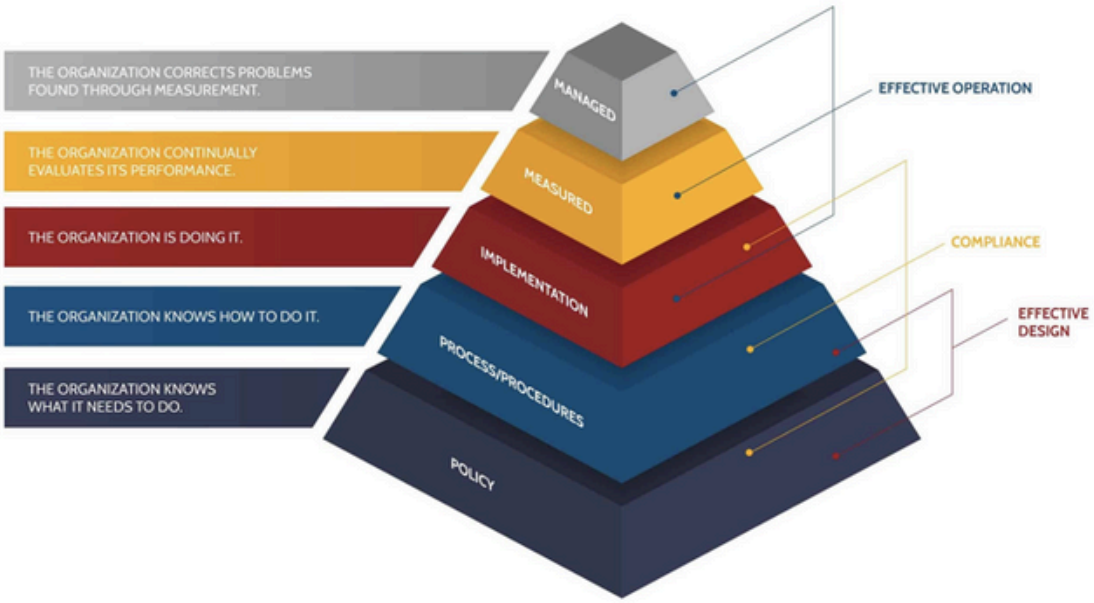
Big companies can often weather the storm of a security breach by throwing capital at the problem. They typically replace their entire security team at an executive level (if they ever had one) and spend millions on consultants to prevent future breaches while spending further millions on firms that specialize in reputational harm. Small companies and startups don't have the luxury of endless budgets and often have one or two large customers that are critical to their survival. A security breach is often the end of the road for small and medium businesses.

While there is no way to guarantee your company is secure, the SOC 2 report and the Trust Services Framework often reveal risks that aren't adequately mitigated. Its popularity has grown in recent years because it provides external validation of your information security program.

The Value of SOC 2

Suppose you don't achieve a SOC 2 Type 2 report as a vendor or service provider. In that case, you will have to convince your potential customers that your information security program is up to their standards. Usually, this involves filling out information security questionnaires, talking to security and risk officers from your potential customer, and ultimately losing deals to competitors that have obtained SOC 2 compliance. A few years ago, having SOC 2 was a nice outside validation of a security program that customers appreciated but didn't necessarily expect from their vendors. Today customers expect their services providers and vendors to have SOC 2 at a minimum. Many enterprise-level customers will not work with any vendor that doesn't have a SOC 2 or similar compliance audit.

In summary, being SOC 2 compliant will help your sales team when working with enterprise customers and force you to follow a set of best practices that will improve the way you safeguard your customer's data.



6 Reasons to Pursue SOC 2 Type 2

Start working on SOC 2 compliance as soon as possible. Don't wait until the most significant customer you've ever landed tells you they require all of their vendors to be compliant. We've had hundreds of clients come to us with unrealistic timeframes driven by landing the proverbial big-fish client, only to be disappointed when they realize this is a months or even years-long project. Even if you don't plan to go through the actual audit for a while, don't delay putting processes and procedures in place to safeguard customer data.

SOC 2 Improves Security

Security Ideals has worked with hundreds of clients on SOC 2 projects, and we've yet to meet a customer who didn't improve their security when undergoing SOC 2 compliance. The SOC 2 trust service framework and associated controls help build a robust information security program that focuses on protecting customer and business data.

SOC 2 Improves Company Culture

Introducing new layers of security and additional controls can be an uphill battle. Employees may complain about the extra steps involved when using multi-factor authentication or a long passphrase's complexity. However, educating employees through security awareness training and the introduction of technologies like password managers can often be a tool that helps protect your employees in their private lives and at work. The smaller and younger a company directly correlates with how hard or easy it is to introduce new processes and policies. It's always easier to improve and scale a process as your company grows than wait until you're well established and you have to make sweeping changes.

SOC 2 Makes Sales Easier

Sales departments love compliance reports because it makes their jobs easier. When customers ask about data security and the protections around their data, providing a SOC 2 report immediately alleviates concerns and helps convert potential customers without any hassles or hangups due to risk, compliance, or information security.

SOC 2 Creates Documentation

Nobody loves creating documentation on processes and procedures, but it's the difference between an immature company and one that has its ducks in a row. Having well-documented procedures will improve scalability, communication, consistency and helps when onboarding new employees. Documentation is critical when going through a new round of venture capital funding, mergers and acquisitions, and future compliance goals such as PCI, ISO 27001, CMMC, etc.

SOC 2 Helps Minimize Risk

While your company may be the rare exception that has a mature information security function, the majority of clients we work with can stand to improve their risk management programs if one currently exists at all. Good risk management isn't just about passing an audit or lowering your cyber insurance premiums, and it involves capturing risks from the entire organization and treating them appropriately. Risk management should ultimately dictate how and where you spend your budget on information security.

SOC 2 Improves Communication

While SOC 2 can be applied to organizations of all sizes, it's often attempted by organizations that have a few dozen to a few thousand employees. Most organizations have departments that become siloed over time. SOC 2 is an audit primarily focused on information security controls, including components from your entire organization. Human resources, C-level executives, Information Technology, Information Security, Sales, Marketing, Finance, and Operations are often involved in the audit process and must work together. These compliance projects often create better communication and friendship between departments that otherwise wouldn't interact on a daily basis.

Security Ideals: How We Can Help!

It's a good idea to consider SOC 2 compliance as early in your company's journey as possible. If you are selling a service in the United States to enterprise or medium-sized businesses, you will be asked for a SOC 2.

While it is challenging to undergo a SOC 2 audit when your company is still small and under-resourced, it can be much more complicated once you grow larger. Implementing policies and procedures, training, security products, and risk assessment is always more straightforward when your company is still small. While many mature companies do undergo SOC 2 compliance, it's a more difficult road since the company's culture, processes, and tools are well established and relied upon by a significant number of employees.

Three Levels of Support

Advisory Role

Suppose your company already has security policies, procedures, an information security team, documented change controls, vendor management, security or risk committee meetings, business continuity plans. You just need help with understanding SOC 2 controls and the auditing process. In that case, the advisory program may be right for you. We will help decipher the evidence requests from your auditing firm and provide direction and advice on any items your organization may be missing.

Full Assistance

We help you build everything. Company security policies, access control, vendor management, data classification, human resources processes, change management, logging and monitoring, acceptable use policies, risk assessment and business continuity planning, incident response, etc. Everything that is needed to elevate your company's security posture and controls to receive an excellent audit.

Virtual Chief Information Security Officer (vCISO)

For company's that are constrained by resources and can't devote the appropriate amount of time to the SOC 2 project, we offer vCISO. With this level of support, we become one of your team members, and we bring in additional resources from our team to help with everything in the "Full Assistance" plan, including full project planning, and as many additional InfoSec resources as needed to complete your audit on time and with no major findings.

Summary

SOC 2 projects are complex and time-consuming, but they're worth it! They help improve your organization's security, sales, and resiliency while providing a third-party validation regarded as the gold standard for service organizations.

Using the insights and information in this white paper should help demystify SOC audits and the audit process itself. If you have any questions about SOC audits or other compliance frameworks, please contact us today! We provide all new clients a free 30-minute consultation where we can share additional strategies, discuss pricing, and various support models that will help you achieve your goals.

SECURITY IDEALS