CS-107 · Compliance & Frameworks

SOC 2

An attestation report on how a service organization protects customer data.

Executive Summary

SOC 2 is an attestation report, based on the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria, that describes how a service organization protects the data it handles for customers. An independent auditor examines the organization's controls and issues a report that customers can review instead of running their own audit. It is especially common among software, cloud, and technology vendors that hold customer data.

What It Is

SOC 2, short for System and Organization Controls 2, is a report produced by an independent certified public accounting firm that expresses an opinion on a service organization's controls. Unlike a certification with a pass or fail badge, it is an attestation: the auditor examines the controls against the Trust Services Criteria and describes what they found. The criteria cover security, and, when relevant to the service, availability, processing integrity, confidentiality, and privacy. Security is the foundational category most reports include. The organization defines the system in scope and the controls it operates, and the auditor tests whether those controls are suitably designed and, in a Type II report, whether they operated effectively over a period of time.

Why It Matters

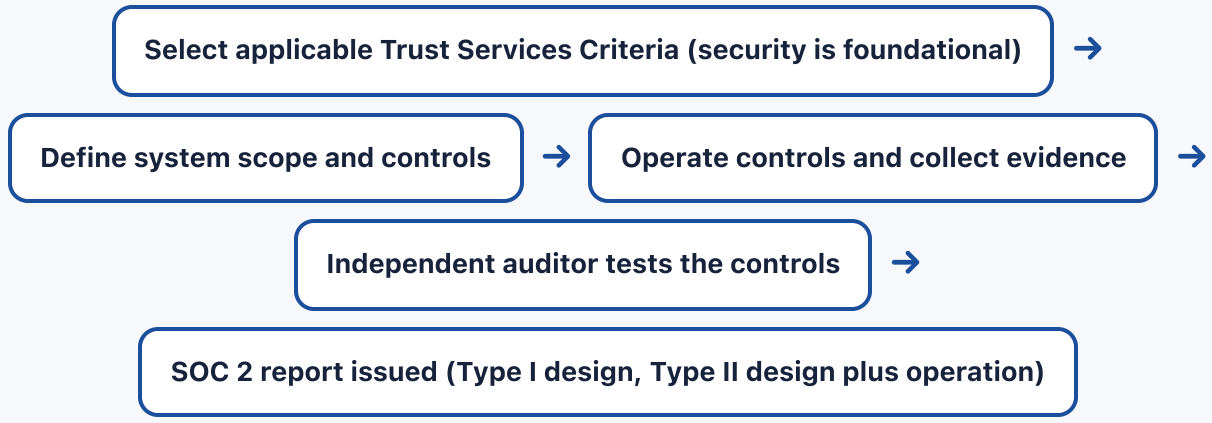
For technology and service providers, a SOC 2 report has become a standard requirement in enterprise sales and vendor risk reviews. Rather than each customer auditing the vendor separately, the vendor commissions one independent report that many customers can rely on. A clean report shortens sales cycles and builds trust, while gaps flagged in a report can stall deals. For professionals, SOC 2 work sits at the intersection of security operations, compliance, and

audit, and demand for people who can prepare for and manage these examinations is strong wherever software is sold to businesses.

How It Works

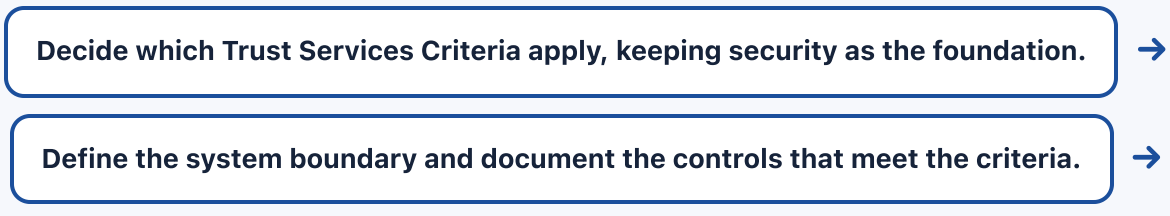
The organization first decides which Trust Services Criteria apply based on the promises it makes to customers, with security nearly always included. It defines the system boundary and the controls that meet the criteria, then operates those controls and collects evidence that they work. A Type I report evaluates whether the controls are suitably designed at a point in time. A Type II report goes further and evaluates whether the controls operated effectively over a review period, often several months to a year, which is why customers usually prefer it. An independent auditor performs the examination, tests a sample of evidence, and issues the report with an opinion. Because the report expires, organizations typically pursue a fresh Type II report each year.

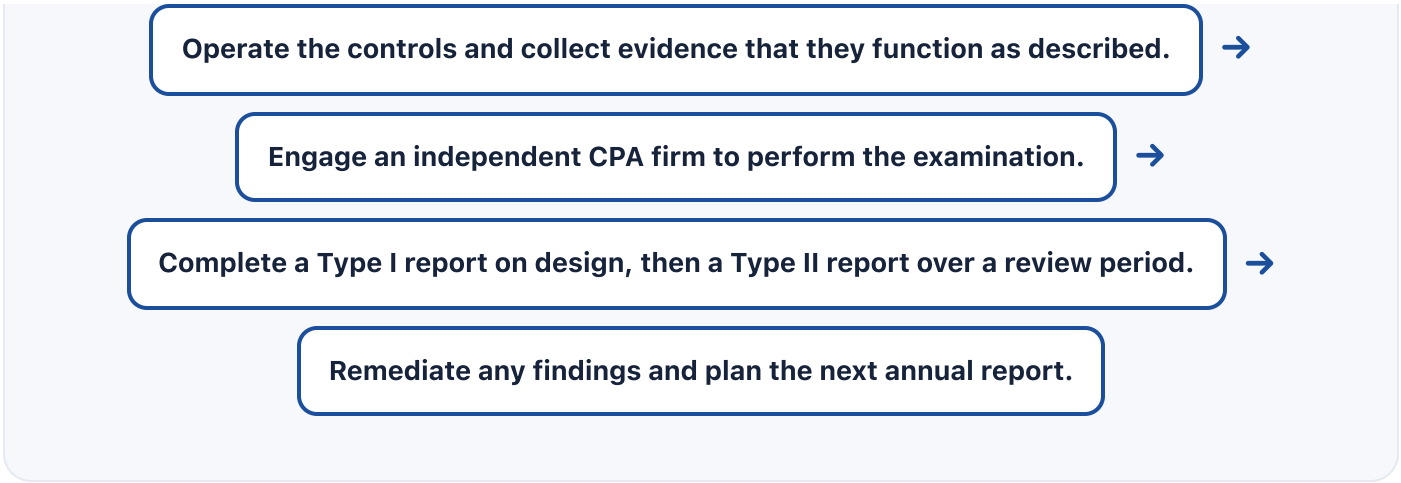
Architecture Diagram



A SOC 2 report is produced when an auditor tests a service organization's controls against the Trust Services Criteria.

Visual Workflow





Common Attacks

- Choosing criteria or a scope that looks good but omits systems that actually handle customer data
- Preparing only for a Type I when customers expect a Type II covering operation over time
- Collecting evidence only near the audit rather than throughout the review period
- Documenting controls that are not actually performed consistently in practice
- Letting a report lapse and losing customer trust between annual cycles

Common Mistakes

- Confusing SOC 2 with a certification and expecting a simple pass or fail badge
- Under-scoping the system so the report does not cover what customers care about
- Treating evidence collection as a one-time scramble instead of an ongoing routine
- Overlooking exceptions in a report and assuming any report means the vendor is safe
- Ignoring that criteria beyond security may be needed for certain services

Best Practices

- Scope the system honestly to include what customers actually rely on
- Include the security category and add other criteria only when they fit the service
- Automate and schedule evidence collection so it spans the whole review period
- Map SOC 2 controls to frameworks you already run to reuse effort
- Read the auditor's opinion and any exceptions carefully, not just the cover page

- Plan for an annual Type II report rather than a single point-in-time review

Quick Checklist

- [x] Applicable Trust Services Criteria selected and justified
- [x] System boundary and controls documented
- [x] Evidence collected continuously across the review period
- [x] Independent CPA firm engaged for the examination
- [x] Type I or Type II report scope agreed with the auditor
- [x] Findings tracked to remediation and next report scheduled

Recommended Tools

GRC platform
Maps controls to criteria and organizes evidence for the auditor

Evidence collection automation
Gathers proof of control operation across the review period

Policy management system
Maintains the policies that support many SOC 2 controls

Ticketing and access review tools
Provide records that controls such as access reviews actually ran

Industry Standards

AICPA Trust Services Criteria
The criteria a SOC 2 examination is performed against

AICPA attestation standards
The professional standards governing how the auditor performs the examination

ISO/IEC 27001
Related certification that overlaps with many SOC 2 controls

Career Relevance

SOC 2 is central work for GRC analysts, compliance analysts, security auditors, and CISOs at service and software companies, who prepare the environment, run controls, gather evidence, and manage the auditor relationship. Vendor risk and procurement teams read these reports to judge suppliers. For the privacy and AI governance professionals AI-Governance-Jobs.com serves, SOC 2 is a common lens through which customers evaluate whether a data-handling service can be trusted.

Interview Questions

- What is SOC 2, and how is an attestation different from a certification?
- Explain the difference between a Type I and a Type II report.
- What are the Trust Services Criteria, and which one is foundational?
- How would you scope a SOC 2 examination for a cloud service?
- What would you look for when reviewing a vendor's SOC 2 report?

Related Certifications

AICPA CPA (for the auditor role) | ISC2 CISSP | ISACA CISA

Further Reading

- AICPA SOC for Service Organizations
- AICPA Trust Services Criteria
- NIST Cybersecurity Framework

Key Takeaways

- SOC 2 is an independent attestation report based on the AICPA Trust Services Criteria.
- It is common for software, cloud, and service vendors that hold customer data.
- Security is the foundational criterion, with others added when they fit the service.
- A Type II report tests that controls operated over time, which customers usually prefer.

- Reports expire, so organizations typically pursue a fresh Type II each year.

FAQ

▶ **Is SOC 2 a certification?**

▶ **What is the difference between SOC 2 Type I and Type II?**

▶ **How is SOC 2 different from ISO/IEC 27001?**

Related Careers

RELATED ROLES

Grc Analyst | Compliance Analyst | Security Auditor | Ciso

RELATED CERTIFICATIONS

AICPA CPA (for the auditor role) | ISC2 CISSP | ISACA CISA

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **SOC 2**
3. Go deeper: ISO/IEC 27001
4. Go deeper: NIST Cybersecurity Framework (CSF)
5. Validate it: work toward **AICPA CPA (for the auditor role)**

6. Find the role: browse current openings

RELATED SHEETS

CS-106 ISO/IEC 27001 | CS-104 NIST Cybersecurity Framework (CSF) | CS-001 Cybersecurity | CS-085 Risk Ratings | CS-009 Core Security Principles