

SOC 2 (AICPA Trust Services Criteria)

SOC 2 assesses and reports on a service organization's controls for security, availability, processing integrity, confidentiality, and privacy.



What it is

SOC 2 — System and Organization Controls for Trust Services Criteria is an auditing framework that enables organizations to assess and report on the effectiveness of their internal controls related to security, availability, processing integrity, confidentiality, and privacy. The primary purpose of SOC 2 is to help service organizations demonstrate their ability to protect customer data and manage key operational risks.

Developed and maintained by the American Institute of Certified Public Accountants (AICPA), SOC 2 is widely used by technology, cloud, and service providers that process or store sensitive information on behalf of clients. The framework focuses on evaluating cybersecurity controls and risk management practices through independent attestation reports, often in support of customer or regulatory requirements.

At a glance

<div>PUBLISHER</div> American Institute of Certified Public Accountants (AICPA)	<div>TYPE</div> Certification / Assurance Program	<div>VERSION</div> SOC 2 (based on AICPA Trust Services Criteria)
<div>EFFECTIVE</div> 2017	<div>DOMAIN</div> Cybersecurity	<div>FAMILY</div> SOC Frameworks
<div>REGION</div> United States	<div>INDUSTRY</div> Cloud & Technology Providers	<div>ADOPTION MODEL</div> Certification
<div>IMPLEMENTATION COMPLEXITY</div> High		

Source: <https://www.aicpa-cima.com/topic/audit-assurance/soc-2>

Why it matters

- **Strengthen cybersecurity governance** Establishes clear policies and controls for effective oversight of information security across organizational processes and technology environments.
- **Enhance regulatory and customer alignment** Enables organizations to meet regulatory expectations and address customer requirements through independent attestation of trust service principles.
- **Increase audit readiness** Supports systematic evidence collection and documentation, making regulatory or client-driven audits more efficient and less disruptive.
- **Protect sensitive customer data** Implements robust controls to safeguard confidentiality and privacy, reducing the risk of data exposure or unauthorized access.

How SmartSuite supports SOC 2

Trust Services Criteria Control Library

Organize controls across Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Control Ownership and Operating Cadence

Assign control owners and schedule recurring activities to ensure consistent execution.

Evidence Collection and Audit Trail

Capture evidence with timestamps, reviewers, and linkage to specific controls.

Control Testing and Exception Management

Track testing results, deficiencies, and remediation actions across the audit period.

Risk and Vendor Alignment for SOC 2 Scope

Connect risks and third parties to SOC 2 criteria for scoped audit coverage.

SOC Examination Readiness Reporting

Provide real-time views of control status, gaps, and readiness for SOC examinations.

Common framework mappings

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

ISO 27017

ISO 27018

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

Official resources

SOC 2 Trust Services Criteria

Provides the criteria for evaluating controls related to security, availability, processing integrity, confidentiality, and privacy.
aicpa.org/topic/audit-assurance/soc-2

AICPA SOC 2 Implementation Guide

Offers guidance on implementing SOC 2 controls and preparing for compliance assessments.
aicpa.org/cpe-learning/course/soc-2

SOC 2 Reporting Framework Overview

Describes the structure and key components of the SOC 2 reporting framework.
aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

AICPA System and Organization Controls Suite

Outlines the various SOC reports and their focus areas, including SOC 2.
aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

Frequently asked questions

What is SOC 2 used for?

SOC 2 is used to evaluate and report on the effectiveness of internal controls related to security, availability, processing integrity, confidentiality, and privacy in service organizations. It is commonly requested by customers to ensure that their data is managed securely and in accordance with industry standards.

Is SOC 2 certification mandatory or certifiable?

SOC 2 is not a regulatory requirement and does not result in a formal certification. Instead, organizations receive an attestation report from an independent auditor verifying compliance with the Trust Services Criteria.

What organizations need to comply with SOC 2?

SOC 2 typically applies to technology, cloud, and service providers that store, process, or transmit sensitive customer data on behalf of clients. Organizations pursuing business with enterprises or highly regulated customers often seek SOC 2 attestation to meet contractual or due diligence obligations.

What are the key artifacts required for SOC 2?

Key SOC 2 artifacts include a documented system description, risk assessment records, written security policies, control design documentation, evidence of control operation, and auditor-issued Type I or Type II reports. These demonstrate how the organization meets the Trust Services Criteria.

How does a SOC 2 audit work?

A SOC 2 audit involves defining the scope, mapping controls to the Trust Services Criteria, gathering evidence, and undergoing evaluation by an independent CPA firm. Type I reports assess control design at a point in time, while Type II reports assess control effectiveness over a review period.

How does SOC 2 relate to other frameworks like ISO 27001?

SOC 2 and ISO 27001 both address information security controls and risk management, but SOC 2 focuses on U.S.-based Trust Services Criteria and provides a third-party attestation report. ISO 27001 is a certifiable international standard with a broader focus on management systems.

What are the ongoing compliance requirements for SOC 2?

Ongoing SOC 2 compliance requires regular risk assessments, continuous control monitoring, periodic policy updates, evidence collection, and annual or ongoing audits. Organizations must remediate any control gaps and maintain documentation to demonstrate continued adherence.

How would SmartSuite support SOC 2?

SmartSuite facilitates SOC 2 compliance by providing modules for risk tracking, control management, and evidence collection. The platform enables automated audit readiness, supports remediation workflows, and delivers reporting tools to help organizations monitor controls and demonstrate compliance with the Trust Services Criteria.

License included / downloadable: No SOC 2 reporting standards are published by the American Institute of Certified Public Accountants (AICPA). Access to official guidance typically requires purchasing AICPA publications. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/soc-2-system-and-organization-controls-for-trust-services-criteria