

SOC 3 (AICPA)

SOC 3 is a public attestation report that confirms an organization's controls for security, availability, processing integrity, confidentiality, and privacy.



What it is

SOC 3 — System and Organization Controls Public Assurance Report is an external attestation report that allows organizations to communicate the effectiveness of their internal controls related to security, availability, processing integrity, confidentiality, or privacy to a broad audience. This report provides stakeholders with confidence that an independent CPA has evaluated how the organization manages risks related to information security and data protection.

Developed and published by the American Institute of Certified Public Accountants (AICPA), SOC 3 reports are most often utilized by service organizations seeking to assure customers, business partners, and the general public about their cybersecurity and compliance posture. SOC 3 shares the same Trust Services Criteria as SOC 2, but is intended for public distribution and does not include detailed descriptions of controls or results.

At a glance

<div>PUBLISHER</div> American Institute of Certified Public Accountants (AICPA)	<div>TYPE</div> Guidance	<div>VERSION</div> SOC 3 (based on AICPA Trust Services Criteria)
<div>EFFECTIVE</div> 2011	<div>DOMAIN</div> IT Governance	<div>FAMILY</div> SOC Frameworks
<div>REGION</div> United States	<div>ADOPTION MODEL</div> Certification	<div>IMPLEMENTATION COMPLEXITY</div> Moderate

Source: <https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services>

Why it matters

- **Build stakeholder trust** Demonstrate to customers and the public that internal controls have been independently evaluated and meet recognized security standards.
- **Increase audit readiness** Provide a streamlined, externally validated report that supports ongoing audit requirements and reduces time spent on repetitive due diligence.
- **Enhance regulatory alignment** Support compliance efforts by aligning internal processes with widely accepted criteria from the AICPA Trust Services Criteria framework.
- **Strengthen data protection practices** Offer assurance that mechanisms to safeguard sensitive and confidential information are both present and regularly assessed for effectiveness.

How SmartSuite supports SOC 3

Trust Criteria Scope and Controls

Manage the scope and controls that underpin the SOC 3 examination.

Evidence Collection and Operating Cadence

Centralize evidence and recurring control activities to maintain consistent operation.

Control Testing and Exception Tracking

Document test results and manage exceptions through remediation and retesting.

Customer and Public Assurance Assets

Organize SOC artifacts and supporting evidence for broad stakeholder sharing.

Post-Audit Improvements and Policy Updates

Track post-audit improvements, control enhancements, and policy updates.

SOC Readiness Reporting

Report posture, gaps, and readiness across criteria and control owners.

Common framework mappings

SOC 2 (AICPA TSC 2017)

COBIT 2019

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

SOC 1

SOC 2

Official resources

SOC 3: Trust Services Criteria

Defines the criteria used for evaluating security, availability, and confidentiality controls.
aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022

SOC 3 Overview

Provides an introduction to SOC 3 reports and their role in public assurance.
aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

SOC Suite of Services

Outlines all SOC services, including SOC 3, emphasizing security and compliance standards.
aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

Frequently asked questions

What is SOC 3 used for?

SOC 3 is used to publicly demonstrate that an organization's internal controls related to security, availability, processing integrity, confidentiality, and privacy have been independently assessed and found effective. It provides assurance to customers, partners, and the general public about the organization's cybersecurity and compliance posture.

Is SOC 3 a mandatory or certifiable requirement?

SOC 3 is not mandatory by law or regulation; it is a voluntary attestation report. Unlike a formal certification, SOC 3 is a third-party assurance provided by an independent CPA firm, confirming that controls were evaluated against the AICPA Trust Services Criteria.

What is the scope of SOC 3 reports?

SOC 3 reports apply primarily to service organizations that want to communicate their control environment to a broad, non-technical audience. The scope covers internal controls relevant to the Trust Services Criteria but does not provide detailed descriptions of controls or test results, ensuring suitability for public distribution.

What key concepts or artifacts are required for SOC 3?

Key artifacts for SOC 3 include the description of the system in scope, the articulation of applicable Trust Services Criteria, and evidence showing control design and operational effectiveness. The final report summarizes the auditor's opinion without disclosing sensitive details.

How does an organization implement SOC 3?

Organizations implement SOC 3 by mapping their internal controls to the Trust Services Criteria, performing risk assessments, and establishing governance and monitoring processes. Preparation involves internal control evaluation, remediation of gaps, and engagement with a service auditor to perform the attestation.

How does SOC 3 relate to SOC 2 or other frameworks?

SOC 3 is based on the same Trust Services Criteria as SOC 2 but is intended for general public consumption and contains no detailed control testing results. Unlike SOC 2, which is shared only under NDA with customers, SOC 3 can be freely distributed and often complements broader compliance efforts such as ISO 27001.

What are the ongoing compliance requirements for maintaining SOC 3?

Organizations maintaining SOC 3 assurance must have continuous internal control monitoring, periodic risk assessment, robust governance, and timely remediation processes. Annual or regular engagement with a qualified service auditor is usually required to issue updated public reports.

How would SmartSuite support SOC 3?

SmartSuite supports SOC 3 by enabling organizations to import control libraries mapped to the Trust Services Criteria, manage risks with a centralized register, collect and store audit evidence, track remediation activities, and generate dashboards and reports for audit readiness. These features streamline control management and facilitate external assurance processes.

License included / downloadable: No SOC 3 reporting standards are published by the American Institute of Certified Public Accountants. Access to official guidance typically requires purchasing AICPA publications. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/soc-3-system-and-organization-controls-public-assurance-report