SOC 2 TRUST SERVICES CRITERIA.



A SOC 2 report is a CPA's attestation under AICPA standards, not a certification. Management draws the system boundary, picks the trust services categories and writes the description; the auditor opines on it against the 2017 Trust Services Criteria. **You define the system; the auditor tests what you claimed about it.**

OPINION, NOT CERTIFICATE | YOU DEFINE THE SYSTEM | 61 CRITERIA, 33 COMMON | TYPE 2 COVERS A PERIOD

01 THE MECHANISM

An Opinion, Not a Badge

A SOC 2 is an examination under the AICPA attestation standards (AT-C sections 105 and 205). The CPA expresses an opinion on management's description and controls against the trust services criteria. **Nothing is awarded; the deliverable is an opinion, not a certificate.** [02] [01]

You Draw the Boundary

Management defines the system: the infrastructure, software, people, procedures and data needed to provide a service, plus the commitments to customers and the system requirements behind them. It chooses which categories the report covers. **The auditor tests the system as described.** [02] [03]

Criteria, Not Controls

TSP section 100 sets 61 outcome-based criteria: 33 common criteria in nine series (CC1–CC9) plus category-specific series for availability, processing integrity, confidentiality and privacy. Points of focus illustrate each criterion, and **points of focus need not each be addressed**. [02]

02 THE FLOW

How a SOC 2 Is Built SCOPE

1. **Fix the system and the promises:** name the services, the system boundary and the principal service commitments and system requirements drawn from contracts, service levels and public statements. "To meet the entity's objectives" means meeting those commitments. [02] [03]
2. **Choose categories and report type:** security, availability, processing integrity, confidentiality and privacy may be reported alone or together; the common criteria apply to every category. A type 1 covers design as of a date; a type 2 covers design and operation over a period. [02]
3. **Describe, assert, examine:** management writes the description under the 2018 description criteria (revised 2022) and signs a written assertion; the service auditor examines both and reports. Subservice organizations are carved out or included, and the description says which. [03] [09]

How to Read One READ

1. **Start at the opinion, then the tests:** a type 2 report holds the description, management's assertion and the auditor's report, with the tests of controls and their results. Read the results, not just the opinion; a type 1 carries neither tests nor an operating-effectiveness opinion. [02]
2. **Find what was not tested:** under the carve-out method a subservice organization's controls sit outside the examination; the description names them and the controls the report assumes the customer operates. The opinion depends on those assumptions holding. [03]
3. **Check the period and the audience:** a type 2 opinion covers only the stated period, and a bridge letter after it is management's own statement, not an attestation. A SOC 2 is restricted to parties who understand the system; SOC 3 is the general-use report, freely distributed. [06] [02]

03 TRUST SERVICES CATEGORIES & CRITERIA

CATEGORY	WHAT IT COVERS
CC1–CC9	33 criteria in every report: COSO's 17 principles plus access, operations, change and risk mitigation (CC6–CC9).
Security	Protection against unauthorized access, disclosure and damage; the common criteria alone are the complete set.
Availability	Systems available for operation and use as promised; the A series adds capacity, backup and recovery-plan testing.
Processing	Processing integrity: processing that is complete, valid, accurate, timely and authorized; PI series, 5 criteria.
Confidential	Confidentiality: information designated confidential is protected until its final disposal; C series, 2 criteria.
Privacy	Personal information collected, used, retained, disclosed and disposed of as promised; P series, 18 criteria.

04 SOC REPORTS COMPARED

REPORT	TSC OPINION OVER A PERIOD?	WHAT IT MEANS
SOC 1 Type 2	No	Controls relevant to user entities' financial reporting (ICFR) under AT-C section 320, judged by control objectives, not the TSC.
SOC 2 Type 1	No	Description fairly presented and controls suitably designed as of a date; no opinion on operating effectiveness, no tests reported.
SOC 3	Yes	Opinion on design and operating effectiveness against the same criteria, without the detailed tests; general use, freely distributed.
SOC 2 Type 2	Yes	Description, management's assertion, and an opinion on design and operation over the period, with tests and results; restricted use.

SOC 2 TRUST SERVICES CRITERIA.

SCOPE · ATTEST · READ

05 PROGRAM OPERATIONS

Scope on purpose, in writing. Decide which services, systems and categories the report covers, and tie each commitment in contracts, service levels and public statements to a system requirement. A category is complete only when every criterion for it is addressed or shown not to apply. [02]

Operate for the whole period. A type 2 opinion covers design and operating effectiveness throughout the period, so controls must run and leave evidence all year, not just before fieldwork. Track owners, change tickets and access reviews so the tests find records, not reconstructions. [02] [09]

Manage what you carved out. Criterion CC9.2 has the entity assess and manage vendor and business partner risks, and management still monitors carved-out controls. Collect subservice reports, map their complementary controls to yours, and tell customers which controls they must operate. [02] [03]

Choose the auditor as carefully as the scope. SOC reports are CPA services under AICPA standards; the AICPA refers unlicensed firms to state boards and in May 2026 alerted peer reviewers to quick-turn, platform-driven SOC 2 work. Ask about licensure, peer review and timelines before signing. [01]

06 CONTROL MAPPING

COSO 2013 (17 PRINCIPLES)

The common criteria are aligned to the 17 principles of COSO's Internal Control—Integrated Framework, revised in 2013: CC1 to CC5 restate them as control environment, communication, risk assessment, monitoring and control activities. CC6 to CC9 supplement principle 12 with access, operations, change and risk mitigation. [02]

SSAE 18 & AT-C 205

Examinations run under AT-C sections 105 and 205, codified by SSAE No. 18 (effective for reports dated on or after May 1, 2017) and amended since; the AICPA's August 2026 compilation is current. SSAE No. 21 reporting requirements apply to service auditor reports dated on or after June 15, 2022. [08] [09] [02]

SOC 1 & SOC FOR CYBER

SOC 1 reports on controls relevant to user entities' internal control over financial reporting under AT-C section 320. SOC for Cybersecurity reports on an entity-wide cybersecurity risk management program for general users and may use the TSC for security, availability and confidentiality as control criteria. [05] [07] [02]

NIST CSF, ISO 27001, GDPR

The AICPA publishes spreadsheets that compare each framework's requirements to the relevant TSC categories, including NIST CSF (May 4, 2018), ISO 27001 and GDPR (October 7, 2020). A mapping shows where requirements overlap; it does not make a SOC 2 opinion an ISO 27001 certificate or a GDPR compliance finding. [10]

07 WHAT THIS DOES NOT SOLVE

Not a Certification

A CPA opines on a described system for a date or period. **No body certifies and nothing is awarded.** [02] [01]

Not a Fixed Checklist

Criteria are outcomes met with the entity's own controls, so **two clean reports can test different things**. [02]

Not the Whole Company

It covers the system management described; **carved-out subservice controls are outside the exam**. [03]

Not Public Proof

A SOC 2 is restricted to parties who know the system; **SOC 3 is the general-use version, with less detail**. [06]

08 MYTHS VS. REALITY

MYTH	REALITY
"We are SOC 2 certified."	There is no SOC 2 certification; a CPA issues **an attestation report with an opinion** against the criteria. [02] [01]
"A clean report means zero deviations."	A type 2 prints the tests and their results; **readers weigh deviations against the opinion**, not a pass mark. [02]
"Security is just one optional category."	The common criteria apply to all five categories, so **they are in scope whatever categories are chosen**. [02]
"A type 1 is a weaker type 2."	Different subjects: design as of a date versus operation over a period; **a type 1 has no opinion on operation**. [02]
"The 2027 criteria already apply."	A draft; comments close January 15, 2027; proposed for **engagements beginning on or after December 31, 2027**. [04]

09 SPEAK THE PROGRAM — KEY TERMS

TRUST SERVICES CRITERIA

TSP section 100; AICPA control criteria, **2017 edition with 2022 points of focus**.

POINTS OF FOCUS

Characteristics illustrating a criterion; **not a checklist, each need not be addressed**.

TYPE 1 / TYPE 2

Type 1 opines on design as of a date; **type 2 adds operating effectiveness over a period**.

CARVE-OUT METHOD

The subservice organization's controls are **excluded from the description and the exam**.

USER ENTITY CONTROLS

Complementary controls the report **assumes the customer operates** to meet the criteria.

BRIDGE LETTER

Management's own statement covering the gap after a report; **not a CPA attestation**.