SOC 1 REPORTS AND ICFR.



A SOC 1 is a CPA's examination under AT-C section 320 of controls at a service organization likely to be relevant to user entities' internal control over financial reporting. Written for those customers and their auditors, **it asks whether a vendor could misstate your books, not whether it is secure.**

ICFR, NOT SECURITY | MANAGEMENT SETS OBJECTIVES | FOR USER AUDITORS | RESTRICTED USE REPORT

01 THE MECHANISM

Financial Reporting Lens

SOC 1 covers controls at a service organization that are likely to be relevant to user entities' internal control over financial reporting. Payroll, custody and transaction processing are typical. **A failure that could not misstate a customer's books is outside SOC 1.** [01] [02]

Management Sets Objectives

Management, not a criteria list, sets the control objectives (or names the outside party that did) and designs the controls. The auditor judges whether the objectives are reasonable in the circumstances. **Two reports can carry different objectives for similar services.** [02] [04]

Restricted by Design

The report is intended solely for management of the service organization, user entities in the period and their auditors. Its criteria mean little to readers who do not know how the system feeds financial reporting. **It is evidence for an audit, not a public credential.** [02]

02 THE FLOW

How a SOC 1 Is Built SCOPE

1. **Draw the system and the objectives:** the description names the services and transactions, the period (or date, for a type 1), the control objectives and who set them, and the controls, including those assumed of user entities and of subservice organizations. [02] [04]
2. **Choose the type and the subservice method:** a type 1 covers design as of a date; a type 2 adds operation over a period. The carve-out method excludes a subservice organization's objectives and controls from the scope; the inclusive method brings them in. [02] [03]
3. **Assert, examine, opine:** management signs a written assertion. The service auditor checks the criteria against the minimums in AT-C 320, judges whether the objectives are reasonable, tests the controls and opines under the AICPA attestation standards. [02] [07]

How a User Auditor Reads It RELY

1. **Match the period and the services:** AU-C 402 has the user auditor confirm that the type 2 period fits the audit, that its tests speak to the user entity's assertions, and how much time has passed since the tests. A type 1 is as of a date and proves nothing about operation. [05]
2. **Read the tests, not just the opinion:** the report identifies the controls tested, whether all items or a selection were examined, the nature of the tests, and every deviation with the number of items tested, even when the control objective was achieved. [02] [05]
3. **Operate your side of the design:** complementary user entity controls are assumed in the design as necessary to the objectives, and the service auditor has not evaluated them. Carved-out subservice controls are outside too; ask that organization for its own report. [02] [03]

03 PARTS OF A SOC 1 TYPE 2 REPORT

COMPONENT	WHAT IT CONTAINS
Description	Management's account of the system: services, period, control objectives and who set them, controls, CUECs.
Assertion	Management's written statement that the description is fair and the controls were designed and operated well.
Opinion	The independent service auditor's report under AICPA attestation standards on all three matters, with limits.
Tests	Each control tested, whether all items or a selection, the nature of the test, deviations and item counts.
CUECs	A statement that the auditor did not evaluate user entity controls and that objectives depend on them working.
Use Alert	A separate paragraph: solely for service organization management, user entities and their auditors.

04 SERVICE ORGANIZATION REPORTS COMPARED

REPORT	ICFR CONTROL OBJECTIVES?	WHAT IT MEANS
SOC 2 Type 2	No	An opinion on a system against the trust services criteria, covered in the SOC 2 brief; use restricted to parties who know the system.
SOC 1 Type 1	Yes	The description fairly presents the system and controls are suitably designed as of a date; no tests and no opinion on operation.
ISAE 3402 Type 2	Yes	The IAASB standard on the same subject matter, for user entities and their auditors under the ISAs; design and operation over a period.
SOC 1 Type 2	Yes	Description, assertion, opinion on design and operation over the period, plus the tests and results; restricted to specified parties.

SOC 1 REPORTS AND ICFR.

SCOPE · ATTEST · RELY

05 PROGRAM OPERATIONS

Write objectives a user auditor can use. Tie each control objective to assertions common in user entities' financial statements, such as existence and accuracy, which access controls protect, and keep the set complete. An outside party that sets objectives owns their completeness. [02]

Keep the boundary honest. The description covers only what is likely to matter to user entities' financial reporting; controls over the service organization's own financial statements stay out. Name each subservice organization, the method used and the user entity controls assumed. [02] [04]

Run controls all period and record changes. A type 2 assertion covers operation throughout the specified period, and prior-year evidence does not cut this year's testing. Significant changes belong in the description, and superseded controls are tested before the change where possible. [02]

Send the right report to the right reader. The alert restricts use and the service auditor does not police distribution, so the service organization must. Prospects, procurement and security questionnaires are not specified parties; offer SOC 2 or SOC 3 there. [02] [07]

06 CONTROL MAPPING

AU-C 402 (USER AUDITOR)

The auditing standard for audits of entities that use a service organization, effective for periods ending on or after December 15, 2012. It lets a type 2 report serve as evidence that controls operated and has the user auditor weigh its period, tests and complementary user entity controls. [05]

ICFR (17 CFR 240.13A-15)

The SEC definition: a process under the principal executive and financial officers that gives reasonable assurance about reliable financial reporting, covering records, authorizations and safeguarding of assets. An issuer's management evaluates it yearly against a recognized framework. [09]

ISAE 3402 (IAASB)

Released December 18, 2009 and effective for service auditors' reports covering periods ending on or after June 15, 2011. It reports on the description, design and operating effectiveness of controls at a service organization for user entities and their auditors under the ISAs. [08]

SSAE 18 & SSAE 23

AT-C section 320 comes from SSAE No. 18 (service auditors' reports dated on or after May 1, 2017), which recodified AT section 801; AT-C 105 and 205 also apply. SSAE No. 23 aligns the standards with quality management for engagements beginning on or after December 15, 2025. [02] [06]

07 WHAT THIS DOES NOT SOLVE

Not a Security Report

Scope is controls relevant to financial reporting; **security counts only where it threatens an objective**. [02]

Not Other Subjects

Controls over compliance, production or quality, not financial reporting, **fall under AT-C 205, not 320**. [02]

Not General Use

The alert names management, user entities and their auditors; **it is not a credential for prospects**. [02]

Not the Whole Chain

Carved-out subservice controls and user entity controls **sit outside the service auditor's procedures**. [02]

08 MYTHS VS. REALITY

MYTH	REALITY
"A SOC 1 proves our vendor is secure."	It reports on controls relevant to financial reporting; **security matters only where an objective needs it**. [02]
"SOC 1 and SOC 2 are interchangeable."	Different subject matter, criteria and readers: **SOC 1 serves user entities and their auditors on ICFR**. [01]
"A clean opinion means no exceptions were found."	A type 2 lists every deviation with the number of items tested, **even when the objective was achieved**. [02]
"It covers the vendor's own vendors too."	The carve-out method **excludes a subservice organization's objectives and controls** from the scope. [02]
"Anyone who asks can rely on it."	Solely for management, user entities in the period and their auditors; **SOC 3 is the general-use report**. [02] [01]

09 SPEAK THE PROGRAM — KEY TERMS

USER ENTITY

An entity using a service organization whose controls are **likely relevant to its ICFR**.

USER AUDITOR

The auditor of a user entity's financial statements; **the report's primary reader**.

CONTROL OBJECTIVE

The aim or purpose of specified controls; **they address the risks controls mitigate**.

COMPLEMENTARY CONTROLS

Controls the design assumes **user entities (CUECs) or subservice organizations** will run.

SUBSERVICE ORGANIZATION

A service organization another one uses for services **relevant to user entities' ICFR**.

INCLUSIVE METHOD

The description and the exam **include the subservice organization's controls**.