SOC Reporting Guide

Choose the right report and prepare for the work

Reviewed October 31, 2026

A customer has asked for a SOC report. Before buying software or requesting an audit quote, find out what they need to rely on: which service, which risks, which report, and by when. Those answers shape the work and help avoid paying for a report that misses the point.

This guide explains the choices and the practical steps toward an audit. The actual engagement scope and reporting decisions belong in a conversation with your CPA firm.

Start with the report your customer needs

Report	What it addresses	Where it fits
SOC 1	Controls relevant to customers' internal control over financial reporting.	A service can affect a customer's financial reporting, such as processing payroll. Ask which processes and control objectives matter.
SOC 2	Controls relevant to selected Trust Services Criteria categories: Security, Availability, Processing Integrity, Confidentiality and Privacy.	A customer needs detailed assurance about the system delivering your service. Agree the system boundary and relevant categories.
SOC 3	A general-use report on controls relevant to Trust Services Criteria, with less detail than a SOC 2 report.	You need a report that can be freely distributed. Confirm it will satisfy the customer's request; it does not provide the detailed control tests found in a SOC 2 Type 2 report.

SOC 1 and SOC 2 reports are intended for specified users who can understand their scope and limitations. They are not interchangeable. Some organizations need both because they serve different customer needs. SOC 3 is not a higher level of SOC 2.

For SOC 1 and SOC 2, Type 1 addresses management's description of the system and whether controls are suitably designed as of a specified date. Type 2 also addresses whether controls operated effectively over a specified period and includes the auditor's tests and results. If a customer needs evidence of operation over time, check whether a Type 1 report would actually meet the request.

A question worth asking: "Will this specific report, for this service and period, meet your requirement?" Get the answer before promising a delivery date. Preparation, the reporting period and the auditor's work each take time; there is no single duration that fits every engagement.

Define what is actually being audited

A product name alone is not a system boundary. Write a short scope brief that your team, customer and auditor can discuss:

- **The service and its commitments.** What do customers receive, and what have you promised about it?
- **The people and technology behind it.** Include hosting, applications, APIs, data flows, support access and shared services that matter to the system.
- **Outside dependencies.** Which cloud or other providers help deliver the service? Identify responsibilities you retain and what you expect customers to do.
- **The reporting need.** Record the requested report and type, proposed categories or objectives, customer deadline and intended users.
- **Changes and unknowns.** Flag a migration, new product, missing records or unresolved scope question before quotes are finalized.

For SOC 2, categories group the underlying criteria. Criteria are the benchmarks against which controls are evaluated; controls are the actual policies and activities your organization uses. Selecting a category does not hand you a universal list of products to buy or control frequencies to adopt.

Devil's advocate: "Our cloud provider has a SOC report, so we're covered." Their report can support your assessment of their services. It does not automatically cover your own access decisions, application changes or other responsibilities. Check the report's scope and relevant customer responsibilities.

Give the work clear owners

- **Management** defines and operates controls, owns the system description and assertions, and provides complete, accurate supporting information.
- **The independent, licensed CPA firm** performs the examination and issues the SOC report. Discuss readiness support and independence before assuming your auditor can also design or run the program.
- **An advisor** can help with scope, gaps and preparation. Agree the deliverables and who remains accountable internally.
- **Software** can organize work and collect evidence. A green dashboard does not establish that a control operated effectively, and a platform cannot guarantee the auditor's opinion.

Keep evidence tied to what happened

A policy tells someone what should happen. Evidence helps show what did happen. Start with a small register: the control, accountable owner, when it operates, expected evidence, where that evidence is kept, and any open issue. Use the existing editable readiness checklist to organize the work, rather than creating a second competing tracker.

For recurring or event-driven activities, preserve the relevant population and the record of performance. The auditor determines the testing approach; collecting a few convenient screenshots is not a substitute for complete information.

A simple example

Illustrative only: A company reviews access to its customer application under its own approved review schedule. The owner exports the relevant users and permissions, records how the list was checked for completeness, and sends it to an authorized reviewer. The reviewer documents decisions. One unnecessary administrator account is removed, and the team retains the removal record and closeout.

The useful evidence is the connected story: population, review, decision and correction. A screenshot saying "review complete" would leave much of that story unanswered. The appropriate schedule and testing depend on the control and engagement; this example does not establish a required frequency.

Deal with gaps before they become surprises

1. Record what is missing or did not operate as intended, the affected system and period, and the potential impact.
2. Assign an owner and a realistic correction date. Keep the original evidence and the explanation; do not backdate records or silently replace history.
3. Retain proof of the correction and any follow-up check. Explain remaining limitations to the auditor.
4. Discuss the reporting implications. An exception does not automatically mean a particular opinion. The auditor evaluates the facts and their significance; SOC reporting is not a simple pass-or-fail certificate.

The same discipline applies to technical testing. Decide which systems and risks the testing needs to address, what was actually covered, and how findings were resolved. A scan, penetration test or red-team exercise serves a different purpose. Do not buy one solely because its name appears on a generic audit checklist.

Take the next step

Before requesting quotes: send the scope brief, requested report and type, proposed timing, known gaps and major dependencies. Ask firms to explain what is included, who does what, and what could change the cost or schedule.

Before fieldwork: confirm that owners can explain the controls, retrieve supporting records and account for exceptions. Reconcile your tracker to the systems and processes actually in scope.

Use the editable SOC readiness checklist:

Open the editable readiness checklist

For help with your next step:

Contact SSAE-16.com

Sources and scope

AICPA primary resources support the report definitions and distinctions in this guide. The workflow and worked example are practical guidance, not a prescribed control set or a substitute for engagement-specific advice.

1. AICPA SOC suite of services

2. AICPA SOC 1 overview

3. AICPA SOC 3 overview

4. AICPA 2017 Trust Services Criteria with revised points of focus 2022

5. AICPA SOC 2 report review checklist

6. AICPA FAQs about SOC 2 tools