SOC 2 Readiness: a practical navigation guide

What SOC 2 actually asks of you, how to scope it without boiling the ocean, and the evidence you need to walk into an audit with confidence.

SOC 2 · Updated 2026-08-22 · 12 min read

What SOC 2 is (and is not)

SOC 2 is an attestation report produced by an independent CPA firm on how your organization manages customer data against the AICPA Trust Services Criteria. It is not a certification and there is no pass/fail badge — the deliverable is an auditor's opinion plus a description of your controls and how they operated.

- Type I describes your controls at a point in time (design).
- Type II tests that those controls operated effectively over a period — typically 3 to 12 months.
- Buyers almost always want Type II; a Type I is a reasonable first milestone on the way there.

> **THE ONE-LINE VERSION**
> SOC 2 is you writing down the security promises you make to customers, then proving — with evidence over time — that you actually keep them.

The five Trust Services Criteria

Every SOC 2 includes Security (the Common Criteria). The other four are optional and chosen based on the promises you make to customers.

- Security — protection against unauthorized access (always in scope).
- Availability — the system is up and usable per commitments (SLAs, uptime).
- Confidentiality — information designated confidential is protected.
- Processing Integrity — processing is complete, valid, accurate, and timely.
- Privacy — personal information is collected, used, and disposed of per your notice.

Most first reports scope Security + Availability + Confidentiality. Add Privacy or Processing Integrity only when a real customer commitment or contract requires it.

Scoping without boiling the ocean

Scope is the single biggest driver of cost and pain. Define the system: the product(s), the infrastructure and cloud accounts that run them, the people with access, and the vendors in the data path.

1. Name the product(s) and environments in scope (prod only, to start).
2. Inventory the cloud accounts, repos, and data stores that support them.
3. List the subservice organizations (e.g., AWS, GCP) you rely on — most are 'carved out'.
4. Decide the criteria (Security + the ones you actually commit to).
5. Pick your observation window for Type II (a 3-month window is common for a first report).

> Anything you leave out of scope you must be able to defend as genuinely separate. When in doubt, keep the boundary tight and honest rather than broad and aspirational.

Evidence is the whole game

A control you cannot evidence does not exist as far as the auditor is concerned. For Type II you need artifacts that show the control operated throughout the window, not just on the day you remembered.

- Access reviews with dates, reviewers, and remediation tickets.
- Change management: PRs, approvals, and CI/CD logs tying deploys to reviews.
- Onboarding/offboarding tickets proving access was granted and revoked on time.
- Vulnerability scans, patch records, and endpoint/MDM compliance reports.
- Backup and restore tests, incident records, and vendor due-diligence files.

Automate collection where you can. Manual screenshots the week before the audit are how observation windows get extended.

Common pitfalls

- Over-scoping criteria you do not actually commit to — every extra criterion is more evidence forever.
- Policies that describe an aspirational company, not the one that exists — auditors test reality.
- No owner for evidence collection, so it becomes a fire drill at window's end.
- Treating the report as the finish line instead of the operating baseline it renews annually.

The path to your report

1. Readiness assessment — map current controls to the criteria and find the gaps.
2. Remediate — write the missing policies, turn on the missing controls, assign owners.
3. Select an auditor and (optionally) a compliance automation platform.
4. Open the observation window and let controls run — collect evidence continuously.
5. Audit fieldwork — the auditor tests samples across the window.
6. Receive the report — then keep operating; renewal is continuous, not a redo.

> **WHERE INTSIGNAL FITS**
>
> We run the operational controls behind most of this — identity and access reviews, endpoint and patch compliance, logging and monitoring, backup testing, and evidence collection — so your window produces artifacts by default instead of by scramble.