FREE GUIDE

Your First 5 SOC 2 Moves

Five plain-English moves to get audit-ready — before you spend twenty thousand dollars on a platform, a consultant, and an audit.

A customer asks for your SOC 2 report and suddenly it's a fire drill. It doesn't have to be. SOC 2 is a security audit against a set of common-sense criteria — and most of the early work is things a small team can do itself. These five moves get you going in the right direction without the panic.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

Move 1 — Understand what SOC 2 actually is

What it is

SOC 2 (System and Organization Controls 2) is an independent report on how well your controls meet a set of Trust Services Criteria (TSC) — security first, and optionally availability, confidentiality, processing integrity, and privacy.

Why it's first

Teams panic because they picture a mysterious exam. It's not. It's an auditor checking that you do the sensible security things, consistently, and can show it. Knowing that reframes everything that follows.

Do this

Learn the basics: Type I (your controls at a point in time) versus Type II (that they worked over a period, usually three to twelve months). Most customers want Type II — so plan for an observation window.

Move 2 — Scope it before you build anything

What it is

Deciding which Trust Services Criteria you'll include and which systems and data are in scope.

Why it matters

Scope decides how much work the audit is. Too broad and you've signed up for months of needless effort; too narrow and the report won't satisfy your customers.

Do this

Start with the Security criteria (required) and add others only if customers ask. Draw a simple boundary: which product, which systems, which data. Write it down — it's the backbone of the whole project.

Move 3 — Turn on the controls auditors always check

What it is

The handful of basic safeguards that show up in nearly every SOC 2.

Why it matters

A few controls account for most early findings. Turning them on now removes the most common gaps before an auditor ever looks.

Do this

Turn on two-step login (multi-factor authentication, or MFA) everywhere, run access reviews, encrypt data in transit and at rest, enable logging, and require code review and background-checked onboarding. None of these need a platform to start.

Move 4 — Write the handful of policies you'll be asked for

What it is

The short set of written policies auditors expect to see.

Why it matters

SOC 2 is partly "say what you do, then do what you say." Auditors will ask for written policies — and a customer's security reviewer often will too.

Do this

Draft the core set: information security, access control, change management, incident response, vendor management, and business continuity. Keep them short and true to what you actually do — a policy you don't follow is worse than none.

Move 5 — Start collecting evidence now, not the week before

What it is

Quietly keeping the records that show your controls are working.

Why it matters

A Type II audit looks back over months. If you start collecting evidence the week before, you can't recreate the past — so the audit slips. Starting early is the single biggest time-saver.

Do this

Begin saving the proof now: access-review records, onboarding and offboarding tickets, change approvals, incident notes. Pick where it lives and keep it current — your future self will thank you.

Where to go from here

The free SOC 2 readiness check shows where you stand in a few minutes, and it runs entirely in your browser, so we never see your answers: sylvanassurance.com/free/soc2/

When you're ready to turn that into a full readiness plan with the policies, evidence trackers, and templates, the SOC 2 toolkit lays it out: sylvanassurance.com/soc2-readiness

Scan for the free assessment that goes with this guide.
sylvanassurance.com/go/free-soc2-readiness