CybrGen

CYBERSECURITY & TRUST ADVISORY

SOC 2 Type I Readiness Guide

A practitioner's guide to getting audit-ready — what SOC 2 actually asks of you, where teams stall, and how we get you to a Type I report.

START HERE

Trust you can evidence — not just claim.

SOC 2 has become the price of entry for selling software to the enterprise. This guide is the practitioner's version: what the framework genuinely requires, the difference between Type I and Type II, and the readiness path that gets you to a clean report without months of thrash.

Who this is for

- **SaaS and platform teams** losing or stalling enterprise deals because they can't show a SOC 2 report.
- **Fintech and regulated suppliers** who need to prove control maturity to customers and partners.
- **Founders and engineering leads** who want a clear, time-boxed path rather than an open-ended compliance project.

What's inside

- SOC 2 in brief, and the Type I vs Type II distinction that decides your timeline.
- The five Trust Services Criteria and how to scope them.
- A five-phase readiness journey and an "are you audit-ready?" checklist.
- Where readiness most often stalls — and how we run it to a guaranteed Type I outcome.

THE ESSENTIALS

SOC 2, and why the report type matters.

SOC 2 is an attestation against the AICPA's **Trust Services Criteria**. The report is always issued by an **independent licensed CPA firm** — not by your advisor and not by you. Readiness is the work of designing, implementing and evidencing the controls so that audit goes smoothly. Those are two distinct roles, and keeping them separate is what keeps the report credible.

Type I `point in time`

An opinion that your controls are **suitably designed and implemented** as at a specific date. It tests design and existence — not how the controls have performed over time.

Type II `over a period`

An opinion that your controls **operated effectively** across a window (commonly 3–12 months). It depends on you running the controls consistently, day after day.

WHY THIS DISTINCTION IS THE WHOLE GAME

Type I is about design and implementation — things a competent team can get right and prove at a point in time. Type II is about **operating discipline sustained over months**. Most teams clear Type I and then drift before Type II because nobody owns the day-to-day. Knowing which report you're pursuing — and what it demands of you — is the first real decision.

SCOPE

The five Trust Services Criteria.

You don't have to be assessed against all five. **Security is mandatory**; the rest are included only if they're relevant to what you promise customers. Scoping tightly is the single biggest lever on cost and timeline.

REQUIRED

Security (Common Criteria)

Protection of systems and data against unauthorised access. The mandatory baseline every SOC 2 covers.

OPTIONAL · IF RELEVANT

Availability

Systems are available for operation and use as committed — uptime, resilience, disaster recovery.

OPTIONAL · IF RELEVANT

Confidentiality

Information designated as confidential is protected as committed — relevant for sensitive customer data.

OPTIONAL · IF RELEVANT

Processing Integrity

System processing is complete, valid, accurate and timely — relevant where you process transactions for others.

OPTIONAL · IF RELEVANT

Privacy

Personal information is collected, used, retained and disposed of as committed and per applicable law.

THE PATH

From zero to Type I — in five phases.

A structured readiness program is built for speed without cutting corners. Each phase has defined deliverables, so you always know where you stand.

PHASE 01 · WEEK 1–2

Scoping & gap assessment

Define the SOC 2 scope and boundary, select the relevant criteria, and identify gaps against the Trust Service Criteria. You leave with a readiness roadmap.

PHASE 02 · WEEK 2–5

Control design & policy build

Design controls to meet the criteria, draft the policies, and define the evidence each control will produce.

PHASE 03 · WEEK 5–10

Evidence collection & testing

Implement controls, configure evidence workflows, validate that everything operates as designed, and assemble the audit package.

PHASE 04 · WEEK 10–12

CPA audit & fieldwork

Coordinate with the independent CPA firm, manage fieldwork and respond to requests through to a clean Type I report.

PHASE 05 · ONGOING

Operate & sustain

Keep controls running for the Type II window. This is where most teams need a system of record — not a spreadsheet.

SELF-ASSESSMENT

Are you audit-ready?

If you can tick most of these honestly, you're close. If not, that's exactly what a gap assessment surfaces.

- ✓ **Scope and boundary defined** — systems in scope and criteria selected.
- ✓ **Risk assessment completed** — documented and current.
- ✓ **Policies documented and approved** — and actually reflect how you operate.
- ✓ **Controls implemented and mapped** — each control traced to a criterion.
- ✓ **Access, change and vendor management** — running, with evidence.
- ✓ **Evidence centralised** — collected and retained, not scattered across tools.
- ✓ **System description drafted** — your services, boundaries and controls in writing.
- ✓ **Independent CPA firm engaged** — chosen early, not at the last minute.

FROM THE FIELD

Where readiness stalls.

The same handful of mistakes cost teams weeks. Most are avoidable with the right sequencing.

- **Treating it as a document exercise.** Policies without implemented controls fail at fieldwork. The controls have to exist and operate, not just be written down.
- **Scoping too broadly.** Pulling in optional criteria you don't need multiplies effort and cost for no commercial gain.
- **Scattered evidence.** If evidence lives across a dozen tools with no system of record, you'll scramble at audit and risk gaps.
- **Engaging the auditor too late.** The CPA's scope and timing shape your plan; involve them early.
- **Confusing Type I readiness with Type II sustainment.** Passing Type I is a point in time; Type II is won by operating the controls every day for months.

HOW CYBRGEN RUNS IT

Senior-led readiness, with a Type I you can count on.

We design and implement your controls and prepare your evidence — practitioner-led, not handed to juniors — and work alongside an independent CPA firm for the attestation. Because design and implementation are within our control, we stand behind the Type I outcome.

TYPE I SUCCESS GUARANTEE

When we scope and run the readiness program together and your controls are **implemented as designed**, we stand behind the outcome: if the Type I audit doesn't return an unqualified opinion, **we keep working at no additional advisory cost until it does.** The CPA's opinion remains entirely independent.

TYPE II, SUSTAINED

MyTrustForge keeps evidence and control posture live, so the controls keep operating after we leave — the hard part of Type II.

BEYOND SOC 2

One control model maps across ISO 27001, ISO 42001 and 30+ frameworks — answer once, satisfy many.

WHO YOU WORK WITH

Senior practitioners with Big 4 backgrounds across PwC, Deloitte and KPMG.

Book a free gap assessment.

Leave with a clear, scoped path to Type I — built around your current maturity.

cybrgen.nz → Book a gap assessment