Comp AI

SOC 2
READINESS

The 13-Point SOC 2 Readiness Check

What to sort out before you talk to any vendor, including us.

Most SOC 2 checklists run thirty pages and end in a demo request. This is the short version: the decisions and conditions no platform can make on your behalf. Deliberately absent are policy drafting, evidence collection, and control monitoring, because any modern platform should do that work for you. What follows is the part that stays yours.

01
Scope

Four decisions. No tool can make them for you.

- [ ] **Type I or Type II?** Type I tests whether controls are designed properly at a single moment. Type II tests whether they actually ran over an observation window, typically 3 to 12 months. Most enterprise buyers want Type II, so check the contract before you choose.
- [ ] **Which Trust Services Criteria are in scope?** Security is mandatory. Availability, Confidentiality, Processing Integrity, and Privacy are optional. Add one only if a customer contract names it. Each extra criterion widens the audit and the bill.
- [ ] **Where is your system boundary?** Which products, environments, and subprocessors are included. Vagueness here is the most common source of scope creep once the audit is underway.
- [ ] **What is the real deadline?** Usually a specific deal. Work backwards: for Type II, the observation window has to close before a report can be issued, so the deadline sets your start date, not the other way around.

02
Your organization

Facts that must be true before automation has anything to work with.

- [ ] **Someone owns this.** A named person with authority to approve policies and make scoping calls. Compliance without an owner stalls no matter how good the tooling is.
- [ ] **An HR system of record.** Who works here, when they started, when they left. Nearly every access control traces back to it, so if it is wrong, the evidence built on top of it is wrong.
- [ ] **A real list of subprocessors.** Every vendor touching customer data, and what data each one sees. Integrations discover most of this, but only you know the handshake deals and the one-off contractors.
- [ ] **An incident response plan you have rehearsed.** Generating the plan is easy. Running a tabletop exercise against it is the part that has to involve actual humans, and the part auditors ask about.

03
Your systems

Configuration in your own stack. A platform can prove these, not create them.

- [ ] **MFA enforced everywhere.** Cloud consoles and admin accounts especially. One standing exception can become a finding.
- [ ] **Access granted and revoked promptly.** Continuous monitoring will evidence this automatically, but only if it is genuinely happening. Automation surfaces the gap, it does not close it.
- [ ] **Company devices locked down.** Disk encryption, screen lock, and antivirus actually enabled on every machine.
- [ ] **Change management in your repo.** Pull request reviews, approvals, and branch protection turned on.
- [ ] **Logging, monitoring, and backups running.** With at least one restore you have actually tested. A backup nobody has restored is not evidence of anything.

04

What it costs and what you get

The traditional vendor stack, compared.

	TRADITIONAL VENDORS	COMP AI
Cost, year one (all in)	$32,000 – $70,000	**$9,000 – $30,000+**
What the price covers	Platform, CPA audit, and pentest quoted, contracted, and renewed separately	One flat fee covering platform, CPA audit, and pentest. No hidden line items
How the price is set	Per line item, often after several calls. Support hours billed on top	By the frameworks you need and your headcount
Time to audit-ready	3 to 6 months+	**10 days on average**
Your team's time	400 to 600 hours	**Under 10 hours**
How the work gets done	Manual evidence collection: screenshots, spreadsheets, chasing people	AI-native. Agents pull evidence continuously from 580+ integrations
Support	Ticket queues and email chains	1:1 Slack with in-house compliance experts who walk you through each step

Traditional figures are 2026 market rates for assembling the pieces yourself. Use them to pressure-test any proposal you receive, ours included.

05

Three things that stall audits

Consistently, and expensively.

Starting the observation window too early. If a control was not actually running on day one, the clock effectively restarts. Get controls live and generating evidence before you open the window.

Policies nobody has read. Auditors sample acknowledgments. A complete policy set with three signatures against it is worse than a smaller set everyone has signed.

Missing offboarding evidence. A former employee with live access is the single most common finding, and one of the few that is genuinely hard to remediate after the fact.

QUESTIONS

Happy to be a resource, customer or not. katya@trycomp.ai