Agency

THE STARTUP COMPLIANCE SERIES · CHECKLIST

SOC 2

The startup

SOC 2 Readiness Checklist

Everything you need in place before your first audit — in one place you can actually use.

A practical companion checklist for founders & engineering leaders

© Agency Cyber Inc. 2026

June 22, 2026 • getagency.com

SOC 2 · READINESS CHECKLIST

How to use this checklist

This is the short, high-level version of what auditors look for — organized the way you'll actually tackle it. It won't replace a readiness assessment, but it will tell you, in about ten minutes, roughly how ready you are and where the gaps are.

Score yourself honestly as you go: ■ done · ◪ partial · ☐ not started. If you finish with a lot of ◪ and ☐, that's normal for a first-timer — it just tells you how much work is ahead and which path makes sense for getting it done.

> **A quick reminder before you start:** A checklist tells you *what* needs to be true. It doesn't do the work of *making* it true — writing the policy, configuring the control, fixing what's failing, or proving it to an auditor. Keep that gap in mind as you tally your score.

---

1. Scope & foundations

Get these decisions right first — they shape everything else.

- ◇ Decided **Type I vs. Type II** for your first report
- ◇ Confirmed which **Trust Services Criteria** apply (almost always **Security** to start; add Availability, Confidentiality, Processing Integrity, or Privacy only if a customer requires it)
- ◇ Defined the **systems and data in scope** (which products, environments, and data stores the report covers)
- ◇ Identified your **observation window** and target report date
- ◇ Named a clear **owner** for the program with the time and authority to drive it

2. Security policies

Auditors expect written policies that match how you actually operate — not generic templates nobody follows.

- ◇ Information Security Policy
- ◇ Acceptable Use Policy
- ◇ Access Control Policy
- ◇ Change Management / SDLC Policy
- ◇ Risk Assessment & Management Policy
- ◇ Incident Response Policy

- Business Continuity & Disaster Recovery Policy
- Vendor / Third-Party Risk Policy
- Data Classification & Retention Policy
- Policies **reviewed, approved, and acknowledged** by employees

3. Access & identity

Who can get to what — the most heavily tested area.

- **Single sign-on (SSO)** in place for critical systems
- **Multi-factor authentication (MFA)** enforced across the board
- **Role-based access** following least privilege
- Documented **onboarding** (granting access) and **offboarding** (revoking it promptly)
- **Periodic access reviews** performed and recorded
- Strong **password / credential** standards enforced

4. Infrastructure & cloud security

The technical backbone of your controls.

- **Encryption** in transit and at rest
- **Firewalls / network controls** and sensible segmentation
- **Endpoint protection** on company devices (incl. laptops)
- **Vulnerability scanning** and a patching cadence
- **Backups** configured, running, and periodically tested
- **Infrastructure access** restricted, logged, and monitored

5. Monitoring & logging

You can't prove what you don't capture.

- **Centralized logging** for key systems
- **Security monitoring / alerting** for suspicious activity
- Defined process to **triage and respond** to alerts
- **Audit trails** retained for the observation window

6. Change management & development

Showing that changes to production are controlled.

- **Version control** for code
- **Code review / approval** before merging
- **Separate environments** (dev / staging / prod)
- **CI/CD with controls** on who can deploy
- Production **changes are tracked** and documented

7. Vendor & third-party risk

Your auditor will ask about the companies you rely on.

- **Inventory of vendors / subprocessors** that touch your data
- Collected and reviewed **vendors' security reports** (e.g., their SOC 2)
- **Risk-ranked** vendors by sensitivity of access
- **Data Processing Agreements** in place where needed

8. People & HR security

The human side of security.

- **Background checks** for employees where appropriate
- **Security awareness training** at onboarding and annually
- **Confidentiality / IP agreements** signed
- Documented, repeatable **onboarding and offboarding** procedures

9. Risk assessment

- Conducted a **formal risk assessment**
- Maintain a **risk register** with owners and treatment plans
- Risks **reviewed on a regular cadence**

10. Incident response & resilience

- **Incident response plan** documented with clear roles
- Team knows **how to report and escalate** an incident
- **Business continuity / disaster recovery** plan documented

- Plans **tested** (e.g., a tabletop exercise)

11. Evidence & audit prep

Where good operations turn into an audit-ready report.

- Evidence is **collected continuously**, not reconstructed at the deadline
- Controls **mapped** to the criteria you're being audited against
- **System description** prepared (how your environment works)
- Engaged an **independent audit firm** and aligned on timeline
- A clear **owner** for auditor requests and follow-ups

Now the real question: who's going to do all this?

If you scored mostly ☐ and ◪, don't panic — that's the normal starting point. The harder question isn't *what's on the list*; it's *who does the work*. There are three common answers:

Do it yourself with spreadsheets. Workable for very early, technical teams with time to spare — but evidence collection is manual and easy to let slip, and the cost shows up in founder and engineer hours.

Buy a GRC platform like Vanta or Drata and run it yourself. A big step up: these tools connect to your stack and automate evidence collection and monitoring. Just remember a platform surfaces the work and tracks your status — it doesn't write your policies, remediate failing controls, or face the auditor for you. It assumes a capable operator in-house.

Have it operated for you. A dedicated team runs the program end to end — usually on top of a platform like Vanta or Drata — so your engineers stay on the roadmap and the report gets done right the first time.

(For a deeper breakdown of these three paths and how to choose, see our companion piece, The Startup's Guide to Buying SOC 2.)

Where Agency fits

This checklist comes from **Agency** — a security and compliance team you don't have to hire. U.S.-based forward-deployed engineers, supercharged by our own AI, run your SOC 2 end to end on top of the tools you already trust like **Vanta** and **Drata**: virtual CISO, control implementation, evidence collection, continuous monitoring, vendor risk, and audit coordination, all included without adding headcount. Agency has served more than 1,000 companies and is backed by Y Combinator.

Want us to turn this checklist into an audit-ready SOC 2 program?

Get a free readiness review — we'll tell you where you stand and the fastest path to done.

Assemble your GRC team ›

This checklist is for general educational purposes and isn't legal, audit, or compliance advice. Your specific requirements depend on your business, systems, and customer commitments.