ZAPLIO.IO

SOC 2 Type 2 Audit Preparation Checklist

A practical, phase-by-phase readiness checklist for IT and compliance teams preparing for their first or next SOC 2 Type 2 audit.

Most SOC 2 Type 2 audits do not fail in the auditor's conference room. They fail months earlier, when evidence collection is treated as something to sort out after the engagement letter is signed. A Type 2 report tests whether your controls operated effectively over an observation period of three to twelve months, not whether they exist on paper. Use this checklist to work through the five phases that separate a clean first-time pass from a qualified report and a re-test.

PHASE 1 Scoping & Trust Service Criteria Selection

- [ ] Confirm Security is in scope (mandatory for every SOC 2 audit)
- [ ] Review the last 3 enterprise contracts and security questionnaires to determine real customer requirements
- [ ] Decide whether Availability, Confidentiality, Processing Integrity, or Privacy are contractually required
- [ ] Avoid adding optional criteria your customers have not asked for
- [ ] Document final scope and get sign-off from leadership before proceeding

PHASE 2 Policy & Control Documentation

- [ ] Information Security Policy drafted, reviewed, and formally approved
- [ ] Access control policy defined (provisioning, deprovisioning, least privilege, MFA)
- [ ] Change management policy with documented approval workflow
- [ ] Incident response plan written and assigned an owner
- [ ] Vendor risk management policy covering third-party and subprocessor review
- [ ] Data classification policy distinguishing sensitive from non-sensitive data
- [ ] Confirm each policy maps to an operating control, not just a written statement

PHASE 3 Evidence Collection Setup

- [ ] Select and deploy a compliance automation platform for continuous evidence collection
- [ ] Map each control to its corresponding evidence source (logs, tickets, screenshots, exports)
- [ ] Set up automated alerts for control failures or missed evidence windows
- [ ] Assign an evidence owner for every control category
- [ ] Run a test collection cycle before the observation period begins

PHASE 4 The Observation Period

- [ ] Confirm observation period start date and required duration (3 to 12 months)
- [ ] Monitor evidence collection weekly for gaps or missed entries
- [ ] Document any control failures along with remediation steps taken
- [ ] Run an internal mid-period readiness check at the halfway mark
- [ ] Address any flagged gaps before fieldwork begins, not during it

PHASE 5 Auditor Fieldwork & Report Delivery

- [ ] Select a CPA firm with SOC 2 experience in your industry (specialist firm vs Big Four)
- [ ] Prepare control owners for auditor interviews
- [ ] Organize evidence repository for easy auditor access and sampling
- [ ] Review draft findings before the final report is issued
- [ ] Plan for annual renewal: identify what can be reused and what needs updating

Audit Readiness Self-Assessment

Score yourself honestly against each item below. A gap found here costs nothing to fix. The same gap found during auditor fieldwork costs billable hours, and possibly a re-test.

- [ ] Information Security Policy documented and formally approved
- [ ] Access control procedures enforced (MFA, least privilege, timely deprovisioning)
- [ ] Change management process with a documented audit trail
- [ ] Vendor risk management program in place and reviewed annually
- [ ] Incident response plan tested within the last 12 months
- [ ] Continuous evidence collection tool deployed and actively used
- [ ] Employee security training completed by 100% of staff
- [ ] Formal risk assessment conducted within the last 12 months

Scored below 6 of 8? Run remediation before engaging your auditor, not during fieldwork.

Cost & Timeline Reference

Use this as a starting benchmark. Actual figures depend on company size, the number of Trust Service Criteria in scope, and your starting security maturity.

Component	Typical Range	Notes
Readiness Assessment	$5,000 – $15,000	Identifies gaps before engaging an auditor
Auditor Fee (Security only)	$15,000 – $30,000	Mid-tier specialist firm, single criterion
Compliance Automation Tooling	$5,000 – $20,000 / yr	Continuous evidence collection
Internal Staff Time	100 – 200 hours	Spread across IT, HR, Legal, Engineering
Observation Period	3 – 12 months	Non-negotiable, drives total timeline

Need an independent review before you engage an auditor?
The Zaplio team works with mid-market IT and compliance leaders to pressure-test SOC 2 readiness before fieldwork begins. **zaplio.io/contact**
