

SOC 2 compliance checklist

Tick each box as the work is done. Owners and timing are starting points: adjust them to your team and your auditor's plan. Checklist updated 2026-10-14. Full guidance for each step: <https://soc2auditors.org/insights/soc-2-compliance-checklist/>

Checklist by phase

Scope

Task	Owner	Output	When
☐ 1. Choose Type 1 or Type 2	Executive sponsor	Report type and target date	Start
☐ 2. Select the Trust Services Criteria	Security lead, with sales	Criteria in scope	Start
☐ 3. Define the boundary and system description	Engineering lead; legal and executive sign-off	Signed boundary, draft description	Before building controls

Build

Task	Owner	Output	When
☐ Build the ten control areas	One owner per control	Policies, configurations, first review records	Before the window opens (Type 1: before fieldwork)

Readiness

Task	Owner	Output	When
☐ 4. Run a gap assessment	Security or compliance lead	Gap register	Before the window opens (Type 1: before fieldwork)

Task	Owner	Output	When
☐ 5. Build the evidence repository	Audit coordinator	Evidence folders by control	Before the window opens (Type 1: before fieldwork)
☐ 6. Assign owners and run a mock audit	Security lead	Owner register; findings fixed	Before the window opens (Type 1: before fieldwork)

Audit

Task	Owner	Output	When
☐ 7. Engage the auditor	Executive sponsor or legal	Engagement letter with the period dates	Type 2: before the window opens. Type 1: 4–6 weeks before fieldwork
☐ Run controls and close evidence monthly	Control owners, audit coordinator	Monthly evidence manifest	3 to 12 months (Type 2 only)
☐ 8. Prepare for fieldwork	Audit coordinator	PBC tracker with evidence staged	Before fieldwork
☐ 9. Support fieldwork	Audit coordinator	Closed request log	Fieldwork, a few weeks
☐ 10. Review the draft and prepare bridge letters	Executive sponsor, audit coordinator	Management response; final report	After fieldwork
☐ 11. Set up annual renewal	Security lead	Next period's control calendar	The day the window ends

Control areas to build

Build times are our planning estimates; evidence is what an auditor may request.

Control area	Est. build time	Evidence auditors request	Common finding	Guide
☐ Access control	3–6 weeks	<ul style="list-style-type: none">Quarterly access review records with manager sign-offMFA enforcement screenshotsProvisioning and termination workflow logs	Undocumented reviews or active accounts for terminated employees	Access Control Policy
☐ Data encryption	2–4 weeks	<ul style="list-style-type: none">Encryption standard policy (approved, versioned)KMS configuration screenshotsKey rotation audit log	Keys co-located with the data they protect; rotation schedule in policy but not followed in practice	
☐ Security policies	4–8 weeks	<ul style="list-style-type: none">Policy documents with version historyExecutive approval evidenceEmployee acknowledgment log (name, date, policy)	Policy exists but no executive approval or acknowledgment log	
☐ Logging and monitoring	3–5 weeks	<ul style="list-style-type: none">SIEM configuration screenshotsLog retention evidence covering the observation windowReview sign-off records	Log retention gaps or no evidence of periodic review by a named reviewer	Logging and Monitoring
☐ Change management	2–4 weeks	<ul style="list-style-type: none">Change tickets with request, peer review, test result, and deployment recordCI/CD pipeline configuration	Emergency changes approved after the fact; no separation of duties on approvals	Change Management
☐ Incident response	3–6 weeks	<ul style="list-style-type: none">Tabletop exercise records (dated, named participants, findings)Post-incident reviews for any incidents in the period	Plan exists on paper but no tabletop exercise record	
☐ Vulnerability management	3–5 weeks	<ul style="list-style-type: none">Authenticated scan reports (monthly)Remediation tracking ticketsRisk-acceptance records for approved delays	Critical findings aged past the policy's own SLA with no risk-acceptance sign-off	

Control area	Est. build time	Evidence auditors request	Common finding	Guide
☐ Vendor risk	4–8 weeks	<ul style="list-style-type: none"> • Vendor inventory with risk classification • SOC 2 Type 2 reports or ISO 27001 certificates from critical vendors • Contracts with security and breach notification clauses 	Vendors onboarded without assessment; no security clauses in contracts	
☐ Employee training	2–3 weeks	<ul style="list-style-type: none"> • Training completion log (name, date, course) • Phishing simulation results, if you run them 	Completion records not tracked or missing for new hires	Security Controls
☐ Business continuity	6–12 weeks	<ul style="list-style-type: none"> • RTO and RPO for each critical system • Backup configuration evidence • Recovery test results with the gaps found and how they were fixed 	Recovery plan never tested; no RTO or RPO validated by a real test	Business Continuity