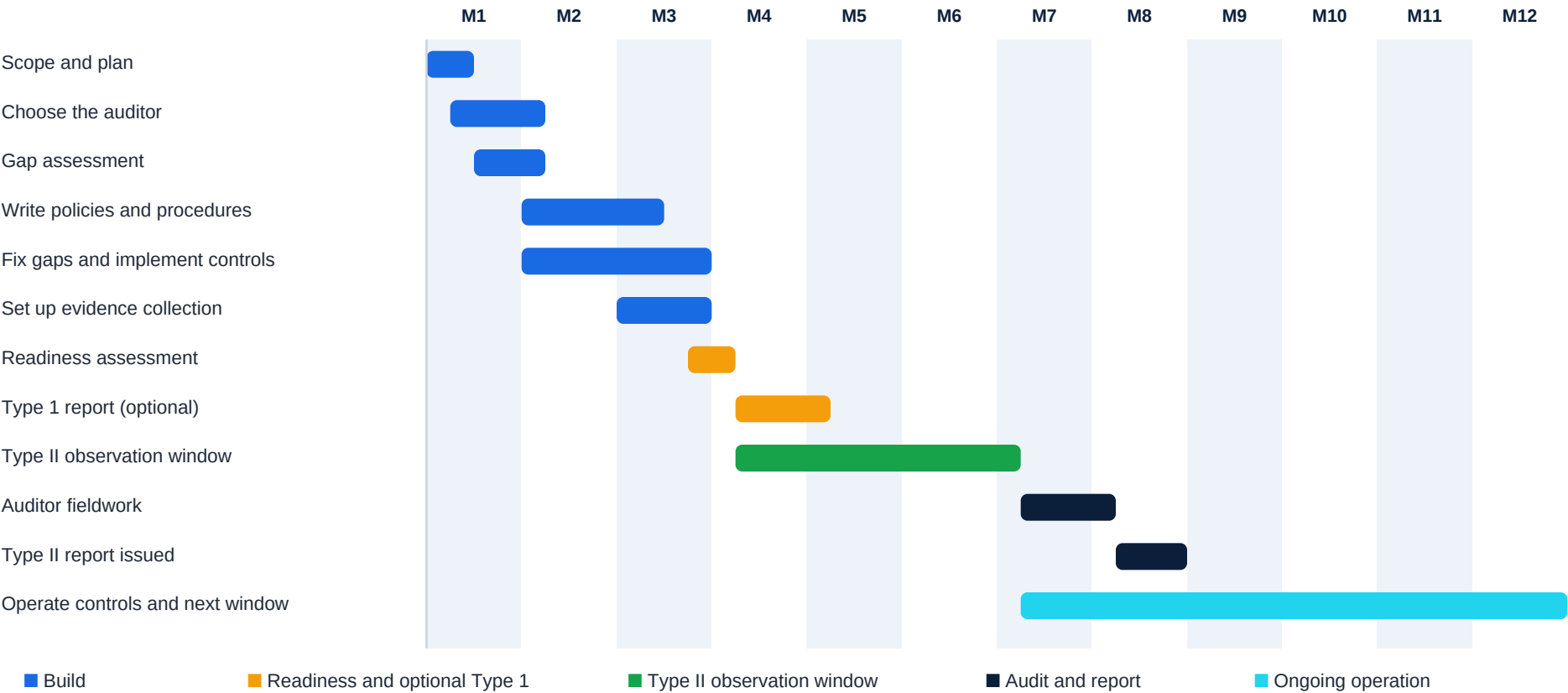


SOC 2 Readiness Roadmap

A month-by-month plan from kickoff to a first SOC 2 Type II report, for ExampleCo, a fictional 40-person B2B SaaS company hosted on AWS. Your own timeline depends on your scope, your starting point and your auditor.



Assumptions: Security criterion only (the Common Criteria), cloud-hosted product with no offices of its own, a three-month first observation window, and a team that can give the project about four to six hours a week per control owner.

Phase by phase

When	Phase	What happens	Deliverables	Owner
Weeks 1 to 2	Scope and plan	Choose the Trust Services Criteria, define the system boundary (product, infrastructure, people, data, vendors), and name control owners.	System description draft, scope statement, project plan	CEO, Compliance Manager
Weeks 2 to 6	Choose the auditor	Shortlist licensed CPA firms, confirm scope, timing, report type and price, and book the observation window start date.	Signed engagement letter	CEO, COO
Weeks 3 to 6	Gap assessment	Compare current practice against the criteria and list every missing or weak control with an owner and a due date.	Gap register, control matrix	Compliance Manager
Months 2 to 3	Policies and procedures	Write and approve the policy set: information security, access control, change management, incident response, vendor management, risk assessment, business continuity and more.	Approved policies, staff acknowledgements	Security Lead
Months 2 to 3	Fix gaps and implement controls	Enforce MFA and SSO, set up access reviews, logging and alerting, vulnerability scanning, backups, onboarding and offboarding checklists, security training, and a risk assessment.	Working controls, risk register	CTO, control owners
Month 3	Evidence collection	Connect systems to the compliance platform, set evidence owners and frequencies, and run each recurring control at least once.	Evidence calendar, first evidence samples	Compliance Manager
Months 3 to 4	Readiness assessment	Test every control as an auditor would. Fix anything that would cause an exception before the window starts.	Readiness report, remediation list	Compliance Manager
Months 4 to 5 (optional)	Type 1 report	The auditor tests that controls are designed properly at a point in time. Useful if a customer needs a report quickly.	SOC 2 Type 1 report	Auditor
Months 4 to 7	Type II observation window	Operate every control and keep evidence. The auditor later tests samples from across the whole window.	Evidence for the full period	All control owners
Months 7 to 8	Auditor fieldwork	The auditor requests samples, interviews control owners and tests operating effectiveness.	Responses to auditor requests	Compliance Manager
Month 8	Report issued	The auditor drafts the report, you review the management assertion and system description, and the final report is issued.	SOC 2 Type II report	Auditor, CEO
Month 7 onward	Operate and renew	Keep controls running, start the next 12-month window, and issue bridge letters to customers between reports.	Continuous evidence, bridge letters	All control owners

Decisions that change the timeline

Type 1 or straight to Type II. A Type 1 report tests control design at one date. A Type II report tests that controls operated over a period. Enterprise buyers usually ask for Type II. A Type 1 can bridge the gap while the window runs.

Length of the first observation window. Type II windows usually run from three to twelve months. Many first reports use three to six months, then move to a twelve-month cycle. Ask your auditor and your key customers what they will accept.

Which criteria are in scope. Security is always included. Availability, Confidentiality, Processing Integrity and Privacy each add controls and evidence. Add only the ones your customers need.

Your starting point. A team that already uses SSO, infrastructure as code and code review closes gaps faster. A team with no written policies needs more time in months 2 and 3.

Auditor availability. Good CPA firms book up. Choose the auditor early so fieldwork can start soon after the window ends.

What auditors look for in a first report

- Every control ran for the whole window, not just at the end of it.
- Evidence is dated and shows who did the work, such as access review sign-offs and change approvals.
- New hires and leavers were handled on time, with training, background checks and access removal recorded.
- Exceptions are rare, explained and fixed. A few exceptions do not fail a report, but they appear in it.
- The system description matches what actually runs in production.

This roadmap is an illustration for a fictional company, not a quote or a guarantee. SOC 2 reports are issued by licensed CPA firms under AICPA attestation standards. Use the free nank.ai SOC 2 compliance checklist at www.nank.ai/templates-and-tools/soc-2-compliance-checklist/ to see which controls you already have, or book a free readiness assessment at www.nank.ai/soc-2-compliance-service/.