eBOOK · SOC 2

SOC 2 Type II in 90 Days: A Realistic Timeline for SaaS Teams

How growing SaaS companies achieve SOC 2 Type II without derailing engineering — with a week-by-week project plan.

28 pages · PDF · Updated May 2026 · **goironfort.com**

Introduction

"Can you send us your SOC 2 report?" — the question that turns a promising enterprise deal into a multi-month delay. SOC 2 has become the baseline security credential for B2B SaaS, and the companies that achieve it fastest close more enterprise deals. This guide gives you an honest, realistic roadmap to SOC 2 Type II.

■ *Honest caveat: "SOC 2 in 90 days" refers to being Type II observation-period-ready, not having a published report. The 6–12 month observation period still applies. This timeline gets you ready to start — and gets your Type I done fast.*

Understanding the Timeline: Type I vs. Type II

	SOC 2 Type I	SOC 2 Type II
What it proves	Controls are suitably designed at a point in time	Controls operated effectively for 6–12 months
Time to achieve	4–8 weeks (with Iron Fort)	6–12 months after Type I
Value	Satisfies initial procurement security reviews	Required for most enterprise contracts
Observation period	None — point-in-time	Minimum 6 months (12 recommended)
Cost (audit fees)	$8,000–$20,000	$20,000–$50,000

The 90-Day Roadmap

Weeks 1–2 — Scoping & Setup

- Define your SOC 2 scope boundary (systems, services, geographic locations)
- Select Trust Service Criteria relevant to your product and customer contracts
- Connect infrastructure to Iron Fort (AWS, GCP, Azure, GitHub, Okta)
- Generate initial control inventory and gap analysis

Weeks 3–5 — Policy & Controls Gap

- Draft or import all required policies using Iron Fort's policy library
- Identify control gaps with prioritized remediation tasks
- Assign ownership of each control to engineering, IT, or HR
- Set up vendor risk management — identify all in-scope vendors

Weeks 6–9 — Remediation

- Implement missing controls (MFA, logging, access reviews, encryption)
- Complete policy approval workflows in Iron Fort
- Conduct workforce security training with completion tracking
- Execute vendor questionnaires for all in-scope vendors

Weeks 10–12 — Type I Readiness

- Run Iron Fort's pre-audit readiness check
- Engage auditor and share evidence vault access
- Complete auditor requests and resolve findings
- Receive SOC 2 Type I report

The 5 Most Common SOC 2 Delays (and How to Avoid Them)

■ **Scope creep:** Define scope tightly. Start with your core SaaS product and the systems that directly support it. Add additional systems after Type I.

■ **Missing vendor reviews:** Get your vendor list done in Week 1. SOC 2 CC9.2 (vendor management) is the most commonly missed control at audit time.

■ **Policy bottlenecks:** Use a policy library and template-driven drafting. Don't write policies from scratch — it adds weeks and introduces gaps.

■ **Evidence scrambles:** Use continuous evidence collection (Iron Fort). Manual evidence collection adds 3–6 weeks of sprint work at audit time.

■ **Auditor availability:** Book your auditor in Week 4, not Week 10. Good SOC 2 auditors are booked 8–12 weeks out.

Book a Free SOC 2 Scoping Call

Iron Fort gets SaaS companies to Type I in 30 days and Type II-ready in under 6 months. Book a free scoping call at **goironfort.com/demo** — walk away with a project plan specific to your stack.