COMPLIANCE · TEMPLATE

# The *90-Day* SOC 2 Readiness Sprint

KAANSYSTEMS.COM/LIBRARY/90-DAY-SOC2-READINESS-SPRINT · JULY 9, 2026

## ABOUT THIS TEMPLATE

You picked SOC 2. Now what? A week-by-week plan that takes you from nothing to the start of your Type II observation window in one focused quarter.

## THE TEMPLATE

The week-by-week checklist. Each item has a clear done state. Run it in order; don't start a phase until the prior one's blocking items are closed.

**Weeks 1-2: Scope + gap assessment**

- [ ] System boundary defined in writing (what's in scope, what's explicitly out)
- [ ] Trust Services Criteria selected (Security + only what buyers require)
- [ ] Gap assessment complete: every gap named, owner assigned
- [ ] Report type decided (Type I as a stepping stone, or straight to Type II)

**Weeks 3-5: Policy + process**

- [ ] Core policy set drafted and approved (8-10 policies)
- [ ] Each policy describes what the team will actually do (no aspirational controls)
- [ ] Process owners assigned for every recurring control
- [ ] Policies published where employees can find them, acknowledgement tracked

**Weeks 6-9: Implement controls**

- [ ] MFA + SSO enforced across in-scope systems
- [ ] First access review performed and recorded
- [ ] Centralized logging + alerting live, routes to on-call

- [ ] Change management enforced: prod changes tied to reviewed PRs
- [ ] Encryption at rest + in transit verified across in-scope stores
- [ ] Vendor / sub-processor list built, annual review scheduled
- [ ] Onboarding + offboarding checklists documented and in use

**Weeks 10-12: Evidence + kickoff**

- [ ] Evidence pipeline generating artifacts automatically
- [ ] Readiness assessment complete, findings closed
- [ ] Auditor engaged, observation window start date set
- [ ] Observation window started

## HOW TO USE IT

The window is not a break. The single most common way teams fail their first Type II is treating the observation window as "done" and letting the controls lapse. The access review you performed in Week 6 has to happen again next quarter, on time, recorded. The evidence pipeline has to keep running. Compliance is a continuous practice, and the window is where that practice gets measured.

Budget for a dedicated owner. A 90-day sprint with a designated compliance owner is 90 days. The same sprint squeezed into the margins of everyone's real job is the year-long stall this article opened with. The work isn't hard. It's just work, and work needs an owner.

The second framework is cheaper than the first. Almost everything you build here — the policies, the evidence pipeline, the access review cadence — carries directly into HITRUST, ISO 27001, or a HIPAA assessment later. The 90 days buys you SOC 2 and most of the readiness for whatever comes after it.