COMPLIANCE · TEMPLATE

SOC 2 for Startups: The *Complete* Readiness Guide

KAANSYSTEMS.COM/LIBRARY/SOC2-FOR-STARTUPS-COMPLETE-GUIDE · SEPTEMBER 16, 2026

ABOUT THIS TEMPLATE

SOC 2 for startups is almost always sales-driven. Here's the whole path — Type I vs II, the five criteria, the timeline, the real cost, and the engineering work that actually earns the report.

THE TEMPLATE

A SOC 2 readiness roadmap. Work top to bottom; each phase makes the next meaningful. Score each item Not started / In progress / Done.

Phase 1 — Scope

- ☐ Confirmed the business trigger (a real deal / lost deals in security review)
- ☐ Chosen Type I-then-II vs. straight-to-Type-II
- ☐ Scoped criteria (Security + only the others you commit to)
- ☐ Defined the systems/boundaries in scope

Phase 2 — Gap assessment

- ☐ Mapped current controls to the Common Criteria
- ☐ Identified the gaps (access, change mgmt, logging, encryption, vendor risk, evidence)
- ☐ Named an owner for the program

Phase 3 — Remediate (the engineering work)

- ☐ SSO + universal MFA; least-privilege roles; one-action offboarding
- ☐ Long-lived credentials eliminated in favor of federated, short-lived access

- [ ] Change management: reviewed PRs + gated pipeline with traceable history
- [ ] Centralized, tamper-resistant logging + alerting
- [ ] Encryption at rest + in transit with managed keys
- [ ] Subprocessor list + signed DPAs + review cadence
- [ ] Backup/DR + a tested restore
- [ ] Incident-response plan documented and exercised

Phase 4 — Evidence + observe

- [ ] Compliance platform integrated (or an evidence pipeline stood up)
- [ ] Evidence collection automated, not manual
- [ ] Observation window started; controls running continuously

Phase 5 — Audit

- [ ] Auditor engaged; penetration test complete
- [ ] Type I issued (if used as interim)
- [ ] Type II window closed; report issued and shareable with prospects

Most startups find Phase 3 is 80% of the effort and Phase 4 is where discipline pays off or falls apart. Both are engineering problems more than compliance ones.

WHAT'S ACTUALLY IN SCOPE: THE FIVE TRUST SERVICES CRITERIA

SOC 2 is built on five Trust Services Criteria (TSC). Only the first is mandatory; the rest are scoped to what you commit to.

CRITERION	MANDATORY?	WHAT IT COVERS	SCOPE IT WHEN…
Security (Common Criteria)	**Yes**	Access control, change management, risk management, monitoring — the baseline	Always
Availability	No	Uptime, DR, capacity, monitoring	You make uptime commitments (SLAs)
Confidentiality	No	Protecting data designated confidential	Contracts promise confidentiality beyond the norm

CRITERION	MANDATORY?	WHAT IT COVERS	SCOPE IT WHEN…
Processing Integrity	No	Processing is complete, valid, accurate, timely	You process transactions/data on customers' behalf
Privacy	No	Handling of personal information per your notice	You collect consumer PII and make privacy commitments

Most startups scope **Security only** for the first report, occasionally adding Availability or Confidentiality when a contract explicitly requires them. Adding criteria multiplies the controls you must build and evidence — so scope to the commitments you've actually made, not to look thorough.