SOC 2 Compliance: Trust Services Criteria and Audit Strategy for SaaS

Bev Waller & Erik Jones December 16, 2025

Executive Summary

SOC 2 has become the table-stakes compliance certification for B2B SaaS. Enterprise procurement teams ask for it before signing contracts of any meaningful size, security questionnaires reference it as the baseline, and the absence of a clean SOC 2 report stalls deals during legal review. This guide explains the framework's structure, the practical steps to a clean Type II report, and the tooling decisions that separate a six-month sprint from an eighteen-month grind.

Why SOC 2 Matters for B2B SaaS

Unlike HIPAA or PCI DSS, SOC 2 is not a regulatory requirement — it is a market requirement, driven by buyers who need to demonstrate to their own auditors that their vendors meet a defined security bar. The

framework is governed by the **AICPA** and audited by licensed CPA firms.

A SOC 2 report is not a pass/fail certification; it is an opinion document describing the control environment and any exceptions noted during testing. The *"AICPA Trust Services Criteria"* publication is explicit on this point: *"the auditor's opinion expresses whether management's description fairly presents the system and whether the controls were designed and operated effectively."* Buyers read the report — not just the cover letter — which means the design and operation of controls matter as much as the auditor's signature.

The Five Trust Services Criteria

SOC 2 is structured around five Trust Services Criteria (TSC), defined in **TSP Section 100**. **Security** is the only mandatory criterion (sometimes called the Common Criteria) and forms the baseline for every SOC 2 engagement.

Security: The Common Criteria

The Security TSC contains nine series of criteria (CC1 through CC9) covering control environment, communication, risk assessment, monitoring, control activities, logical and physical access, system operations, change management, and risk mitigation. Every SOC 2 report must address all nine series.

CC6 Logical and Physical Access

The most-tested area at growth-stage SaaS audits. SSO with MFA, role-based access control, formal access reviews, terminated-employee de-provisioning workflows. Most exceptions found in SOC 2 audits trace back to access management gaps.

CC7 System Operations

Monitoring, anomaly detection, incident response. The criterion that most often pulls observability tooling into the audit scope; Datadog dashboards, PagerDuty rotations, and runbooks become evidence.

CC8 Change Management

Production change controls, code review, segregation of duties between development and deployment. The CI/CD pipeline becomes audit-relevant the day the criterion is in scope.

Optional Criteria

Availability: uptime commitments, capacity planning, DR. Required when contracts reference SLAs.

Confidentiality: protection of confidential information beyond personally identifiable data. Common for SaaS handling enterprise IP.

Processing Integrity: system processing is complete, valid, accurate, timely, authorized. Common for fintech and data-processing SaaS.

Privacy: notice, choice, consent, collection, use, retention, disclosure of personal information. Often skipped in favor of GDPR/CCPA-specific programs.

Most B2B SaaS scopes Security plus Availability for the Type II. Adding Confidentiality is common; the others are situational.

Type I vs Type II

The two report types differ in observation period.

Type I: Point-in-Time

Documents control design as of a single date. Useful for early-stage companies that need an attestation for a specific procurement deal but cannot yet show a track record. Typical timeline: **3-4 months** from kickoff to report.

Type II: Period of Time

Documents control operation across a 3-12 month observation period. The format enterprise buyers actually want. Most first-time audits run a 6-month observation; mature programs run 12-month observations aligned to the fiscal calendar.

The Type I to Type II Transition

Companies often run a Type I in year one to demonstrate the program exists, then transition to Type II in year two with a longer observation

window. The Type I work directly accelerates the Type II by establishing the control environment and remediation history.

Practical Implementation

The path from "we do not have a SOC 2" to a clean Type II report follows a recognizable arc.

Phase 1: Readiness Assessment (Weeks 1-4)

Gap analysis against the Common Criteria. Identify missing controls, document exceptions, and produce a remediation roadmap. The output is a ranked backlog with effort estimates.

Phase 2: Control Implementation (Weeks 4-16)

The work happens here. Common implementations:

> **Identity:** Okta or Azure AD for SSO, MFA mandatory, conditional access policies, formal access review cadence (quarterly minimum)
>
> **Endpoint:** Jamf, Kandji, or Intune for MDM with disk encryption, automated patching, and compliance reporting
>
> **Logging and monitoring:** Datadog, AWS CloudTrail, GuardDuty, Security Hub centralized logging with retention aligned to audit period

Vulnerability management: SAST in CI, SCA on dependencies, DAST against staging, annual penetration testing

Vendor management: documented vendor risk assessment, periodic re-review of subprocessors

Incident response: tabletop exercises, written runbooks, post-incident reviews

Phase 3: Observation Window (Months 4-10 for Type II)

Controls run continuously. Evidence accumulates automatically (CloudTrail logs, Datadog dashboards, ticket history). The observation window is where automation pays off; manual evidence collection across a 6-month period consumes weeks of engineering time.

Phase 4: Audit Fieldwork (Weeks following observation)

The auditor samples evidence, tests controls, requests interviews, and writes the report. Typical fieldwork runs 4-6 weeks for a mid-sized SaaS.

Common Pitfalls

Treating SOC 2 as a checklist: the auditor evaluates control operation, not just existence. A documented access review that nobody runs is worse than an undocumented one.

Late evidence collection: trying to assemble 6 months of evidence in the last week before fieldwork is the most-common cause of audit overruns. Automate evidence collection from day one.

Auditor-as-consultant confusion: the audit firm cannot help design the controls they will then audit. Engagement scope must be explicit.

Scope creep in optional criteria: adding Privacy to a first-time audit doubles the work. Land Security and Availability first; expand later.

Generic GRC platform deployments: a GRC platform with no control owners is a database. Without operational ownership, the platform becomes shelfware.

Measured Outcomes

3-4 month timeline for Type I from readiness to report

6-12 month observation window for Type II, plus 4-6 weeks fieldwork

Over 95% audit success rate in our engagements

Sub-30-day remediation for issues identified during fieldwork, included in the SOW at no additional cost

Audit-ready evidence package generated continuously rather than collected manually before fieldwork

How Jacobian Helps

SOC 2 is one program; the cloud infrastructure, identity stack, and engineering practice that the controls run on top of are another. Our team brings both — compliance practitioners who run the audit program, and SREs who build the infrastructure the controls depend on. We map your existing controls to the Common Criteria, design the gaps, run the implementation, and produce the audit-ready evidence package. We pair well with GRC platforms (continuous controls verification, automated evidence collection) when you want the tooling, and we run with our team alone when the platform overhead does not justify itself.

Resource Details

Author: Bev Waller & Erik Jones

Published: December 16, 2025

Categories:

Compliance | Security | SOC 2

Download

Full Document

About This Resource

A practical guide to SOC 2 for B2B SaaS companies. Covers the five Trust Services Criteria, Type I vs Type II decision-making, control implementation patterns, and what auditors actually look for during fieldwork.

Categories:

Compliance Security SOC 2