DCYBR - SOC 2 READINESS CHECKLIST

The Practical Pre-Audit Guide Used by SaaS Teams to Avoid Audit Delays

Purpose: This checklist helps you quickly determine whether your company is truly audit-ready - not just "platform green."

Most SOC 2 delays happen *after* controls are tracked but *before* auditors accept evidence.

Use this checklist to identify gaps early.

1. Security Ownership & Governance

☐ Security owner formally assigned
☐ Security policies approved by leadership
☐ Risk assessment completed within last 12 months
☐ Incident response plan documented
☐ Security awareness training defined

Warning sign: Policies exist but are never operationalized.

2. Access Control

☐ Centralized identity provider (Okta / Google / Azure AD)
☐ MFA enforced for all production systems
☐ Access reviews performed quarterly
☐ Terminated users removed within 24 hours
☐ Least-privilege access documented

Auditor Focus: Evidence timestamps matter more than screenshots.

3. Infrastructure Security

☐ Production hosted in AWS / GCP / Azure
☐ Logging enabled for critical systems
☐ Backup strategy documented and tested
☐ Encryption enforced in transit and at rest
☐ Vulnerability scanning active

Common Gap: Tools installed but alerts ignored.

4. Vendor & Data Management

☐ Vendor inventory maintained
☐ Critical vendors risk-reviewed
☐ DPAs signed where required
☐ Customer data classification defined
☐ Data retention policy enforced

Reality: Vendor management fails more audits than policies.

5. SOC 2 Platform Configuration (If Using Drata / Vanta / Secureframe)

☐ Controls mapped correctly to environment
☐ Automated tests reviewed monthly
☐ Evidence reviewed — not auto-accepted
☐ Failed checks remediated with documentation
☐ Manual controls assigned owners

Important: Green dashboards ≠ audit readiness.

6. Evidence Readiness

☐ Evidence stored in organized structure
☐ Screenshots replaced with system exports where possible
☐ Evidence linked directly to controls

☐ Audit trail preserved
☐ Mock audit performed internally

Auditors evaluate consistency, not volume.

7. Audit Preparation

☐ Auditor selected or shortlisted
☐ Scope clearly defined (Type 1 vs Type 2)
☐ Observation period planned
☐ Engineering time allocated (<5 hrs/week typical)
☐ Internal readiness review completed

⚑ Quick Self-Assessment

Count how many sections are fully complete:

- **0–2 sections:** Early stage - plan required
- **3–5 sections:** Platform-ready, not audit-ready
- **6–7 sections:** Likely ready for audit engagement

Need a Second Opinion?

Most teams discover gaps only after the auditor arrives.

Book a 20-minute SOC 2 Readiness Call
We'll estimate the timeline, risks, and effort required.

www.dcybr.com

Disclaimer: *This checklist is provided for informational purposes only and does not constitute legal, audit, or certification advice. SOC 2 readiness requirements vary by organization and auditor. Completion of this checklist does not guarantee audit success or report issuance.*