IMPACT
RISK ADVISOR

Top 10 Common SOC 2 Gaps for Startups

1. No Formal Risk Assessment

Startups often skip a documented enterprise risk assessment. Auditors expect risks to business operations, technology, and security to be identified, assessed, and reviewed annually.

2. Missing Vendor Risk Management

Relying on cloud providers without reviewing their SOC reports or contractual commitments leaves gaps. SOC 2 requires documented vendor risk reviews and agreements.

3. Weak Access Controls & Reviews

Founders may rely on convenience over security. Auditors expect role-based access, MFA, and regular user access reviews to critical systems.

4. Lack of Centralized Policies

Policies pulled from templates with no tailoring are a red flag. SOC 2 requires approved, version-controlled, and organization-specific policies.

5. Incomplete Logging & Monitoring

Startups assume Google or Microsoft “cover it.” In reality, you must show logging is enabled, retained, and reviewed, with incident response tied to alerts.

6. No Documented Incident Response Plan

SOC 2 requires a tested plan. Without an IR plan and at least one tabletop exercise, startups risk a major gap.

7. No Defined Data Retention & Disposal

Data often lives indefinitely in email, Dropbox, or Google Drive. SOC 2 requires documented retention timelines and secure disposal of client data.

8. Missing Security Awareness Training

Founders may handle onboarding informally. Auditors expect annual training and phishing simulations to demonstrate a culture of security.

9. Weak Change Management Practices

Startups rely on GitHub or quick fixes without approvals. SOC 2 requires evidence of peer review, testing, and approval for code and configuration changes.

10. Over-Reliance on Vendor Security

Cloud services are secure, but SOC 2 expects you to manage shared responsibility. Without clear documentation of what your company does vs. your vendor, gaps remain.