SAV

5 SOC 2 Red Flags That Derail Audits

More than half of SOC 2 audits uncover the same handful of issues. They slow down the process, increase costs, and leave customers questioning your control environment. By spotting these red flags early, you stay ahead of delays, rework, and credibility gaps.

1. Scope is Fuzzy

What it is: System boundaries, dependencies, or subservice providers are vague or incomplete.

Why it hurts: Surprises mid-audit create coverage gaps and extra work.

How to spot it: Scope documents are vague or leave out critical vendors and dependencies.

2. Risk & policies are weak

What it is: Policies exist but they're outdated, not enforced, or not backed by a recent risk assessment.

Why it hurts: Auditors flag design deficiencies and clients lose confidence.

How to spot it: Policies are outdated, poorly communicated, or not backed by a current risk assessment.

3. Access controls don't add up

What it is: User access reviews, MFA, or termination processes aren't consistent.

Why it hurts: One of the most common SOC 2 findings. A single missed review can undermine your report.

How to spot it: Inactive accounts remain open or access reviews are infrequent.

4. Logging & incidents fall short

What it is: Logs exist, but they're scattered, incomplete, or not tied to an incident response plan.

Why it hurts: You can't prove controls operated throughout the audit period.

How to spot it: Logs aren't centralized, retention isn't enforced, or incident tickets lack closure.

5. Vendor & data risks ignored

What it is: Third-party SOC reports are outdated, exceptions aren't tracked, or data flows aren't secured.

Why it hurts: Even strong internal controls are undermined by weak vendors.

How to spot it: Vendor SOC reports are stale or repeat exceptions remain unresolved.

Pro Tip: Run a dry-run check before your audit window. Collect the evidence your auditor will request and confirm it covers the full reporting period.

Big 4 expertise with boutique agility.

Quick Wins

Practical steps you can take right now to strengthen readiness and show progress before your audit:

- **Refresh your risk assessment** before every major product or system change
- **Centralize vendor SOC reports** and follow up on open exceptions
- **Automate user access reviews** on a quarterly cycle, not annually
- **Test your incident response plan** with post-mortems and assign clear owners
- **Document control evidence** as you go instead of scrambling at year-end

Quick wins like these not only reduce audit pain, they also strengthen your reputation with customers and investors.

Next Steps

If these red flags sound familiar, now is the time to act. **Book a 30-minute consult** with SAV Associates today and get a clear plan to eliminate gaps, streamline evidence collection, and walk into your audit with confidence.

About **SAV Associates**

SAV Associates is a full-service CPA firm and a recognized leader in SOC reporting, audits, and readiness assessments. With offices in Canada and the U.S., we combine the depth of Big 4 expertise with the agility of a boutique practice.

Our Assurance & Risk Advisory team helps SaaS companies, startups, and enterprise clients navigate the complexity of SOC 2 and related frameworks with confidence. We don't just deliver reports — we guide clients through readiness, close critical gaps, and build stronger control environments that stand up to scrutiny.

By partnering with SAV, organizations accelerate enterprise sales cycles, strengthen trust with customers and investors, and reduce the risks and costs of failed or delayed audits.

Get in Touch

Sanjay Chadha
Partner

Canada
sanjaychadha@savassociates.ca
647-831-8322

USA
sanjayc@scus.cpa
650-384-9786

www.savassociates.ca

Big 4 expertise with boutique agility.