A Practical Guide

SOC 2 Type II: What Auditors Actually Test

Written by Mario Kamburov, Security Professional

2026

Context before we dig into Controls

This is a book for

- Founders who suddenly face enterprise security questions
- Engineering leaders forced into compliance ownership
- First GRC hires in scaling startups
- Companies without a formal security org

Why SOC 2 Exists

Before cloud computing, companies ran their own infrastructure. If something broke, they blamed themselves.

Then cloud computing happened. The era of rapid growth of SaaS, PaaS and IaaS services.

Suddenly:

- Payroll runs in someone else's system
- Customer data lives in someone else's database
- Infrastructure runs in someone else's cloud

And enterprises started asking:

> "Why should we trust you with our data?"

But here's the challenge:
Every company started inventing its own security requirements and questionnaires. One customer would send 300 questions. Another would send 500. Some would ask about encryption. Some would ask about your fire extinguishers. It became chaotic.
The accounting industry stepped in and created a standardized trust mechanism: SOC 2 by AICPA

Not built by hackers. Not built by regulators. Built by accountants, initially starting as SOC 1

Why does this matter? Because SOC 2 inherited the audit methodology from SOC 1:

- Identify controls
- Define control owners
- Define frequency
- Heavy Sampling
- Document deviations and exceptions

Most important SOC 2 Control Domains

Domain 1 – Access Management

Identity is the real perimeter in modern Cloud companies. SOC 2 heavily tests how access is granted, reviewed, and removed.

Auditors typically request:

- Full employee listing
- Terminated employee listing
- Newly onboarded employee listing
- Privileged access employee listing
- Access request evidence
- Access review documentation
- MFA configuration evidence

They sample joiners, leavers, and privileged accounts to verify:

- Proper approval, granting of access
- Timely provisioning
- Timely deprovisioning
- Least privilege enforcement
- Periodic review

Minimal viable structure:

- Central identity provider
- HR-driven joiner/leaver workflow (onboarding/offboarding checklist)
- Documented privileged access approvals
- Quarterly access reviews
- Logged deactivation timestamps

Anti-patterns and Real Risks:

- Anti-pattern: Engineers access production databases directly using persistent credentials stored locally on laptops.
- Incident scenario: A developer's laptop is compromised via a malicious browser extension and the attacker reuses cached DB credentials to query customer data.

SOC 2 Steering Group Team

As noticeable SOC 2 touches on company-wide operations, engineering operations, service operations and this requires a broad set of knowledge, responsibilities and accountability across the company, so the people involved in the audit could be the following roles:

- Head of Engineering
- Head of Infrastructure
- Head of People
- Head of Operations
- Head of Security
- Head of IT
- Head of Legal
- CTO / CEO – Leadership roles

What hurts most?

Many startups fail to understand the Segregation of Duties or set the right level or risk tolerance, where it is really needed and where it can be skipped or automated.

For many entrepreneurs, who strive for innovation, they often forget about risk and focus just on delivery, the word process sounds like a swear or a bad word. Process is not about manually approving a decision or change, but about controlling and governing behaviour and risk. Processes could be manual, semi-automated or fully automated. It could be administrative or technical. Do not be afraid of processes, just focus on and keep your mind on a pragmatic and risk-based approach. Focus on the biggest risks first.

Preparing for Sampling Without Panic

The most stressful part of a SOC 2 audit is not writing policies.
It is responding to sampling requests.

Auditors repeatedly ask for “system-generated listings,” “complete population reports,” and “evidence of completeness.” These phrases confuse teams that have never been audited before.

Understanding what they mean changes everything.

System-Generated Listing

A system-generated listing is a report exported directly from the authoritative system of record (Single Source of Truth System). For example:

- All active users in your identity provider or HR / IdP System
- All production deployments within the audit period
- All terminated employees during the audit window
- All security incidents logged in your ticketing system

The key word is system-generated.

Auditors do not want manually assembled spreadsheets. They want raw output directly from the system because it reduces manipulation risk. Usually you’d need to programmatically obtain that list.

If the population can be altered manually, sampling integrity collapses.

That is why screenshots of dashboards are often rejected. They are views, not populations.