GUIDE

SOC 2 Study Guide

The Trust Services Criteria in plain English

How to use this guide

This guide condenses my free SOC 2 Deep Dive course into a reference you can keep next to you while you study or prepare for an audit. It follows the same order as the course: what SOC 2 is, the five categories, the nine Common Criteria one by one, the optional categories, and then how the audit actually works.

In my experience, trying to memorize thirty three criteria with codes like CC6.3 doesn't work. What helped me was picturing a restaurant: the owner, the cooks, the keys and the safe, the security camera, the suppliers. You will see that picture in a short "Restaurant view" note in each major section.

What SOC 2 is and who asks for it

SOC 2 is an attestation report, not a certificate. An independent CPA firm examines your controls and writes an opinion under the AICPA's SSAE 18 standard. The report tells your customers whether your controls are well designed and, in a Type 2, whether they actually worked over a period of time.

Who asks for it: mostly B2B customers, especially larger ones, who send you data and want independent proof that you protect it. Their security and procurement teams ask for your report in vendor reviews, and big deals often wait for it.

Four words you need from day one:

- **Control:** something you do on purpose to reduce a risk. Example: remove a leaver's access within one business day.
- **Evidence:** proof the control happened. A ticket, a log export, a screenshot, signed minutes.
- **Population and sample:** the population is every time a control ran in the period (every leaver, every change). The auditor picks a sample from it to test. The auditor picks, not you.
- **Exception:** a sample where the control didn't work as described. It is written into the report, with management's response.

> **Restaurant view:** Customers can't walk into your kitchen. The SOC 2 report is the independent health inspection they read instead.

The five categories

The Trust Services Criteria are grouped into five categories. Only Security is mandatory.

Category	Criteria	Include it when
Security	CC1 to CC9, the Common Criteria	Always. It is in every SOC 2 report.
Availability	A1.1 to A1.3	You promise uptime in contracts or an SLA.
Confidentiality	C1.1 and C1.2	Customers hand you business data you promise to keep secret and delete.
Processing Integrity	PI1.1 to PI1.5	Correct processing is the product: billing, payroll, payments, data pipelines.
Privacy	P1 to P8	You collect and use personal information for your own purposes, like a consumer app.

The Common Criteria come in two acts. **CC1 to CC5** come from COSO, a classic framework for internal control: they are about how you run the business, not technology. **CC6 to CC9** are specific to SOC 2: they are about how you protect the system.

A short way to remember all nine: CC1 culture, CC2 information, CC3 risks, CC4 monitoring, CC5 rules, CC6 keys, CC7 alarms, CC8 changes, CC9 the outside world.

Criteria, points of focus and controls. A criterion is the goal you must reach. Points of focus are guidance, not a checklist. Controls are your own house rules. Two companies can meet the same criterion with different controls, and the auditor judges whether yours are enough.

CC1: Control environment

What it means. The foundation: values, oversight, structure, competent people and accountability. Five criteria, from the top of the company down.

- CC1.1 Integrity and ethics: a written code of conduct.
- CC1.2 Board oversight: someone independent watches management.
- CC1.3 Structure and authority: org chart, reporting lines, a named security owner.
- CC1.4 Competence: hire the right people, check backgrounds, train them.
- CC1.5 Accountability: performance reviews and a disciplinary process that is actually used.

What auditors look for. A sample of joiners from the period, each with a signed code of conduct, a background check before the start date and completed security training. Proof that existing staff signed again and trained again during the year. A security update to the board or an advisory group.

Common evidence. Signed acknowledgements, background check records, training completion exports (KnowBe4 or your compliance platform), a dated org chart, job descriptions, board slides and minutes, exported performance reviews.

Common mistakes. Joiners who never signed or signed weeks late. No record at all of board oversight. An outdated org chart. A policy that says yearly performance reviews when part of the team skipped them.

> **Restaurant view:** Walk from the owner's office down to the kitchen. What do we believe in (no expired food)? Who watches the manager (the investors)? Who reports to whom? Are the cooks trained? Are there consequences? CC1.2 is the arrow pointing up, CC1.5 is the arrow pointing down.

CC2: Communication and information

What it means. Information has to be reliable and has to flow. CC2.1: get reliable information. CC2.2: share it inside the company. CC2.3: share it with outsiders.

What auditors look for. A system inventory, data flow diagrams and logs nobody can quietly edit. Policies that staff actually received and acknowledged, plus a channel to report concerns. External commitments in contracts, a security page or trust center, a way to report vulnerabilities, and records of customer notifications.

Common evidence. Inventory and diagrams reviewed yearly, audit logs from AWS CloudTrail, Google Cloud Audit Logs and the GitHub audit log, policy acknowledgement records, training records, customer agreement templates, the trust center.

Common mistakes. The classic one: an access review that looked perfect, but the user list behind it was pulled from the wrong system and filtered to active employees only, so contractors were missing. Auditors check how a report was made, not only what it says. Document the system, the query and the filters for every report you use as evidence. Another common miss: promises on the website that no control actually supports.

> **Restaurant view:** Fix the thermometer, post the hygiene rules on the kitchen wall, put the allergen notice on the menu. And never print "organic" unless it's true.

CC3: Risk assessment

What it means. Thinking ahead about what could go wrong.

- CC3.1: define your objectives, because without them you can't see what threatens them.

- CC3.2: identify and analyze risks, with likelihood and impact, and decide how to treat each one: mitigate, transfer, avoid or accept.
- CC3.3: consider fraud, someone inside cheating on purpose.
- CC3.4: reassess when something big changes, like a cloud migration, an acquisition or a new region.

What auditors look for. A dated risk assessment, at least yearly, with a risk register where every risk has an owner and a treatment decision. Fraud named explicitly. Notes showing extra reviews after significant changes.

Common evidence. The risk register, management sign-off, workshop notes, a policy listing the triggers for extra reviews.

Common mistakes. A risk assessment older than a year. Risks with no owner or no treatment. A register frozen for years. A template filled in without any real discussion.

> **Restaurant view:** The owner sits down with a notebook: food poisoning, fire, the fridge dying on a Friday night. And the uncomfortable one: what if the cashier takes money from the till?

CC4: Monitoring activities

What it means. Checking that controls actually work, and making sure problems reach someone who fixes them. CC4.1 covers ongoing checks (built into daily work) and separate evaluations (a point in time review). CC4.2 covers reporting deficiencies to the right people in time.

What auditors look for. Monitoring history across the whole period, someone reviewing it, and proof that failed checks became tickets with an owner and a due date. A yearly internal audit or self assessment by someone who doesn't own the controls, and a penetration test.

Common evidence. Compliance platform check history, cloud posture reports (AWS Security Hub, Wiz), management review notes, internal audit report, pentest report, remediation tickets.

Common mistakes. A monitoring tool installed that nobody looks at. Failing checks open for months. A promised internal audit that never happened. Trying to hide failing checks right before the audit: a problem found and fixed with a ticket is better evidence than a suspiciously clean year.

> **Restaurant view:** The internal inspector walks around with a clipboard every month, and the city inspector comes once a year. When the fridge runs warm, the manager hears about it the same day.

CC5: Control activities

What it means. Turning risks into rules. CC5.1: choose controls that bring each risk to an acceptable level, both preventive and detective. CC5.2: general controls over technology (access, changes, operations, backups); CC6 to CC8 give the details. CC5.3: write policies and procedures that put the controls into action.

What auditors look for. A control matrix that maps risks to controls. Segregation of duties for risky work. Ten to twenty policies, each with an owner, management approval, a review within twelve months, version history and staff acknowledgements.

Common evidence. Control matrix, policy documents with version history, approval records, acknowledgement reports.

Common mistakes. A policy not reviewed in twelve months. An author who approved their own policy. And the most common one: a procedure that says one thing while the team does another. Templates are a great start and a dangerous finish. Write numbers you can actually meet.

> **Restaurant view:** The rule "two signatures to take cash out" is CC5. The inspector watching whether people follow it is CC4.

CC6: Logical and physical access

What it means. The biggest group, with eight criteria and the most audit exceptions.

- CC6.1: protect systems with unique identities, SSO, enforced MFA, network segmentation and encryption with carefully managed keys.
- CC6.2: joiners and leavers. Approval before access, removal everywhere on the last day.
- CC6.3: access changes for people who stay, least privilege, role-based groups and periodic access reviews.
- CC6.4: physical access. In the cloud, the provider runs the data centers and is covered by its own SOC 2 report.
- CC6.5: dispose of data and devices so nothing is readable afterwards.
- CC6.6: protect the perimeter against outside threats: firewall rules, WAF, admin access through VPN or zero trust, scans and pentests.
- CC6.7: protect data in motion: TLS, MDM rules, DLP, limits on sharing.
- CC6.8: prevent malware and bad packages: endpoint protection and dependency scanning.

What auditors look for. A sample of about twenty five joiners and leavers from the HR list, checked for approval before access and removal on time. Quarterly access reviews with real removals. MFA enforcement settings, cloud IAM exports, endpoint and encryption coverage against the device list, and a yearly review of your cloud provider's SOC 2 report.

Common evidence. Identity provider settings (Google Workspace, Microsoft Entra ID, Okta), access tickets in Jira or Linear, review records, MDM compliance reports, scan and pentest reports, laptop return and wipe records.

Common mistakes. An admin account outside SSO. MFA enabled but not enforced. A contractor who was never in HR, so nobody offboarded them. Rubber stamped access reviews. Leavers' laptops never returned. A device marked non-compliant for weeks with no owner.

> **Restaurant view:** Every person gets their own key, never one under the doormat. Leavers return every key the same day. The waiter doesn't open the safe. CC6.2 is joining or leaving; CC6.3 is staying but changing jobs.

CC7: System operations

What it means. Detecting and handling security events, like a movie in four scenes.

- CC7.1: find weak spots before anything happens: configuration baselines and vulnerability scanning, fixed within your written deadlines.
- CC7.2: monitor for anything abnormal with logs and alerts.
- CC7.3: triage events and decide which ones are incidents.
- CC7.4: respond with an incident response plan: contain, remove the cause, communicate.
- CC7.5: recover and learn, with postmortems and tracked action items.

What auditors look for. Critical and high findings closed within your policy deadlines. Logging enabled and retained, a list of alert rules and what happened to real alerts. A log of triaged events. An approved incident plan, a tabletop exercise in the period, and postmortems with closed actions.

Common evidence. Scan results (Amazon Inspector, Nessus, Dependabot, Snyk), patching tickets, CloudTrail and SIEM settings, alert rules, the event log in Jira Service Management or incident.io, tabletop notes, postmortems.

Common mistakes. A critical finding open for forty days when the policy says seven, with no record of why. A signed, dated risk acceptance would have turned that into a decision. Claiming zero incidents with no event log to prove you looked. A response plan never rehearsed. Postmortem actions never closed.

> **Restaurant view:** The manager checks doors and windows before opening (CC7.1). The camera records the storeroom at 3 a.m. (CC7.2). Someone decides: thief or forgetful cook (CC7.3)? Call security (CC7.4). Fix the door and learn the lesson (CC7.5).

CC8: Change management

What it means. A single criterion, CC8.1: every change to production is authorized, built, tested, documented, approved and deployed carefully. That includes code, infrastructure, database changes and settings in key SaaS tools.

What auditors look for. The population of production changes in the period, usually merged pull requests or deployments. For each sampled change: approved by someone other than the author, approved before deployment, tests passed, and a ticket or clear reason.

Common evidence. GitHub branch protection or ruleset settings, pull request history, CI results (GitHub Actions), Terraform repositories, the emergency change process and its records.

Common mistakes. The one I see most: administrators allowed to bypass branch protection, and a senior engineer merging their own fix. Also self approved pull requests, direct pushes to main, console changes never captured in code, and emergency changes never reviewed afterwards. Small teams can still do peer review on every pull request.

> **Restaurant view:** A new recipe is written down, tasted by someone other than the cook, and approved by the head chef before it reaches the dining room.

CC9: Risk mitigation

What it means. Risks that come from outside your walls. CC9.1: business disruption, covered by a business continuity and disaster recovery plan, backups and insurance. CC9.2: vendors and business partners.

Two numbers matter for CC9.1. The **RTO**, recovery time objective, is how long you can be down. The **RPO**, recovery point objective, is how much data you can lose.

What auditors look for. An approved plan, a test inside the audit period and fixes for what the test found. A complete vendor list with tiering, due diligence before signing, yearly review of critical vendors' SOC 2 or ISO 27001 reports, and security terms in contracts.

Common evidence. The plan with its approval date, restore test records, the vendor inventory, vendor review notes, contracts and data processing agreements.

Common mistakes. A plan never tested. Promising one hour of recovery when a restore takes a day. A vendor list built from memory. Build it from data instead: compare the apps connected to your identity provider and the vendors finance pays with your list.

> **Restaurant view:** A backup generator and insurance for the night the power fails, and a health certificate from every supplier, checked again every year.

The optional categories

Availability (A1). Include it if you promised uptime. A1.1: watch capacity and add resources before you run out. A1.2: backups and recovery infrastructure. A1.3: test recovery and compare results with your RTO and RPO. Common exception: backups configured but never restored.

Confidentiality (C1). The most common addition for business software. C1.1: classify confidential data, know where it lives, limit access, encrypt it, bind people with NDAs. C1.2: delete it when promised and keep proof. Common exceptions: no proof of deletion after a customer left, and production data copied into staging.

Processing Integrity (PI1). Include it only when correct processing is the product. Five criteria follow one order's journey: specifications, input validation, processing, outputs, and keeping records. Typical control: a daily reconciliation that opens a ticket on any mismatch. Common exception: a reconciliation documented but never performed.

Privacy (P1 to P8). For companies that use personal information for their own purposes. It covers the privacy notice, choice and consent, collection, use and retention, access requests, disclosure to subprocessors and breach notification, data quality, and monitoring with a named privacy owner. SOC 2 Privacy is not GDPR: passing one never proves the other.

The trap. Confidentiality is about business secrets under agreement. Privacy is about people. Ask one question: is it about a person?

> **Restaurant view:** Availability is the opening hours on the door. Confidentiality is the secret recipes in the safe. Processing Integrity is getting every order right. Privacy is the reservation book.

Type 1 vs Type 2

	Type 1	Type 2
Tests	Design of controls	Design and operating effectiveness
Time covered	One point in time	An audit period, usually 3 to 12 months
Evidence	Settings and documents as they are	Samples from across the whole period
Typical use	First report, to unblock deals	What most customers ask for

Design asks: would this control work if people followed it? **Operating effectiveness** asks: was it followed every time? In a Type 2, one missed offboarding or one skipped quarterly review shows up in the report. Consistency beats a perfect first day.

The audit process and timeline

Every company and audit firm is different, so treat this as a typical sequence, not a schedule.

1. **Scope.** Choose the categories and the systems in scope, based on your real commitments to customers.
2. **Readiness and gaps.** Compare what you do with the criteria, write or fix policies, and close the gaps. This is usually the longest phase for a first audit.
3. **Choose an audit firm.** Talk to a few CPA firms, agree on scope and dates, and ask early about judgment calls like board oversight in a small company.
4. **Type 1 (optional).** A point in time report to show customers while the Type 2 period runs.
5. **Audit period.** Controls run and evidence builds up, usually for three to twelve months.
6. **Fieldwork.** The auditor requests populations, picks samples and tests them. Exceptions get a management response.
7. **Report.** The auditor's opinion, your system description, the controls and test results.
8. **Repeat.** A new period starts right after, usually every year.

> **Restaurant view:** Opening the restaurant takes the longest. After that, the health inspector comes back every year and looks at how you ran the place the whole time, not only on inspection day.

How compliance platforms help

Platforms like Vanta, Drata and Sprinto connect to your identity provider, cloud, code repositories, HR system and MDM. They run automated checks every day, track policy acknowledgements and training, hand the auditor ready-made populations, and collect evidence as you go.

What they automate well: MFA and encryption checks, policy acknowledgements, training tracking, branch protection checks, app discovery for your vendor list, review reminders.

What stays human: risk assessment discussions, board minutes, access review decisions, triage and incident response, restore tests, reading vendor reports, and deciding what to tell customers. A green dashboard is not a passed audit. Someone still has to read the red checks and act.

Glossary

Term	Meaning
AICPA	The US accounting body that owns the SOC 2 framework and the Trust Services Criteria.

Term	Meaning
Attestation report	A CPA firm's opinion on your controls. SOC 2 is a report, not a certificate.
Audit period	The months a Type 2 report covers, usually 3 to 12.
Carve out	Leaving a provider's controls out of your report because its own report covers them.
Common Criteria	CC1 to CC9, the Security category included in every SOC 2.
Complementary controls	Controls one party expects the other to run, listed in each SOC 2 report.
Control	Something you do on purpose to reduce a risk.
Control matrix	A table of your controls with owner, frequency, mapped criteria and evidence.
COSO	An internal control framework. Its principles are the basis of CC1 to CC5.
Deficiency	A control that is missing or not working.
Evidence	Proof that a control happened.
Exception	A sample where a control didn't work as described, written into the report.
Operating effectiveness	Whether a control ran as designed every time across the period.
Points of focus	Guidance that explains each criterion. Not a checklist.
Population	Every instance of a control in the period, for example every leaver.
RTO and RPO	How long you can be down, and how much data you can lose.
Sample	The items from a population the auditor picks to test.
Segregation of duties	No single person does risky work alone, like approving their own change.
Subservice organization	A vendor, like your cloud provider, whose controls support your system.
System description	Your written description of the services, infrastructure, people, data and boundaries in scope.

Next steps

Every section in this guide has a full lesson, with real examples and the restaurant story, in my free **SOC 2 Deep Dive** course on YouTube: watch the playlist. If you are preparing for your first audit and want to talk it through, book a free 30 minute call.