CHECKLIST

SOC 2 Readiness Checklist

The checks to finish before you call an auditor

How to use this checklist

This checklist is for IT, security and operations people at startups and SaaS companies preparing for their first SOC 2. Founders who keep getting security questionnaires from customers will find it useful too.

Work through it one area at a time. Each check describes something an auditor will ask to see, so for every item ask yourself one question: **can I show the proof today?** If the answer is "we do it, but there's no record," leave the box empty.

A SOC 2 Type 1 report checks that your controls are well designed on a single day. A Type 2 report checks that they actually ran, every time, across an audit period of usually three to twelve months, and it is the one most customers ask for.

	Type 1	Type 2
What it tests	Design of controls	Design and operation of controls
Time covered	One point in time	An audit period, usually 3 to 12 months
What the auditor samples	Settings and documents as they are today	Records from across the whole period
Good for	A first report to unblock deals	What most customers expect long term

> **Tip:** Two words you will hear a lot. A **control** is something you do on purpose to reduce a risk (for example, removing a leaver's access within one business day). **Evidence** is the proof it happened (the ticket, the log, the screenshot).

Scope and planning

- [ ] You have decided which Trust Services Categories are in scope. Security is always included. Add Availability, Confidentiality, Processing Integrity or Privacy only if you made matching promises to customers.
- [ ] You have a written list of in-scope systems: product, cloud accounts, databases, identity provider, code repositories and key SaaS tools.
- [ ] You have a data flow diagram that shows where customer data enters, where it is stored and where it leaves.
- [ ] Your customer commitments (uptime, security, deletion, confidentiality) are written down in one place, taken from contracts, your website and your security page.
- [ ] You have chosen a start date for the audit period, and every control will be running before that date.

Governance and policies

- [ ] A code of conduct exists, and every employee signs it at hire and again every year.
- [ ] A current, dated org chart is exported and saved, with a named security owner.
- [ ] Leadership or the board gets a security update at least once a year, with slides and minutes as evidence.
- [ ] Your core policies are written: information security, access control, change management, incident response, vendor management, data classification and retention, business continuity. (Most companies end up with ten to twenty.)
- [ ] Each policy has a named owner, an approval by management (not only by its author) and a review date within the last twelve months.
- [ ] Every number in your policies is one you can really meet: review frequencies, patching deadlines, offboarding times.
- [ ] A risk assessment has been done in the last twelve months: a dated risk register with likelihood, impact, owner and treatment for every risk, signed off by management. Fraud risk is named explicitly (for example, an admin abusing access or someone changing billing data).
- [ ] Each significant risk maps to at least one control in a control matrix.

> **Tip:** Auditors test exactly what your policy promises. I have seen a policy say "access reviews every quarter," and the team could only find two of the four. Nothing broke, but it became an exception in the report. Change the policy or change reality, before the audit period starts.

People and HR

- [ ] Your HR system (BambooHR, Rippling, HiBob or similar) is the single source of truth for joiners, leavers and contractors. Contractors are in it too, not only in a spreadsheet.
- [ ] Background checks are completed before start dates, where the law allows, with a record per person.
- [ ] Security awareness training is done at onboarding (for example, within thirty days) and then every year, with completion dates you can export.
- [ ] Every employee and contractor acknowledges the security policies at hire and when they change.
- [ ] Employees and contractors sign an NDA or confidentiality agreement at hire.
- [ ] Performance reviews happen on the schedule your policy states, you can export completed reviews, and a written disciplinary process exists for policy violations.
- [ ] Staff have a known way to report security concerns, including an anonymous option.

Access control

- [ ] Every person has a unique account, with no shared logins, and single sign-on through one identity provider (Google Workspace, Microsoft Entra ID, Okta or JumpCloud) covers in-scope tools.
- [ ] MFA is **enforced**, not just available, for the identity provider, cloud consoles and code repositories.
- [ ] No admin or cloud account sits outside SSO without a documented reason. Break glass accounts are listed, protected and monitored.
- [ ] Access is granted only after a dated approval, tracked in a ticket (Jira, Linear or your IT helpdesk).
- [ ] Access is granted through roles and groups, based on a written access matrix (role, systems, permission level).
- [ ] Leavers lose access to every system within the deadline in your policy (for example, one business day), with a ticket as proof.
- [ ] Access reviews of critical systems run on schedule (often quarterly), with reviewer, date, decisions and proof that flagged access was removed.
- [ ] Production access and encryption key management (AWS KMS, Google Cloud KMS) are limited to a small, named group.

> **Tip:** One of the most common exceptions I see is the contractor nobody offboarded. They were never in the HR system, so no offboarding ticket was created, and their cloud access stayed open for a month. If HR doesn't know about someone, neither does your offboarding process.

Endpoints and devices

- [ ] Every company laptop is enrolled in an MDM (Jamf, Kandji or Microsoft Intune), appears on a device inventory, and has screen lock and OS updates enforced.

- [ ] Disk encryption is enforced on every laptop: FileVault on Mac, BitLocker on Windows.
- [ ] Endpoint protection (CrowdStrike Falcon, SentinelOne or Microsoft Defender for Endpoint) runs on every laptop, and coverage matches the device list.
- [ ] Leavers return their laptop, with a return ticket and an MDM wipe record as proof. Old hardware gets a certificate of destruction or a documented secure wipe.

Infrastructure and change management

- [ ] Branch protection on the main branch blocks direct pushes and requires at least one approval from someone other than the author. It applies to administrators too.
- [ ] CI tests (GitHub Actions, GitLab CI or similar) must pass before a pull request can merge, and each change links to a ticket or states a clear reason.
- [ ] Development, staging and production are separate, and code reaches production only through the deployment pipeline.
- [ ] Infrastructure changes go through code (Terraform or similar) and pull requests, not console clicks.
- [ ] A written emergency change process exists, and every hotfix is reviewed within a day or two.
- [ ] No production customer data is copied into test or staging. Fake or masked data is used instead.
- [ ] Network rules keep databases off the internet, public endpoints sit behind a web application firewall where needed, and data is encrypted at rest and in transit (TLS everywhere, including between services).
- [ ] Vulnerability scanning runs on servers, containers and dependencies (Amazon Inspector, Nessus, Dependabot, Snyk or Trivy).
- [ ] A patching policy sets deadlines by severity (for example, critical in 7 days, high in 30), and you can show findings closed on time or a signed risk acceptance.
- [ ] A penetration test by an outside tester was done in the last twelve months, and findings have tickets and fixes.

Monitoring, logging and incident response

- [ ] Audit logs are on for your cloud accounts (AWS CloudTrail, Google Cloud Audit Logs), identity provider and GitHub, and they are sent to a central place (Datadog, Splunk, Elastic or a SIEM like Wazuh) and kept for the retention period in your policy.
- [ ] Alerts exist for events that should never happen: root account use, logging disabled, mass downloads, unusual admin logins.
- [ ] Uptime and performance monitoring pages someone on call (PagerDuty or Opsgenie).
- [ ] Failing checks from your compliance platform or cloud posture tool are reviewed weekly and turned into tickets with an owner and due date.
- [ ] An incident response plan is approved, with named roles, severity levels and rules for notifying customers.

- [ ] Security events are logged with a triage decision, even small ones (a reported phishing email, a lost encrypted laptop).
- [ ] A tabletop exercise was run in the last twelve months, with notes and follow-up actions.
- [ ] Incidents have a postmortem, and every action item has an owner, a due date and proof of closure.
- [ ] An internal audit or control self assessment has been done by someone who doesn't own the controls.

> **Tip:** Don't hide failing checks before the audit. A problem found on Tuesday and fixed on Wednesday, with a ticket, is great evidence that monitoring works. A year with zero issues looks like nobody was checking.

Vendors

- [ ] A complete vendor inventory exists, with owner, data touched and a risk tier for each vendor. It is built from data, not memory: apps connected to Google Workspace or Microsoft 365 sign-in, plus every vendor finance pays.
- [ ] Critical vendors were reviewed before signing, and their SOC 2 or ISO 27001 report is collected and read every year, including exceptions.
- [ ] Your cloud provider's SOC 2 report is reviewed yearly, with a short written note of the complementary controls they expect from you.
- [ ] Contracts with critical vendors include security, confidentiality and breach notification terms, plus a data processing agreement where personal data is involved.
- [ ] Offboarded vendors have their access removed and data deletion confirmed.

Backups and continuity

- [ ] Automated backups are on for databases and storage (AWS Backup, Amazon RDS snapshots, Cloud SQL backups, bucket versioning), encrypted, and stored in a separate account or region.
- [ ] Backup failures alert someone, and someone acts on them.
- [ ] A business continuity and disaster recovery plan is approved, with recovery time and recovery point objectives (how long you can be down, how much data you can lose).
- [ ] A real restore test was done in the last twelve months, timed and compared with your objectives, with tickets for anything that failed.
- [ ] Customer data is deleted at contract end according to your retention schedule, with a ticket and deletion log as proof.

Evidence and audit prep

- [ ] Every control has a named owner, a frequency and a known place where its evidence lives.

- [ ] For each recurring control you can pull a complete population: every joiner, leaver, change, access review or incident in the period.
- [ ] Reports used as evidence are documented: which system, which query, which filters, plus a screenshot.
- [ ] A compliance platform (Vanta, Drata or Sprinto) or an evidence folder is set up and connected to your identity, cloud, code and HR tools.
- [ ] A draft system description exists: services, infrastructure, people, data and the boundaries of the system.
- [ ] A readiness assessment or gap review is complete, and every gap has an owner and a fix date before the period starts.
- [ ] You have talked to two or three audit firms, agreed on scope and categories, and set dates for the audit period and fieldwork.

Next steps

If some boxes are still empty, that's normal. Each area is explained step by step in my free **SOC 2 Deep Dive** course on YouTube: watch the playlist. If you want a second opinion on your gaps, book a free 30 minute call.