

SOC 2 Readiness Checklist

Tick what is already true. The blanks are your gap list. Each line says why an auditor cares and what evidence they will accept, so you can tell the difference between a control you have and a control you can prove.

Updated September 2026. Written for B2B software companies preparing for a first SOC 2, usually because a customer's security review asked for one.

Before you start: five facts that shape everything else

- It is an attestation, not a certification.** A licensed CPA firm examines your controls against the AICPA Trust Services Criteria (the 2017 criteria, with the points of focus revised in 2022) and issues a report with its opinion. Buyers say "SOC 2 certified"; nobody issues a certificate.
- Security is the only required category.** The Common Criteria (CC1 to CC9) cover it. Availability, Confidentiality, Processing Integrity and Privacy are optional. Add one only when a customer contract commits you to it, because each adds controls and evidence for every period that follows.
- Type 1 or Type 2.** A Type 1 says your controls were designed properly on one date. A Type 2 says they operated over a period, usually 3 to 12 months. Most enterprise buyers want a Type 2. A Type 1 is a common first step when a deal needs something now.
- The observation window is the long pole.** A Type 2 cannot finish sooner than the window you pick, and the window cannot start until your controls actually run. Evidence has to exist for the whole period.
- You scope the system, not the company.** The report covers the product and infrastructure your customers rely on. A tight, honest scope is cheaper and easier to defend.

A realistic timeline for a small SaaS company

Stage	Typical duration	What happens
Readiness	6 to 12 weeks	Gap assessment, policies written and approved, missing controls built, evidence collection switched on.
Type 1 examination	2 to 6 weeks	The auditor tests design as of one date. Optional, but useful when a deal cannot wait.
Type 2 observation window	3 to 12 months	Controls run and produce evidence. First reports often use 3 to 6 months.
Fieldwork and report	4 to 8 weeks after the window	Sampling, walkthroughs, exceptions discussed, report drafted and issued.

1. Governance and risk (CC1 to CC3, CC5)

☐ A named owner for the security program, with time to do it

CC1 asks who is accountable. "The CTO, in theory" fails in practice because nobody runs the calendar.

Evidence: an org chart or role description naming the owner; board or leadership minutes that mention security at least quarterly.

☐ An information security policy set, approved and reviewed in the last 12 months

Policies are the design the auditor tests against. Unapproved drafts count as nothing.

Evidence: policies with version, owner, approval date and approver. The usual set: information security, acceptable use, access control, change management, incident response, business continuity and disaster recovery, vendor management, data classification and retention, encryption, secure development, and a code of conduct.

☐ Employees acknowledge the policies when they join and every year

A policy nobody has read is not operating. This is one of the first samples an auditor pulls.

Evidence: signed or clicked acknowledgements with dates, for a sample of hires across the window.

☐ A risk assessment done at least annually, with a risk register

CC3 requires you to identify risks, including fraud risk, and decide what to do about each. The register drives which controls you need.

Evidence: the register with likelihood, impact, owner, treatment and review date; the meeting or sign-off where it was reviewed.

☐ Background checks for new hires, where the law allows

CC1.4 covers competence and integrity. In Canada, criminal record checks need consent and should be proportionate to the role; many firms check only roles with production or customer data access.

Evidence: a policy stating who is checked, and completion records for sampled hires.

☐ Security awareness training at onboarding and annually

Phishing is still the most common way in. Auditors sample training completion across the window.

Evidence: completion reports with names and dates from your training tool.

2. Access control (CC6.1 to CC6.3, CC6.6)

☐ MFA on every system that touches production or customer data

Cloud console, identity provider, email, source code, CI/CD, databases and support tools. An auditor will ask for the setting, not your word.

Evidence: screenshots or exports of the MFA enforcement setting in each system, and the identity provider's user list showing enrolment.

☐ **Single sign-on where the tool supports it**

One place to remove access makes offboarding provable. Tools outside SSO become separate offboarding steps you must evidence.

Evidence: your system inventory marking which apps use SSO.

☐ **Documented onboarding and offboarding, with access removed within a set time**

Terminated users who kept access are the classic SOC 2 exception. Pick a target you can meet, commonly 24 hours or one business day, and meet it every time.

Evidence: a ticket per joiner and leaver showing the request, the approval and the date access was granted or removed, matched against HR dates.

☐ **Quarterly access reviews for production and sensitive systems**

Access drifts. A review proves someone looked and acted on what they found.

Evidence: the user list reviewed, the reviewer, the date and the changes made. A review that changed nothing, four times running, invites questions.

☐ **Least privilege, and no shared admin accounts**

Shared credentials make every action unattributable, which undermines logging, change management and incident response at once.

Evidence: role definitions; the admin list for each critical system; break-glass accounts documented and monitored.

☐ **Production access is limited and logged**

Who can touch customer data directly is the question every buyer's security team asks next.

Evidence: the list of people with production access and why; logs showing access is recorded.

3. Change management and secure development (CC8.1)

☐ **Every production change is reviewed and approved by someone other than the author**

This is the control auditors sample hardest. Branch protection makes it automatic rather than a habit.

Evidence: branch protection settings requiring review; a sample of pull requests with an approver who is not the author.

☐ **Changes are tested before release, and emergency changes are reviewed after**

Hotfixes happen. The control is that they are documented and reviewed within a set time, not that they never occur.

Evidence: CI test runs attached to changes; an emergency change log with after-the-fact approvals.

☐ **Infrastructure changes follow the same path as code**

Console clicks bypass review. Infrastructure as code, or a ticketed process, brings them into scope.

Evidence: Terraform or equivalent under review; or change tickets for console changes.

- ☐ **Secure development basics: dependency scanning and secrets kept out of code**
Not a named SOC 2 control on its own, but buyers ask, and it supports CC7.1 and CC8.1.
Evidence: scanner configuration and a sample of findings being fixed.
-

4. System operations and monitoring (CC7.1 to CC7.2)

- ☐ **Centralised logging with a set retention period**
You cannot investigate what you did not keep. Retention of at least 12 months is common and covers a full Type 2 window.
Evidence: log sources, retention settings, and who can delete logs (ideally nobody routinely).
 - ☐ **Alerts on the events that matter, and someone who answers them**
An alert that nobody triages is not a control. Start small: failed logins, privilege changes, root or owner account use, and security group changes.
Evidence: the alert rules, and tickets showing alerts were investigated.
 - ☐ **Vulnerability scanning on a schedule, with fix timelines by severity**
Auditors look for a defined remediation timeline and proof you meet it. A common pattern is critical within 7 to 15 days, high within 30, medium within 90.
Evidence: scan reports across the window; tickets showing findings closed within your stated timelines.
 - ☐ **An annual penetration test by a qualified independent tester**
SOC 2 does not name a pentest explicitly, but most auditors expect one and nearly every buyer questionnaire asks for the summary.
Evidence: the report or a letter of attestation, and remediation tickets for the findings.
 - ☐ **Encryption in transit and at rest, with key management described**
CC6.1 and CC6.7. Cloud defaults cover most of it, but you must show the setting and who controls the keys.
Evidence: TLS configuration, storage and database encryption settings, KMS key policies.
 - ☐ **Endpoint protection and device management for staff laptops**
Laptops hold credentials to everything. Auditors ask for disk encryption, screen lock and patching on company devices.
Evidence: MDM compliance report showing encryption and OS versions.
-

5. Incident response (CC7.3 to CC7.5)

☐ **A written incident response plan with named roles**

It must say who decides, who communicates and who fixes, and how you judge severity.

Evidence: the approved plan. Our Incident Response Plan Template in this set is a starting point.

☐ **The plan was tested in the last 12 months**

A tabletop exercise is enough. Auditors want to see that the plan was used, even in rehearsal.

Evidence: tabletop notes: date, scenario, attendees, what went wrong, and follow-up actions.

☐ **Real incidents are logged and closed with a root cause**

Having incidents is not a finding. Having no record of them is.

Evidence: an incident log with detection, response and lessons learned.

6. Vendors, availability and recovery (CC9, A1 if in scope)

☐ **A vendor inventory with a risk rating for each**

CC9.2 covers vendors and business partners. Your critical vendors are part of your control story.

Evidence: the register with data access, criticality and review date; the SOC 2 reports you collected for critical vendors, with notes on their complementary user entity controls (the controls they expect you to run).

☐ **Contracts with confidentiality and security terms for vendors handling customer data**

This is also a Canadian privacy requirement. PIPEDA holds you accountable for personal information you pass to a processor and expects contractual protection.

Evidence: DPAs or security terms for each critical vendor.

☐ **Backups run, and a restore was tested**

A backup never restored is a hope. Test at least annually and record the result and the time it took.

Evidence: backup configuration; a restore test record with date, scope and outcome.

☐ **A business continuity and disaster recovery plan, tested**

Required if Availability is in scope, and expected in practice regardless.

Evidence: the plan with recovery objectives (RTO and RPO) and a test record.

7. Evidence: the part teams underestimate

☐ Evidence is collected as the work happens, not rebuilt before the audit

Reconstructed evidence is slow to produce and easy to spot. Recurring controls (reviews, training, scans) need a calendar and an owner.

Evidence: a control calendar; a compliance platform or a disciplined shared folder with dated evidence per control.

☐ You know your population for each sampled control

Auditors sample from complete lists: all hires, all leavers, all changes, all incidents in the window. If you cannot produce the full list, sampling stalls.

Evidence: exportable lists from HR, the identity provider, source control and ticketing.

Common mistakes that cause exceptions or delays

- Scoping every system and every Trust Services Category on the first report.
- Starting the Type 2 window before the controls actually run, then finding months with no evidence.
- Policies that promise more than the team does. The auditor tests the policy as written.
- Offboarding that removes the SSO account but not the tools outside SSO.
- Access reviews that are signed off without anything being checked.
- Choosing an auditor on price alone, then discovering their timeline does not meet the deal date.

Canadian notes

- **PIPEDA.** You must report breaches of security safeguards that create a real risk of significant harm to the Office of the Privacy Commissioner, notify affected people, and keep a record of every breach for 24 months. Build this into your incident response plan.
- **Quebec Law 25.** If you hold personal information about Quebec residents: designate a person in charge of personal information, keep a confidentiality incident register, and assess privacy impacts before sending personal information outside Quebec.
- **Picking an auditor.** Canadian and US CPA firms both issue SOC 2 reports. Confirm the firm issues under AICPA standards, which is what US buyers expect, and ask how many SOC 2 reports it signs each year.

What to do next

1. Mark every box above as done, partly done or missing. Be strict: "partly" means it would not survive a sample.
2. Write down the date your first customer needs the report. Work backwards through the timeline table to see whether a Type 1 first makes sense.

3. Fix access, change management and evidence collection first. They carry the most samples and cannot be backfilled.
4. Start the observation window only once every recurring control has run at least once.
5. Ask two or three audit firms for quotes against the same written scope, so the prices are comparable.

Want a second pair of eyes? TrazTech runs security and compliance readiness as fixed-scope work for software companies. We prepare you for the audit; an independent CPA firm examines you and signs the report. Book a free 30-minute readiness call at traztech.ca/free-readiness-call, or get The Compliance Brief, one short email every Tuesday, at traztech.ca/brief.

© 2026 TrazTech Inc. · traztech.ca · Prepared by Jacob Masse, Principal. A starting point, not legal or audit advice.