

SOC 2 Readiness Checklist

26 questions across the 10 areas auditors review, for SOC 2 Type 1 and Type 2. Tick one box per question, then score yourself on the last page.

Prefer it online? Take the checklist

Our team previously worked at

Apple · Google · Microsoft · Tesla · Visa · Robinhood · Brex · NSA

Be strict with Yes

Only tick Yes if it's in place today and you could show proof. Tick Partially if it's started or inconsistent.

Watch the key controls

The 8 questions marked **Key** count double. A No on any of them can hold up an audit on its own.

Line up the evidence

Each area lists what auditors ask to see. They test evidence, not intent.

01

Access control

Who can get into what, and how you prove it.

		Yes	Partially	No
1	Is multi-factor authentication (MFA) turned on for every work tool, including email, cloud (AWS/GCP/Azure), GitHub, Slack, and your password manager? Key	☐	☐	☐
2	Does each person only have the access they need for their job? That means no shared admin logins, and production access limited to a few people.	☐	☐	☐
3	Do you review who has access to your key systems at least every quarter, and keep a record of each review?	☐	☐	☐
4	When someone leaves, is all their access removed within a day or so, following a checklist? Key	☐	☐	☐

What auditors ask for

An export of users and roles for each key system, your MFA settings, your last quarterly access review with sign-off, and offboarding tickets showing when each person's access was removed.

SOC 2 criteria CC6.1–CC6.3

02

Security policies

The written rules your audit is measured against.

		Yes	Partially	No
5	Do you have written security policies (for example information security, acceptable use, access control) that leadership has formally approved? Key	☐	☐	☐

		Yes	Partially	No
6	Has every employee read and acknowledged those policies, with a record you can show?	☐	☐	☐

What auditors ask for

Approved policy documents with version history and approval dates, and a signed acknowledgment from each employee.

SOC 2 criteria CC2.2, CC5.3

03 HR and training

How you vet, bind, and train the people with access.

		Yes	Partially	No
7	Do you run background checks on new hires, where the law allows?	☐	☐	☐
8	Does everyone sign a confidentiality agreement when they join?	☐	☐	☐
9	Does everyone complete security awareness training when they join and at least once a year?	☐	☐	☐

What auditors ask for

Background check confirmations, signed confidentiality agreements, and security training completion records for a sample of employees.

SOC 2 criteria CC1.1, CC1.4, CC2.2

04 Infrastructure and endpoints

How your data and devices are protected.

		Yes	Partially	No
10	Is customer data encrypted at rest, including databases, file storage, and backups?	☐	☐	☐
11	Is all data encrypted in transit, with HTTPS everywhere, including internal services and APIs?	☐	☐	☐
12	Are company laptops managed with a device management (MDM) tool that enforces disk encryption, screen lock, and updates?	☐	☐	☐
13	Do you scan for vulnerabilities and patch them on a regular schedule?	☐	☐	☐

What auditors ask for

Encryption settings for databases, storage, and backups, your TLS configuration, an MDM report covering every laptop, and recent vulnerability scans with the fixes that followed.

SOC 2 criteria CC6.1, CC6.7, CC6.8, CC7.1

05 Change management

How code gets from a laptop to production.

		Yes	Partially	No
14	Does every code change get reviewed and approved by someone other than the author before it reaches production? Key	☐	☐	☐
15	Do you have separate environments for development/testing and production, with no real customer data used in testing?	☐	☐	☐
16	Are production deployments traceable, so you can see who deployed what, and when?	☐	☐	☐

What auditors ask for

A sample of production changes, each with its pull request, an approval from someone other than the author, and the matching deployment record.

SOC 2 criteria CC8.1

06

Logging and monitoring

Whether you'd know if something went wrong.

		Yes	Partially	No
17	Are logs from your app, cloud, and identity provider collected in one central place and kept for a set period? Key	☐	☐	☐
18	Do you get alerts for important events (unusual logins, admin changes, outages), with a named person responsible for responding?	☐	☐	☐

What auditors ask for

Log retention settings, your alert rules and who receives them, and examples of alerts that were investigated.

SOC 2 criteria CC7.2

07

Incident response

What happens on your worst day.

		Yes	Partially	No
19	Do you have a written incident response plan that says who does what, and when to tell customers? Key	☐	☐	☐
20	Have you tested that plan (for example with a tabletop exercise) in the last 12 months?	☐	☐	☐

What auditors ask for

Your incident response plan, notes from your last tabletop exercise, and records of any real incidents and how they were handled.

SOC 2 criteria CC7.3–CC7.5

08

Vendor management

The tools and companies you share data with.

		Yes	Partially	No
21	Do you keep an up-to-date list of vendors that handle your company or customer data?	☐	☐	☐
22	Do you review the security of key vendors (for example their SOC 2 report) before signing and about once a year?	☐	☐	☐

What auditors ask for

Your vendor list with a risk rating for each, and the security reviews (such as SOC 2 reports) you collected for key vendors.

SOC 2 criteria CC9.2

09

Risk assessment

How you decide what to worry about.

		Yes	Partially	No
23	Have you done a formal risk assessment in the last 12 months that covers what could go wrong, how likely it is, and what you're doing about it? Key	☐	☐	☐

		Yes	Partially	No
24	Is one person clearly responsible for security and compliance, and does leadership review security at least once a year?	☐	☐	☐

What auditors ask for

Your risk register with likelihood, impact, and an owner for each risk, the date it was last reviewed, and notes from leadership's security review.

SOC 2 criteria CC3.1–CC3.4

10 Backups and business continuity

Whether you can recover when things break.

		Yes	Partially	No
25	Are backups automatic, and have you actually restored from one in the last 12 months to prove it works? Key	☐	☐	☐
26	Do you have a written plan for keeping the business running if a key system, cloud region, or vendor goes down?	☐	☐	☐

What auditors ask for

Backup schedules and retention settings, a record of your last restore test, and your business continuity plan.

SOC 2 criteria CC7.5, CC9.1, A1.2–A1.3

Score yourself

Yes is 1 point, Partially is ½, No is 0. Key controls count double. The most you can score is 34.

Your points

_____ / 34

Readiness (points ÷ 34)

_____ %

Key controls answered No

Under 50%: Early stage

Start with the key controls: MFA, written policies, and a risk assessment.

50 to 79%: Getting close

Close the specific gaps and get evidence ready for what you already do.

80% and up: Audit ready

As long as no key control is a No. Next, line up evidence for each control.

Your buyer wants SOC 2. We can get you there.

YSecurity is the on-demand cybersecurity team for startups. Book a free 15-minute call and we'll turn your gaps into a plan with a realistic audit timeline.

[Book a free 15-min call](#)

[Take the online checklist](#)

This is a self-assessment based on common SOC 2 audit areas. It isn't an audit and doesn't predict an audit outcome. Questions? Email hello@ysecurity.io.