IMPACT
RISK ADVISOR

SOC 2 FAQ – Impact Risk Advisors

www.impactriskadvisor.com

1. Do I need SOC 2 if I don’t handle sensitive customer data?

You might. SOC 2 isn’t just about PII — it covers how you manage system security, availability, processing integrity, confidentiality, and privacy. Many customers ask for it regardless of whether you handle sensitive data.

2. What are Trust Services Criteria, and which ones do I need?

There are 5:
1. Security (required)
2. Availability
3. Processing Integrity
4. Confidentiality
5. Privacy
You can choose only Security, which is standard for most startups. Others are optional depending on your services.

3. What’s the difference between Type 1 and Type 2 again?

Type 1 = Snapshot in time: 'Do your controls exist?'
Type 2 = Operating over time: 'Do your controls work in practice?' over 3–12 months.

4. Can I go straight to a Type 2, or do I need a Type 1 first?

You can go straight to a Type 2. Type 1 is optional but helpful if you want a “quick win” while building your compliance program. Some clients will accept a Type 1 as proof of intent.

5. Do I need a readiness assessment?

It’s not required, but it’s highly recommended — especially if this is your first audit. A readiness assessment helps you identify gaps, fix them, and avoid surprises when the actual audit starts.

6. Do I need to include privacy, or can I do security only?

You can absolutely choose Security only. That’s the most common choice. The other Trust Services Criteria are optional and based on your services.

7. Do I need a separate Incident Response or DR Plan if I already have an InfoSec Policy?

Yes. While your InfoSec Policy can include summaries, auditors usually expect standalone Incident Response and Disaster Recovery/BCP Plans with clear steps, roles, and timelines.

8. If I use a GRC tool, do I still need help from an expert?

Yes. GRC tools (like Vanta, Drata, Tugboat, etc.) are great for automation, but they don’t know your business. You'll still need someone who understands SOC 2 to:

- Set the right scope
- Customize policies
- Interpret evidence expectations
- Guide remediation

9. Who can issue a SOC 2 report?

Only a licensed CPA firm can issue a SOC 2 report. Look for firms that specialize in SOC 2 and are listed with the AICPA. Readiness assessments, however, can be done by consultants or advisory firms (like us).

10. Can I do SOC 2 myself?

Technically yes — but practically, it’s a heavy lift. Most companies bring in outside help at least for the readiness phase, scoping, or policy work. Compliance can be built internally, but audit prep usually requires expert guidance.

11. How long does SOC 2 take?

Readiness: 2–3 months (depending on your maturity)
Audit period for Type 2: 3–12 months of evidence collection
Audit + report writing: 1–2 months
You can typically complete the whole process in 6–9 months if you start organized.

12. What’s in scope for SOC 2?

Only what you decide. Common scoping items include:

- Cloud infrastructure (MS 365, AWS, GCP)
- Applications you build or support
- End-user devices
- Data flows and integrations

A readiness assessment helps you define this cleanly.

13. What do auditors look for?

They look for:
- Written policies and evidence they’re followed
- Security practices (MFA, backups, logging, etc.)
- Employee access and termination procedures
- Vendor management
- Risk and incident management
- Supporting documentation or logs

14. Can a solo founder pass a SOC 2 audit?

Yes — we’ve helped solo teams do it. It’s all about having controls, not headcount. Just make sure your responsibilities are documented and you have supporting evidence for each control.

15. Is a SOC 2 report public?

No. Your SOC 2 report is a private deliverable that you share selectively with prospects, partners, or clients under NDA or access control.

For more support, visit Impact Risk Advisors