What Enterprise Buyers Really Mean When They Ask About SOC 2

Enterprise buyers don't ask "Do you have SOC 2?" just to tick a box.

They're trying to answer a deeper question:

"Can we trust you with our data without creating a career-limiting mistake?"

This guide breaks down what they're really looking for—and how to respond whether you're pre-SOC 2, in progress, or already audited.

1. What "Do you have SOC 2?" is actually asking

When a prospect asks about SOC 2 (or ISO 27001), they're usually trying to understand:

1. Do you have a real security program, or just good intentions?
    - Are there documented policies, processes, and owners?
    - Or is everything tribal knowledge in Slack and people's heads?
2. Will you create work or risk for them internally?
    - Will their security team have to chase you for evidence?
    - Can they defend choosing you to their own auditors, regulators, and board?
3. Are you going to slow down their roadmap?
    - If they integrate you, will security issues pop up later and block launches?
    - Are you likely to surprise them with "We don't do that yet" at the worst time?

SOC 2 is shorthand for:

"Show me that you run your systems in a disciplined, repeatable way—and that you can prove it."

2. How buyers think about SOC 2 (even if they don't say it)

Most enterprise buyers fall into one of three camps:

Camp 1 – "SOC 2 is mandatory"

- Regulated industries (healthcare, finance, some EU/UK orgs)
- Internal policy literally says "SOC 2 Type II or ISO 27001 required"

Here, no report = very high friction. Deals can still happen, but they'll demand strong compensating evidence and a clear plan.

Camp 2 – "SOC 2 is the default proof"

- They don't have a written rule, but:
    - Their security team is overloaded
    - SOC 2 is the easiest way to say "we did our diligence"

Here, SOC 2 is a shortcut to yes. Without it, they need more time and more evidence.

Camp 3 – "SOC 2 is a proxy for maturity"

- Smaller enterprises or fast-moving teams
- They care more about your actual practices than the logo on the report

Here, a thoughtful explanation of your program can go a long way—even if you're pre-SOC 2.

3. How to respond if you're...

A. Pre-SOC 2 (no audit yet)

The worst answer is: "No, we don't have SOC 2."

The best answer is: "Here's what we do instead, and here's our plan."

You want to show:

- You have core controls in place (access control, backups, incident response, vendor risk).
- You have Minimum Viable Evidence (MVE): a small, organized set of proof.
- You have a roadmap toward SOC 2 or ISO, with realistic dates.

Example response:

"We don't have a SOC 2 report yet.

What we do have is a documented security program: access control, change management, incident response, and vendor risk processes, plus regular backups and monitoring.

We maintain a core evidence pack (policies, diagrams, risk register, and key logs) that we can share under NDA, and we're planning a SOC 2 Type II audit in [quarter/year]. I'm happy to walk your security team through our current controls and roadmap."

B. In progress (working toward SOC 2)

Focus on timeline, scope, and what's already real:

- Which Trust Services Criteria are in scope
- Which systems are included
- Where you are in the audit process (design vs operating effectiveness)

Example response:

"We're currently in a SOC 2 Type II readiness/audit cycle with [auditor].

The audit covers our core SaaS platform and supporting infrastructure.

We've already implemented the required controls and are operating them; the audit period runs through [date], and we expect the report by [quarter/year]. In the meantime, we can provide our control matrix, key policies, and evidence samples under NDA."

C. Post-SOC 2 (you have a report)

They're still not just asking for the PDF. They want to know:

- Does the scope match what they'll actually use?
- Do you understand your own controls, or are you just forwarding a report?

Example response:

"Yes—we have a current SOC 2 Type II report covering our core SaaS platform and supporting services.

We can share the report and our bridge letter under NDA. I'm also happy to walk your team through the scope, key controls, and how we handle incidents, vendor risk, and customer data in practice."

4. What to have ready before the question comes

Whether or not you have SOC 2 today, enterprise buyers expect you to be prepared.

At minimum, have:

1. A short "Security & Privacy Overview"
    - 1–2 pages or slides: architecture, key controls, incident response, vendor risk, data handling.
2. A Minimum Viable Evidence (MVE) pack
    - Core policies (information security, access control, incident response, vendor risk)
    - High-level architecture diagram
    - Sample logs or screenshots (access reviews, backups, monitoring)
    - Risk register or summary of key risks and mitigations
3. A simple roadmap
    - Where you are now
    - What you're doing in the next 6–12 months (e.g., SOC 2 readiness, ISO 27001, privacy program build-out)

This doesn't replace SOC 2—but it shows you're serious, organized, and not starting from zero.

5. When to bring in help

You might need outside help if:

- Security questionnaires are slowing deals down.
- Different people at your company are giving different answers to the same questions.
- You've been "planning SOC 2" for a year with no real progress.
- You're adding AI features and buyers are now asking about AI risk on top of SOC 2 and privacy.

That's exactly where Lodestone works: turning "we know we should do something about this" into a concrete program and evidence pack that supports sales instead of blocking it.

6. A simple next step

If you're getting more SOC 2 questions than you're comfortable with, start small:

- Inventory what you already have (policies, controls, evidence).
- Identify the 3–5 biggest gaps that would make buyers nervous.
- Build a Minimum Viable Evidence pack you can share under NDA.

From there, you can decide whether a full SOC 2/ISO program is the right next move—or whether right-sized controls and documentation are enough for your current stage.