FOUNDERS

SOC 2 for Your First Enterprise Deal

A practical walkthrough of what founders and growing teams should actually focus on for SOC 2, and what can safely wait.

Cyberneza LLC | Veteran-Owned | Orlando, FL
cyberneza.com | info@cyberneza.com

Ready to get started?
Book a free 15-minute readiness call:
calendly.com/larry-cyberneza

Why Enterprise Buyers Ask for SOC 2

Enterprise procurement teams are not trying to make your life difficult. They have their own compliance obligations. When they bring on a new vendor, they need to demonstrate to their auditors and stakeholders that they performed reasonable due diligence on third-party risk.

A SOC 2 report is one of the most widely accepted ways to do that in the U.S. market. It tells the buyer: "An independent auditor looked at our security controls and confirmed they're working."

What the buyer is really asking

- Can we trust you with our data?
- Do you have documented, repeatable security practices?
- Will our auditors accept you as a vendor?
- Are we taking on risk by working with you?

SOC 2 answers all four of these questions with evidence, not just promises.

How SOC 2 Impacts Your Sales Timeline

The biggest misconception founders have is that SOC 2 is a one-time project you complete and forget about. In reality, it becomes part of how you sell.

Without SOC 2

- Security reviews drag on for weeks or months
- You answer the same questionnaire differently each time
- Prospects ask for compensating controls or risk exceptions
- Legal gets involved, adding more friction and delay
- Some deals stall entirely or go to a competitor who has SOC 2

With SOC 2

- You send the report and most security questions are answered immediately
- Questionnaire responses are consistent because they reference your controls
- Procurement teams can check the box and move forward
- Deal velocity increases, especially in mid-market and enterprise
- You signal maturity before the conversation even starts

What Auditors Actually Look For

Auditors are not expecting perfection. They are looking for evidence that you have intentional, documented controls and that your team follows them in practice.

The essentials

- Access control — Who can access what, and how do you manage that?
- Change management — How do code and infrastructure changes get reviewed and deployed?
- Incident response — What happens when something goes wrong?
- Monitoring — How do you detect issues and unusual activity?
- Risk assessment — Have you identified your key risks and how you address them?
- Vendor management — How do you evaluate the third parties you rely on?

What customers usually ask about

- Encryption — Is data encrypted in transit and at rest?
- Multi-factor authentication — Is MFA required for production systems?
- Backups and recovery — Can you recover from data loss?
- Employee security training — Does your team know the basics?
- Data retention and deletion — Can you delete their data when asked?
- Subprocessors — Who else touches their data?

There is significant overlap between these two lists. Building your SOC 2 program well means you answer customer questions almost automatically.

What to Focus on First

You do not need to build a Fortune 500 security program overnight. Here is a practical priority list for early-stage and growth-stage teams:

1. Enable MFA everywhere — Production systems, cloud accounts, code repositories, and email. This is the single highest-impact control.
2. Document your access control process — Who approves access? How do you remove it when someone leaves? Write it down and follow it.
3. Set up code review — Require pull request reviews before merging to production. Most teams already do this; make sure it is enforced, not optional.
4. Write an incident response plan — Cover: how you detect issues, who responds, how you communicate, and how you do a post-mortem.
5. Enable logging and monitoring — Turn on audit logs in your cloud provider and key SaaS tools. Set up basic alerts for suspicious activity.
6. Conduct a risk assessment — List your most important assets, the threats to them, and what you are doing about each one. Update it at least annually.

What Can Safely Wait

Founders often over-build their compliance program because they are not sure what is required versus nice to have. These are valuable but can come later:

- Formal security operations center (SOC) — Basic alerting and a documented response process is sufficient. You do not need 24/7 monitoring.
- Penetration testing — Valuable, but not required for SOC 2 Type I. Plan for it before your Type II audit period.
- GRC platform — Tools like Vanta are helpful, but you can start with spreadsheets and docs if budget is tight.
- ISO 27001 — If your market is U.S.-focused, SOC 2 is the right first step. Plan ISO later when international customers require it.
- Advanced privacy controls — Unless your product handles sensitive personal data, the Privacy Trust Services Category can wait.

Type I vs. Type II: Which One First?

SOC 2 Type I

- Point-in-time snapshot of your controls
- Faster to achieve (2–3 months typical)
- Proves controls are designed and in place
- Good enough for many early enterprise deals
- Lower cost and effort to get started

SOC 2 Type II

- Covers a 3–12 month observation period
- Proves controls are operating effectively over time
- Required by most enterprise customers eventually
- More credible and comprehensive
- Plan for this after Type I is complete

Our recommendation: Start with Type I to unblock deals now, then begin your Type II observation period immediately after. Many auditors can run them back-to-back so you have a Type II report within 6–9 months of starting.

How to Prepare Without Overbuilding

Right-size your scope

SOC 2 does not require you to audit your entire company. Scope it to the systems and processes that handle customer data.

- Start with Security (required) — add other Trust Services Categories only if customers ask
- Include only production systems and the teams that support them
- Exclude internal tools, marketing systems, and anything that does not touch customer data

Build for repeatability

SOC 2 is not a one-time project. You will audit annually. Every control you build should be something your team can sustain without heroic effort.

- Automate evidence collection where possible (Vanta, cloud-native tools)
- Write policies that reflect what you actually do, not aspirational goals
- Assign control owners so nothing falls through the cracks
- Schedule quarterly reviews to catch drift before your next audit

Common Mistakes Founders Make

- Waiting until a deal is on the line — SOC 2 takes months, not days. Start before you need it.
- Copying someone else's policies — Auditors can tell. Write policies that match your actual environment.
- Over-scoping — Including every system and Trust Services Category makes the audit longer and more expensive.
- Treating it as an engineering project — SOC 2 touches HR, operations, and leadership. It is a company effort.
- Skipping the readiness assessment — A gap analysis before the audit saves time and prevents surprises.

Ready to get SOC 2 done right?

A short conversation can help you figure out the fastest path to a SOC 2 report that fits your team and stage.

calendly.com/larry-cyberneza