SOC 2 Readiness

What Nobody Tells You Before You Start

A Practical Guide From People Who Have Led Compliance Programs at Scale

---

A Valukoda Whitepaper

valukoda.com | 888.380.7212

Let's Talk About Why You're Reading This

You are probably reading this because a customer asked for your SOC 2 report and you did not have one. Or because your sales team lost a deal when the prospect's security questionnaire came back and the honest answers were uncomfortable. Or because your board or investors said "you need SOC 2" and you nodded while quietly wondering what that actually involves.

All of those are legitimate reasons to pursue SOC 2 attestation. But before you engage a consultant, hire a GRC platform, or start Googling "SOC 2 in 30 days," you need to understand something that most SOC 2 guides will not tell you:

> *SOC 2 is not a certification you achieve. It is an attestation that your controls are designed properly and operating effectively over a period of time. That distinction matters because it means you cannot cram for this. You need a genuine control environment that functions consistently, not a paper exercise that looks good during audit week.*

This guide provides a practical roadmap based on what we have seen work across multiple SOC 2 engagements, and equally important, what we have seen fail. We are not going to give you a checklist of 200 controls you can download from the AICPA website. We are going to tell you what actually matters, what trips companies up, and where your money is best spent.

Before You Start: Decisions That Shape Everything

Type I vs. Type II: Make the Right Call

SOC 2 Type I evaluates whether your controls are designed properly at a specific point in time. Type II evaluates whether they operated effectively over a period, typically six to twelve months. Most guidance says "start with Type I, then move to Type II." That advice is often wrong.

Here is why: Sophisticated buyers (the enterprise clients you are trying to win) know the difference. A Type I report tells them you had controls in place on one specific day. A Type II report tells them those controls actually worked, consistently, for months. When an enterprise procurement team reviews your SOC 2 report, a Type I from a company that has been operating for years raises more questions than it answers. Why only Type I? What are you hiding about your operational track record?

The exception: if you are a startup with less than a year of operating history, Type I makes sense as a bridge. You cannot demonstrate twelve months of operating effectiveness when you have only existed for eight months. In that case, Type I is credible. For everyone else, target Type II from the start and build the control evidence along the way.

Scoping: The Decision That Controls Your Budget

The single biggest cost driver in SOC 2 is scope. Every system, application, and process you include is a system, application, and process you need to document, control, monitor, and provide evidence for. Scope everything and you will spend twice as much and take twice as long. Scope too narrowly and sophisticated buyers will notice the gaps.

The right approach is to scope the services your customers actually care about. If you are a SaaS company, your production environment and the data pipeline that feeds it are in scope. Your internal HR system probably is not, unless it directly affects how customer data is handled.

A mistake we see repeatedly: companies include their entire AWS environment when only three of their fourteen accounts touch customer data. That turns a manageable audit into an expensive one, and it does not provide your customers with meaningfully better assurance.

Trust Services Criteria: You Probably Only Need Two

SOC 2 is built around five Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. Security (Common Criteria) is required for every SOC 2 report. The other four are optional.

Most companies should start with Security and Availability. Security covers the controls your customers care most about: access management, incident response, change management, risk assessment, and monitoring. Availability covers uptime commitments, disaster recovery, and business continuity, which your customers also care about because they depend on your service being operational.

Adding Processing Integrity, Confidentiality, or Privacy is not wrong, but it expands scope, cost, and audit complexity. Add them when your customers require them, not because your consultant recommended the “comprehensive” package.

The Actual Work: What Auditors Look For

SOC 2 consultants love to talk about control frameworks and policy templates. Here is what your auditor actually evaluates, and where companies actually fail:

Access Management: Where 60% of Findings Come From

Access control findings dominate SOC 2 reports, and the reason is simple: access management requires ongoing discipline, not one-time configuration. Your auditor is going to pull a population of user accounts and test whether each one follows your stated policy. They are going to check:

Are terminated employees deprovisioned within your stated SLA? Not "within a few days." It means within whatever specific timeframe your policy states. If your policy says 24 hours and it took 72 hours for three out of fifty terminations, that is a finding.

Are access reviews happening on schedule? If your policy says quarterly, they will ask for evidence of Q1, Q2, Q3, and Q4 reviews. A single missed quarter is a finding. And "we did it but did not document it" is not a defense.

Is the principle of least privilege enforced? Your auditor will look at administrator accounts and ask why twelve people have root access to production when only three of them are in operations roles.

> *The fix is not technical. It is operational. You need a process, not a tool. A process that runs on schedule, produces evidence automatically, and triggers alerts when it does not. The companies that fail access management controls are not the ones with bad technology. They are the ones with inconsistent execution.*

Change Management: The Control Developers Hate

Your development team ships code fast. They deploy multiple times per day. They use feature flags, blue-green deployments, and automated testing. They are going to hate change management controls.

Here is the reality: your auditor does not care about your deployment velocity. They care that every change to production was authorized, tested, and documented. That does not mean you need a change advisory board meeting for every deployment. It means you need a process that produces evidence of approval, testing, and deployment for every change, and that process needs to be automated enough that your developers follow it consistently.

What works: Pull request approvals as your authorization evidence. Required CI/CD pipeline stages as your testing evidence. Deployment logs with user attribution as your implementation evidence. This maps to how your team already works and produces audit evidence automatically.

What fails: A change management policy written for a waterfall methodology applied to an agile team. Nobody follows it, so there is no evidence, and the auditor finds a control failure.

Incident Response: You Need to Have Actually Done It

Your auditor will ask for your incident response plan. They will also ask for evidence that you have tested it. A tabletop exercise, a simulated incident, a documented response to an actual event. Something that demonstrates the plan is not just a document on a SharePoint site.

Companies that have been through real security incidents have a significant advantage here, because they have actual evidence of their response process. Companies that have never had an incident need to

manufacture this evidence through realistic tabletop exercises that test their plan against plausible scenarios.

The scenario matters: "What if a developer's laptop is stolen" is a reasonable tabletop. "What if we are hit by a nation-state APT" is not, unless you are actually in a sector targeted by nation-states. Auditors and customers can tell when your exercise was realistic versus theatrical.

Vendor Management: The Quiet Time Bomb

If you use AWS, Azure, or GCP, you inherit some of their controls. If you use Stripe for payments, Twilio for messaging, or any third-party service that touches customer data, those vendors are subservice organizations that your auditor needs to evaluate.

The most common failure mode: companies cannot produce a current SOC 2 report for a critical vendor. Or they can produce the report but have never actually reviewed it for relevant findings. Your auditor will ask: "Have you reviewed your subservice organization's SOC 2 report, and what complementary user entity controls are you required to implement?" If you do not know what complementary user entity controls are, you have homework to do.

Realistic Timelines

The SOC 2 industry is full of promises about speed. "SOC 2 in 30 days!" "Automated compliance!" Here is reality:

Scenario	Timeline	What This Assumes
Best Case	**3–4 months**	Strong existing security practices. Documented policies already in place. Dedicated internal owner with authority. Type I only.
Typical	**6–9 months**	Good security hygiene but limited documentation. Need to build policies and evidence collection. Some control gaps to remediate. Type II observation period required.
Challenging	**12+ months**	Significant gaps in security fundamentals. No existing policies. Limited internal bandwidth. Multiple control remediation projects. Type II with observation window.

The "30-day SOC 2" vendors are selling you a Type I report with a narrow scope and templated policies. It will check the box for unsophisticated buyers. It will not hold up to scrutiny from an enterprise

customer who has reviewed hundreds of SOC 2 reports and knows what a real program looks like versus a paper exercise.

The GRC Platform Question

You are going to be pitched compliance automation platforms: Vanta, Drata, Secureframe, Sprinto, and others. These platforms can genuinely help by automating evidence collection, tracking control effectiveness, and streamlining audit preparation.

But they are not magic. A GRC platform automates the collection and organization of evidence. It does not create the controls that produce the evidence. If your access reviews are not happening, a platform will helpfully show you a red dashboard widget confirming that your access reviews are not happening. That is useful, but it is not the same as fixing the problem.

> *Think of a GRC platform as a dashboard for your car, not the engine. It tells you how fast you are going, whether the engine is overheating, and when you are low on fuel. But it does not drive the car. You still need someone who knows the road.*

Our recommendation: a GRC platform is worth the investment if you have someone internally who owns the compliance program and uses the platform as their operational tool. If you are hoping the platform will replace that person, you are going to be disappointed.

Where Companies Actually Fail

After supporting multiple SOC 2 engagements, we see the same failure patterns:

They Treat It as a Project, Not a Program

SOC 2 is not something you “finish.” Type II reports cover a specific observation period, and your customers will expect a current report every year. The controls you build need to operate indefinitely. If you staff this as a project with an end date, you will scramble every year when audit season arrives.

They Write Policies Nobody Follows

Your auditor will test whether employees follow your policies, not just whether the policies exist. If your password policy requires 14-character passwords with complexity requirements, your auditor will check your identity provider configuration. If your incident response policy says you classify incidents within one hour, your auditor will review your incident log for evidence. Write policies that describe what you actually do, not what you aspire to do.

They Ignore the Observation Period

For Type II, your auditor evaluates controls over a continuous period, typically six to twelve months. If you implement a control in month three and your observation period started in month one, those first two months are a gap. Plan your control implementation timeline so everything is operational before the observation period begins.

They Pick the Wrong Auditor

Not all audit firms are equal. A top-tier firm's SOC 2 report carries more weight with enterprise customers than a report from a firm nobody has heard of. But top-tier firms are also more rigorous and more expensive. The right choice depends on who your customers are and how closely they scrutinize audit reports.

A Smarter Approach

Based on what we have seen succeed:

Month 1–2: Scope definition, gap assessment, auditor selection. Invest the time to get scope right because it determines everything else. Commission or conduct a gap assessment against the Trust Services Criteria you plan to include. Select your auditor early so they can provide input on your approach.

Month 3–5: Policy development, control implementation, evidence collection setup. Write policies that match your actual operations. Implement controls for any gaps identified in the assessment. Set up automated evidence collection wherever possible. Manual evidence collection is the single biggest ongoing cost of SOC 2 compliance.

Month 6–11: Observation period (Type II). Your controls operate. Your evidence accumulates. You conduct your access reviews on schedule. You run your tabletop exercise. You review your vendors' SOC 2 reports. You document everything.

Month 12: Audit. If you have done the work, the audit is a validation exercise, not a discovery exercise. Your auditor should find what they expect to find, because you have been operating consistently.

About Valukoda

Valukoda provides IT consulting and managed services with True CIO™ and True CISO™ executive leadership. Our leaders have built and maintained compliance programs at major financial services organizations under regulatory scrutiny from the SEC, FINRA, OCC, and state regulators. We apply that real-world compliance experience to growing companies navigating SOC 2 for the first time or improving an existing program.

valukoda.com