DRUMMOND

THE SOC 2 TYPE 2

READINESS PLAYBOOK:

How to Avoid Audit Surprises



SOC 2 Type 2

Preparing for a SOC 2 Type 2 audit can feel like gearing up for a marathon. Though there are five Trust Service Criteria, Security is the mandatory "common criteria" in every SOC 2 audit, so getting it right is not just important; it is foundational.

This six-step checklist is built to streamline your preparation, eliminate guesswork, and give your team the clarity and control needed to approach the audit with confidence. It focuses squarely on the core security requirements, leaving out the optional criteria like ***Availability, Confidentiality, Processing Integrity,*** and ***Privacy*** to keep the process clear and actionable. The goal is to help you avoid common pitfalls, reduce unnecessary rework, and build a smoother, more predictable readiness review.



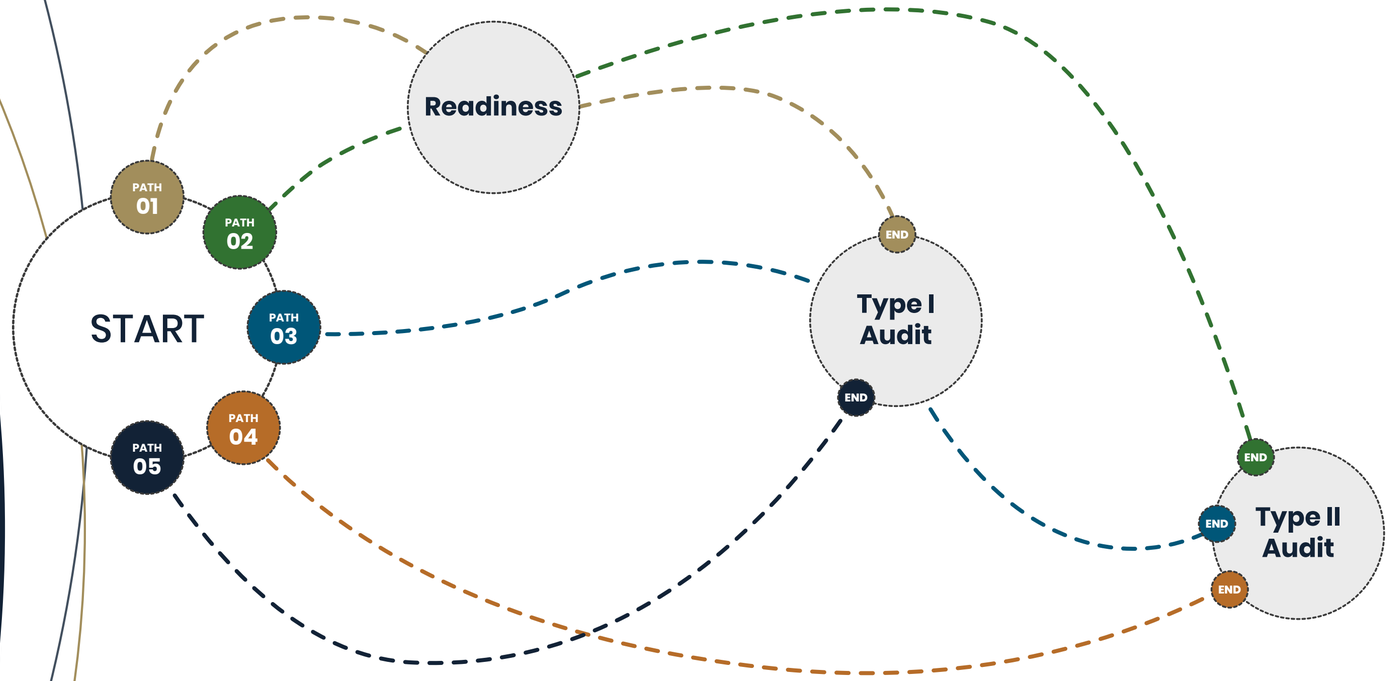
Before diving in, it helps to understand what a Type II audit is actually measuring. Unlike a Type I report, which confirms that controls are properly designed at a point in time, a Type II requires demonstrating that those controls operated consistently throughout the audit window, typically three to twelve months.

Evidence collection, access reviews, and change management documentation need to reflect actual operations, not just policy intent.

Organizations arrive at Type II readiness from different starting points, as illustrated in the accompanying pathways graphic. Some are building on a recent Type I assessment, others are pursuing Type II directly, and some are leveraging external expertise to accelerate the process.

While each path presents its own challenges, all ultimately require the same outcome: demonstrating that controls are operating effectively over time. Regardless of which path best reflects your organization's journey to Type II readiness, the preparation activities in this checklist will help establish the operational consistency and evidence needed for a successful audit. That distinction shapes every step in this checklist.

Keep in mind that this checklist is a preparation aid and not a substitute for a formal readiness assessment.



PATH 01 - CAUTIOUS START

Readiness, then Type I

Lower maturity. Need a report soon, but not ready for a direct audit.

PATH 02 - PREPARED

Readiness, then Type II

Targeting Type II directly. Want gaps caught before the window opens.

PATH 03 - SEQUENTIAL

Type I, then Type II

Need a formal report fast. Build toward Type II afterward.

PATH 04 - DIRECT

Straight to Type II

Mature controls, ≥3-month runway, customers explicitly require Type II.

PATH 05 - ENDPOINT

Type I as the endpoint

Current customers accept Type I. Short-term posture, not a long-term strategy.

1

Defining System Boundaries and Scope

Identify in-scope systems and data flows

Clearly document which applications, infrastructure, and data stores fall under the SOC 2 security audit. Include cloud services, on-premise systems, and any third-party services (subservice organizations) that impact security controls.

Map out boundaries

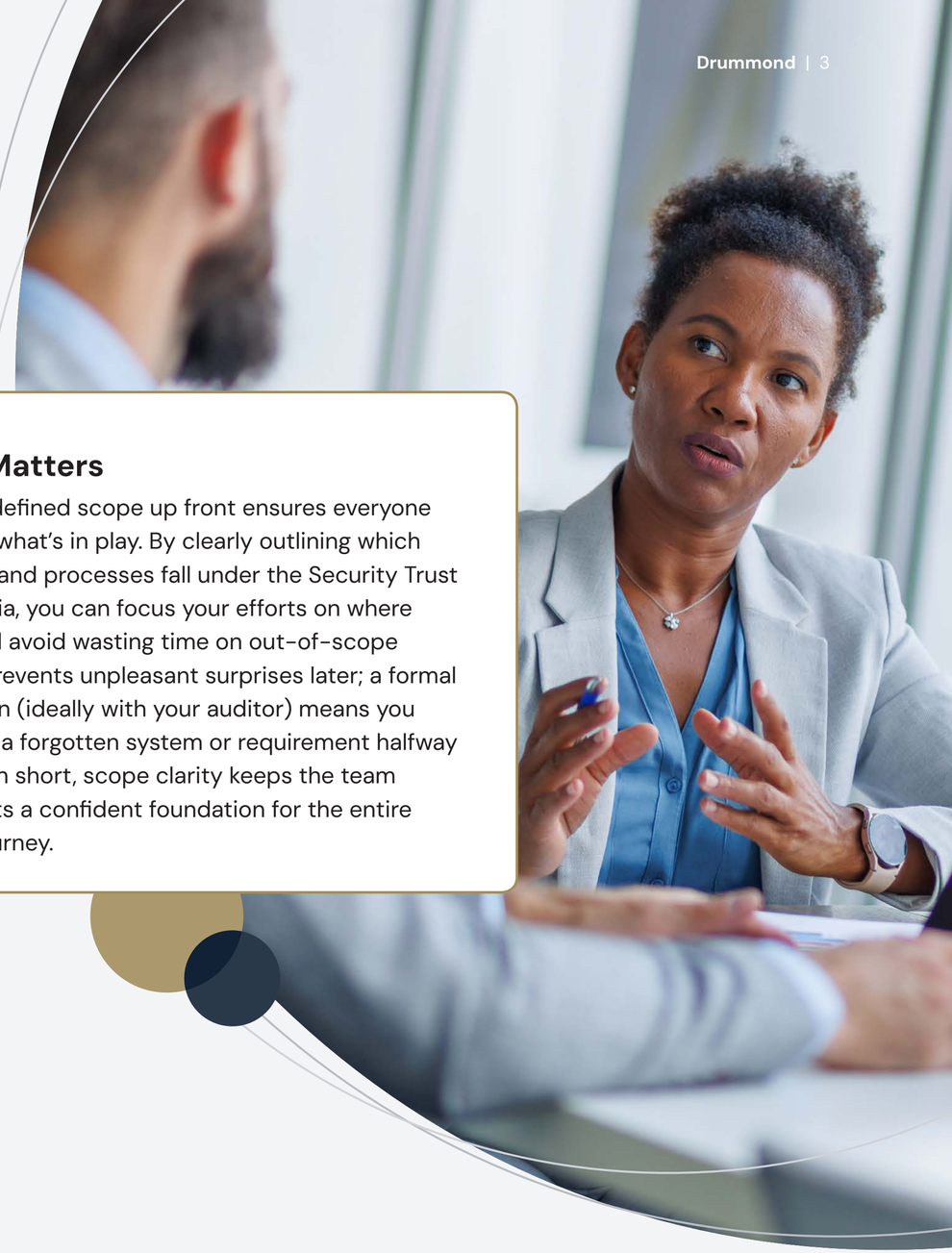
Draw the line around what's in and out of scope. For example, perhaps only your customer-facing platform and its supporting network are in scope, while internal IT or unrelated products are out. This prevents scope creep and focuses on efforts where they matter.

Choose the audit parameters

Decide on the **audit period** for your Type 2 (e.g. 3, 6, or 12 months) and confirm you're only including the ***Security*** criteria (since we're focusing on Security TSC).

Document it

Write a formal scope statement or diagram for your records and for the auditor. Ensure leadership and stakeholders agree on this scope.



Why This Matters

Having a well-defined scope up front ensures everyone knows exactly what's in play. By clearly outlining which systems, data, and processes fall under the Security Trust Services Criteria, you can focus your efforts on where they count and avoid wasting time on out-of-scope items. It also prevents unpleasant surprises later; a formal scoping session (ideally with your auditor) means you won't discover a forgotten system or requirement halfway through prep. In short, scope clarity keeps the team aligned and sets a confident foundation for the entire compliance journey.

2

Confirming Core Documentation

(Policies, IR Plans, Asset Inventories)

Gather your security policies

Ensure you have all the foundational policies required by the security criteria, such as an Information Security Policy, Access Control Policy, Acceptable Use Policy, Change Management Policy, and Incident Response Plan (IRP). These should be formally documented, approved by management, and communicated to employees.

Inventory your assets

Maintain an up-to-date asset inventory of all critical systems, devices, and data repositories in scope. This document should list what you have and who owns it as auditors often ask for it to verify you know your environment.

Document procedures and guidelines

Beyond policies, make sure you have procedure documents or guidelines for operational tasks (e.g., how access reviews are performed, how incidents are handled, and how backups are done). If you claim to do it, write it down!

Update and review

Check that each document has been reviewed recently and reflects reality. An outdated incident response plan or policy that's not enforced can be worse than none at all. Have leadership sign off on the current versions.

On Paper

- Policies
- IR Plan
- Asset Inventory
- Procedures

In Practice

- Enforced access
- Logged incidents
- Real system ownership
- Actual workflows

Why This Matters

Having all your core security documentation current and accurate gives your audit real credibility. Auditors will look for tangible proof that policies, incident response plans, and asset inventories are not just paperwork for show, but are meaningful, maintained, and actually followed in practice. Ensuring your documents reflect how the business truly operates spares you from awkward gaps where a policy says one thing, but day-to-day work does another. In short, up-to-date documentation aligned with reality builds trust with the auditors and makes the audit go smoother, because you won't have to reconcile any disconnect between "on paper" and actual operations.

3

Validating That Key Controls Are Operating

Perform an internal control review

Before the official audit, do a self-audit or internal assessment of your security controls. **Simulate auditor tests,** for example, pick a sample of user accounts and verify their access is appropriate, or walk through a recent code change to see if it followed the change management process. Identify any control that isn't working as intended.

Test access controls

Ensure user access provisioning and deprovisioning is working. For instance, if an employee left 3 months ago, verify their accounts were indeed disabled. Run an access rights review for key systems to catch any permission creep. These checks confirm that your **Access Control Policy** is not just on paper but in action.

Check logging and monitoring

Verify that security logs are being captured for critical systems and that someone is actually reviewing them. Try generating a test security event and see if it's logged and triggers an alert. Auditors love to ask about log monitoring, be ready to show that you **"regularly review security logs"** (as required by security criteria).

Examine change management records

Pull a few recent change tickets or deployment records. Were they approved, tested, and documented according to your process? A quick dry run here can catch lapses in your **Change Management Policy** enforcement.

Fix issues now

If any control is found to be failing (e.g. missing logs, unremoved access, unpatched systems), take corrective action immediately. It's better if you find it than the auditor.



Why This Matters

Regularly double-checking that your key controls work is a proactive way to catch security weaknesses before they become audit findings. The goal is an honest read on control maturity.

Controls that are documented, consistently operated, and evidenced by real activity will hold up under audit scrutiny. Controls that were recently implemented or haven't been tested outside your own team are the ones most likely to produce findings during the observation period, and those findings will appear in a report your customers read.

If a control isn't functioning as intended, it is far better to discover and fix that now than for an auditor to find it during the observation window. This kind of internal testing also reinforces accountability: each control has an owner responsible for keeping it effective, so no one can set a control up once and walk away from it.

Validating that controls operate properly closes gaps early and gives your team an accurate picture of where you actually stand before the audit clock starts.

4

Collecting Early Evidence Samples

Start gathering evidence now

Don’t wait until the auditors are in the (virtual) lobby to pull together your evidence. Begin assembling **sample evidence for each control** early. For example, export a **user access** log from last month, pull a **report of terminated accounts,** take a screenshot of a security configuration, or compile a snippet of your audit trail for code changes.

Organize by control

Create an evidence folder or tracker aligned to your controls and policies. Under “Logging & Monitoring,” for instance, save copies of log review reports or alerts. Under “Incident Response,” have your last incident report and post-mortem ready. This way you can quickly show evidence for each requirement when asked.

Verify evidence quality

As you collect samples, check that they actually prove what they’re supposed to. Does the access log show the required details (user, timestamp, action)? Does the incident report include the necessary steps and dates? If something looks thin, you have time to improve the process or gather additional records.

Keep an evidence log

Maintain a list of what evidence you’ve collected, noting what control or criteria it supports. This can later be expanded to cover the whole audit period.



Why This Matters

Gathering evidence well before the audit gives you an early pulse on your compliance readiness, which helps eliminate big surprises down the line. By collecting sample logs, reports, or screenshots in advance, you can spot issues and correct them with plenty of time to spare, rather than scrambling to fix something under the auditor’s gaze. This proactive approach also makes the formal audit more efficient. You’ll have much of the required proof organized and vetted already, so responding to auditor requests is faster and more confident, without the chaos of last-minute evidence hunting.

5

Aligning Internal SMEs and Points of Contact

Identify your control owners

Make a roster of who in the organization is responsible for each major control or domain. Who manages identity and access? Who oversees logging and infrastructure security? Who handles HR onboarding/termination processes? Assign names to each of these areas; these are your **Subject Matter Experts (SMEs)** and points of contact for the audit.

Brief the team

Hold a kickoff meeting or informal training to explain the SOC 2 readiness and audit process to your key players. Let them know what to expect – auditors may ask them to **walk through processes or provide details** about how controls work in practice. Make sure each person understands their role and the narrative of how their control safeguards security.

Establish an internal coordination plan

Determine how requests will flow during the audit. For instance, perhaps all evidence requests go through a compliance lead, but that person will rely on the SME for answers. Set up a channel (Slack, email, war room) for quick comms among the team during the audit.

Ensure backup support

If an SME is out on vacation when the audit happens (it does happen!), have a backup person who can speak to that area. The goal is no blank stares when an auditor asks a specific question, such as your vulnerability scanning schedule.



Why This Matters

Compliance is a team sport. One common mistake organizations make is underestimating the time needed for team coordination. Don't assume everyone will magically come together on audit day. By aligning your internal experts ahead of time, you create a united front. This means faster responses to auditor questions, consistent and accurate information, and fewer "let me get back to you on that" delays. From an ROI perspective, think about the cost of each hour an auditor spends waiting for you to chase answers; it adds up.

Having your people prepped can avoid delays and surprises during fieldwork, which ultimately can shorten the audit timeline (less billable time) and prevent costly confusion. Plus, involving your SMEs early has a side benefit: it builds internal buy-in and accountability for security. When each owner knows they'll need to show off their control, they tend to keep it in better shape.

6

Scheduling a Readiness Review with Drummond

Engage a third-party readiness assessment

Once you've done the internal homework above, bring in a third-party assessor for a formal SOC 2 readiness review**.** Treat it like a dress rehearsal for the real audit, because that's essentially what it is. Schedule this well **before** your target audit start date, allowing time to fix any issues they find.

Prepare for the review

Provide your third-party assessors with your scope, policies, and evidence samples. They'll likely do interviews and walkthroughs of your controls, much like an auditor would. Be candid with them – their goal is to surface weaknesses now so you can address them.

Receive and digest the feedback

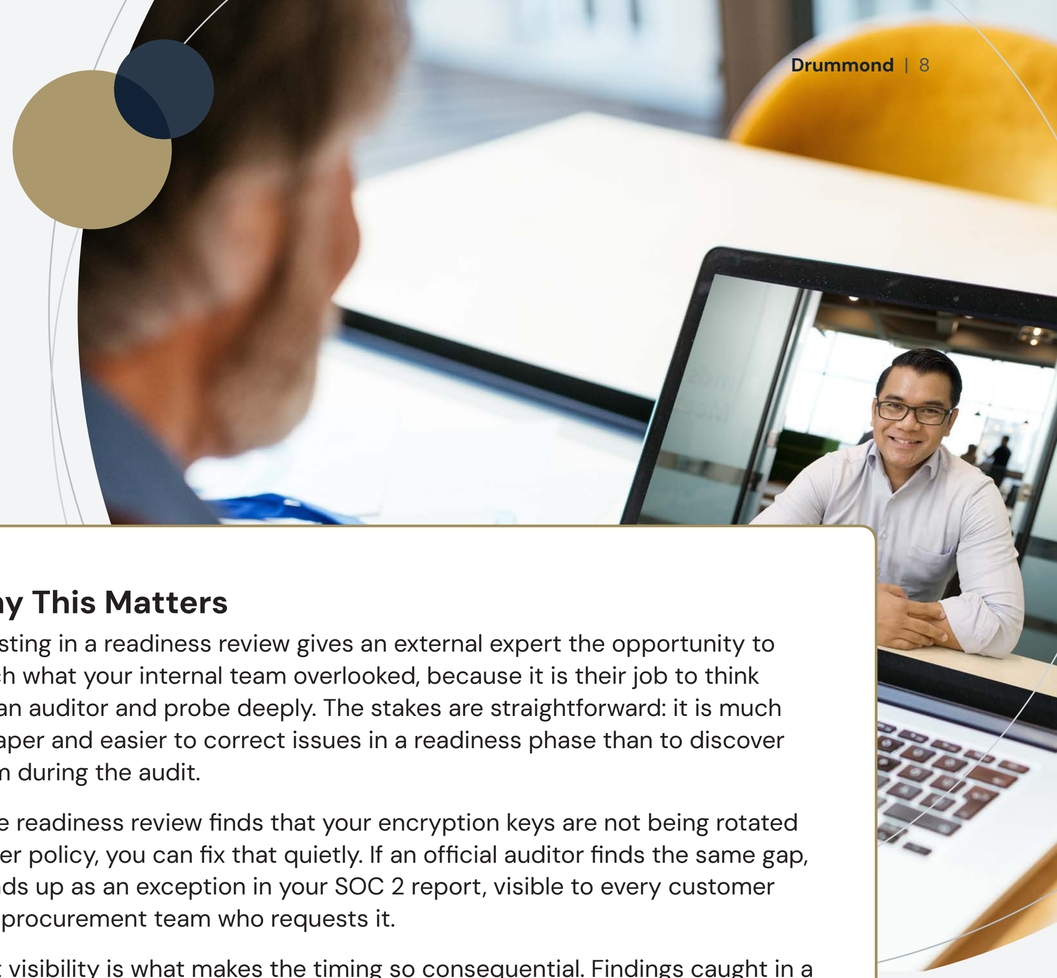
Afterwards, your third-party assessor will deliver a report or management letter detailing any gaps, weaknesses, or immaturities in your security controls. Maybe they'll point out that your asset inventory is incomplete, or that your incident response testing is insufficient. Take this feedback seriously and create a remediation plan for each item.

Remediate before the real audit

Fix the identified issues, bolster any weak controls, and collect any additional evidence suggested. If there are major findings, you might even do a quick follow-up with Drummond to ensure the fixes are on track.

Coordinate audit scheduling

With the readiness review done and gaps closed, you can confidently schedule your official SOC 2 Type 2 examination (perhaps even with the same firm's audit division, if applicable). Share the readiness results with the auditors – it shows initiative and can help focus the audit on what matters.



Why This Matters

Investing in a readiness review gives an external expert the opportunity to catch what your internal team overlooked, because it is their job to think like an auditor and probe deeply. The stakes are straightforward: it is much cheaper and easier to correct issues in a readiness phase than to discover them during the audit.

If the readiness review finds that your encryption keys are not being rotated as per policy, you can fix that quietly. If an official auditor finds the same gap, it ends up as an exception in your SOC 2 report, visible to every customer and procurement team who requests it.

That visibility is what makes the timing so consequential. Findings caught in a readiness phase stay between you and your assessor. Findings from a formal Type II audit do not. Organizations that overestimate their control maturity and skip the readiness review are the most likely to surface problems mid-observation period, and control rework during an active audit window can extend timelines and weaken the evidence narrative your report depends on.

Failing to do a pre-audit readiness check can result in incorrect scoping, wasted effort, and audit delays, all of which hit the budget and timeline hard. Scheduling a readiness review with Drummond before the observation window opens is the most direct way to avoid that outcome.

The Bottom Line:
Turn Readiness into Advantage

Preparing for SOC 2 Type 2 is not only about avoiding surprises. It is about building a security foundation that speeds up your audit, reduces rework, and strengthens trust across your entire ecosystem. The effort you invest upfront pays off when the auditors arrive, giving you efficiency, clarity, and control instead of last-minute scrambling.

Internal preparation can take you far, but it cannot replace the insight and nuance that come from working with professionals who live inside these standards every day. That is where Drummond steps in.

Use your internal work to tighten processes and address gaps early, then rely on Drummond to validate decisions, uncover blind spots that only seasoned auditors recognize, and guide you through the complexities that shape audit success.

In the end, you are not simply pursuing a clean SOC 2 Type 2 report. You are building a security program that accelerates buyer confidence, shortens sales cycles, and positions your organization to scale with credibility. With the right preparation and Drummond's expertise, readiness becomes more than compliance. It becomes your competitive edge.

DRUMMOND

(877) 437-8666
sales@drummondgroup.com
www.drummondgroup.com

© 2026 Drummond Group, LLC. All rights reserved. All brand names and trademarked logos used are for identification purposes only and are the property of their respective owners. Their inclusion here does not imply endorsement, sponsorship, or affiliation with Drummond.