



MandateMind

SOC 2 READINESS GUIDE

The practical cookbook for preparing your organization for a SOC 2 examination — from scope and controls to evidence, gaps, remediation, and auditor readiness.

Prepare smarter. Prove what you have. Find what is missing.

How to use this guide

Work through the chapters in order for a first-time SOC 2 preparation effort, or jump directly to the checklist, evidence, gap assessment, and remediation sections when you are already underway.

Powered by MandateMind AI

Evidence intelligence • Control mapping • Gap detection • Readiness visibility

Table of Contents

A practical path from “we need SOC 2” to an organized, evidence-backed readiness program.

Chapter	Topic	What it covers
1	SOC 2 in Plain English	What SOC 2 is, what it is not, and what auditors evaluate.
2	Choose Your Scope	Define the system, services, boundaries, people, vendors, and criteria.
3	Build Your Control Program	Turn requirements into owned, repeatable controls.
4	Build the Evidence System	Understand evidence and avoid evidence chaos.
5	Run a SOC 2 Gap Assessment	Find missing controls, weak controls, and unsupported claims.
6	Remediate Before the Examination	Prioritize issues, assign owners, and prove fixes.
7	Prepare for the Auditor	Create a clean, traceable examination package.
8	Using MandateMind for SOC 2	Turn evidence into readiness intelligence.
9	SOC 2 Readiness Master Checklist	Printable end-to-end checklist.
10	Common Mistakes & Final 30-Day Plan	Avoid late surprises and execute a final sprint.

Important

This guide is educational and operational. It does not provide legal advice, does not perform a SOC 2 examination, and cannot guarantee a SOC 2 report. Work with your independent CPA firm for examination-specific requirements and conclusions.

1. SOC 2 in Plain English

SOC 2 is an attestation/reporting framework used to provide information about controls relevant to security and other Trust Services Criteria. A SOC 2 examination is performed by an independent CPA firm. Before the examination, your job is to establish the right scope, design and operate appropriate controls, and maintain evidence that supports what you say your organization does.

Type 1 vs. Type 2

Type 1: focuses on whether controls are suitably designed and implemented at a specified point in time. Type 2: also evaluates operating effectiveness over a period of time. The exact examination period and testing approach are determined with your service auditor.

Concept	What your team should be able to answer
Scope	What system/service is being examined? What is outside scope?
Control	What activity is performed, by whom, and how often?
Evidence	What artifact demonstrates the control was designed/operated as described?
Owner	Who is accountable for performing or reviewing the control?
Gap	What is missing, inconsistent, ineffective, stale, or unsupported?
Readiness	Can we explain and support our control environment to the auditor?

The golden rule

Never treat a policy as proof that a control operates. Your readiness program should connect the control statement to actual operating evidence.

2. Choose Your Scope

Scope decisions can make or break a SOC 2 project. Define the service or system being examined before you try to collect thousands of artifacts.

Scope worksheet

- ☐ Name the service/product and business purpose in scope.
- ☐ Identify production environments, applications, cloud accounts, repositories, and critical infrastructure.
- ☐ Document relevant locations, personnel, teams, and functions.
- ☐ Identify material vendors and subservice organizations.
- ☐ Define what data the system handles and why.
- ☐ Confirm which Trust Services Criteria are relevant.
- ☐ Document clear in-scope and out-of-scope boundaries.
- ☐ Confirm scope assumptions with your service auditor.

Scope questions to ask

- What customer-facing service are we making commitments about?
- Which infrastructure actually supports that service?
- Which employees or contractors can materially affect security?
- Which vendors are relied upon for the service?
- Which systems create or store the evidence we will need?

3. Build Your Control Program

A control is an activity, process, or mechanism intended to address a risk or requirement. Strong controls are specific enough that another person can understand what happens, who does it, how often it happens, and what evidence should exist afterward.

A strong control statement contains

- Action: what is actually done.
- Owner: who is responsible.
- Frequency: when/how often it happens.
- Trigger: what starts the activity when applicable.
- Evidence: what artifact proves the activity happened.
- Review: who validates the result when independent review is needed.

Example

Weak: "We review access regularly."

Stronger: "The Security Manager reviews privileged access to production systems quarterly, documents the review, investigates exceptions, and retains the approval record."

Control ownership checklist

- ☐ Every relevant control has an accountable owner.
- ☐ Owners understand what they must do and what evidence they must retain.
- ☐ Control frequency matches the risk and policy commitment.
- ☐ Exceptions are documented and approved.
- ☐ Control changes are reviewed when systems or processes change.

4. Build the Evidence System

Evidence is the proof layer of your readiness program. The goal is not to collect the largest number of files. The goal is to collect appropriate evidence that is relevant, attributable, complete enough for the control, and traceable to the activity it supports.

Common SOC 2 evidence categories

- Policies and procedures
- Access reviews and user-management records
- Security awareness and training records
- Vulnerability and patch-management records
- Logging, monitoring, and alert evidence
- Change-management tickets and approvals
- Incident response records and exercises
- Risk assessments and treatment records
- Vendor due diligence and monitoring
- Business continuity / disaster recovery evidence
- Cloud configuration and infrastructure evidence
- System-generated reports and screenshots

Evidence quality test

- ☐ Does the evidence clearly relate to the control?
- ☐ Does it cover the relevant date or period?
- ☐ Can we identify the system, user, owner, or source?
- ☐ Is the evidence complete enough to support the control?
- ☐ Can we explain anomalies or exceptions?
- ☐ Is the artifact protected from inappropriate alteration?
- ☐ Could another reviewer understand what the artifact proves?

Avoid the evidence dump

A folder containing hundreds of screenshots is not a readiness strategy. Every artifact should have a purpose: what control does it support, what does it prove, and what period or event does it represent?

5. Run a SOC 2 Gap Assessment

A gap assessment compares what your program is expected to do with what it actually does and what evidence exists to demonstrate it.

Classify every finding

Status	Meaning
Missing	No control, process, or evidence exists.
Incomplete	Something exists, but important elements are missing.
Inconsistent	The process exists but is not performed reliably.
Unsupported	The organization claims a control, but evidence does not adequately demonstrate operation.
Stale	Evidence or documentation is outdated relative to the current environment.
Remediated	The issue has been addressed and the fix has supporting evidence.

Gap assessment questions

- ☐ What controls are required for our selected scope and criteria?
- ☐ Which controls have no evidence?
- ☐ Which controls have evidence but weak coverage?
- ☐ Which evidence items are stale or inconsistent?
- ☐ Which findings are highest risk or most likely to affect the examination?
- ☐ Who owns each remediation item and when will it be closed?
- ☐ How will we verify that the remediation actually worked?

6. Remediate Before the Examination

Remediation is where readiness becomes operational. Do not simply close a spreadsheet row. Fix the underlying process, then collect evidence that demonstrates the fix.

Prioritize using four questions

- Risk: Could this weakness materially affect the service?
- Scope: How broadly does the issue affect people, systems, customers, or evidence?
- Recurrence: Is this a one-time exception or a broken process?
- Evidence: What will prove the remediation operated as intended?

Remediation record template

Field	What to capture
Finding	Plain-language description of the gap.
Risk	Why it matters and affected scope.
Owner	Named person accountable for closure.
Action	Specific process, technical, or documentation change.
Due date	Target completion date.
Validation	How the fix will be tested and evidenced.

7. Prepare for the Auditor

Your auditor should not have to reconstruct your program from random folders. Create a clean, traceable operating model that shows scope, controls, owners, evidence, exceptions, and remediation status.

Auditor-readiness checklist

- ☐ Confirm the examination scope and criteria with your service auditor.
- ☐ Maintain a current system description and supporting documentation.
- ☐ Have control owners identified and available.
- ☐ Have evidence organized by control or logical evidence category.
- ☐ Resolve or clearly document known gaps and exceptions.
- ☐ Maintain change records for significant changes during the relevant period.
- ☐ Document incidents, investigations, and corrective actions as applicable.
- ☐ Prepare a clear method for auditor requests and responses.
- ☐ Provide read-only access or controlled evidence sharing where appropriate.
- ☐ Keep a record of what was provided and when.

Think like the auditor

For every important control, ask: “If I had never seen our environment before, could I understand what this control is, who performs it, how it operates, and what evidence demonstrates it?”

8. Using MandateMind for SOC 2

MandateMind is designed to reduce the manual interpretation and tracking work that makes compliance programs difficult to manage. Use it as the intelligence layer around your existing security and compliance processes.

Recommended MandateMind workflow

- 1. Start with your mandate: select SOC 2 and establish the relevant scope and criteria.
- 2. Bring in evidence: upload policies, logs, screenshots, tickets, configurations, reports, and other supporting artifacts.
- 3. Interpret the evidence: use MandateMind's evidence intelligence to understand what an artifact appears to demonstrate.
- 4. Map evidence to controls: connect evidence to the controls it supports.
- 5. Find gaps: identify missing, weak, stale, or unsupported coverage.
- 6. Remediate: assign actions and track progress alongside your existing workflow.
- 7. Reassess: validate that new evidence supports the remediated control.
- 8. Prepare the audit view: provide an organized, controlled view for appropriate stakeholders.

MandateMind is not the auditor

MandateMind helps you organize, analyze, map, score, and improve readiness. Your independent CPA firm remains responsible for the SOC 2 examination and report.

What to upload first

- Current security and compliance policies
- Access-control procedures and recent review records
- Change-management procedures and representative tickets
- Vulnerability/patch reports
- Incident response plan and recent exercise evidence
- Vendor-management documentation
- Risk assessment materials
- Cloud/security configuration evidence
- Security awareness records

9. SOC 2 Readiness Master Checklist

Print this section or use it as the backbone of your readiness project.

Governance & Scope

- ☐ Scope defined and approved
- ☐ System description drafted and reviewed
- ☐ Relevant Trust Services Criteria confirmed
- ☐ Control owners assigned
- ☐ Key vendors/subservice organizations identified

Security Program

- ☐ Security policies approved and current
- ☐ Risk assessment performed
- ☐ Security awareness program operating
- ☐ Access management operating
- ☐ Joiner/mover/leaver process operating
- ☐ Vulnerability management operating
- ☐ Logging and monitoring operating
- ☐ Incident response process operating
- ☐ Change management operating
- ☐ Backup / recovery processes operating

Evidence

- ☐ Evidence inventory created
- ☐ Evidence mapped to controls
- ☐ Evidence dates checked
- ☐ Evidence owners identified
- ☐ Exceptions documented
- ☐ Stale evidence replaced

Readiness

- ☐ Gap assessment completed
- ☐ High-priority remediation completed
- ☐ Remediation independently validated
- ☐ Auditor request workflow established
- ☐ Final readiness review completed

10. Common Mistakes & Final 30-Day Plan

The final sprint is about closing gaps, validating fixes, and making auditor collaboration predictable.

Common mistakes

- Starting with documents instead of scope. You may create controls that do not apply to the system being examined.
- Collecting evidence without mapping it. More files do not automatically mean stronger evidence.
- Writing controls nobody actually performs. A polished policy cannot substitute for operation.
- Leaving remediation until the end. Late fixes can create evidence-period problems, especially for Type 2 examinations.
- Ignoring changes. New infrastructure, vendors, employees, applications, and processes can change your control environment.
- Treating the auditor like a project manager. Your team owns the readiness program; the auditor independently examines it.

Final 30-day readiness sprint

Days	Focus	Output
1-5	Scope + inventory	Approved scope, systems, owners, evidence sources
6-12	Controls + evidence	Control/evidence map and initial gaps
13-20	Remediation	High-priority fixes and validation evidence
21-25	Reassessment	Updated readiness view and unresolved exceptions
26-30	Auditor preparation	Request workflow, evidence package, and owners

Your next step

If you already have evidence, don't start over. Upload your existing materials into MandateMind, map what they prove, identify what is missing, and turn the gaps into a prioritized readiness plan.

See MandateMind AI: www.mandatemind.com

Evidence intelligence • Control mapping • Gap detection • Readiness visibility