Your First SOC 2 Moves

SOC 2 Audit-Readiness Assessment

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-10-06

Contents

What SOC 2 actually is 1
The five first moves 1
What it really costs 2

About This Guide **3**

A plain-English guide to System and Organization Controls 2 (SOC 2) for founders and first security hires.

A customer just asked for your SOC 2 report, and the quotes for a platform, a consultant and an audit arrived before anyone explained what SOC 2 is. This guide is the part nobody sells you: what it actually requires, and the first moves that get you ready, in plain English.

What SOC 2 actually is

SOC 2 is an independent accountant's report on how well your company protects the data it holds. A licensed auditor (a CPA firm) examines your controls against a set of criteria, the Trust Services Criteria (TSC), and writes an opinion. It is **not** a certificate, not a one-time box-tick, and not a product you install. It is evidence that your controls were designed well (a **Type I** report) and operated reliably over a period of time (a **Type II** report).

You do not need to understand all of it at once. You need to do five things first.

The five first moves

1. Decide your scope before you spend a dollar. SOC 2 has five criteria, but Security (the Common Criteria) is the only one always required. Most small teams start with Security alone and add Availability or Confidentiality only when a buyer actually asks. Scope decides cost more than any other choice.

2. Draw your system boundary. Write down what is in scope (which product, which systems, which data, which vendors) and what is out. This becomes the system description in the report, and it is the single biggest lever on how much work the audit is.

3. Turn on the access basics. Multi-factor authentication (MFA) everywhere it matters, a real joiner/mover/leaver process so leavers lose access promptly, and a periodic access review you keep a dated record of. Access control is the most-sampled area in a typical audit; these three moves cover most of it.

4. Start collecting evidence as you go. A Type II report proves a control ran across the whole window, not that it existed the night before fieldwork. The moment you start, begin saving dated records: access reviews, change tickets, backup-restore tests. Evidence gathered continuously is the difference between a clean opinion and a scramble.

5. Run a gap assessment and make a dated plan. Score each control honestly on where it actually stands today, rank the gaps, and give each one a one-step plan, an owner, and a date. That plan *is* your road to audit-ready, and it is the work the free assessment and the toolkit are built to do with you.

What it really costs

You will be quoted for up to three things, separately: a compliance platform (an annual subscription priced per company; the main vendors do not publish list prices), the audit itself (priced by the audit firm for your scope and report type), and often a readiness consultant. None of that is required to *start*. Understanding what you need first is what keeps you from overspending on tools before you know which ones you need.

Want to see exactly where you stand? The free SOC 2 Audit-Readiness Assessment scores you across all eight control areas (scope, governance, access, change, vendors, monitoring, availability, and evidence) in about ten minutes, and shows you the gaps to close first. It runs in your browser; your answers never leave your device.

Provided by Sylvan Assurance, LLC as part of the SOC 2 Audit-Readiness Assessment. This is general, plain-English guidance, not professional advice, not a SOC 2 audit. Compliance with applicable law and the readiness of your own programme remain your responsibility; verify anything here against your own circumstances and, where needed, a qualified professional.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience translated into plain-language guidance for small business owners.

It provides **general guidance and recommended practices**. It is **not** legal advice. Every recommendation is **optional** - a widely accepted way to reduce a common risk. Responsibility for your business remains with you.

For full terms, see the Terms of Use provided with the SOC 2 Audit-Readiness Assessment.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/

Where to go from here

Scan for the full toolkit that builds on this guide.
sylvanassurance.com/go/toolkit-soc2-readiness

Scan for the companion book - the full story, in plain English.
sylvanassurance.com/go/soc2-plain-english