QOS MSP
Managed Services

SOC 2 COMPLIANCE
STRATEGY GUIDE

Type 1 vs Type 2, the Trust Services Criteria, real timelines and costs — what business leaders should know before the first audit.

+1 (877) 800-7672

www.qosmsp.com

The SOC 2 Compliance Strategy Guide

Somewhere in your pipeline, a customer has asked for your SOC 2 report — or is about to. Before you commit months and a five-figure budget, you should know what SOC 2 actually involves, which report you really need, and where the costs hide.

This guide is the plain-English version: what the framework is, how the two report types differ, the readiness roadmap we use with clients, and honest answers on timeline and budget.

1. What SOC 2 Actually Is — and Who Asks for It

SOC 2 is an auditing framework from the AICPA (the American Institute of Certified Public Accountants). An independent licensed CPA firm examines how your organization protects customer data and issues an attestation report. There is no "SOC 2 certificate" — the deliverable is the report itself, and sophisticated buyers read it.

Who asks for it: enterprise and mid-market procurement teams, vendor-risk programs, and security-conscious customers of SaaS products, IT service providers, and any company that stores or processes client data as a service. For many software deals it has quietly moved from "nice to have" to a condition of the contract.

The Rule:

SOC 2 is usually bought to win and keep contracts — treat it as a revenue project with a security dividend, and scope it around what your customers actually require.

2. Type 1 vs Type 2 — Which Report Do You Need

- **Type 1** — the auditor examines whether your controls are suitably designed and in place **at a single point in time**. Faster and cheaper; a legitimate first milestone that shows customers you're on the path.
- **Type 2** — the auditor examines whether your controls **operated effectively over a review period**, usually 3–12 months. This is the report most enterprise customers mean when they say "SOC 2," because it proves the controls ran, not just that they existed on audit day.

The Rule:

Ask your customer which report and what review period they require. Many companies do a Type 1 first, then run straight into their first Type 2 observation window.

3. The Five Trust Services Criteria — and What's Actually Mandatory

Every SOC 2 audit covers **Security** (the "common criteria") — that one is not optional. The other four are added only if they're relevant to what you sell: **Availability** (uptime commitments), **Confidentiality** (sensitive business data), **Processing Integrity** (accurate, complete processing), and **Privacy** (personal information).

The Red Flag:

A proposal that scopes all five criteria by default. Every added criterion adds controls, evidence, and cost — most companies genuinely need two or three.

4. The Readiness Roadmap

1. **Scope it** — which systems, teams, and vendors touch customer data, and which criteria your customers actually demand. Tight scoping is the biggest cost lever you control.
2. **Readiness assessment** — measure your controls against the criteria and get a risk-ranked gap list.
3. **Remediate by risk** — close the gaps in priority order; this is where most of the calendar goes.
4. **Run the observation window** — for Type 2, controls must operate and generate evidence for the full review period. Collect proof as you go, not in a panic before the auditor arrives.
5. **The audit** — your CPA firm tests and issues the report.

The Red Flag:

Booking the audit before a readiness assessment. Failing controls in front of your auditor is the most expensive way to discover a gap.

5. Timelines and Cost Drivers, Honestly

Timeline: a focused Type 1 can move in two to four months; a first Type 2 typically takes six months to a year — remediation plus the observation window dominate, not paperwork.

Where the money goes:

- **Audit firm fees** — commonly $15,000–$50,000+ depending on scope, criteria, and report type
- **Compliance tooling** — monitoring and evidence-collection platforms
- **Remediation work** — the largest and most variable line
- **Internal time** — evidence, coordination, and control ownership
- **Program management** — keeping all of it moving

The Rule:

The audit fee is quotable up front; remediation is where budgets blow up. A readiness assessment prices the whole journey before you commit to any of it.

6. Staying Compliant After the First Report

A SOC 2 report covers a period — customers expect a fresh one every year. Controls drift, staff turn over, vendors change, and the next observation window starts as soon as the last one ends.

What keeps it: quarterly control checks, evidence collected continuously, vendor reviews on a schedule, and one owner for the program.

The Red Flag:

A compliance program that only wakes up the month before the annual audit.

7. How QOS MSP Helps

We carry organizations through the full journey — readiness assessment, risk-ranked remediation, written policies, evidence discipline through the observation window, and the ongoing program management that keeps every year's report clean — at flat Compliance-plan rates, founder-led since 2007. One honest boundary: the audit itself must come from an independent licensed CPA firm. We don't replace them — we make sure they find what they expect to find.

The Final Word

The organizations that struggle with SOC 2 treat it as an audit event. The ones that sail through treat it as a program that happens to produce a report.

Next Step:

Ask your customer which report and criteria they require, then get a readiness assessment scoped. QOS MSP will do that scoping call at no cost: call +1 (877) 800-7672 or visit www.qosmsp.com.