SOC 2 for Growing Companies:

What CFOs Need to Know

A practical reference for finance leaders expanding into US markets

What SOC 2 Is and Why It Matters Now

SOC 2 (System and Organisation Controls 2) is the US standard for demonstrating that a company handles customer data securely, reliably, and in line with defined commitments. It was developed by the American Institute of Certified Public Accountants (AICPA) and is the dominant security certification requirement for US enterprise procurement.

Unlike ISO 27001, SOC 2 is not a pass/fail certification — it produces an audit report that describes your controls and whether they operated effectively. The report is shared with customers under NDA as evidence of your security posture.

The Five Trust Service Criteria

Criteria	What It Covers	Required?
Security	Protection against unauthorised access	Always mandatory
Availability	System availability per agreed commitments	If your SLA matters to customers
Processing Integrity	Complete and accurate data processing	If you process transactions
Confidentiality	Protection of confidential information	If you handle sensitive client data
Privacy	Personal information handling	If you process personal data

Most growing companies start with Security only, then add Availability and Confidentiality as customer requirements evolve.

Type I vs Type II — the practical difference

Type I

Confirms your controls are designed correctly as of a specific date. It's faster and useful for early sales conversations.

Type II

Confirms your controls operated effectively over a period — typically 6 or 12 months. Enterprise customers want Type II.

A common path is to achieve Type I first to unblock pipeline, then move to Type II within the year.

What SOC 2 Requires From You as CFO

You don't need to run the audit. You need to own the budget, sign off on the right things, and ensure your organisation can produce clean evidence when your auditor asks for it.

These are the key approvals SOC 2 requires from executive leadership:

What You're Signing	When	What the Auditor Checks
Security Policy	Before audit, reviewed annually	Signed version, approval date, version history
Risk Assessment	Before control implementation	Documented methodology and results, signed off
Vendor Management Policy	Before audit	Signed policy, vendor inventory, assessment records
Incident Response Policy	Before audit	Signed policy, evidence of testing
Management Assertion	At each audit	Your formal statement that controls are operating — this is in the audit report
Annual Policy Reviews	Annually	Each policy showing review date and sign-off

The management assertion is the most important sign-off most CFOs don't know about. In every SOC 2 report, management formally asserts that the system description is accurate and that controls operated effectively. That assertion is signed by a named executive. Auditors hold you to it.

High-Level Implementation Checklist

1

Phase 1 — Readiness

- Define audit scope — which systems, services, and data are in scope
- Select Trust Service Criteria — start with Security as minimum
- Appoint compliance owner (not CFO — but CFO named as executive sponsor)
- Select SOC 2 auditor — must be a licensed CPA firm
- Complete readiness assessment — gap analysis against Trust Service Criteria
- Set up document management with version control

2

Phase 2 — Risk Assessment

- Build asset and data inventory — what you hold, where it lives, who has access
- Complete risk assessment — identify threats, score likelihood and impact
- CFO signs off on risk treatment decisions
- Document residual risk acceptance with named owner

3

Phase 3 — Policy Documentation

- Draft and approve core policies: Information Security, Access Control, Incident Response, Change Management, Vendor Management, Business Continuity
- Obtain formal sign-off from named approver for each policy
- Publish to all relevant staff with acknowledgment records

4

Phase 4 — Control Implementation

- Access controls — least privilege, MFA, access reviews, joiner/mover/leaver process
- Monitoring and logging — system activity logs, alerting, retention
- Vulnerability management — scanning schedule, patch process, penetration test
- Vendor assessments — security questionnaires sent to key vendors, responses documented
- Incident response testing — tabletop exercise, documented results
- Business continuity testing — backup verification, recovery test documented

5

Phase 5 — Type I Audit

- Auditor fieldwork — evidence requests, control testing, walkthroughs
- Management assertion signed by named executive
- Auditor issues Type I report
- Share report with customers under NDA

6

Phase 6 — Type II Observation Period

- Controls operate continuously throughout the observation period
- Evidence generated automatically (access logs, change records, training completions)
- Quarterly internal reviews to confirm control effectiveness
- Auditor fieldwork at end of period
- Management assertion signed — Type II report issued

Manual vs. Automated: What Good Looks Like

SOC 2 Requires	Manual Reality	With Governance Automation
Risk register with sign-offs	Spreadsheet, last updated before the audit	Live register with tracked approvals and dates
Policy approvals	Email thread or verbal agreement	Timestamped sign-off with version history
Vendor assessments	Sent once, stored in shared drive	Recurring workflow tied to contract renewal
Audit evidence on request	Week-long scramble across teams	Retrievable in minutes
Control monitoring evidence	Manually gathered pre-audit	Maintained continuously throughout observation period

> The Type II observation period is where manual compliance breaks down most visibly. Controls need to be operating and evidenced throughout — not reconstructed at the end.

Companies that do it right

Treat evidence maintenance as a continuous workflow and enter their Type II audit clean.

Companies that don't

Spend weeks trying to reconstruct six months of activity — creating risk, cost, and delay right before the audit.

How Fortifai Supports This

Fortifai is governance workflow infrastructure built for growing companies. The platform automates the three workflows SOC 2 requires: sign-off routing and tracking, disclosure document management, and information request handling — pre-configured for SOC 2 with templates ready on day one.

The same platform supports ISO 27001, GDPR, and other frameworks simultaneously — so if you're pursuing both SOC 2 and ISO 27001, the governance workflows overlap significantly and the evidence base is shared.

Sign-off Routing & Tracking

Automated workflows ensure every policy and assertion is routed to the right executive, timestamped, and stored with full version history.

Disclosure Document Management

All audit-ready documents maintained in one place, retrievable in minutes — not after a week-long scramble.

Information Request Handling

Structured workflows for responding to auditor and customer requests, with evidence maintained continuously throughout the observation period.

Book a 30-minute walkthrough at fortifai.co