GROWING TEAMS

Planning Your Path from SOC 2 to ISO 27001

Guidance for teams that have completed SOC 2 and are now thinking about ISO 27001, including realistic timelines and scope decisions.

Cyberneza LLC | Veteran-Owned | Orlando, FL
cyberneza.com | info@cyberneza.com

Ready to get started?
Book a free 15-minute readiness call:
calendly.com/larry-cyberneza

Why Add ISO 27001 After SOC 2?

Market drivers

- International expansion — European and Asia-Pacific customers often require ISO 27001 specifically
- Government and regulated industries — Many RFPs require ISO certification, especially outside the U.S.
- Enterprise maturity signal — ISO 27001 demonstrates a management-system approach to security
- Competitive advantage — Having both SOC 2 and ISO 27001 closes almost every compliance door

What you already have

The good news is that SOC 2 and ISO 27001 overlap by roughly 70–80%. If you have a clean SOC 2 Type II report, you have already done most of the hard work. The transition is about filling gaps and restructuring — not starting over.

- Access control policies and procedures
- Risk assessment methodology
- Incident response process
- Change management controls
- Vendor management program
- Monitoring and logging infrastructure

Key Differences You Need to Understand

SOC 2 approach

- Attestation report from a CPA firm
- You choose which Trust Services Categories to include
- Focus on controls over customer data
- Annual audit (Type II covers 3–12 months)
- Report shared with customers under NDA
- Flexible — you define your control descriptions

ISO 27001 approach

- Certification from an accredited body
- Must address all 93 Annex A controls (justify any exclusions)
- Focus on an Information Security Management System (ISMS)
- 3-year certificate with annual surveillance audits
- Certificate is public; detailed findings stay private

- Prescriptive — requires specific documentation (SoA, ISMS scope, etc.)

The biggest mindset shift: SOC 2 asks "Do your controls work?" ISO 27001 asks "Do you have a system for managing information security?" It is less about individual controls and more about governance, continuous improvement, and management commitment.

What You Can Reuse from SOC 2

Do not rebuild from scratch. Here is what carries over:

Direct reuse (minimal changes)

- Access control policies — Update to reference ISO 27001 Annex A controls A.5.15–A.5.18
- Incident response plan — Add ISO-required notification timelines and management review
- Risk register — Expand to cover all information assets, not just in-scope SOC 2 systems
- Change management procedures — Usually maps directly to A.8.32
- Vendor assessments — Expand to cover A.5.19–A.5.22 supplier relationship requirements
- Security awareness training — Add ISO-specific topics (ISMS awareness, roles and responsibilities)

Needs adaptation

- Risk assessment methodology — ISO requires a formal, repeatable methodology with defined criteria for risk acceptance
- Monitoring and measurement — ISO requires defined metrics and objectives for the ISMS
- Internal audit program — Must be formalized with defined scope, frequency, and auditor independence
- Management review — Requires formal, documented reviews with specific inputs and outputs

What Is New for ISO 27001

These are the areas where SOC 2 teams typically need to build something new:

1. ISMS scope statement — A formal document defining the boundaries of your information security management system.
2. Statement of Applicability (SoA) — A required document listing all 93 Annex A controls, stating whether each is applicable, and justifying exclusions.
3. Information security objectives — Measurable goals for your security program that must be monitored, measured, and reviewed.
4. Formal management review process — Scheduled reviews where leadership evaluates ISMS performance, audit results, and improvement opportunities.
5. Continual improvement process — Documented evidence that you identify and act on improvement opportunities.
6. Internal audit program — Planned, documented audits of your own ISMS with independent auditors.

Controls That Need Extra Attention

Commonly underbuilt areas

- A.5.1 Information security policies — ISO expects a top-level policy approved by management and supporting topic-specific policies
- A.5.2–A.5.4 Roles, segregation, management — Formal role assignments and segregation of duties
- A.5.8 Information security in project management — Security integrated into project planning
- A.5.23–A.5.30 Cloud and external service security — Classification, labeling, and handling across cloud environments
- A.7 Physical and environmental security — Must address even if fully remote/cloud-only

Often overlooked

- A.5.9 Inventory of information and associated assets — Complete asset register
- A.5.10–A.5.13 Acceptable use, classification, labeling — Information classification scheme
- A.6.1–A.6.8 People security — Screening, terms of employment, disciplinary process
- A.8.10 Information deletion — Formal data deletion and media sanitization procedures
- A.8.16 Monitoring activities — Formal monitoring scope beyond SOC 2 typical requirements

Realistic Timeline

If you have a mature SOC 2 Type II program, here is what to expect:

Phase 1: Gap analysis (4–6 weeks)

- Map existing SOC 2 controls to ISO 27001 Annex A
- Identify gaps in documentation and process
- Draft the ISMS scope and Statement of Applicability
- Estimate effort for remediation

Phase 2: Build and remediate (8–12 weeks)

- Create required ISO documentation (SoA, ISMS scope, objectives)
- Update existing policies to reference ISO controls
- Implement new controls identified in the gap analysis
- Establish the management review and internal audit program

Phase 3: Internal audit (2–4 weeks)

- Conduct your first internal audit of the ISMS
- Document findings and corrective actions
- Complete a management review

- Confirm readiness for external audit

Phase 4: Certification audit (4–6 weeks)

- Stage 1 — Document review (auditor reviews your ISMS documentation)
- Stage 2 — Implementation audit (auditor verifies controls are operating)
- Address any nonconformities
- Receive your ISO 27001 certificate

Total: 4–6 months from a mature SOC 2 program to ISO 27001 certification. Teams starting with a less mature program or broader scope should plan for 6–9 months.

Scope Decisions

Start with your SOC 2 scope

Your SOC 2 system boundary is a natural starting point for your ISMS scope. It already defines the systems, people, and processes involved in delivering your service.

- Use the same system boundary as your initial ISMS scope
- Add any supporting processes ISO requires (HR, physical, legal)
- Document exclusions in the Statement of Applicability

Common scope expansions

- Corporate IT — ISO often requires including endpoint management and corporate systems
- HR processes — Onboarding, offboarding, background checks, and training
- Physical locations — Offices, co-working spaces, data center access
- Additional products or services — Customers may want specific services on the certificate

Choosing a Certification Body

- Accreditation — Verify the body is accredited by a recognized national accreditation body (UKAS, ANAB, JAS-ANZ)
- Industry experience — Choose a body familiar with SaaS and technology companies
- Auditor availability — Certification bodies can have 2–3 month lead times. Book early.
- Cost — Get 2–3 quotes. Initial Stage 1 + Stage 2 audits for SMBs typically run $15K–$30K
- Ongoing relationship — You will work with this body for 3 years, so responsiveness matters

Common Mistakes in the Transition

- Treating ISO as "SOC 2 plus a few documents" — The ISMS governance requirements are genuinely different and require ongoing commitment.

- Over-scoping — Starting with your entire organization when your SOC 2 scope would be sufficient.
- Copying policies from templates — Certification auditors test whether your team understands and follows your policies.
- Skipping the internal audit — This is mandatory, not optional. It is also your best chance to find issues before the auditor arrives.
- Not involving leadership — ISO 27001 explicitly requires management commitment. If leadership sees this as purely technical, the auditor will notice.

Ready to plan your ISO 27001 journey?

A short conversation can help you understand the gap, set a realistic timeline, and decide whether to pursue certification now or over the next 6–12 months.

calendly.com/larry-cyberneza