Teqtivity

ISO 27001 Vs. SOC 2 Selection Guide

Table Of Contents

Finding the Best Fit for Your Organization 03

ISO 27001:2022 Certification Process and Documentation 04

SOC 2 Attestation Process and Documentation 05

ISO 27001 Vs SOC 2 Selection Guide:
Finding The Best Fit For Your Organization

Selecting between ISO 27001 and SOC 2 depends on your security priorities, regulatory obligations, and business goals. Both frameworks strengthen data protection and build trust, but they serve different industries, compliance needs, and geographic markets.

Use this selection guide to determine which certification best aligns with your operations. If your organization requires a structured, globally recognized security framework, ISO 27001 may be the ideal choice. If you primarily serve North American clients and need a flexible, customer-driven approach, SOC 2 might be the better fit.

Explore the key criteria below to make an informed decision.

Choose ISO 27001 if:	Choose SOC 2 if:
You operate internationally: ISO 27001 is a globally recognized certification, ideal for organizations serving clients across Europe, Asia, and other international markets.	**You serve clients in North America:** SOC 2 is widely recognized and often expected by customers in the U.S. and Canada, especially in service-oriented industries.
You need a comprehensive security framework: ISO 27001's Information Security Management System (ISMS) provides a structured, organization-wide approach to managing risks and implementing controls.	**You prioritize customer-specific assurance:** SOC 2 allows you to tailor controls to align with the Trust Services Criteria (e.g., Security, Availability, Confidentiality), addressing client-specific concerns directly.
Compliance with international standards is critical: Many industries and regions require ISO 27001 certification to meet regulatory or contractual obligations, such as GDPR compliance in Europe.	**You need flexibility:** SOC 2's customizable framework enables you to focus on relevant security practices without implementing unnecessary controls.
You have long-term security goals: ISO 27001 emphasizes continual improvement through periodic reviews and audits, helping organizations maintain robust security as they grow.	**A faster certification timeline is important:** SOC 2 can typically be achieved in 2–3 months for Type I audits or 6–12 months for Type II audits, making it a quicker path to demonstrating compliance.

Choose ISO 27001 if:	Choose SOC 2 if:
You want to align with multiple frameworks: ISO 27001 integrates well with other standards like ISO 27701 (privacy), ISO 22301 (business continuity), and GDPR, enabling a unified compliance strategy.	**Your industry emphasizes service assurance:** SOC 2 is ideal for SaaS, IT Asset Management, cloud services, and other technology-driven industries where secure data handling and operational reliability are critical.
You operate in heavily regulated industries: ISO 27001 is particularly suited for industries like healthcare, finance, and energy, where comprehensive security management is essential.	**You're focused on trust and transparency:** SOC 2 attestation reports provide third-party validation of your security practices, enhancing customer trust and supporting business relationships.

ISO 27001:2022 Certification Process And Documentation

Gap Analysis
- Gap Analysis Report

Implementation
- ISMS Scope Document
- Statement of Applicability (SoA)

Audit & Certification
- Stage 1 Audit Report
- Corrective Action Plan (if needed)
- Stage 2 Audit Report
- Corrective Action Plan (if needed)
- ISO 27001 Certification

Maintaining Certification
- Internal Audit Reports
- Surveillance Audit Report
- Continuous Improvement Plan

SOC 2 Attestation Process And Documentation

Define Scope & Objectives
- List of systems, processes, and services handling sensitive data
- Defined scope document outlining boundaries and objectives for compliance

Perform a Readiness Assessment
- Gap analysis report
- Security controls assessment checklist
- Prioritized remediation plan

Build a Compliance Team
- Compliance team structure and roles document
- Departmental responsibilities and involvement plan

Design & Implement Controls
- Access control policies (e.g., MFA, least privilege)
- Data encryption and protection protocols
- Incident response plan
- Monitoring and logging procedures
- Change management procedures
- Employee security training materials

Document Policies & Procedures
- Information Security Policy
- Access Management Policy
- Incident Response Plan
- Data Retention & Disposal Policy
- Vendor Management Policy

Engage a CPA Firm for Audit
- Signed engagement letter with CPA firm
- Audit scope and timeline document
- Checklist of requested documentation for audit

Undergo the Audit
- Evidence of compliance (e.g., access logs, security reports, training records)
- Response to auditor requests and clarifications

Review Findings & Maintain Compliance
- SOC 2 attestation report
- Corrective action plan (if applicable)
- Continuous monitoring plan
- Re-audit preparation checklist