ISO 27001 vs SOC 2 – Comparison Guide

This guide helps organizations compare ISO 27001 and SOC 2 based on focus, scope, certification type, and business relevance. Both frameworks aim to improve your information security posture, but the choice depends on industry, geography, and client requirements.

Comparison Table

Feature	ISO 27001	SOC 2
Origin	International (ISO/IEC)	U.S.-based (AICPA)
Focus	ISMS - InfoSec governance	Trust Criteria - Ops controls
Scope	Org-wide	Specific system/service
Certification	Yes - accredited body	No - CPA attestation
Audit Frequency	Annual + 3-year cycle	Type I (1x) / Type II (ongoing)
Recognition	Global	Strong in U.S.
Typical Use	Finance, healthcare, etc.	SaaS, tech vendors
Time to Prepare	4-12 months	3-9 months

When to Choose Each

Choose ISO 27001 if you:
- Need international credibility
- Operate globally or in regulated sectors
- Want a structured ISMS framework

Choose SOC 2 if you:
- Serve US-based clients
- Provide SaaS or managed services
- Need a CPA-verified control report

Many orgs pursue both to meet global and US expectations efficiently.

Careful Security can help you build a unified program, accelerate readiness, and simplify audits.

Book a free consult at www.carefulsecurity.com