

ISO 27001










VS

SOC 2

ASPECT

ISO 27001

SOC 2

	Jurisdiction	International standard (recognized globally).	Primarily used in the United States but recognized globally.
	Purpose	Establishes a structured Information Security Management System (ISMS).	Evaluates security controls based on the AICPA Trust Services Criteria (TSC).
	Framework Type	Certification standard for information security management.	Attestation report based on the organization's internal controls.
	Regulating Body	Published by the International Organization for Standardization (ISO) and IEC.	Developed and governed by the American Institute of Certified Public Accountants (AICPA).
	Principles	Key principles of ISO 27001 are confidentiality, integrity, and availability (CIA).	The five SOC 2 Trust Principles are security, availability, processing integrity, confidentiality, and privacy.
	Compliance Approach	Requires organizations to implement security controls and undergo certification.	Involves an independent third-party audit that results in an attestation report.
	Certification/Audit	Organizations achieve ISO 27001 certification after a successful audit by an accredited body.	Organizations can receive a SOC 2 Type I or Type II report from an independent auditor.
	Implementation Time	Typically 6-18 months, depending on company size and complexity.	Typically 3-12 months, depending on audit type and readiness.
	Renewal/Frequency	Requires annual surveillance audits and recertification every three years.	Requires annual audits to maintain compliance, based on the entities audit period (3-month, 6-month, 1 year).
	Risk Management	Strong focus on risk assessment and continuous improvement through ISMS.	Risk management is broader than ISO 27001 and evaluates whole organization.
	Third-Party Assurance	Recognized as an international certification that reassures customers and stakeholders.	Provides independent assurance of security controls for clients and partners.
	Cost	Can range from \$5,000 to \$40,000 approx. for a small to medium-sized business, with larger companies potentially spending significantly more.	Varies between \$10,000 and \$80,000 or more depending on audit scope and complexity of your systems.