

















Aspect	ISO/IEC 27001	SOC 2
 Issuing Authority	International Organization for Standardization-ISO and IEC	American Institute of Certified Public Accountants-AICPA
 Outcome Type	Certification issued by an accredited certification body	Attestation report issued by a licensed CPA firm
 Purpose	To implement and maintain an Information Security Management System-ISMS across the organization	To evaluate how a service organization manages data according to selected security and privacy principles
 Framework Focus	Integrated approach to securing information across people, processes, and technology	Focus on evaluating protections around security, availability, data accuracy, privacy, and confidentiality
 Scope	Applies to the entire organization or to specifically defined sectors/fields	Applies only to selected service offerings or technical environments
 Applicability	Applicable to organizations of all sizes and sectors worldwide	Mainly adopted by SaaS companies and tech service providers in North America
 Geographic Recognition	Internationally accepted and adopted across industries	Mostly used by organizations operating in the U.S. and North America
 Audit Type	Certification audit by an ISO certification authority	Independent audit conducted by a CPA, Type I or Type II report
 Duration of Evaluation	Valid for three years with annual surveillance audits	Type I: Point-in-time; Type II: Operational effectiveness over 3-12 months
 Control Framework	Based on ISO/IEC 27001 Annex A controls	Follows AICPA's Trust Services Criteria, where security is mandatory, and others optional
 Level of Modification	Limited flexibility—standardized ISMS methodology	More flexible—controls tailored to organizational needs
 Risk Management	Mandatory risk analysis and risk treatment process	Risk evaluation not directly required, but practically expected
 Target Audience	Regulators, international clients, global partners	U.S.-based clients, especially those in tech and SaaS sectors
 Integration with Other Standards	Easily integrated with ISO 9001, ISO 45001, etc.	Can be used alongside other reports like SOC 1, SOC 3
 Certification or Attestation	Formal certification	Attestation—not a certification
 Cost Consideration	Depends on the organization's size and scope, generally medium to high	Pricing varies on report type, Type I or II and audit scope