ISO 27001 vs. SOC 2

Which Security Approach Is Right for You?

At a time when the global cost of cyber crime is surging, choosing the right information security approach is critical.

ISO 27001 and SOC 2 are two of the most widely recognized approaches to information security. While both address confidentiality, integrity, and availability, they differ significantly in structure, scope, and intended outcomes.

This guide is designed to help you understand these differences and choose the best options for your needs.

What Is ISO 27001?

ISO 27001 is a globally recognized management system standard developed by the International Organization for Standardization. It provides a comprehensive set of requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It allows businesses to achieve certification through a formal third-party assessment, providing recognized validation of their information security practices.

This standard offers guidelines, not strict requirements, making it adaptable for organizations of all sizes and sectors. ISO 27001 is particularly valued for its flexibility and its ability to integrate with other management systems, providing a coordinated approach to risk management.

Learn about the benefits of ISO 27001.

Key Elements of ISO 27001

- **Global standard**
- **Suitable for all organizations**
- **Integrated approach**
- **Certification (via ISO body)**

What Is SOC 2?

SOC 2, developed by the American Institute of Certified Public Accountants (AICPA), is designed for service organizations, especially in the SaaS and cloud services industries. It assesses an organization's controls related to security, availability, processing integrity, confidentiality, and privacy.

SOC 2 attestation reports are used to demonstrate an organization's commitment to maintaining robust information security practices.

These reports, conducted by independent Certified Public Accountants (CPAs), provide assurance to clients, regulators, and stakeholders that the business has effective controls in place to protect customer data. SOC 2's focus on service organizations means that it addresses a range of risks.

Key Elements of SOC 2

- **US-based standard (AICPA defined)**
- **Focused on service organizations**
- **Trust Services Criteria framework**
- **Attestation report (via CPA audit)**

How Do They Compare?

Understanding the key differences between ISO 27001 and SOC2 is critical in ensuring you choose the right approach for your organization. While both are suitable for a wide range of applications, ISO 27001 is more comprehensive and utilizes a structured framework that is recognized internationally.

Discover the key differences between the ISO 27001 and SOC 2:

	ISO 27001	SOC 2
Scope	Comprehensive set of criteria for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS)	Focuses specifically on service organizations' controls related to security, availability, processing integrity, confidentiality, and privacy
Purpose	To provide a systematic approach to managing sensitive company information and ensuring it remains secure	To evaluate and report on the controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy
Structure	Structured set of criteria with specific requirements and controls	Principles-based approach with flexibility in implementation
Focus	Process-oriented, focusing on risk management	Results-oriented, focusing on the effectiveness of controls
Certification	Certification issued by an accredited certification body after a formal audit	Reports (not certifications) issued by licensed CPA firms after audit (Type 1 or Type 2)
Who Created	International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)	American Institute of Certified Public Accountants (AICPA)
Who It's For	Organizations of any size, type, or industry seeking to protect their information assets	Service providers who store, process, or transmit customer data, particularly SaaS companies and cloud service providers
Compliance Duration	3-year certification with annual surveillance audits	Annual renewal (reports typically valid for 12 months)
Geographic Relevance	International standard recognized globally	Primarily US-focused but gaining international recognition
Implementation Time	Typically 6-24 months for full implementation and certification	Dependent on the chosen monitoring period which usually spans 6-12 months
Cost	Generally higher implementation and maintenance costs	Typically lower cost, especially for Type 1
Audit Types	Initial certification audit, followed by surveillance audits and recertification	Type 1 (point-in-time) and Type 2 (over a period, usually 6-12 months)
Control Requirements	93 controls categorized into four themes; Organizational, People, Physical, and Technological	Controls based on the Trust Services Criteria (security, availability, processing integrity, confidentiality, privacy)

Your Decision Checklist

When choosing between ISO 27001 and SOC 2, consider your organization's specific needs. ISO 27001's broad applicability supports comprehensive risk management, while SOC 2 aligns with service sector requirements focusing on specific Trust Services Criteria.

Use this checklist to evaluate which approach best aligns with your strategic and operational requirements:

1	**Industry Requirements**	Are there specific regulatory standards your industry must meet? Does your business primarily operate as a service provider in sectors like SaaS or cloud services?
2	**Organizational Capacity**	Can your business benefit from a flexible approach adaptable to various industries?
3	**Geographical Reach**	Does your business operate internationally, requiring widely recognized standards?
4	**Certification Objectives**	Is formal certification important for enhancing credibility and demonstrating compliance?

Can ISO 27001 and SOC 2 Work Together?

Some organizations benefit from incorporating both approaches, using ISO 27001's guidelines to support SOC 2's criteria, improving your business's overall security posture. This integrated approach can provide a strong defense against potential threats.

Make the Best Choice for Your Business

ISO 27001 and SOC 2 offer valuable approaches for information security management, and the choice between them should be based on your business's specific needs, industry requirements, and strategic goals. By understanding the strengths and applications of each approach, your organization can implement effective security measures to protect its data assets.

- **Contact Amtivo**—as an ANAB-accredited certification body, we can support your certification project and provide certification audits for ISO 27001.
- **Read ISO 27001 vs SOC 2—Key Differences Explained** for more insights and explore our SOC vs ISO 27001 FAQs.
- **Discover more resources** to support your journey towards robust data protection and compliance.

Phone: (303) 456-6010
Email: sales.us@amtivo.com
Web: amtivo.com/us/