ISO 27001 vs SOC 2: What's the Difference?

Teqtivity

EXECUTIVE SUMMARY

This whitepaper examines the key differences between ISO 27001 and SOC 2, two leading security compliance frameworks. ISO 27001 provides a globally recognized Information Security Management System (ISMS) designed for international organizations and highly regulated industries. SOC 2, tailored for North American service providers, emphasizes customizable security controls aligned with customer-specific needs. This document outlines their benefits, implementation processes, and relevance, particularly for IT Asset Management (ITAM) providers, ensuring secure data handling and enhanced credibility.

Key Takeaways

- ISO 27001 is a globally recognized standard for implementing an Information Security Management System (ISMS), ideal for organizations with international compliance needs.
- SOC 2 is a flexible security framework based on Trust Services Criteria, widely used in North America for service providers handling customer data.
- ISO 27001 mandates a fixed set of security controls, whereas SOC 2 allows customization based on an organization's operational priorities.
- ISO 27001 results in a formal certification, while SOC 2 provides an attestation report assessing security controls over a specified period.
- ISO 27001 certification typically takes 3–6 months, while SOC 2 Type I audits take 3–6 months, and SOC 2 Type II audits average 6–18 months, depending on audit scope.
- SOC 2 suits IT Asset Management (ITAM) providers, ensuring data protection and meeting client security expectations.
- Choosing between ISO 27001 and SOC 2 depends on an organization's compliance goals, market focus, and customer expectations.

INTRODUCTION

With evolving cybersecurity threats and increasing regulatory requirements, organizations must adopt robust security frameworks to protect sensitive information. ISO 27001 and SOC 2 provide structured approaches to managing information security, enhancing operational efficiency, and fostering customer trust. While ISO 27001 offers a standardized, risk-based ISMS framework, SOC 2 enables organizations to implement tailored controls based on business needs. This document explores their key differences, implementation processes, and benefits, helping businesses determine which certification aligns with their security and compliance goals.

The Importance of Compliance for Security and Business Success

True compliance is more than a procedural requirement—it's the foundation of a secure and resilient business.

Organizations build trust and credibility by managing risks, safeguarding sensitive data, and ensuring regulatory alignment. Frameworks like ISO 27001 and SOC 2 set the gold standard, strengthening security and streamlining operations for long-term success.

Why Compliance Matters

- **Data Protection:** Compliance frameworks require controls such as encryption, access management, and incident response to secure sensitive data and prevent unauthorized access.
- **Risk Management:** Regular risk assessments identify vulnerabilities and guide mitigation efforts, reducing the likelihood of data breaches, financial losses, and penalties.
- **Regulatory Alignment:** Adhering to frameworks ensures compliance with laws like GDPR or CCPA, avoiding fines and legal consequences.
- **Customer Trust:** Certifications like ISO 27001 and SOC 2 validate security practices, giving clients confidence in an organization's ability to protect their data.
- **Operational Efficiency:** Formalized policies and streamlined processes improve team consistency and clarity, enhancing overall efficiency.
- **Market Differentiation:** Compliance demonstrates reliability and security, providing a competitive edge in industries that require robust security assurances.
- **Incident Preparedness:** Frameworks like ISO 27001 mandate response and recovery plans, ensuring quick and effective action during disruptions or breaches.

THE FOUNDATIONS OF ISO 27001 AND SOC 2

ISO 27001 and SOC 2 are two widely respected frameworks for information security and compliance, each offering a distinct approach to protecting sensitive data and mitigating risks. While both aim to strengthen security and foster trust, they are tailored to meet different organizational priorities and market demands.

ISO 27001 provides a globally recognized standard for implementing and managing an Information Security Management System (ISMS). Its structured approach ensures that organizations can systematically address risks and enforce security measures, making it ideal for international and highly regulated industries.

SOC 2, on the other hand, focuses on the Trust Services Criteria and is primarily designed for service providers, especially in North America. It allows organizations to tailor controls around specific client needs, such as data security, availability, or confidentiality, making it a popular choice for SaaS companies, cloud providers, and IT Asset Management (ITAM) vendors.

Although these frameworks share a common goal—securing information—they differ in scope, implementation, and compliance processes. Understanding these differences is key to selecting the right certification for your business. To help you determine the best fit, we'll examine key principles, industry applications, the certification process, and what to expect regarding timelines and outcomes.

ISO 27001

ISO 27001, officially known as ISO/IEC 27001, is an internationally recognized standard for establishing, implementing, and maintaining an Information Security Management System (ISMS). It is jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is overseen by Subcommittee 27, which focuses on information security, cybersecurity, and privacy protection.

ISO 27001 provides a structured approach to safeguarding sensitive information by integrating people, processes, and technology. It helps organizations mitigate security risks while continuously improving their protection strategies. Designed for adaptability, it evolves alongside technological advancements, regulatory shifts, and emerging threats.

Key aspects of ISO 27001

Risk Assessments
Risk assessments are mandatory and serve as the foundation of an ISMS. Organizations must identify potential vulnerabilities, assess the likelihood and impact of threats, and prioritize mitigation strategies. For example, a financial institution may determine risks like phishing attacks targeting customer account information and implement multi-factor authentication and employee training as mitigation measures.

Controls and Policies
Annex A in ISO 27001 is a catalog of classified security controls organizations use to demonstrate compliance with ISO 27001 Clause 6.1.3 (Information Security Risk Treatment). It supports the creation of an organization's Statement of Applicability (SoA).

In the ISO 27001:2013 version, Annex A contained 114 security controls, categorized into 14 groups covering access control, cryptography, physical security, and incident management topics.

Following the release of ISO 27002, ISO 27001:2022 updated its Annex A structure to align with the new guidelines.

Key Changes in ISO 27001:2022 Annex A

- The new version of ISO 27001 reduces the number of controls to 93.
- 11 new controls have been introduced to address modern security challenges.
- 24 controls were merged, reducing redundancies from the previous version.
- 58 controls were revised to align with current cybersecurity threats.

Annex A Control Categories in ISO 27001:2022

ISO 27001:2022 simplifies Annex A controls into **four main categories** instead of the previous 14.

Organizational Controls (37 controls)

Control Numbers: A5.1 – A5.37
Focus: Policies, procedures, and governance to manage security.

- Information security policies
- Risk management
- Supplier security
- Security awareness training

People Controls (8 controls)

Control Numbers: A6.1 – A6.8
Focus: Managing human security risks.

- Employee background checks
- Security training
- Secure employee offboarding

Physical Controls (14 controls)

Control Numbers: A7.1 – A7.14
Focus: Protecting physical assets and facilities.

- Secure office access
- Equipment disposal
- Visitor management

Technological Controls (34 controls)

Control Numbers: A8.1 – A8.34
Focus: IT security for data, systems, and networks.

- Encryption and access control
- Network security

Continuous Improvement

ISO 27001 promotes continuous improvement through:

- Regular security reviews and audits.
- Incident management and response updates (Annex A.16).
- Enhancements to business continuity plans (Annex A.17).

As new threats emerge, such as ransomware targeting supply chains, the ISMS must evolve to incorporate updated controls and response plans.

Market Applicability of ISO 27001

ISO 27001 is recognized globally, making it valuable for organizations in diverse regions like Europe, Asia, and other markets outside North America. It is preferred for industries with complex regulatory environments, such as finance, healthcare, and telecommunications, where demonstrating compliance with international security standards is critical.

Examples of organizations that benefit from ISO 27001 certification include:

- Multinational Corporations: Ensuring consistency in security practices across regional offices, supply chains, and partnerships.
- Global E-Commerce Platforms: Protecting customer data and payment systems while meeting data protection laws like GDPR in Europe or PIPL in China.
- Cloud Service Providers: Assuring clients worldwide of their ability to manage and secure sensitive data effectively.

By adhering to ISO 27001, companies can enhance trust with global stakeholders, streamline compliance with multiple regulations, and improve their competitive edge in international markets.

ISO 27001 Certification Process

ISO 27001 certification follows a structured approach to ensure organizations meet the standard's requirements. The process involves three key stages:

1

Gap Analysis

The first step is assessing current security practices against ISO 27001:2022 requirements to identify areas for improvement. This includes:

- Reviewing existing policies, procedures, and controls.
- Identifying missing security measures, such as incident response plans or employee training programs.
- Creating a gap analysis report to guide the next steps.

2

Implementation

Once gaps are identified, organizations must take action by implementing required security controls, policies, and processes. Key steps include:

- Defining the scope of the ISMS, including assets, processes, and systems.
- Establishing an asset inventory to track sensitive information.
- Implementing access controls for critical systems and data.
- Conducting employee training on security policies and best practices.
- Developing a Statement of Applicability (SoA) to list applicable Annex A controls.

3

Audit & Certification

A third-party certification body conducts a formal assessment to verify ISO 27001 compliance. The audit process includes:

- **Stage 1 Audit:** A readiness review of ISMS documentation and initial implementation.
- **Stage 2 Audit:** A detailed evaluation of the ISMS, including interviews and operational reviews.
- Addressing any non-conformities identified during the audit.

Upon successful completion, the organization receives an ISO 27001 certification. Maintaining this certification requires ongoing commitment, including regular internal audits, risk assessments, and periodic surveillance audits by the certification body.

ISO 27001 Timelines and Outcomes

The certification process typically takes 3–6 months, depending on the organization's size, complexity, and readiness. Larger organizations with complex operations may require more time to implement and verify controls. The final deliverable is an ISO 27001 certificate, recognized internationally as a mark of excellence in information security management.

ISO 27001 certification demonstrates an organization's commitment to protecting data and provides tangible benefits, such as improved customer trust, reduced risk of security breaches, and enhanced regulatory compliance.

SOC 2

SOC 2 (Service Organization Control 2) is a security and compliance framework developed by the American Institute of Certified Public Accountants (AICPA). It allows organizations to design and assess security controls tailored to their specific operations and customer requirements. SOC 2 reports evaluate a service organization's security, availability, processing integrity, confidentiality, and privacy controls, ensuring they meet industry standards. Unlike ISO 27001, which prescribes a specific set of controls, SOC 2 is based on the Trust Services Criteria (TSC), allowing organizations to prioritize and implement controls that best align with their risk management strategy and business objectives.

SOC 2 reports are intended for users who need detailed information about a service organization's controls, particularly those concerning the security, availability, and processing integrity of systems that handle data and the confidentiality and privacy of the information processed. This flexibility makes SOC 2 a practical choice for organizations that must address specific client requirements and operational goals.

Trust Services Criteria (TSC)

The Trust Services Criteria (TSC) provides a framework for evaluating an organization's security and operational controls. These five principles—Security, Availability, Processing Integrity, Confidentiality, and Privacy—allow organizations to focus their compliance efforts on areas most relevant to their business.

Security (Common Criteria) is mandatory for all SOC 2 reports, as it ensures protection against unauthorized access and security threats. The remaining four criteria—Availability, Processing Integrity, Confidentiality, and Privacy—are optional and can be included based on the organization's services and customer requirements.

SOC 2's customizable nature allows businesses to tailor compliance efforts by prioritizing controls directly supporting their operational and security needs. By selecting the most relevant criteria, organizations can ensure that their compliance strategy is effective and efficient, balancing strong security practices and business flexibility. This adaptability makes SOC 2 particularly valuable for service providers, enabling them to demonstrate a commitment to security while addressing customer-specific expectations.

Mandatory:

- **Security (Common Criteria):** Protecting systems and data against unauthorized access. For example, implementing multi-factor authentication (MFA) and firewalls is shared under this criterion.

Optional:

- **Availability:** Focuses on system uptime and reliability. For instance, a SaaS provider may include redundancy measures like failover systems and backup data centers.
- **Processing Integrity:** Verifies that systems process data accurately and as intended. A financial services company might monitor transaction logs to ensure that no data corruption occurs.
- **Confidentiality:** Addresses the protection of sensitive information such as trade secrets, contracts, or personally identifiable information (PII). Encryption and access controls are commonly implemented under this criterion.
- **Privacy:** Ensures the proper collection, storage, and use of personal data. A healthcare company handling patient information might implement compliance controls aligned with HIPAA or GDPR.

SOC 2 Audit Types

SOC 2 provides two audit options, allowing organizations to select the best approach for their business needs and customer expectations. This flexibility makes it suitable for companies at different stages of security maturity—whether they need an initial validation or a long-term assessment of their controls.

Type I Audit

Evaluates the design and implementation of controls at a specific moment. It provides a high-level snapshot of an organization's security posture, often as a first step to show that controls are in place.

Example: A startup launching a new SaaS platform may pursue a Type I audit to reassure customers that essential security measures have been implemented quickly.

Type II Audit

Assesses the operating effectiveness of controls over a period, typically 6–12 months. This audit provides a deeper evaluation, demonstrating how well security practices are maintained and followed over time.
Example: An IT Asset Management (ITAM) provider may undergo a Type II audit to show enterprise clients that data protection policies are consistently applied and monitored.

Market Applicability of SOC 2

SOC 2 is a key certification for service providers in North America, particularly in the U.S. and Canada, where it is widely recognized as a benchmark for security and compliance. By aligning with the Trust Services Criteria most relevant to their customers, businesses can showcase compliance in a way that directly supports their objectives while strengthening stakeholder confidence. This customer-focused assurance is especially critical in technology-driven industries, including:

- **Cloud Computing Providers** – Ensures data security, availability, and integrity for customers relying on cloud services.
- **Software-as-a-Service (SaaS) Companies** – Demonstrate secure, reliable, and private customer data handling.
- **IT Asset Management (ITAM) Vendors** – Proves adequate safeguards for managing sensitive enterprise asset data.

SOC 2 Attestation Process

The SOC 2 compliance process is thorough but flexible, allowing organizations to tailor compliance efforts based on their specific needs. The process includes:

1

Define Scope & Objectives

Identify the systems, processes, and services handling sensitive customer data, including infrastructure, applications, and data workflows. Determine which Trust Services Criteria (TSC)—Security (mandatory), Availability, Processing Integrity, Confidentiality, or Privacy—are relevant to your organization.

2

Perform a Readiness Assessment

Evaluate existing security controls against SOC 2 requirements to identify gaps, such as weak access controls, insufficient monitoring, or missing incident response plans. Document findings and prioritize remediation efforts to strengthen compliance.

3

Build a Compliance Team

Assign a compliance lead and involve key departments—such as IT, security, HR, and legal—to define roles, ensure smooth implementation, and maintain compliance responsibilities over time.

4

Design & Implement Controls

Address security gaps by aligning with SOC 2 best practices, including:

- **Access Controls** – Enforce least privilege, multi-factor authentication (MFA), and identity management.
- **Data Protection** – Encrypt data at rest and in transit to safeguard sensitive information.
- **Incident Response** – Develop and test response plans to detect, mitigate, and report security incidents.
- **Monitoring & Logging** – Enable continuous monitoring, centralized logging, and alerting for suspicious activities.
- **Change Management** – Implement formalized policies for system updates and modifications.
- **Security Awareness Training** – Educate employees on security best practices to minimize human error and insider threats.

5

Document Policies & Procedures

Establish and maintain documentation outlining security controls, risk management practices, and compliance procedures, including:

- Information Security Policy
- Access Management Policy
- Incident Response Plan
- Data Retention & Disposal Policy
- Vendor Risk Management Policy

6

Engage a CPA Firm for Audit

Evaluate existing security controls against SOC 2 requirements to identify gaps, such as weak access controls, insufficient monitoring, or missing incident response plans. Document findings and prioritize remediation efforts to strengthen compliance.

7

Undergo the Audit

Assign a compliance lead and involve key departments—such as IT, security, HR, and legal—to define roles, ensure smooth implementation, and maintain compliance responsibilities over time.

8

Review Findings & Maintain Compliance

After receiving the SOC 2 attestation report, implement any corrective actions, establish continuous monitoring, and prepare for annual or periodic re-audits to maintain compliance. Communicate SOC 2 compliance to clients and stakeholders to reinforce trust and security commitments.

Timelines and Deliverables

The duration of a SOC 2 audit varies based on the organization's size, complexity, and readiness. A SOC 2 Type I audit typically takes five weeks and two months to complete. For a SOC 2 Type II audit, the process includes an observation period of three to twelve months, followed by an additional six to eight weeks for the auditor to finalize the report. The outcome is an attestation report, providing an in-depth evaluation of the organization's security practices. This report is a valuable tool for building trust and is often shared with customers as proof of compliance.

SOC 2's focus on tailored controls, audit type flexibility, and customer assurance emphasis makes it a powerful choice for service-oriented businesses. Addressing specific operational needs allows organizations to meet customer expectations without overcomplicating their compliance efforts.

ISO 27001 AND SOC 2 PROCESS TIMELINES

The time required to achieve ISO 27001 certification, SOC 2 Type I, and SOC 2 Type II varies depending on:

- **Organizational Complexity:** Larger, more complex organizations may require more time.
- **Existing Security Measures:** Organizations with mature security frameworks can often accelerate the process.
- **Resource Allocation:** Dedicated personnel and external consultants can reduce timelines.
- **Auditor Availability:** Scheduling audits with certification bodies or auditors can add delays.

Here are the general processing timelines for each:

Certification / Report	Preperation Phase	Audit / Observation Phase	Total Time
ISO 27001	3 - 6 months	1 - 2 months	4 - 9 months
SOC 2 Type I	2 - 4 months	A few weeks to 1 month	3 - 5 months
SOC 2 Type II	2 - 4 months	3 - 12 months (observation) + 1 month audit	6 - 18 months

ESSENTIAL TOOLS FOR ISO 27001 AND SOC 2 COMPLIANCE

Achieving ISO 27001 and SOC 2 compliance is easier with the right tools.

These tools help automate security monitoring, manage IT assets, centralize policies, and streamline incident response. By leveraging them, organizations can meet regulatory requirements, reduce risks, and improve operational efficiency. Below are key categories of tools that support compliance:

Automated Monitoring and Reporting
These tools track system activity, detect security threats, and generate reports in real-time. They collect and analyze log data, alerting teams to suspicious activity or compliance violations.
Examples: Splunk, SolarWinds

IT Asset Management (ITAM) Tools
ITAM solutions help track and manage hardware, software, and other IT assets throughout their lifecycle. They provide real-time visibility, automate inventory tracking, monitor usage, and ensure compliance with data protection policies.
Examples: Teqtivity, ServiceNow

Policy Management Software
These platforms centralize the creation, storage, and management of compliance policies. They enable organizations to draft policies, track changes, manage approvals, and ensure employees can access the latest guidelines.
Examples: Confluence, LogicGate

Compliance Management Platforms
These platforms are designed to simplify compliance efforts and automate control tracking, risk assessments, and evidence collection. They integrate with business systems to monitor security practices, generate reports, and provide real-time compliance insights.
Examples: Secureframe, Drata

Incident Response Tools
These tools detect, manage, and mitigate security incidents in real time. They provide automated alerts, track incidents, and coordinate responses to contain threats while maintaining compliance with security standards.
Examples: CrowdStrike Falcon, Rapid7

DRIVING ITAM EXCELLENCE THROUGH CERTIFICATION

Protecting sensitive enterprise data is a core IT Asset Management (ITAM) priority. Certifications like SOC 2 and ISO 27001 help ITAM providers ensure strong security measures, comply with industry regulations, and build client trust. By meeting these standards, they can offer dependable, well-managed services while safeguarding valuable business assets.

ISO 27001's Fit for ITAM

ISO 27001 provides a structured, globally recognized framework for managing risks and securing ITAM operations. Its emphasis on information security, risk assessment, and continuous improvement makes it especially valuable for ITAM providers working with international clients or operating in highly regulated industries.

Key benefits of ISO 27001 for ITAM:

- **Proactive Risk Management** – Mandatory risk assessments help ITAM providers identify and address vulnerabilities, such as unauthorized access to asset data or improper hardware disposal.
- **International Credibility** – Certification assures compliance with globally recognized security standards, instilling confidence among stakeholders and clients worldwide.
- **Standardized Security Practices** – Establishes uniform security policies for IT asset management, ensuring secure handling throughout onboarding, usage, and decommissioning.
- **Regulatory Alignment** – Integrates with frameworks like GDPR and ISO 27701, helping ITAM providers navigate multiple compliance requirements more efficiently.

SOC 2's Fit for ITAM

SOC 2's flexible framework and customer-focused approach make it an ideal choice for ITAM providers in service-driven industries. By allowing providers to tailor controls to specific client needs, SOC 2 ensures security measures are relevant and practical, addressing key concerns efficiently.

Key benefits of SOC 2 for ITAM:

- **Strong Data Protection** – Ensures customer information's confidentiality, integrity, and availability, covering critical assets like hardware inventories, software licenses, and user data.
- **Enhanced Client Confidence** – Third-party attestation validates security measures, reinforcing trust and strengthening customer relationships.
- **Regulatory Alignment** – Supports compliance with data protection laws such as GDPR and CCPA by meeting Trust Services Criteria for Confidentiality and Privacy.

Teqtivity's SOC 2 Type II Compliance

At Teqtivity, maintaining the highest security standards, operational reliability, and customer trust is a core priority. Achieving SOC 2 Type II compliance reinforces our dedication to protecting sensitive data and delivering a secure IT Asset Management (ITAM) experience.

This certification differentiates us in key ways:

- **Transparency:** We provide enterprise clients with detailed attestation reports, demonstrating our robust data security and operational integrity while ensuring clear visibility into our compliance efforts.
- **Reliability:** Ongoing SOC 2 audits verify that our security controls are exceptional, giving clients confidence that their sensitive asset data is managed securely and without disruption.
- **Scalability**: Our SOC 2 compliance enables us to adapt to the needs of enterprises across industries and regions, ensuring secure and efficient IT asset management as organizations grow.

Ready to see how ITAM helps streamline your path to SOC 2 compliance? Take a product tour today and discover how our solutions support your security and compliance goals.

WHICH FRAMEWORK TO CHOOSE?

Choosing between ISO 27001 and SOC 2 depends on your organization's goals, market focus, industry requirements, and compliance priorities. Below is a detailed comparison and breakdown to guide your decision:

Table Comparison: ISO 27001 vs SOC 2

Criteria	ISO 27001	SOC 2
Approach	Comprehensive framework requiring implementation of an Information Security Management System (ISMS).	Audit-based assessment focusing on customer-specific security assurances.
Scope	Covers risk management, policies, procedures, and continuous improvement of security practices.	Evaluates security controls related to the Trust Services Criteria (TSC): Security, Availability, Processing Integrity, Confidentiality, and Privacy.
Market Applicability	Global standard applicable to organizations of all sizes, particularly in regulated industries.	Primarily used in North America, it is most relevant for service organizations handling customer data.
Industry Application	Finance, healthcare, IT, government, and multinational corporations.	SaaS companies, cloud providers, IT asset management (ITAM), and technology service firms.
Certification Process	Conducted by an accredited ISO certification body; results in a formal certificate.	Independent audit conducted by a Certified Public Accountant (CPA); results in an attestation report. SOC 2 includes two audit types: • Type I, which evaluates controls at a specific point in time, and • Type II, assesses control effectiveness over a period.
Timelines	Typically 3–6 months for initial certification, with annual surveillance audits.	Typically 3–6 months for Type I and 6–18 months for Type II
Deliverables	ISO 27001 certification issued by an accredited body.	SOC 2 attestation report verifying compliance with selected Trust Services Criteria.
Rigor	High—requires ongoing risk assessments, audits, and security controls.	Moderate to high—depends on Type I (design-focused) or Type II (operational effectiveness).
Suitability	Best for organizations requiring global recognition and comprehensive information security management.	Best for service providers that need to demonstrate security controls to customers.

Simplified Decision Matrix:

Question	ISO 27001	SOC 2
Do you operate internationally?	☑ Yes, ISO 27001 is globally recognized	☒ SOC 2 is primarily for North America
Do you need a structured risk management framework?	☑ Yes, ISO 27001 provides a comprehensive ISMS	☒ SOC 2 is more flexible and customer-driven
Do you need fast implementation?	☒ Typically takes 3–6 months	☑ Type I can be completed in 3–5 months

Additional Considerations

Budget and Resources:

ISO 27001 typically involves higher upfront costs due to its comprehensive nature and longer certification timeline.

SOC 2 can be more cost-effective, especially if focused on fewer Trust Services Criteria or Type I audits.

Risk Management Focus:

ISO 27001 offers a deeper focus on risk management, making it suitable for organizations with extensive or diverse risk exposure.

SOC 2 provides targeted controls that address customer-specific risks, such as data breaches or availability issues.

Compliance Integration:

ISO 27001 is better suited for organizations that align with international standards or integrate multiple compliance frameworks.

SOC 2 is ideal for companies prioritizing customer-driven requirements, particularly in North America.

Future Business Goals:

ISO 27001 is preferred for organizations planning global expansion or operating in heavily regulated markets.

SOC 2 is better suited for businesses that build trust with North American clients or expand in service-oriented industries.

Making the Final Decision

- **Global Presence and Long-Term Strategy:** ISO 27001 is the better choice for international organizations or those requiring a rigorous, standardized security framework with broad applicability.
- **Client-Focused Assurance and Regional Focus:** SOC 2 is ideal for organizations prioritizing flexibility, customer-specific compliance, and faster certification timelines, especially in North America.

CONCLUSION

ISO 27001 and SOC 2 are highly regarded for managing information security but serve distinct purposes. ISO 27001 offers a globally recognized, structured approach to risk management, making it well-suited for organizations operating internationally or in highly regulated industries. SOC 2, focusing on customer-specific security assurances and flexible audit options (Type I for point-in-time assessments and Type II for ongoing control effectiveness), is ideal for service providers—particularly in North America—who must demonstrate trust and compliance to clients.

For IT Asset Management (ITAM) providers, SOC 2 certification aligns closely with industry standards by emphasizing Trust Services Criteria such as Security and Confidentiality, ensuring strong security practices.

Choosing the proper framework ensures your organization meets its security, regulatory, and business goals while building stakeholder trust. Evaluating your market, client needs, and operational priorities will help determine whether ISO 27001's structured approach or SOC 2's customer-focused flexibility best fits. Achieving certification strengthens trust, transparency, and competitive advantage regardless of the path chosen.

Teqtivity: Leading ITAM Solutions for Security & Compliance

At Teqtivity, we understand IT Asset Management (ITAM) 's critical role in achieving SOC 2 and ISO 27001 certification—because we've been through the process ourselves. Our SOC 2 Type II certification reflects our commitment to security, compliance, and best practices in ITAM.

Having successfully navigated these standards, we know what it takes to help your organization do the same. Our expertise allows you to streamline compliance efforts, strengthen security, and confidently manage your IT assets.

Let's make certification simpler. Contact us today to discover how our ITAM solutions can support your SOC 2 and ISO 27001 journey.

IT Asset Management Made Easy.

Reduce IT costs, improve security,
and boost productivity with Teqtivity.

Contact us today to schedule a
30-minute product demo & Q&A:

hello@teqtivity.com
www.teqtivity.com

Teqtivity