ISO 27001 Compliance

2023 COMPLETE GUIDE

strongdm

Table of Contents

In this article, we will examine the value that achieving ISO 27001 compliance and certification can offer an organization. You'll learn about the history of ISO/IEC 27001, the benefits of certification, and the difference between ISO 27001 compliance and other related security standards.

By the end of this article, you'll understand how these international security standards support DevOps processes, what controls must be in place to become ISO 27001-compliant, and how ISO 27001 guidelines can help your organization develop a more secure information security management system (ISMS).

01

What is ISO 27001?

ISO/IEC 27001, or ISO 27001, is the international standard that defines best practices for implementing and managing information security controls within an information security management system (ISMS).

ISO/IEC 27001 is one part of the overarching **ISO 27000 family of security standards** determined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The purpose of ISO 27001 is to address how organizations establish, monitor, maintain, and improve their ISMS to keep their data, documents, and other information assets secure.

Organizations that can demonstrate their processes and controls meet ISO 27001 compliance requirements during a two-stage audit are eligible to receive certification from their country's certifying body. This certification verifies that the organization's security systems and IT processes follow current best practices.

02

History of ISO 27001

As cybersecurity needs evolved and more organizations adopted ISMSes, the British Standards Institute Group (BSI Group) sought to define IT standards outlining how organizations should design their ISMS to secure their information assets.

In 1995, the BSI partnered with the United Kingdom Government's Department of Trade and Industry (DTI) to write vendor-neutral standards that uphold the availability, confidentiality, and integrity of an organization's data and proprietary information. These essential IT standards—known as BS 7799—became the foundation for today's ISO 27001 standard.

The first part of BS 7799 focused on general information security management standards. After multiple revisions, the ISO adopted the first part of BS 7799 in 2000 and called it ISO/IEC 17799. After further revision, it was renamed ISO/IEC 27002 in 2007. ISO 27002 provides additional guidance to implement security controls recommended in ISO 27001.

The second and third parts of BS 7799 ultimately became the ISO 27001:2005 standards. These guidelines specify how to implement an ISMS and define standards for analyzing risk within ISMS processes, procedures, and controls. The ISO adopted both parts in 2005 and incorporated a certification option for organizations to demonstrate their ISO 27001 compliance.

The latest version of ISO 27001 cybersecurity by definition—updated in 2013—helped standardize ISMS design and implementation by introducing the Annex SL template. This high-level structure ensures that all systems share a similar look, feel, compatibility, and functionality to comply with multiple ISO standards. The updated version also defines additional controls that further support protecting an organization's information assets.

03

Why is ISO 27001 Important?

As data breaches become more common, companies have become increasingly vigilant about their cybersecurity methods. Now, many organizations expect their partners and vendors to manage their data with a similar level of vigilance.

Keeping data, organizational information, and other information assets safe is a top priority, with many clients and partners expressly dictating security expectations within their contracts. As the only globally recognized standard for information security management, ISO 27001 certification has become a competitive advantage that proves an organization effectively manages its information assets.

"[With ISO 27001] multiple teams are trained and committed to proactively protecting company information and data to maintain high compliance standards."

Compared to similar regional standards defined by individual countries, ISO 27001 is often considered a more rigorous security standard. In part, that's because ISO 27001 focuses on all three pillars of information security: people, processes, and technology.

Unlike IT security initiatives that don't extend past the IT department, the ISO 27001 information security standards involve protecting information assets across the organization. That means multiple teams are trained and committed to proactively protecting company information and data to maintain high compliance standards.

The documentation required for ISO 27001 certification requires businesses to clearly define the business processes and procedures designed to maintain, monitor, and improve the ISMS for exceptional asset security.

It also defines who is responsible for managing these processes. This can improve operational efficiency, reduce human error, improve identity and access management practices, and ultimately provide a more cost-effective way to handle security management.

Since improvement is built into the certification and recertification process, your organization can proactively prevent security breaches and unexpected security gaps, too. Achieving and maintaining ISO 27001 compliance involves regular internal and external audits to find nonconformities and improvements. Plus, management audits ensure that teams successfully complete recommended implementations.

04

Benefits of ISO 27001 Certification

Meeting the rigorous ISO 27001 standards for certification can be resource-intensive and time-consuming, often taking up to 18 months from the start of the initial **certification process** in addition to the baseline **ISO 27001 certification cost**. Despite these requirements, ISO 27001 certification comes with many benefits that set your organization apart from the competition.

For example, as the only internationally recognized security standard for ISMS management, some organizations require the companies they work with to demonstrate ISO 27001 compliance or certification. Thus, certification can help you attract and retain clients.

This gives organizations of all sizes a clear business advantage and a strong reputation within the international marketplace. Plus, even before your organization is officially certified, external audits showing your alignment with ISO 27001 ISMS standards can offer peace of mind to new customers or clients.

The regular auditing schedule required for compliance also helps improve your security posture, streamline regulatory and compliance reporting, and present new opportunities to strengthen your ISMS as your organization grows and new risks emerge. This is a clear benefit of ISO 27001 for startups.

An **ISO 27001 audit** conducted by an auditing firm or certifying body also provides valuable insight that can help your organization create more efficient policies or procedures, close security gaps, and improve controls. Stronger security practices reduce the likelihood of a successful breach, so your organization can avoid fines and maintain customer trust.

As your organization scales and grows, the documentation process that accompanies certification helps clearly define who is responsible for individual security management practices. Yearly auditing lets your team regularly review existing security practices and maintain a strong foundation that strengthens your organization as a whole, showcasing an obvious benefit of ISO 27001 for a small business.

05

ISO 27001 Structure

When the ISO 27001 was updated in 2013, the new version of the ISO 27001 framework adopted a two-part structure. This ISO 27001 overview answers the question, "What does the ISO 27001 standard cover?" in detail.

Part 1 of ISO 27001

The first part of what is in ISO 27001 details 11 clauses (numbered 0-10) that cover the general standards plus the mandatory requirements and necessary documents an organization needs for ISO 27001 compliance. The first four clauses offer context to help your organization better understand what ISO 27001 is for and how to prepare for an ISO 27001 audit, detailing:

1. An introduction to ISO 27001 standards
2. The scope of ISO 27001
3. Normative references
4. Relevant terms and definitions

Clauses 4-10 in the ISO 27001 guidelines explain the fundamental requirements and essential documentation needed to meet during your two-stage initial certification audit, including:

The Context of the Organization

This section details how to create the ISMS Scope document. This document defines the boundaries of your organization's ISMS, what elements of your ISMS are reviewed for certification, and which controls are relevant to the scope of your project.

Leadership

This section helps organizations create a Policy Statement, which explains the stakeholders involved in your ISMS implementation, demonstrates the leadership team's commitment to achieving ISO 27001 compliance, and details who will complete ISMS maintenance tasks.

Planning

This section helps organizations to create objectives based on risks and opportunities. Organizations use this information to establish a plan to maintain a risk-based approach to ISMS management and determine how they will monitor and measure their objectives.

Support

This section leads organizations to determine how they will manage resources to maintain and improve their ISMS in alignment with five essential activities: competence, awareness, communication, documentation, and records management.

Performance Evaluation

This section guides organizations to define procedures for measuring, monitoring, and maintaining ISMS records. It also includes information establishing an internal audit schedule and management reviews to address remediation actions for issues discovered during audits.

Operation

This section helps organizations mitigate risk by creating a required risk assessment report and risk treatment plan.

Improvement

Helps organizations create a process for recording and managing recommendations for improvement and non-conformities discovered during audits.

The initial certification process for ISO 27001 certificate eligibility comprises two stages: a documentation review audit and an evidential audit. The clauses detailed in part 1 of the ISO 27001 structure help organizations prepare written documentation, processes, procedures, and guidelines that explain your ISMS implementation and the business processes that support it.

These documents are then reviewed by an approved, objective auditor during the Stage 1 Documentation Review. During this first stage, the auditor ensures that a company's documentation aligns with ISO 27001 standards and may recommend them for certification.

Part 2 Of ISO 27001

During Stage 2 of the initial certification process, an approved auditor from an accredited certifying body reviews your organization's ISMS processes and controls in action. This audit includes finding evidence that shows controls in place work effectively, efficiently, and in alignment with the documented processes reviewed in Stage 1.

The second part of ISO 27001 is referred to as Annex A. This section details 114 controls across 14 domains that organizations should implement or follow, depending on the scope of their ISMS certification.

Not every control will apply to every company's implementation. Instead, the company defines which controls are relevant based on their scope in a Statement of Applicability (SoA). In the SoA, the organization justifies which of the 114 ISO 27001 controls to implement or not based on their risk assessment, business need, or legal/contractual obligation.

Once the relevant controls are defined, an auditor collects evidence to prove that the controls identified in the SoA align with the standards outlined in Annex A. If the implementation of these controls and appropriate business processes operates as expected, an organization is eligible for ISO 27001 certification.

06

ISO 27001 Controls

The controls defined in Annex A go beyond the responsibility of IT. The 114 controls sorted into 14 category domains detail security measures that support information asset management best practices across the organization, even if the scope of an organization's ISMS ISO 27001 certifications is more limited. These 14 domains include:

- Information Security Policies
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operational Security
- Communications Security
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Compliance
- Information Security Aspects of Business Continuity Management

Creating controls for risk management and demonstrating their success is an essential part of achieving ISO 27001 certification. As part of the organization's risk treatment plan, some control objectives must be put in place during the certification process.

Businesses explain their choice to use or not use each control in Annex A within their SoA. However, based on the updated guidelines in ISO 21007:2013, there is no express requirement to use the controls suggested in Annex A. These controls simply provide a framework for organizations to create controls that help them identify, monitor, and mitigate risks and support their risk treatment plan.

If organizations choose to adopt these controls, ISO 27002 contains further information on how to implement the controls in Annex A. Otherwise, organizations may also choose to implement different controls that may be more applicable to their business, legal, or contractual needs.

07

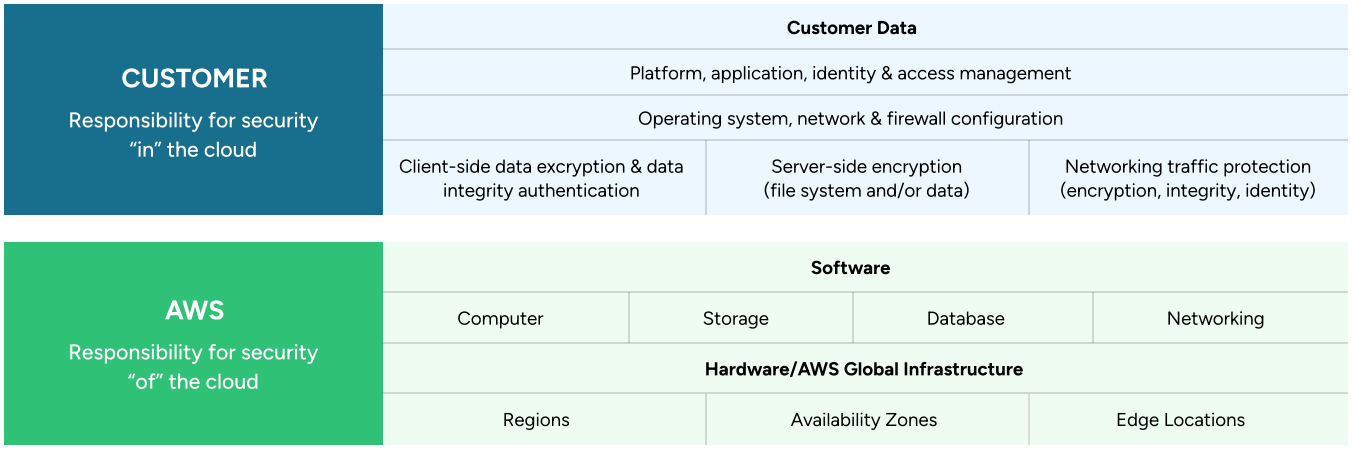
ISO 27001 and DevOps

As organizations scale, continuous deployments performed by traditional DevOps teams may seem to conflict with the expectations of compliance teams eager to achieve or maintain ISO 27001 alignment. However, as more DevOps teams leverage automation to prioritize security controls, pursuing ISO 27001 compliance actually makes a production environment even more secure.

It's undeniable that new development introduces new risks into the production environment. Often, these new risks accrue more frequently than internal audits can reasonably be conducted. Many of the existing controls recommended in Annex A aren't currently designed to support the rapid adoption of cloud environments and DevOps processes.

However, with a robust understanding of new infrastructure environments and ISO 27001 requirements, companies can gain significant benefits to strengthen their security policies within DevOps. Many organizations work with an auditor or consultant to design controls that support their production needs and circumstances.

For example, many modern companies using cloud platforms like Amazon Web Services (AWS) have found it has helped them better manage their security controls. In part, this is because AWS maintains a **shared security model** with its customers. In a shared security model, AWS commits to maintaining the security of the cloud platform's hardware and software, while it expects customers to maintain security standards for information stored within the platform.



Source: aws.amazon.com/compliance/shared-responsibility-model/

Since AWS is ISO 27001-certified and offers services to help organizations meet security standards for ISO 27001 for the cloud, they can assist customers with designing and implementing controls in cloud environments. These security controls allow organizations to streamline DevOps and ensure more secure deployments.

Another critical element of ISO 27001 guidelines that DevOps teams encounter is a thorough separation of duties (SoD) intended to reduce fraud risks and mitigate insider attacks. Many traditional DevOps teams that encourage developers to push code to production independently of additional controls or checks can encounter **challenges with the SoD requirements**.

Under ISO 27001 guidelines, an organization must have separate development, testing, and operational environments; however, these guidelines do not clarify how users are to be divided across those environments. For some organizations, that may require allowing certain developers access to the production environment while others only have access to the development environment.

These requirements leave room for organizations to find the best way to support their workflows and reduce errors by only allowing experts relevant access to certain environments. Leveraging granular access management controls helps intentionally divide duties across your team and protect your organization against insider threats, too.

Some organizations remain concerned that ISO 27001 compliance will add unnecessary roadblocks to DevOps' rapid production schedules. But, automation makes it easier than ever to support the DevOps culture while prioritizing security.

To effectively manage a DevOps environment, companies can use automation to log, monitor, and audit all data access and every command executed. Plus, organizations can incorporate automated audits into your software development lifecycle and continuous integration/continuous delivery (CI/CD) pipeline to meet compliance needs without slowing down DevOps workflows.

08

ISO 27001 vs. SOC 2 vs. ISO 27002 vs. ISO 27003 vs. ISO 17999

ISO 27001 is far from the only standard that covers information security management best practices. In fact, the ISO has many standards that contribute to and support ISO 27001 compliance, offering organizations more tips and recommendations to help them prepare for ISO 27001 certification.

It's important to understand the differences between these individual standards and how they may work together to help your organization strengthen its security posture.

ISO 27001 vs. SOC 2

Service Organization Control 2—or **SOC 2**—is a security framework developed by the American Institute of Certified Public Accountants (AICPA) that aims to control and secure data.

Like ISO 27001, SOC 2 gives organizations a way to discover opportunities to improve their cybersecurity efforts and controls. However, SOC 2 only reviews the existing security controls an organization has in place. Meanwhile, ISO 27001 looks beyond controls to define how the whole ISMS should be implemented, monitored, and maintained.

While SOC 2 is considered an international standard, it is primarily implemented by North American organizations and does not feature a formal certification program. Plus, it's not considered as rigorous or extensive in scope as ISO 27001 regulations.

As regulations across SOC 2 and ISO 27001 do overlap and complement one another, organizations that have achieved ISO 27001 certification may choose to undergo SOC 2 audits to further strengthen their security standards and controls.

Learn more about ISO 27001 and SOC 2 differences.

ISO 27001 vs. ISO 27002

ISO 27002 was first implemented as a guideline for best practices for general information security management. Although ISO 27002 was standardized before ISO 27001, it has become a supporting set of standards designed to complement the guidelines outlined in ISO 27001.

While ISO 27001 defines the standards for certification and alignment with the international best practices for ISMS management, ISO 27002 essentially **provides an ISO 27001 checklist** to help organizations implement the practices and controls needed for certification.

For example, while Annex A of ISO 27001 details the 114 recommended controls for an ISMS, ISO 27002 provides more insight into how to incorporate those controls into your system and prepare for your certification audits.

ISO 27001 vs. ISO 27003

Similar to ISO 27002, ISO 27003 provides additional guidance to help organizations complete their ISMS implementation in alignment with ISO 27001 requirements.

While ISO 27001 details what a compliant ISMS looks like, ISO 27003 gives more information on how to design and develop a compliant ISMS prior to the initial certification process. With the guidance in ISO 27003, organizations can conduct a more streamlined and effective ISMS implementation, knowing that the final product will align with ISO 27001 standards.

Learn more about ISO 27001, ISO 27002, and ISO 27003 differences.

ISO 27001 vs. ISO 27004

While ISO 27002 and 27003 provide actionable guidance on designing the ISMS and implementing the appropriate controls, ISO 27004 provides support to help organizations analyze and evaluate the ISMS on an ongoing basis.

These standards define how to monitor and measure objectives within the ISMS in alignment with ISO 27001 requirements, which is an integral part of maintaining ISO 27001 compliance.

ISO 27001 vs. ISO 17799

ISO 17799:2005 is an obsolete standard that previously offered information on implementing and maintaining security controls to support the required ISO 27001 risk assessment. Now, information covered in ISO 17799 has been replaced by the current ISO 27002 and ISO 27004 standards.

09

ISO 27001: Frequently Asked Questions

Q: What is the current ISO 27001 standard?

ISO/IEC 27001:2013 is the current standard for information security management best practices.

Although the current guidelines reference the most recent comprehensive update in 2013, ISO 27001 incorporates revisions made in 2017 as well. However, the 2017 alterations did not create any new requirements for certification.

Q: When was the last update to ISO 27001

A comprehensive update of ISO 270001 was completed on October 25, 2022.

Q: Is ISO 27001 mandatory?

There is no legal or regulatory obligation for any organization to adopt ISO 27001 or pursue certification.

As each organization requires different controls and has variable business needs that impact how it implements or designs an ISMS, ISO 27001 compliance continues to be optional. However, ISO 27001 certification may be a requirement for some contractual obligations.

Q: Who needs ISO 27001?

While no organization is legally required to obtain ISO 27001 certification, the certification is a common objective for organizations in industries such as financial services, IT, telecommunications, and government agencies.

Organizations of any size that manage sensitive data can benefit from adopting ISO 27001 standards. Certification is also strongly recommended for organizations working with clients internationally.

Q: Is ISO 27001 a framework?

Yes—ISO 27001:2013 is considered a standards framework that organizations can adopt to improve their information security management practices and align with the leading industry best practices.

Q: What are the benefits of ISO 27001?

ISO 27001 certification differentiates an organization, demonstrating its commitment to high information security standards. The increased trust and confidence that accompanies an ISO 27001 certification can help organizations secure new contracts and retain existing clients, especially in industries where organizations maintain a lot of sensitive data.

Some organizations may be contractually obligated to be ISO 27001-certified to work with clients and partners internationally, and certification offers them a clear advantage over their competitors.

Additionally, the rigorous standards of ISO 27001 can help organizations form a solid foundation for maintaining a strong security posture. Regular auditing, documented procedures, and clear roles and responsibilities give organizations a defined structure to maintain high security standards as they grow. The ISO 27001 framework helps organizations reduce risk across their organization and reduce the likelihood of security breaches.

Q: Which model is followed in ISO 27001 standards?

The 2005 version of ISO 27001 incorporated a Plan, Do, Check, Act (PDCA) process model when making changes to the ISMS. However, the most recent version of the standard—ISO 27001:2013—does not recommend a defined process model, encouraging organizations to choose a process model for change and ongoing improvement that supports their unique business processes and objectives.

Q: How many controls does ISO 27001 have?

Annex A currently lists 114 suggested controls across 14 domains as part of the ISO 27001 standard.

10

Simplify ISO 27001 Certification with StrongDM

Meeting and maintaining the rigorous ISO 27001 certification standards can be tough without the right tools and support. Modern organizations need security tools that support how their teams do business without interrupting their work. That's where StrongDM can help.

Our comprehensive dynamic access management platform makes logging, monitoring, and managing your ISMS and security controls easier than ever before. With our all-in-one platform, Security and Compliance teams can easily pull reports and detailed logs for audits, revealing every command, session, and query recorded across your entire IT infrastructure.

Plus, our extensive Identity and Access Management tools help your organization clearly define the segregation of duties and manage access control with granular control policies, even for DevOps teams.

11

Reap the Benefits of ISO 27001 Sooner Than You Think

Our extensive Identity and Access Management tools help your organization clearly define the segregation of duties and manage access control with granular control policies, even for DevOps teams.

However, that's only the beginning of what the dynamic access management platform can do. Our detailed **ISO 27001 compliance guide** spells out all the requirements that StrongDM can support for your organization. Extensive controls and customization options give your organization the power to achieve ISO 27001 certification and create an ISMS that meets your unique needs.

12

More ISO 27001 Resources

- ISO 27001 Audit: Everything You Need to Know
- ISO 27001 Certification Process: a Definitive Guide
- ISO 27001 vs. 27002 vs. 27003: What's the Difference?
- ISO 27001 Checklist: Easy to Follow Implementation Guide
- How Much Does ISO 27001 Certification Cost?
- ISO 27001 vs. SOC 2: Understanding the Difference

StrongDM is a Dynamic Access Management platform that puts people first by giving technical staff a direct route to the critical infrastructure they need to be their most productive. End users enjoy fast, intuitive, and auditable access to the resources they need. Administrators gain precise controls, eliminating unauthorized and excessive access permissions. IT, Security, DevOps, and Compliance teams can easily answer who did what, where, and when with comprehensive audit logs. It seamlessly and securely integrates with every environment and protocol your team needs, with responsive 24/7 support.