ISO 27001 Implementation: Comprehensive Guide

Information Security – or IS – is among the most important aspects of running a business. Ensuring your data is secure is vital for long-term success, and undergoing an IS certification is one of the best ways to achieve this. While all businesses can agree on that, not many understand what the ISO 27001 standard is about and what is needed to implement it. We decided to answer the questions you might have on this topic. With ISO/IEC 27001:2022 deadlines approaching in October 2025, now is the right time to ensure your organization is aligned with the updated controls and requirements.

In this guide, we provide an overview of how to implement ISO/IEC 27001:2022 for companies that decide to proceed with this process based on SecComply more than five years of experience as a trusted compliance partner. We will cover key implementation milestones and challenges, along with the benefits of ISO 27001 implementation and some useful tips on how to avoid common traps.

What is ISO 27001?

ISO/IEC 27001:2022 is an international standard designed to help businesses create a robust Information Security Management System (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It

encompasses people, processes, and IT systems by applying a risk management process to daily data management workflows.

ISMS is a top-down approach ensuring the company has a transparent policy on who can access what information and how they can use it. In addition, it introduces a framework for data handling, which ensures that everyone from C-level to common staff members knows what information they can (and cannot) access. Its main goal is to ensure the CIA (Confidentiality, Integrity, and Availability) of mission-critical sensitive data, both during normal business operations and when under attack by hackers.

To that end, ISO/IEC 27001:2022 provides a comprehensive set of controls comprising best practices in information security. The standard applies to any industry and any company size. It can help small, medium, and large businesses in all sectors keep information assets secure. It is also a basis for adopting enterprise-grade software like Microsoft Active Directory.

More importantly, as an internationally recognized information security standard, ISO 27001 implementation provides a distinct advantage for those businesses that obtained certification. The standard demonstrates the company's ability to securely handle information throughout all business operations and is often included as one of the prerequisites for governmental tenders and corporate contracts. As of today, more than 20,000 companies worldwide are already ISO/IEC 27001:2022 certified.

On top of that, many other certifications are based on ISO/IEC 27001:2022, including SOC 1/2 and TISAX. Even GDPR and DPA's technical requirements are quite well matched with ISO 27001. So, the ISO 27001 implementation is a good foundation for a company to be ready to respond to various IS (information security) requirements according to the industry's best practices.

ISO 27001 Implementation: Key Benefits

Implementing ISO/IEC 27001:2022 provides a lot of benefits that can significantly enhance an organization's security posture and operational efficiency. Here are the key advantages that come with embracing this international standard:

Enhanced Security Measures

The primary benefit of ISO 27001 implementation is the strengthened security of your company's information assets. By establishing and maintaining an ISMS, your organization provides continuous improvement in data protection. This proactive approach reduces the risk of security breaches and data theft, safeguarding your business reputation and maintaining trust with clients and stakeholders.

Compliance with Regulatory Requirements

ISO 27001 ensures that your business complies with various legal, regulatory, and contractual requirements. By aligning your ISMS with ISO 27001, you are better prepared to meet the demands of GDPR, HIPAA, and other privacy laws, which can vary significantly across different locations and industries.

Improved Risk Management

With its systematic approach to risk assessment and mitigation, ISO 27001 implementation process helps businesses identify potential threats to their information assets and implement appropriate controls to manage or reduce them. This process helps in prioritizing security efforts and assists in making informed decisions that protect the organization from various vulnerabilities.

Operational Resilience

ISO 27001 encourages organizations to develop strength against disruptions to their operations. Businesses guarantee consistency even in adverse situations by preparing for potential information security issues. This results in less downtime and quicker recovery from incidents, ensuring minimal impact on business operations.

Competitive Advantage

In a market where clients are increasingly concerned about data security, ISO 27001 certification provides a competitive edge. Demonstrating compliance with an internationally recognized standard reassures clients and partners of your commitment to security, making your business a more attractive proposition in competitive tenders and negotiations.

Cost Effectiveness

Although implementing an ISMS requires an initial investment, the long-term savings from avoiding security incidents can be substantial. The reduction in incidents leads to lower costs related to data breaches, such as legal fees, fines, and remediation costs, not to mention the costs of a damaged reputation.

Streamlined Processes

ISO 27001 helps organizations streamline processes by integrating risk management with business operations. This integration leads to more efficient workflows and improved performance. Employees gain a clearer understanding of their roles and

responsibilities regarding information security, which enhances productivity and reduces the likelihood of errors.

Implementing ISO 27001: The difference between 27001:2013 and 2022 Update

In February 2022, the standard was updated to its newest version 27001:2022. If you implemented 27001 before with the previous 2013 version, you should be aware of all the changes. Therefore, if your company has implemented the ISO 27001 standard with the version of 2013, it is necessary to update to the new 2022 version by October 2025 to maintain compliance.

Fundamental differences of the 2022 revision are as follow:

- First of all, the changes touch only security controls, not the body of the standards. Only the security controls listed in ISO 27001 Annex A have been updated.
- The number of controls has decreased from 114 to 93, and controls are not grouped into 4 sections instead of 14.
- There are 11 new controls, and some controls were merged.

Overall, these changes make the standard more logical and applicable to modern IT and software realities. The 2025 transition deadline also means that organizations currently certified under the 2013 version should start their update process as soon as possible to avoid compliance gaps. Contact our experts to get advice on the ISO 27001 implementation roadmap for your company.

Contact our experts to get advice on the implementation roadmap for your company.

Talk to us

The business value of ISO 27001 implementation

Below we describe the business value delivered by four main sections of this standard that form the ISMS core.

Risk assessment

The risk management process starts with identifying and quantifying the threats to the company's business assets present in the existing operations. Once quantified, such risks form a risk profile that can be managed by applying specific security controls. It allows companies to mitigate security threats by reducing them to acceptable levels for a business based on its risk appetite.

Security policies

These policies are written instructions on the approach an organization should take to deploy and manage the security controls. Defining these policies helps enforce such controls consistently across the entire organization.

Organization of information security

This aspect of the process enables structuring the IS roles and responsibilities within the organization, which is needed to properly manage and maintain the ISMS. As a part of this process, adequate information security training and periodic skill checks are introduced, along with risk profile reviews and implementation process steering meetings.

Asset management

This ISMS component aims to compose and manage a list of assets (any information of business value, like the employee's personal details, CRM data, intellectual property, etc.). Maintaining such a list helps organizations better control the information whose CIA must not be compromised.

As mentioned above, the risks to digital assets must be identified and quantified, appropriate security controls must be deployed, and the risk levels should thus be reduced to the degree the organization feels comfortable with.

The above sections form the core of the ISMS and provide the most business value to every company. The rest of the standard's sections contain instructions on ensuring watertight information management security. They cover the workflow of security incident identification, management, and resolution. On top of that, other sections contain business continuity plans and critical recommendations for controlling physical access to key elements of the organization's ISMS.

After implementing these instructions, your company will benefit from a robust IS management framework, streamlined data security workflows, and industry-leading best practices for incident resolution.

How to implement ISO 27001

Many consider a gap analysis to be a good start for ISMS implementation workflow. It allows organizations to understand the level of operational maturity and readiness for ISO 27001. But, in our experience, a gap analysis doesn't make much sense unless a company has a dedicated IS department. The reason is the lack of skills required to identify the challenges. That's why it's better to dive straight into implementation and solve the issues as they arise.

General overview

Typically, the ISMS is organized in the PDCA (plan–do–check–act or plan–do–check–adjust) cycles. PDCA, also known as the Deming circle/cycle/wheel, is an iterative four-step management method used in business to control and continuously improve processes and products.

For ISO 27001, ISMS goes in year-long PDCA cycles. Here is what each stage encompasses:

Phase	What has to be done	Timeline
Plan	- Define ISMS objectives and goals - Organisation of information security - Implement risk management framework	1-3 months
Do	- Develop key policies (BYOD, HR, Physical security, Encryption, etc.) - Implement Annex A controls to mitigate risks - Perform activities and create periodic records required by the policies	3-6 months
Check	- Accomplish internal ISMS audit - Perform monitoring, measurement, analysis, and evaluation	1-2 months
Act	- Fix issues and non-conformities identified during the internal audit	1-2 months

The most heavyweight phases are Plan and Do. Check and Act are meant to verify and correct what has been done.

After successfully completing one cycle, a company can apply to become ISO 27001 certified. While normally the PDCA cycles are one year long, the initial cycle can be shortened to speed up the certification process.

Companies can implement ISO 27001 themselves or get implementation guidance from certified professionals.

Timeline

On average, expect the ISO implementation to take 6-12 months. The exact timeline depends on many factors: company size, readiness level, management focus, resources, etc. Some companies do it faster, e.g., in a few months, but they are cutting corners instead of practically working on the system. It is not advisable, as you can create technical debt that you will have to pay off with a project on your hands, and the cost of failure can be rather high.

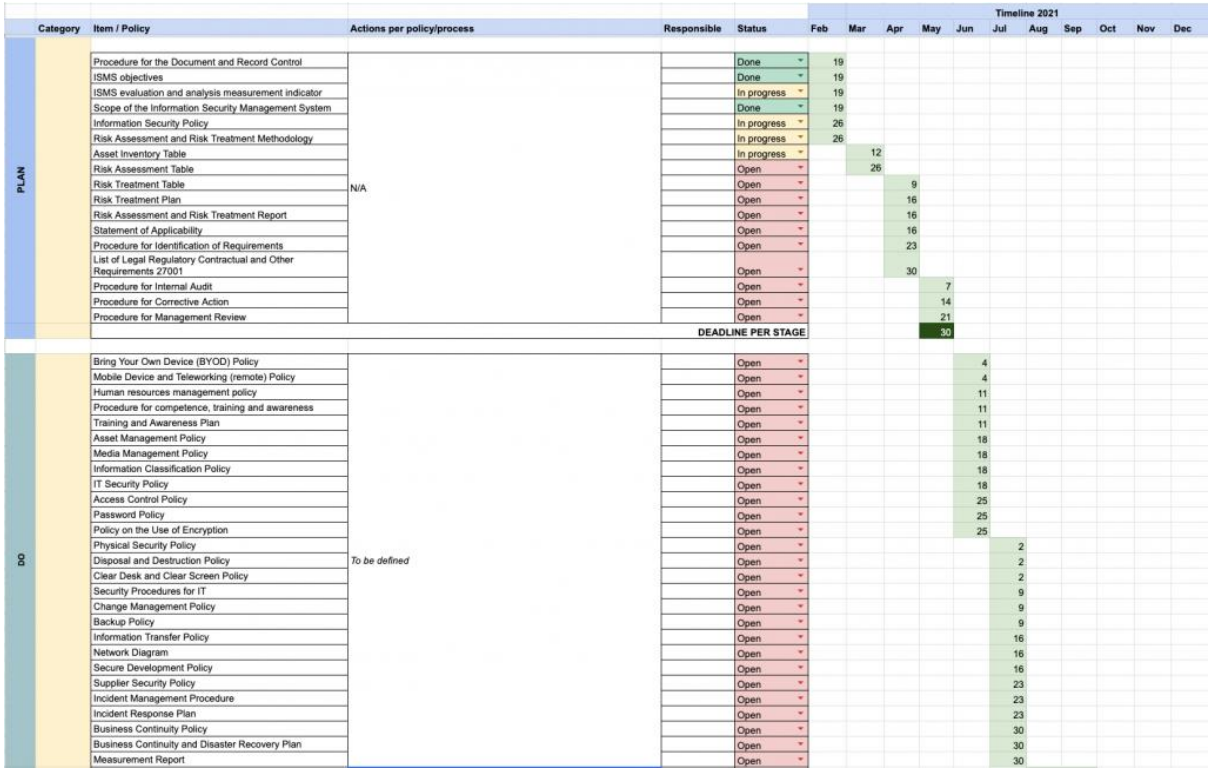
Treating ISMS as a project

To make ISMS implementation efficient and to meet the set deadlines, you need to treat this process as a separate project. It means:

- Having a dedicated PM (Project Manager) or IS manager who has expertise in organizing things and documentation
- Using a project management system like Jira, Youtrack, Trello, Asana, or others to assign the tasks and oversee their completion
- Having a project plan in place and following it
- Performing regular check-ins to ensure the team does not digress.

Having a good project plan in place is extremely important! This is what we normally do as one of the first steps when guiding clients to implement ISO 27001. You can

come up with your own or use the Excel template we provide:



	Category	Item / Policy	Actions per policy/process	Responsible	Status	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
						Timeline 2021										
PLAN		Procedure for the Document and Record Control			Done	19										
		ISMS objectives			Done	19										
		ISMS evaluation and analysis measurement indicator			In progress	19										
		Scope of the Information Security Management System			Done	19										
		Information Security Policy			In progress	26										
		Risk Assessment and Risk Treatment Methodology			In progress	26										
		Asset Inventory Table			In progress		12									
		Risk Assessment Table			Open		26									
		Risk Treatment Table	N/A		Open			9								
		Risk Treatment Plan			Open			16								
		Risk Assessment and Risk Treatment Report			Open			16								
		Statement of Applicability			Open			16								
		Procedure for Identification of Requirements			Open			23								
		List of Legal Regulatory Contractual and Other Requirements 27001			Open			30								
		Procedure for Internal Audit			Open				7							
		Procedure for Corrective Action			Open				14							
		Procedure for Management Review			Open				21							
					DEADLINE PER STAGE				30							
DO		Bring Your Own Device (BYOD) Policy			Open					4						
		Mobile Device and Teleworking (remote) Policy			Open					4						
		Human resources management policy			Open					11						
		Procedure for competence, training and awareness			Open					11						
		Training and Awareness Plan			Open					11						
		Asset Management Policy			Open					18						
		Media Management Policy			Open					18						
		Information Classification Policy			Open					18						
		IT Security Policy			Open					18						
		Access Control Policy			Open					25						
		Password Policy			Open					25						
		Policy on the Use of Encryption			Open					25						
		Physical Security Policy			Open						2					
		Disposal and Destruction Policy	To be defined		Open						2					
		Clear Desk and Clear Screen Policy			Open						2					
		Security Procedures for IT			Open						9					
		Change Management Policy			Open						9					
		Backup Policy			Open						9					
		Information Transfer Policy			Open						16					
		Network Diagram			Open						16					
		Secure Development Policy			Open						16					
		Supplier Security Policy			Open						23					
		Incident Management Procedure			Open						23					
		Incident Response Plan			Open						23					
		Business Continuity Policy			Open						30					
		Business Continuity and Disaster Recovery Plan			Open						30					
		Measurement Report			Open						30					

Assembling a team

Of course, the team can vary from company to company based on your industry, size, level of operational maturity, and other factors. But here're the approximate team structure and roles you would need:

Role	Function
PM/IS manager	ISMS implementer. This person should be skilled in IS and understand what the ISO standard is. Some ISMS implementers might be less experienced in ISO 27001 specifically. If this is the case, they should be backed up with external experts. Main responsibilities: orchestrating the project, managing/writing most of the documentation, keeping track of the project status, etc.

Role	Function
IT and system administration	Lots of ISMS activities depend on the IT department in one way or another. So, good cooperation and dedication from IT are required.
C-level support	ISO standard implementation requires making many company-wide decisions, so a wholehearted buy-in from C-level executives is a must. Somebody with the authority to make decisions and supply a budget must oversee the project.
Departments heads	SO 27001 touches different areas of the company, so all the key stakeholders (e.g., head of engineering, head of PM, head of recruitment/HR) should be onboard.
Expert ISO 27001 or Virtual CISO	In case you don't have an experienced ISO 27001 implementer with dozens of projects behind, external experts will save you from mistakes, point you to important gaps, and prepare you for the audit in general.
Internal auditor	It's often an underestimated role. An internal auditor is needed to make an independent internal evaluation of the ISMS readiness level and identify any gaps.

Be ready to allocate enough capacity for these resources; otherwise, it will drag the project away from timelines.

How to get certified

Certification involves the organization's ISMS being assessed for compliance with ISO 27001 by the certification body. Normally, it's an on-site visit by an auditor lasting several days (up to one week) of interviews. If everything is successful, a company gets a certificate valid for three years.

Finding an auditor is the task for an organization that needs to get a certification. We recommend contacting your local vendors to get quotes since it's always easier to address local providers. It's preferable to work with certification bodies accredited by

one of the IAF members as they guarantee that the certificate will be recognized without any issues.

It's also important to get in touch at the beginning of the project so that auditors keep your organization in mind and set the audit date in advance. Waiting until the last minute is a bad idea as auditors may be booked, and your certification can be delayed.

Remember that auditors are humans, too. So it's your task to help them understand what you've done, explain the processes, and talk through everything.

Expert Tips How to Implement ISO 27001

Based on SecComply extensive cybersecurity expertise, ISO implementation is a complex process. And there are certain things to keep an eye out for. So here are some expert tips:

Tip #1. Properly implement the following policies and controls:

- Risk management
- Device/laptop and BYOD policies
- Access control
- Physical security
- Information classification and protection
- Incident management: reporting and incident recovery

From experience, these controls are especially significant for IT companies. Hence, to make ISO 27001 practically useful, we recommend not cutting corners when implementing them.

Tip #2: Create clear and concise documentation

For an average employee, there will be a lot of documents to get familiar with, which can be overwhelming. To help your personnel learn new rules, create something more distilled, with your key IS rules outlined in 1-2 pages.

Tip #3: Make documents easy to access and navigate

People will not remember everything and will have to look things up. Store the key ISMS policies and documents on a corporate Google Drive or equivalent secure cloud storage. Ensure your ISMS provides easy-to-access information on where to report incidents, how to reach out to IS people, etc.

Tip #4: Invest enough in training your staff

Make it practical and useful, not just pro forma. For the ISO to provide actual business value, all the participants must be on board. Everyone should clearly understand what happens and why it is done this way and not the other.

Conclusion

Yes, implementing ISO 27001 in IT requires a lot of resources, but it’s worth it. Firstly, you will be sure you have watertight data security. Secondly, being ISO-certified shows the high-quality level of your services to customers, partners, and contractors.

Should you have any additional questions on how to implement ISO 27001, feel free to contact us and get a consultation from our experts!

Hear directly from our CEO as she breaks down ISO 27001, its business value, and how organizations can achieve certification smoothly.