

ISO 27001

The Complete Playbook



ISO 27001:

An overview

ISO 27001 is an international standard that outlines the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Co-developed by ISO and the IEC, it offers a structured approach to protecting sensitive information by ensuring its confidentiality, integrity, and availability.

As the only auditable standard in the ISO/IEC 27000 family, ISO 27001 serves as a vital benchmark for organizations committed to demonstrating strong information security practices.

Establishing an Information Security Management System (ISMS) requires you to clearly define your security needs.

These needs stem from three key areas:



Understanding the risks that could impact business objectives



Meeting legal and regulatory obligations



Aligning with the organization's internal information management principles.

Given the comprehensive nature of ISO 27001, knowing what's involved upfront ensures you're prepared for what lies ahead.








Understanding the ISO 27001 Framework

ISO 27001

The ISO 27001 is structured around a set of key clauses and a comprehensive list of controls outlined in its annexes.

Clauses

ISO 27001 includes 10 core clauses, but only clauses 4 to 10 are auditable requirements. They outline the essential requirements for establishing, implementing, and maintaining the ISMS

 Clause 4 Context of the organization	Defines the boundaries of your ISMS. It requires you to understand the internal and external factors that influence your organization and how they impact information security. Also requires determining which stakeholder needs should be addressed by the ISMS.
 Clause 5 Leadership	Emphasizes the importance of top management's commitment to the ISMS. It involves defining roles, responsibilities, and ensuring that security policies align with business objectives
 Clause 6 Planning	Focuses on risk management and setting clear objectives for the ISMS. This includes identifying risks, planning treatment actions, and defining how to measure success. Includes Clause 6.3: Planning of Changes, ensuring that ISMS modifications are systematically managed.
 Clause 7 Support	Ensures that adequate resources, including skilled personnel and communication, are available. Documentation and awareness programs are critical here.
 Clause 8 Operation	Deals with the implementation of security controls and procedures. It involves managing and mitigating risks in day-to-day operations.
 Clause 9 Performance evaluation	Stresses the need for continuous monitoring and evaluation of ISMS performance. Internal audits and management reviews must now consider the evolving needs of stakeholders.
 Clause 10 Improvement	Focuses on continually enhancing the ISMS. It includes handling non-conformities and implementing corrective actions to prevent future issues.

Annex A provides a set of 93 controls grouped into 4 themes. These controls are not mandatory but serve as a guideline for organizations to implement based on their risk profile.

ISO 271 Domain	Number of Controls	Annex
Information Security Policies	2	A.5
Organisation of Information Security	7	A.6
Human Resources Security	6	A.7
Asset Management	10	A.8
Access Control	14	A.9
Cryptography	2	A.10
Physical and Environmental Security	15	A.11
Operational Security	14	A.12
Communications Security	7	A.13
System Acquisition, Developement, and Maintenance	13	A.14
Supplier Relationships	5	A.15
Information Security Incident Management	7	A.16
Information Security Aspects of Business Continuity Manage	4	A.17
Compliance	5	A.18

Updated controls

- | | |
|---|---|
| 01 Threat Intelligence | 07 Data Masking |
| 02 Information Security for Cloud Services | 08 Data Leakage Prevention |
| 03 Information Deletion | 09 ICT Readiness for Business Continuity |
| 04 Physical Security Monitoring | 10 Secure Coding |
| 05 Configuration Management | 11 Web Filtering |
| 06 Monitoring Activities | |

NOTE: The number of controls has decreased from 114 to 93 in ISO 27001:2022. However, this is due to the merging, renaming, and reclassification of existing controls, not necessarily a reduction in security coverage. The updated version also introduces 11 new controls that address emerging security concerns such as cloud security, data masking, and threat intelligence.

Gearing up

Before setting up your ISMS, take a moment to think about which areas of your organization are most valuable and where the biggest risks lie.

You need to decide which parts of the organization and which assets—such as systems, processes, and data—will be included in the ISMS. This should reflect not only what you want to protect but also align with your business goals and strategic objectives.



Conduct a risk assessment

Start by identifying all potential threats and vulnerabilities that could impact the information assets within your ISMS scope. Once identified, evaluate each risk based on its likelihood and potential impact.



Treat these risks

For each identified risk, decide how to address it—whether by mitigating, transferring, accepting, or avoiding it. Choose controls that align with your risk appetite and implement them to reduce risks to an acceptable level.



Develop an SOA

Create a Statement of Applicability (SoA) that lists all the controls you've selected, including justifications for their selection or exclusion.

With the risk assessment done and the Statement of Applicability (SoA) finalized, it's time to focus on the practical steps: documenting processes, aligning controls with business needs, and ensuring compliance.

Developing ISMS

Think of your ISMS documentation as the blueprint for your security architecture. The document should have:

◆ ISMS manual

This guide covers the policies, procedures, and controls you have in place to protect your organization's information.

◆ Information security policies

These are the rules and guidelines your organization follows to keep its information safe, ensuring that everyone is on the same page when it comes to security practices.

◆ Statement of Applicability (SoA)

An SoA lists the security controls you've chosen to implement, along with the reasons why each was selected or excluded, based on your organization's specific risks

◆ Risk register

Risk register is a document that records identified information security risks, their likelihood and impact, and the corresponding mitigation measures.

To get the most out of ISO 27001:2022, align Annex A controls with business processes, such as access management or encryption, ensuring they integrate seamlessly into daily operations. The Annex A structure has changed, and controls are now grouped under Organizational, People, Physical, and Technological controls for better alignment with modern security needs.

Additionally, organizations must track legal, regulatory, and contractual obligations to maintain compliance. Documentation is critical—not only should controls and compliance activities be recorded, but integration into daily operations should also be documented.

Maintaining compliance and adapting to emerging threats is an ongoing effort, requiring continuous updates and improvements to ISMS processes.

Implementing controls and beyond

To implement controls, you need to adopt a future proof approach that ensures your controls are flexible enough to handle tomorrow's risks. Building adaptability into your controls is what ensures lasting resilience and sustained compliance.

Assign roles and responsibilities

◆ Information Security Officer

An ISO is responsible for overseeing the development and management of the ISMS, ensuring alignment with business goals.

◆ Risk manager

He/she identifies, assesses, and mitigates risks to the organization's information assets.

◆ Compliance lead

A compliance lead ensures the organization complies with legal, regulatory, and contractual security obligations.

◆ IT security manager

They manage the technical security infrastructure, ensuring systems and controls are up to date.

◆ Internal auditor

An internal auditor conducts audits to assess compliance with ISO 27001 and identifies areas for improvement.

◆ Incident response coordinator

An ISO is responsible for overseeing the development and management of the ISMS, ensuring alignment with business goals.

Implement technical controls

◆ Access control systems

Implement role-based access controls (RBAC), multi-factor authentication (MFA), and privileged access management (PAM) to regulate who can access specific data and systems.

◆ Network security

Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation to protect against external threats.

◆ Monitoring and logging

Set up security information and event management (SIEM) systems to monitor and log security events, enabling quick detection and response to incidents.

◆ Encryption

Use encryption for data at rest and in transit to protect sensitive information from unauthorized access.

◆ Endpoint security

Implement antivirus software, endpoint detection and response (EDR), and device management to secure end-user devices.

◆ Backup and recovery

Establish automated backup solutions and disaster recovery plans to ensure data integrity and availability in case of incidents.

Build a resilient culture

A well-informed team acts as the first line of defense against potential threats, ensuring that security protocols are not just policies on paper but integral parts of daily operations. During audits, the effectiveness of the ISMS is often assessed through staff interviews.

Creating a resilient culture begins with nurturing a proactive mindset across the organization. It's about making sure everyone feels comfortable discussing risks and security practices, where sharing concerns and ideas is encouraged. Regular training and awareness sessions play a vital role in helping employees grasp their roles within the security framework and understand why following policies matters.

Monitor and review

Effectiveness of controls

Make sure your security controls are doing their job. Regularly check if they're reducing risks as expected, and adjust them if they're not keeping up with evolving threats.

Incident logs and reports

Keep track of any security incidents—big or small. Document what happened, how it was handled, and what can be learned from it to avoid future issues.

Compliance with policies

Ensure everyone in the organization is following the security policies you've put in place. This involves routine checks, audits, and training to keep everyone aligned and accountable.

Risk treatment plan

Monitor how well you're managing risks. Stay on top of your risk treatment strategies—whether you're mitigating, transferring, accepting, or avoiding risks—and make sure they're being executed as planned.

Performance metric

Keep an eye on key indicators of how your ISMS is performing. Metrics like incident response times or the number of compliance breaches will help you see where things are working well and where you might need to make improvements.

Internal audits and findings

Internal audits set the stage for a successful external audit by identifying and addressing any non-conformities in your ISMS before they become major issues. They allow you to fine-tune controls, processes, and documentation, ensuring your organization is well-prepared for the formal certification audit.

NOTE: An internal audit doesn't have to be done by your own team—it can be carried out by a third-party auditor for an objective review. Either way, the goal is to ensure your ISMS is compliant, effective, and ready for certification.

Last stretch before the certification



The last stretch before you get certified, is where you do an internal audit to know if you are audit ready. Use this checklist to ensure you're fully prepared for certification.

Information Security Program

- ☐ ISMS scope and objectives clearly defined.
- ☐ Risk assessments conducted regularly.
- ☐ Incident response plan in place.
- ☐ Business continuity plan developed and tested.

Access Control

- ☐ Role-based access controls implemented.
- ☐ Multi-factor authentication enabled.
- ☐ Regular access reviews conducted.
- ☐ Strong password policies enforced.

Data Protection

- ☐ Data classification scheme established
- ☐ Encryption for data at rest and in transit.
- ☐ Data retention and disposal policies defined.
- ☐ Regular data backups performed and tested.

Third-Party Management

- ☐ Vendor risk assessments conducted.
- ☐ Security requirements included in contracts.
- ☐ Regular vendor performance reviews.
- ☐ Monitoring of third-party access.

Monitoring and Logging

- ☐ Centralized log management in place.
- ☐ Regular log review and analysis procedures.
- ☐ Intrusion detection and prevention systems (IDS/IPS).
- ☐ SIEM solution implemented.

Compliance and Audit

- ☐ Internal audit program established and followed.
- ☐ Compliance with relevant regulations (e.g., GDPR, HIPAA).
- ☐ All security controls documented and maintained.
- ☐ Process for tracking and resolving audit findings.

Training and Awareness

- ☐ Regular security awareness training conducted.
- ☐ Phishing simulations and training assessments.
- ☐ Documentation of all training activities.

Scoring Guide

0-14	High Risk Significant work needed	15-21	Moderate Risk Key areas require attention
22-25	Low Risk Minor improvements needed	26-28	Well Prepared Ready for audit

If your internal audit revealed gaps or areas for improvement, don't rush. Take the time to address these issues, refine your controls, and strengthen your ISMS to ensure you're fully prepared before the official audit.

Non-conformities are gaps between your organization's ISMS and the ISO 27001 standard that are identified during internal or external audits. These issues need to be addressed promptly to gain and maintain your certification.

Effectiveness of controls

A major issue where the ISMS fails to meet ISO 27001 requirements, or a situation where information security is severely compromised. Examples include, absence of a critical security control, lack of a risk assessment process, or failure to implement a required policy.

Minor non-conformities

Smaller, isolated issues that don't pose an immediate threat to information security but indicate potential weaknesses. Examples include, incomplete documentation, minor lapses in control implementation, or occasional deviations from internal processes.

Opportunities for improvement (OFIs)

These are areas where enhancements can be made, even though they may not represent immediate risks to information security. Examples include inconsistencies in documentation, minor gaps in control execution, or deviations from best practices that could be strengthened to improve overall system performance.

Before moving forward with certification, make sure you've addressed any gaps or issues. Once you're confident everything's in place, it's time to prepare for the next step: reaching out to a board-certified auditor.

Before the audit, collect all the evidence

Gather documentation that demonstrates the effectiveness of the ISMS. This includes policies, procedures, risk assessments, incident response records, and monitoring logs.

Audit time!

As you near the final stage of your ISO 27001 journey, it's time to bring in an auditor to verify your ISMS. Choosing the right auditor is crucial, as they will be the ones to assess your readiness and guide you toward certification

Think of your ISMS documentation as the blueprint for your security architecture. The document should have:

◆ Reputation and accreditation

Ensure the certification body is accredited by a recognized authority, such as UKAS or ANAB, and has a strong reputation in the industry.

◆ Industry expertise

Look for auditors with specific experience in your industry to ensure they understand the unique challenges and risks you face.

◆ Experience with similar organizations

Choose auditors who have worked with companies of similar size and complexity, as they'll be better equipped to assess your ISMS effectively.

◆ Cost and flexibility

Compare pricing structures and ensure they offer flexibility in audit scheduling to fit your organization's needs.

While you're at it, also review the auditor's plan in advance, so you understand what areas will be covered, how much time the audit will take, and which departments will be involved.

What does the certification process look like?

The certification process involves two steps: a documentation review to assess your ISMS design and an onsite audit to verify its implementation and effectiveness.

STAGE 1

Documentation review (Initial assessment)

In this phase, the auditor evaluates the ISMS documentation to ensure that it aligns with the requirements of ISO 27001. This stage is typically conducted offsite.

What is reviewed	Purpose
<ul style="list-style-type: none">• Information Security Policy• Risk Assessment Reports• Security Procedures and Controls• Incident Response Plans• Training Records and Compliance Documentation	<p>This stage confirms that the ISMS is not only compliant in theory but is actively implemented and effectively managing risks.</p> <p>Outcome</p> <p>The auditor will provide feedback on any areas of non-compliance or documentation that needs improvement before proceeding to Stage 2.</p>

STAGE 2

Onsite audit (Certification audit)

In this stage, the auditor evaluates the operational effectiveness of your ISMS within a cloud environment. The focus shifts from documentation to practical implementation across your cloud infrastructure.

What is reviewed	Purpose
<ul style="list-style-type: none">• The auditor verifies that documented security policies and procedures are being followed, ensuring they are integrated across cloud services and platforms.• Interviews with staff to gauge understanding of security practices and their application in managing your ISMS.• Inspection of cloud security controls (e.g., access management, data storage encryption, and secure configuration of cloud services).• Evaluation of technical measures, such as encryption, intrusion detection, and response protocols tailored for a cloud-native setup.	<p>This stage confirms that the ISMS is not only compliant in theory but is actively implemented and effectively managing risks.</p> <p>Outcome</p> <p>Based on their findings, the auditor will recommend whether or not to grant ISO 27001 certification. If minor non-conformities are identified, they will need to be addressed before certification can be awarded.</p>

After this, if no gaps or non-conformities are identified, you'll receive your ISO 27001 certification, officially validating your compliance and security measures!

On the off chance that the audit revealed any gaps, don't worry—resolving them should be straightforward and manageable.

Similar to the internal audit, the auditor will come back with conformities, major, minor, and areas of improvement, based on which, you will have to remediate to get your certification done.

As soon as a non-conformity is detected during an audit, document it clearly, detailing the nature of the issue, its scope, and any potential impact on your ISMS.

- Define specific actions to correct the non-conformity and prevent its recurrence.
- Address immediate gaps to reduce risk exposure.
- Focus on broader, more sustainable improvements to your ISMS.
- Ensure that the corrective actions are rolled out promptly.

Once certified, ISO 27001 compliance is an ongoing commitment. To maintain certification, organizations must undergo regular surveillance audits, typically conducted annually. These audits ensure that your ISMS continues to operate effectively and adapts to any new risks or changes within the organization.

What is a surveillance audit?

A surveillance audit is a periodic review conducted after you achieve ISO 27001 certification to ensure that your Information Security Management System (ISMS) remains compliant over time.

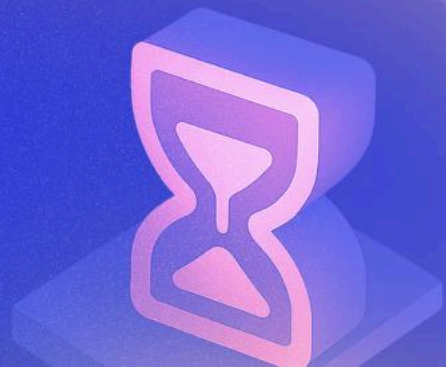
Surveillance audits are typically performed by an **external auditor** from the certification body that issued your ISO 27001 certification.

What can you expect from it?

Surveillance audits, while less extensive than the initial certification, still focus on key areas of your ISMS. The auditor checks for improvements, ensures compliance with any new requirements, and verifies that previous non-conformities have been addressed. Key focus areas include changes in technology or the organization, ongoing risk assessments, continuous improvement efforts, and how well security incidents have been managed.

These audits help ensure your ISMS remains compliant and proactively addresses emerging risks.

Timeline



- **MONTHS 1-2**
Initial preparation
 - Define ISMS scope and objectives.
 - Conduct a risk assessment and choose appropriate controls.
 - Develop key documentation, including policies and procedures.
- **MONTHS 3-4**
Implement controls
 - Deploy and test the selected technical, physical, and human controls.
 - Train staff to ensure awareness of ISMS processes.
- **MONTH 5**
Internal audit & management review
 - Conduct an internal audit to spot any gaps.
 - Perform a management review to assess ISMS performance.
- **MONTH 6**
Stage 1 audit
 - An external auditor reviews your ISMS documentation and readiness.
- **MONTH 7**
Address stage 1 findings
 - Implement corrective actions based on Stage 1 audit feedback.
- **MONTH 8**
Stage 2 audit
 - A comprehensive audit to verify control effectiveness and compliance.
- **MONTH 9**
Certification decision
 - Address any minor non-conformities.
 - Await certification approval.

ISO 27001 certification typically happens after the **Stage 2 audit**, which is in **Month 9**. Once the Stage 2 audit is completed and any minor non-conformities are addressed, the certification decision is made, and you receive your ISO 27001 certification.

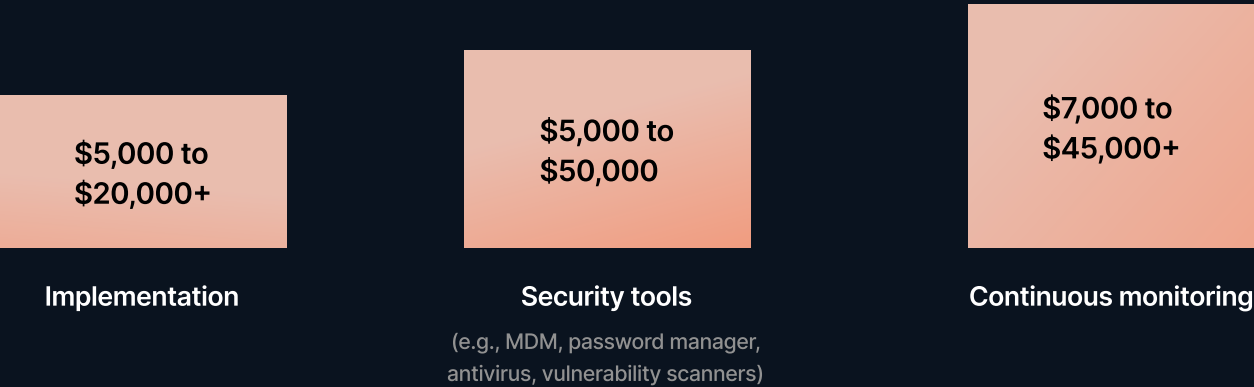
Cost of getting ISO certified



With the timeline in place, it's time to consider another key factor in the certification process. As with any major initiative, there are various elements that can influence the overall investment required.

There's two parts to this, pre-audit cost and the actual audit cost.

Pre audit cost



Security training – \$250 TO \$12,500

Vulnerability assessment & penetration testing (VAPT) – \$1,000 TO \$7,500+

Audit cost

Employee Strength	ISO 27001 Certification	ISO 27001 Surveillance
11-50	\$1,250 - \$2,500	\$1,000 - \$2,000
50-200	\$1,500 - \$4,500	\$1,250 - \$4,000
50-200	\$2,500 - \$6,500	\$2,000 - \$5,500

Think of investment not just from a financial perspective. The man-hours spent managing manual processes like documentation, control implementation, and audit preparation are just as valuable. These efforts can quickly add up, diverting attention and resources away from core business functions.

Here's why Sprinto is your go-to partner for ISO 27001



Manual compliance processes can be time-consuming and resource-heavy. Automation tools, like Sprinto, offer a smarter, more efficient way to streamline compliance efforts and reduce the workload.

◆ **Control mapping**

With Sprinto's integration capabilities, your security controls are automatically aligned with ISO 27001 requirements, ensuring nothing falls through the cracks.

◆ **Effortless monitoring**

Sprinto provides real-time visibility into your compliance status, allowing you to catch potential issues before they escalate.

◆ **No-hassle documentation**

Sprinto automatically collects and organizes all the evidence you need for audits—saving you hours of manual work.

◆ **Continuous support**

From Day 1, Sprinto's team is by your side, guiding you through implementation, training, and audit preparation.

◆ **Automated evidence collection**

Sprinto simplifies the audit process by automatically gathering and maintaining all required documentation and evidence in an audit-friendly format.

◆ **Smart notifications**

Stay on top of your compliance efforts with smart notifications that alert you to any issues or tasks that need immediate attention, ensuring you're always audit-ready.

◆ **Configuration management**

Maintain secure system configurations to reduce vulnerabilities. Regularly review and apply updates to avoid misconfigurations.

◆ **Data Leakage Prevention**

Implement controls to prevent unauthorized access and data exfiltration, such as content filtering and anomaly detection tools.

◆ **Secure coding practices**

Follow secure coding guidelines to reduce software vulnerabilities and prevent exploitation

In just 2 weeks, Officebeacon was ISO 27001 audit-ready. Within 40 days of entering the audit process, they had successfully received their ISO 27001 certification.

[Read Now !](#)



If you're looking for an automated compliance platform to help maximize your cyber security budget, talk to Sprinto's experts today! Sprinto is a compliance automation platform that helps organizations much like yours get compliance-ready in as short a time as possible.

[Schedule a demo today!](#)