Protect ○ Comply ○ Thrive

IT Governance Blog

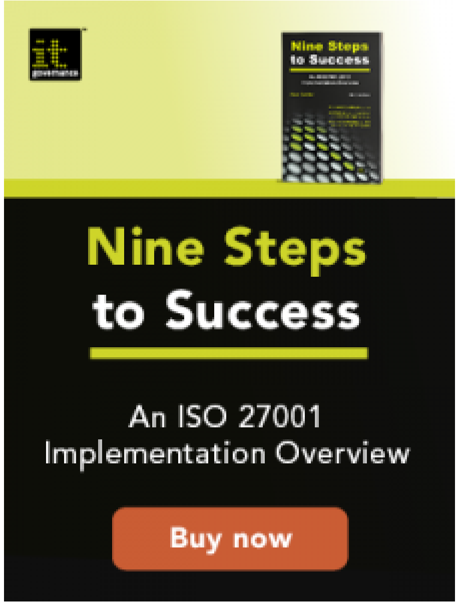
ISO 27001 Checklist: 9-step Implementation Guide

Luke Irwin 18th January 2021

Please note new versions of ISO 27001 and ISO 27002 have now been published.

To learn more about what these updates mean for your organisation, and to buy your copies of ISO 27001:2022 and ISO 27002:2022, please visit our information pages.

We're not going to lie: implementing an ISO 27001-compliant ISMS (information security management system) can be a challenge.



Aide

But as the saying goes, nothing worth having comes easy, and ISO 27001 is worth having.

If you're just getting started with the Standard, we've compiled this 9-step ISO 27001 implementation roadmap to help you.

Step 1: Assemble an implementation team

Your first task is to appoint a project leader to oversee the implementation of the ISMS.

They should have a well-rounded knowledge of information security as well as the authority to lead a team and give orders to managers (whose departments they will need to review).

The project leader will require a group of people to help them. Senior management can select the team themselves or allow the team leader to choose their own staff.

Once the team is assembled, they should create a project mandate. This is essentially a set of answers to the following questions:

- What are we hoping to achieve?
- How long will it take?
- How much will it cost?
- Does the project have management support?

Search the site

Search

CATEGORIES

- Breaches and Ha

? Aide

Step 2: Develop the implementation plan

Next, you need to start planning for the implementation itself.

The implementation team will use their project mandate to create a more detailed outline of their information security objectives, plan and risk register.

This includes setting out high-level policies for the ISMS that establish:

- Roles and responsibilities.
- Rules for its continual improvement.
- How to raise awareness of the project through internal and external communication.

Step 3: Initiate the ISMS

With the plan in place, it's time to determine which continual improvement methodology to use.

ISO 27001 doesn't specify a particular method, instead recommending a "process approach". This is essentially a Plan-Do-Check-Act strategy.

You can use any model provided the requirements and processes are clearly defined, implemented correctly, and reviewed and improved regularly.

- Business Continuity
- Catches of the Month
- Cyber Essentials
- Cyber Resilience
- Cyber Security
- Data Protection
- Education
- Financial Services
- GDPR
- Healthcare
- ISO 27001
- IT Best Practice
- ITIL
- Microsoft Security
- Monthly Data Breaches and Cyber Attacks
- News
- NIS Regulations
- PCI DSS
- Penetration Testing
- Phishing
- Podcast
- Privacy
- Professional Serv

? Aide

You also need to create an ISMS policy.

This doesn't need to be detailed; it simply needs to outline what your implementation team wants to achieve and how they plan to do it.

Once it's completed, it should be approved by the board.

At this point, you can develop the rest of your document structure. We recommend using a four-tier strategy:

1. Policies at the top, defining the organisation's position on specific issues, such as acceptable use and password management.
2. Procedures to enact the policies' requirements.
3. Work instructions describing how employees should meet those policies.
4. Records tracking the procedures and work instructions

Discover how to cut the time and cost involved in ISO 27001 implementation by 50% >>

Step 4: Define the ISMS scope

The next step is to gain a broader sense of the ISMS's framework. This process is outlined in clauses 4 and 5 of the ISO 27001 standard.

- Project Management
- Public Sector
- Ransomware
- Retail
- Risk Management
- Sectors
- Staff Awareness
- Training
- Uncategorised

Aide

This step is crucial in defining the scale of your ISMS and the level of reach it will have in your day-to-day operations.

As such, you must recognise everything relevant to your organisation so that the ISMS can meet your organisation’s needs.

The most important part of this process is defining the scope of your ISMS. This involves identifying the locations where information is stored, whether that’s physical or digital files, systems or portable devices.

Correctly defining your scope is an essential part of your ISMS implementation project.

If your scope is too small, you leave information exposed, jeopardising your organisation’s security. But if your scope is too broad, the ISMS will become too complex to manage.

Step 5: Identify your security baseline

An organisation’s security baseline is the minimum level of activity required to conduct business securely.

You can identify your security baseline with the information gathered in your ISO 27001 risk assessment.

This will help you identify your organisation’s most significant security vulnerabilities and the corresponding ISO 27001 control to mitigate the risk (outlined in Annex A of the Standard).

Step 6: Establish a risk management process

Risk management is at the heart of an ISMS.

Almost every aspect of your security system is based around the threats you’ve identified and prioritised, making risk management a core competency for any organisation implementing ISO 27001.

The Standard allows organisations to define their own risk management processes. Common methods focus on risks to specific assets or risks presented in particular scenarios.

Whatever process you opt for, your decisions must result from a risk assessment. This is a five-step process:

1. Establish a risk assessment framework
2. Identify risks
3. Analyse risks
4. Evaluate risks
5. Select risk management options

You then need to establish your risk acceptance criteria, i.e. the damage that threats will cause and the likelihood of them occurring.

Managers often quantify risks by scoring them on a risk matrix; the higher the score, the bigger the threat.

They'll then select a threshold for the point at which a risk must be addressed.

There are four approaches you can take when addressing a risk:

1. Tolerate the risk
2. Treat the risk by applying controls
3. Terminate the risk by avoiding it entirely
4. Transfer the risk (with an insurance policy or via an agreement with other parties).

Lastly, ISO 27001 requires organisations to complete an SoA (Statement of Applicability) documenting which of the Standard's controls you've selected and omitted and why you made those choices.

Learn more about ISO 27001 risk assessments >>

Step 7: Implement a risk treatment plan

Implementating of the risk treatment plan is the process of building the security controls that will protect your organisation's information assets.

To ensure these controls are effective, you'll need to check that staff can operate or interact with the controls and know their information security obligations.

Aide

You'll also need to develop a process to determine, review and maintain the competencies necessary to achieve your ISMS objectives.

This involves conducting a needs analysis and defining a desired level of competence.

Learn how to create an ISO 27001-compliant risk treatment plan >>

Step 8: Measure, monitor and review

You won't be able to tell if your ISMS is working or not unless you review it.

We recommend doing this at least annually so that you can keep a close eye on the evolving risk landscape.

The review process involves identifying criteria that reflect the objectives you laid out in the project mandate.

A common metric is quantitative analysis, in which you assign a number to whatever you are measuring.

This is helpful when using things that involve financial costs or time.

The alternative is qualitative analysis, in which measurements are based on judgement.

Aide

You would use qualitative analysis when the assessment is best suited to categorisation, such as 'high', 'medium' and 'low'.

In addition to this process, you should conduct regular internal audits of your ISMS.

There is no specific way to carry out an ISO 27001 audit, meaning it's possible to conduct the assessment for one department at a time.

This helps prevent significant losses in productivity and ensures your team's efforts aren't spread too thinly across various tasks.

However, you should aim to complete the process as quickly as possible, because you need to get the results, review them and plan for the following year's audit.

The results of your internal audit form the inputs for the management review, which will be fed into the continual improvement process.

Step 9: Certify your ISMS

Once the ISMS is in place, you may choose to seek ISO 27001 certification, in which case you need to prepare for an external audit.

Certification audits are conducted in two stages.

Aide

The initial audit determines whether the organisation's ISMS has been developed according to ISO 27001's requirements. If the auditor is satisfied, they'll conduct a more thorough investigation.

You should be confident in your ability to certify before proceeding because the process is time-consuming and you'll still be charged if you fail immediately.

Another thing you should bear in mind is which certification body to go for.

There are plenty to choose from, but you must make sure they are accredited by a national certification body, which should be a member of the IAF (International Accreditation Body).

This ensures that the review is actually in accordance with ISO 27001, as opposed to uncertified bodies, which often promise to provide certification regardless of the organisation's compliance posture.

The cost of the certification audit will probably be a primary factor when deciding which body to go for, but it shouldn't be your only concern.

You should also consider whether the reviewer has experience in your industry.

After all, an ISMS is always unique to the organisation that creates it, and whoever is conducting the audit must be aware of your requirements.

Learn more about ISO 27001 certification >>

? Aide

Tackling ISO 27001 implementation?

Even with the advice listed here, you might find the ISO 27001 implementation project daunting.

Nine Steps to Success – An ISO 27001 Implementation Overview is a “must-have” guide for anyone starting to implement ISO 27001.

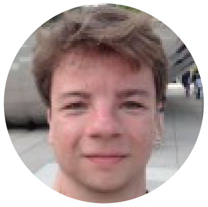
This essential ISO 27001 tutorial details the key steps of the implementation project, from inception to certification and explains your requirements in simple, non-technical language.

A version of this blog was originally published on 18 April 2019.

Recommended reading:

- **Requirements for achieving ISO 27001 certification**
- **What are the 14 domains of ISO 27001?**
- **How do I prepare for ISO 27001 certification?**

About The Author



Luke Irwin

Luke Irwin is a writer for IT Governance. He has a master’s degree in Critical Theory and Cultural Studies, specialising in aesthetics and technology.

No Responses

Aide