DataGuard

GUIDE

ISO 27001 CERTIFICATION: YOUR ULTIMATE GUIDE

INTRODUCTION TO ISO 27001 CERTIFICATION

Obtaining an ISO 27001 certification is the no.1 indicator to suppliers, customers, and stakeholders that you take information security seriously. It's also a great starting point to set up a robust cyber strategy.

In this ultimate guide, we're going to cover the topic from start to finish. At the end, you'll know everything you need to know about the scope of your (potential) ISO 27001 certification journey.

⟶ **Get your free ISO 27001 certification guide**

No matter if you're an SMB or a large-scale corporate, this guide compiles the most relevant information all in one place.

WHAT IS ISO 27001?

ISO 27001 sets the global standard for an information security management system (ISMS) that pursues the ultimate goal of establishing a framework for keeping information secure. In 2022, the ISO 27001:2013 version was updated to its latest version, the ISO 27001:2022.

An ISMS **creates a set of rules and procedures** that help mitigate the damage of a cyber or ransomware attack as well as a security breach, which, nowadays, needs to be on every company's agenda.

The stats speak for themselves: During the third quarter of 2022, a staggering 108.9 million accounts fell victim to breaches, marking a substantial 70% surge compared to the preceding quarter. You can find the full report on What to expect in 2023: Trends and Predictions for Information Security here.

Using an ISO 27001-compliant ISMS lets you easily and affordably **manage the security of your organisation's data**. Plus, it makes your customers, investors, and other important stakeholders feel confident that you're following the best global practices for keeping information safe.

⟶ **Learn "What is ISO 27001"**

WHAT IS THE ISO 27001 CERTIFICATION?

The ISO 27001 certification is granted when you meet the requirements of the ISO 27001 standard. Once you've established your ISMS, an **independent accredited certification body** conducts an audit and **issues a certificate** upon successful completion. A certification body is basically an independent institution that can certify companies with the ISO 27001 certificate after successfully passing an external audit.

The certification essentially **proves you** have taken the appropriate steps to **protect your most valuable information**. This includes intellectual property, trade secrets, proprietary data, and other valuable assets. While the specific term "intellectual property" may not be used, the principles of information security within the ISO 27000 series standards are designed to encompass various forms of valuable and sensitive information, including intellectual property.

WHAT IS THE ISO 27001:2022 STANDARD?

The ISO 27001:2022 edition stands as the most recent iteration of ISO 27001, the global benchmark for information security management systems that you must adhere to receive your certification. If you're already certified and need to transition to the 2022 iteration, then our ISO 27001:2022 transition guide is your go-to resource.

WHAT IS AN ISMS?

An information security management system (ISMS) provides a framework of **documented policies, procedures, and controls** designed to **mitigate information security risks.** Once you've built your ISMS, getting it certified against an international standard such as ISO 27001 is best practice.

⟶ **Learn "How is the ISO 27001 standard related to an ISMS"**

HOW TO ESTABLISH AND IMPLEMENT AN ISMS?

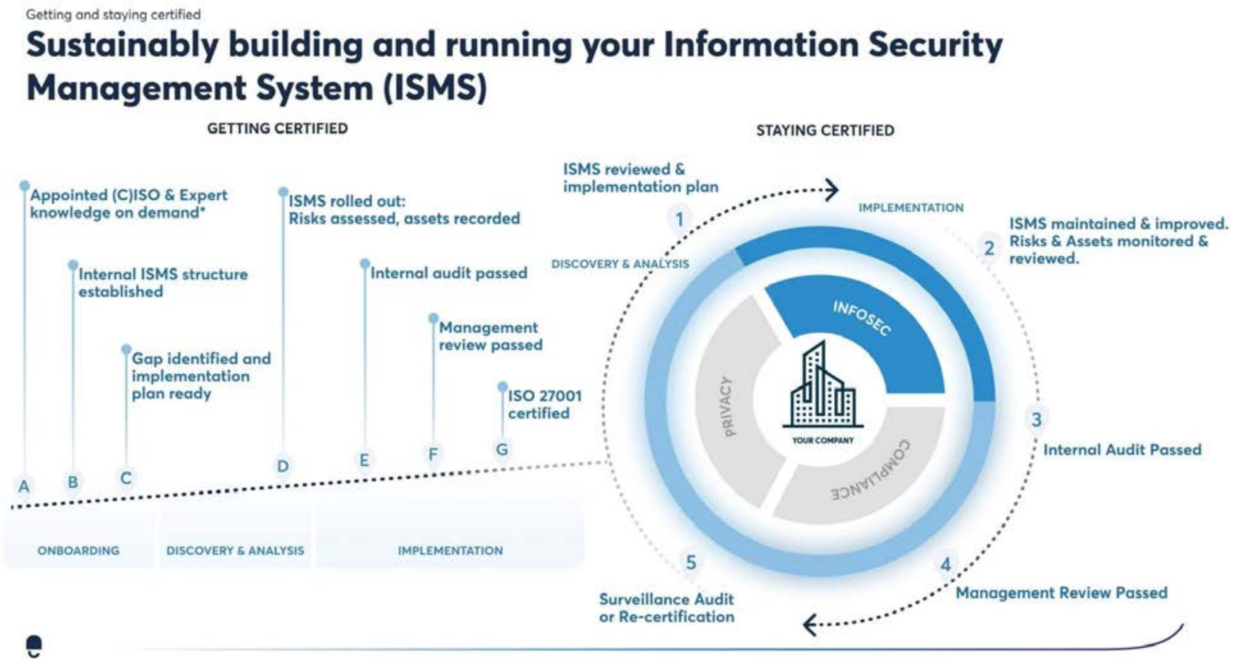
Establishing and implementing an ISMS, in its simplest form, can be broken down into 4 phases, also known as the PDCA cycle:

1. **Plan:** This is the phase in which you establish the ISMS, i.e. get your documentation in check.

2. **Do:** The processes and procedures you established in the plan phase, also need to be implemented and operated — this is what happens during the DO phase of the PDCA cycle.

3. **Check:** Then you check whether your ISMS aligns with the ISO 27001 standard and identify any gaps. This happens during internal and external audits.

4. **Act:** During this phase, you improve the ISMS and close any information security gaps to ensure you can obtain and keep your ISO 27001 certification.


Getting and staying certified
Sustainably building and running your Information Security Management System (ISMS)
GETTING CERTIFIED
STAYING CERTIFIED
Appointed (C)ISO & Expert knowledge on demand*
Internal ISMS structure established
Gap identified and implementation plan ready
ISMS rolled out: Risks assessed, assets recorded
Internal audit passed
Management review passed
ISO 27001 certified
A
B
C
D
E
F
G
ONBOARDING
DISCOVERY & ANALYSIS
IMPLEMENTATION
ISMS reviewed & implementation plan
1
DISCOVERY & ANALYSIS
IMPLEMENTATION
2
ISMS maintained & improved. Risks & Assets monitored & reviewed.
3
Internal Audit Passed
4
Management Review Passed
5
Surveillance Audit or Re-certification
INFOSEC
PRIVACY
COMPLIANCE
YOUR COMPANY

WHY IS ISO 27001 IMPORTANT? WHY GET AN ISO 27001 CERTIFICATION?

The certification is beneficial for a number of reasons; these are the most important ones:

Establishes stakeholder trust:

Possessing an ISO 27001 certificate demonstrates your dedication to safeguarding information and underscores your business's credibility in partners' eyes. This can give you a competitive edge and enhance your brand reputation.

Assists legal compliance:

ISO 27001 certification aids in meeting your various business, legal, financial, and regulatory commitments. By identifying statutory and regulatory requisites, you can mitigate the likelihood of costly breaches, subsequently reducing the risk of expensive legal consequences and fines.

Secures personal data and intellectual property:

The ISO 27001 certification process offers an impartial evaluation of your information security strategy. It could also assist in managing your intellectual property and data sources while creating tangible proof of implementation.

Mitigates costly cyber-related data breaches:

Data breaches come with a hefty price tag. In 2023, the average cost of a data breach was estimated at around $4.45 million (IBM, 2023). The ISO 27001 certification safeguards your information through established procedures and processes, helping you avoid such financial burdens.

Sets the foundation for reducing risk:

Risk management is important to keep your business operations running and should be carried out continuously. Yet setting up a risk management structure from scratch can be immensely time-consuming — ISO27001 gives you a framework to define the criteria of risk management in your company.

Want a more detailed insight into why getting ISO 27001 makes sense? Download our free ISO 27001 - Why Get Certified e-book here.

WHO NEEDS ISO 27001 CERTIFICATION?

The ISO 27001 certification is relevant for pretty much any business dealing with information and data. It's not mandatory, yet it's common practice and often a prerequisite for many business stakeholders. This is because doing business with you without relevant policies and procedures to manage risks could put their information and data at risk.

Industries particularly affected by ransomware and cyber-attacks and where ISO 27001 certification is becoming the norm include:

- Education/Research
- Government/Military aka. the Public sector
- MedTech/Healthcare
- Communications

Yet, with the current upward trend of cyber criminality, all businesses — from SMBs to large-scale corporates - need to consider information security. And getting ISO 27001 certified is a clear roadmap to making it a priority.

HOW HARD IS IT TO GET ISO 27001 CERTIFIED?

Getting ISO 27001 isn't easy by default — in fact, the process does come with its complexities, especially with plenty of stakeholders and complicated processes involved.

Furthermore, ISO 27001 certification is usually a top-down decision, which means that top management must be involved in the process sooner or later. As a business, you should ensure that you have the right experience within the team to convince decision-makers about the certification and to navigate the whole process.

Here are four tips for a successful ISO 27001 certification:

⟶ **Learn "Tips for certification on ISO 27001 & TISAX"**

COMMON PITFALLS TO AVOID WHEN GETTING ISO 27001 CERTIFICATION

As an organisation, implementing ISO 27001 provides you with several benefits including easier compliance with legal requirements, better security for data, and improved stakeholder confidence. The catch: successful implementation of the standard can be a major challenge to organisations doing it for the first time.

Since the ISO 27001 standard is designed to be customisable to your organisation, there are several instances where businesses could go wrong in their implementation process. Based on our extensive experience of working with varied clients, we've compiled a list of the most common pitfalls businesses face when implementing the standard along with advice on what you can do to avoid them.

Not defining the right scope

Finding the right scope for implementing your organisation's ISMS can be tricky. Organisations often set over-ambitious goals for the implementation of their ISMS, leading to the adoption of several redundant and unneeded controls and processes.

This can lead to resource wastage, increased cost of information security, and demotivated employees chasing unachievable targets. On the other hand, an organisation may define their scope too narrowly, and the needed controls may not be adopted. This could lead to noncompliance with the ISO 27001 standard and can make it appear that your organisation is not in control of its ISMS during the certification audit.

Lack of management

Commitment In many organisations, implementing the ISO 27001 is considered to be an IT exercise and the responsibility of the IT department of the business. In reality, it is a management standard for information security. The upper management in an organisation may not see the value the implementation of ISO 27001 adds to the business and they may be hesitant to fully commit to its implementation.

Too few resources

Often, the implementation of the ISO 27001 falls to a particular individual or team within the organisation. This type of approach can create information security silos where only very few individuals are aware of the controls and procedures around the ISMS and other aspects of the standard. The loss of such individuals could cause the collapse of the entire ISMS.

Find out which two other pitfalls are common for all businesses and how you can prevent these pitfalls from happening in our free guide about the most common pitfalls during ISO 27001 Certification.

HOW LONG DOES IT TAKE TO GET ISO 27001 CERTIFIED?

Usually, the process can take 6 to 12 months, depending on business size and complexity. The use of designated solutions like the DataGuard platform, can fasten the process to as little as 3 months (also depending on a business' properties).

This phase is called the ramp-up phase, where the main chunk of work is done. You carry out a gap analysis that aims to close up to 50% of your company's most significant risks in as little as 8 weeks.

Getting through the process involves:

- Defining your scope
- Building your Information Security Management System (ISMS)
- Identifying and managing risks
- Protecting your information assets
- Passing your ISO 27001 audit
- Maintaining your ISMS, keeping your certificate

Also, if you're in the mindset of scaling, we definitely recommend getting started sooner rather than later. Scaling your ISMS alongside your company growth is easier.

DOES THE ISO 27001 CERTIFICATION EXPIRE?

The ISO 27001 certification needs to be **renewed every 3 year**s. Yet, it's recommended to remain **compliant to protect** your company's assets and ensure your information remain safe. Furthermore, companies must pass the annual surveillance audit to verify compliance and to avoid expiry of the certification before the three years cycle.

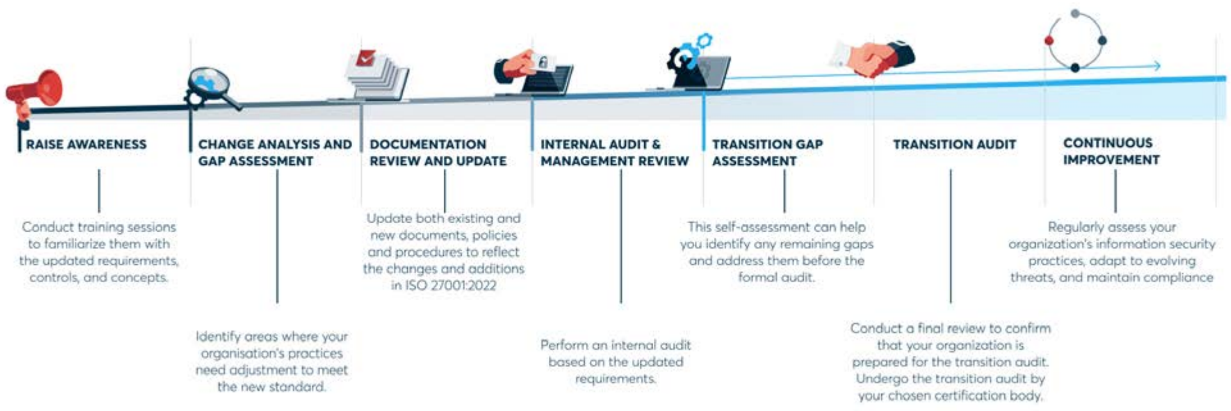
> ***"If an organization does not pass the surveillance audit conducted by the external auditor, their ISO 27001 certification could potentially expire before the full 3-year term is completed. The surveillance audits are typically conducted annually to ensure ongoing compliance with the ISO 27001 standard. If compliance is not maintained, the certification might not be renewed for the full 3-year period."***
>
> *Larissa Bruns*, Associate Consultant Tech Practice Professional Services

HOW DO I TRANSITION TO ISO 27001:2022?

If you already comply with the ISO 27001:2013 certification you don't necessarily need a separate audit to transition to the new revision. You can either undergo a standalone transition audit or you can opt for a transition audit at the time of annual surveillance or re-certification. This depends on where you are in the certification lifecycle.

Here is an overview of a typical transition roadmap:

Your roadmap to transition



RAISE AWARENESS

Conduct training sessions to familiarize them with the updated requirements, controls, and concepts.

CHANGE ANALYSIS AND GAP ASSESSMENT

Identify areas where your organisation's practices need adjustment to meet the new standard.

DOCUMENTATION REVIEW AND UPDATE

Update both existing and new documents, policies and procedures to reflect the changes and additions in ISO 27001:2022

INTERNAL AUDIT & MANAGEMENT REVIEW

Perform an internal audit based on the updated requirements.

TRANSITION GAP ASSESSMENT

This self-assessment can help you identify any remaining gaps and address them before the formal audit.

TRANSITION AUDIT

Conduct a final review to confirm that your organization is prepared for the transition audit. Undergo the transition audit by your chosen certification body.

CONTINUOUS IMPROVEMENT

Regularly assess your organization's information security practices, adapt to evolving threats, and maintain compliance

When it comes to the transitioning timeline, the 2022 revision was issued in October last year and the transitioning timeline has officially begun. By October 2023, UKAs plans to have transitioned all certification bodies to the new standard.

All 2013 certificates will expire on the 31st October 2025, this is the deadline to transition. Your will have to undergo a transitioning audit before this date, so ensure your company has allocated enough time for this transition. Yet you can still certify against the 2013 standard until April 2024, if you wish to do so.

Complying with the new 2022 standard is bound to save your organisation resources and frustrations. This is why we recommend transitioning sooner rather than later. You can gain detailed insights on transitioning in DataGuard's expert insights on the ISO 27001:2022 update.

WHAT ARE THE BENEFITS OF GETTING ISO 27001 CERTIFIED?

The benefits of implementing ISO 27001 are plenty — both for your business and external parties and stakeholders. Here's an overview of the most important ones:

The benefits of achieving ISO 27001 certification:

- Your company or organisation can avoid significant financial losses caused by ransomware attacks.
- Win more deals; having a certified information security system can set you apart from the competition and win trust among potential customers.
- You may be able to secure investment more easily; investors are becoming more and more aware of the threats ransomware attacks have.
- By getting certified, you can experience increased customer trust because, nowadays, tech-savvy customers want to know how you handle data safely.
- Promising to keep your customer's data safe can become your brand's unique selling point.
- Reduced risk of data breaches: By having the proper measures in place — you can avoid the risk of a breach before it even happens.

- Setting up processes and procedures when it comes to how you handle data can also mean increased operational efficiency. Because now you have a standard process instead of different methods.

- Enhanced brand reputation: Customers want to know how you handle their information, and getting ISO 27001 certified is the ultimate promise that you take information security seriously.

IS ISO 27001 COMPLIANCE SUFFICIENT?

If you're looking to establish an information security management system — ISO 27001 is the ultimate baseline that will cover most businesses' compliance and information security needs.

What your customers and suppliers require will depend on where your business operates. ISO 27001 is an internationally recognised standard known as the gold standard, regardless of geographic location or industry. It should be sufficient for every use case, but if you are unsure — having an initial consult with an information security expert makes sense.

→ **Learn "2 minutes quick guide to certification"**

GETTING ISO 27001 CERTIFIED

Accredited vs. non-accredited certification

As we have learned so far, ISO 27001 certification is not mandatory for businesses. However, it's recommended to be compliant with the standard at least. But what's the difference between being certified and being compliant? In general, you must understand the three ways of communicating the implementation of ISO 27001:

- ISO 27001 compliant
- ISO 27001 certified
- ISO 27001 certified by an officially accredited certification bod

The difference is that an independent third certification body validates an accredited certification. A non-accredited certification means you have implemented the ISO standards but have not undergone an external audit, nor have you been issued a certificate for an external certified body.

In the United Kingdom, numerous accredited certification bodies for ISO 27001 exist. These bodies have undergone scrutiny and accreditation by UKAS, the country's national accreditation authority. UKAS guarantees organisational competence and adherence to the highest standards, utilising a thorough audit process to ensure compliance.

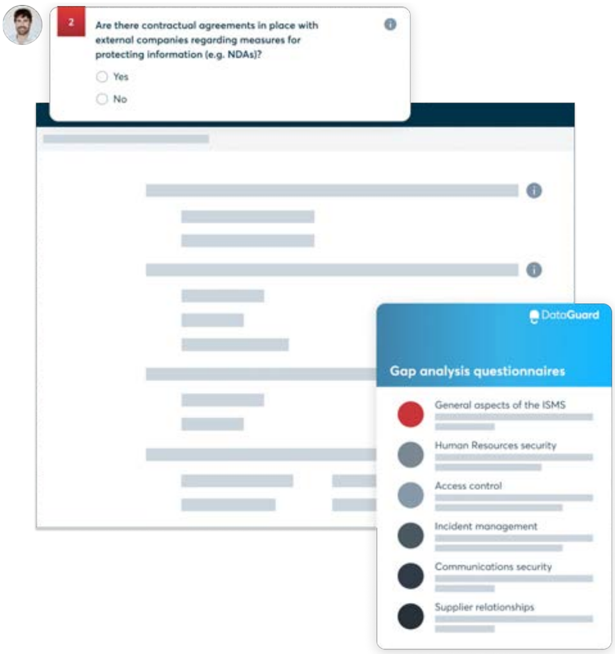
Often, certain contractual agreements require an official accredited certification. Apart from this, **achieving an accredited certification is highly recommended** — you can use it in your communications towards customers and have an external assess your information security to ensure your ISMS is in check.

You can find a list of currently accredited bodies here.

We strongly **recommend seeking certification exclusively through accredited bodies**. Business partners often do not acknowledge certifications lacking confirmation from an international accreditation body. In fact, most contracts mandating ISO 27001 certification implicitly refer to certification by an accredited body. Read more about accredited bodies here.

WHAT ARE THE CERTIFICATION STEPS? WHAT EXACTLY DO I NEED TO DO TO GET ISO 27001 CERTIFIED?

The process of getting certified consists of the following:



2 Are there contractual agreements in place with external companies regarding measures for protecting information (e.g. NDAs)?

○ Yes

○ No

IDENTIFY GAPS AND KICKOFF ISO 27001 IMPLEMENTATION

Begin by familiarising yourself with the ISO 27001 framework. Conduct a gap analysis to identify areas where improvements are needed to meet the requirements. Work with our certified information security experts to build a customised ISO 27001 implementation plan. This plan also defines the scope of your Information Security Management System (ISMS).

BUILD YOUR ISMS

ISMS is a comprehensive set of policies, processes, procedures, and controls designed to improve your organisation's information security practices.

IDENTIFY AND MANAGE RISKS

Information security risks stem from various organisational sources, including people, infrastructure, physical security, and third-party relationships. So, you start with brainstorming hypothetical scenarios to identify the various information security risks your organisation is exposed to. Assess their impact from a financial, reputational, legal, and operational point of view. Afterwards, you can implement technical or procedural measures to mitigate and manage the identified risks.

PROTECT INFORMATION ASSETS

Identify and document all information assets in your organisation like hardware, data, and personnel. Categorise them based on criticality and value to determine appropriate security controls. Define ownership and assign responsibilities for asset management and protection.

PASS YOUR ISO 27001 AUDIT

In the external audit, an accredited auditor assesses all aspects of your organisation's ISMS to verify compliance with the ISO 27001 standard. DataGuard experts help you conduct a thorough internal audit, maximising your chances of external audit success.

THE REAL JOURNEY BEGINS: MAINTAINING YOUR ISMS

Evolving security threats and changes to the organisational infrastructure constantly create new risks. To ensure continued compliance with the ISO 27001 standard, you need to regularly review and update your ISMS. This includes risk assessments, internal audits, and employee training.To stay certified, your organisation must pass annual surveillance audits and a re-audit every 3 years. Continually improve your ISMS as your business grows and matures. Show your commitment to information security with ISO 27001 certification and win more deals.

CONDUCTING A RISK ASSESSMENT

Conducting a risk assessment is not as straightforward as one might think. First of all, there are many different approaches to risk assessments. It's not necessarily common practice, but **scenario-based** is the **most effective way to access risk**. This means considering past occurrences and analysing risky scenarios that may cause an issue.

The risk assessment consists of the following:

1. Identify & assess risk.
2. Treat risks - you decide here how you want to address the risks. E.g., Accept, Avoid, Transfer, Mitigate.
3. Review residual risks.

A platform like DataGuard can help move you through risk assessment in an efficient way with a tested and proven process. Check out the full article on Conducting ISO 27001 risk assessment in 7 steps here.

IMPLEMENTING CONTROLS AND A RISK TREATMENT PLAN TO MANAGE RISKS

An integral element of your information security program is the **risk treatment plan**. This plan is all-encompassing and is devised to execute measures to either accept, avoid, transfer, or **mitigate the possibility or consequences of risks.**

Of utmost importance within a risk treatment plan is the aspect of implementation. Its significance lies in guaranteeing the actual execution of risk treatment procedures.

You can read ISO 27001 risk treatment plan: How to develop the right one here.

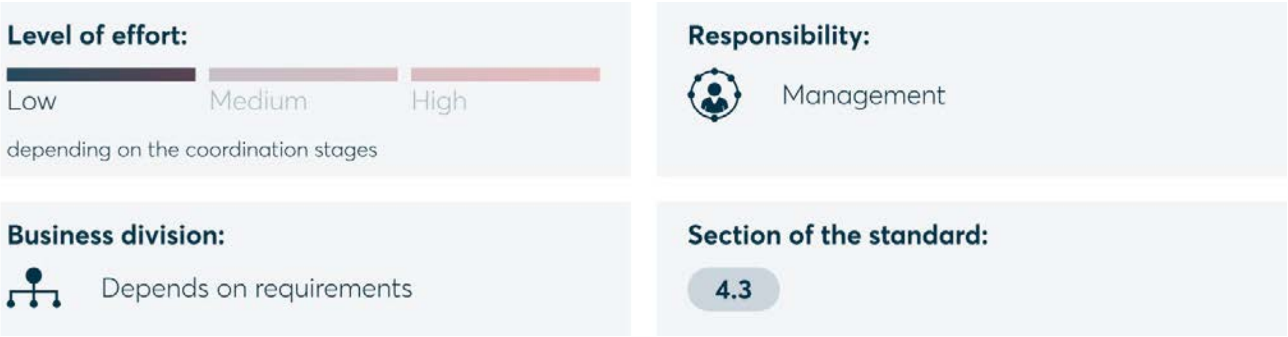
COMPLETE YOUR ISMS DOCUMENTATION

Documentation is the basis of your ISMS and the most important part of getting and maintaining your certification. If it's not documented, it's not relevant.

You need to keep track of many things when it comes to documentation, as there are many things to consider. To give you a complete overview of the documentation required for ISO 27001 certification, along with information on preparing said documentation, we have created a detailed list for the documentation:

Definition of the scope of application of the ISMS (Information Security Management System)

The scope of application of the ISMS is defined in the so-called "Scope Document". This determines which divisions of your company are subject to the ISMS. Your ISMS doesn't necessarily need to be rolled out across the entire company - only the relevant departments and divisions. That said, in the case of smaller companies, it will usually cover all departments.



Level of effort:

Low Medium High

depending on the coordination stages

Responsibility:

Management

Business division:

Depends on requirements

Section of the standard:

4.3

Coordination and documentation of the guideline on information security

The objectives which your company seeks to achieve with your ISMS should be clearly defined in the guideline on information security. This document should also demonstrate why information security is a top priority in your organisation, and that management is responsible for the guideline.

This does not have to be formulated by management themselves but must always be approved by the necessary stakeholders. The ISO standard already specifies the following information security objectives:

- Data confidentiality
- Data availability
- Data integrity

Level of effort:

Low Medium High

Responsibility:

Management

Business division:

Entire company

Section of the standard:

5.2 6.2

Definition of risk assessment and risk management methods

You will need to identify your company's risks, assess them individually and define an appropriate methodology for risk management. The assessment should always be carried out by the respective risk owner and should ultimately be approved by management.

In addition, this area should be coordinated within the company, ideally with your ISO, CISO or risk management department. Given that this process must be repeated on a regular basis, it can result in a lot of effort, especially for small and medium-sized enterprises that lack in-house security and risk experts. Repetitions occur when there are new assets in the company that require a risk assessment.

Level of effort:

Low Medium High

Responsibility:

Risk owner, ISO/CISO, Risk Management and company management

Business division:

All divisions that are to be assessed

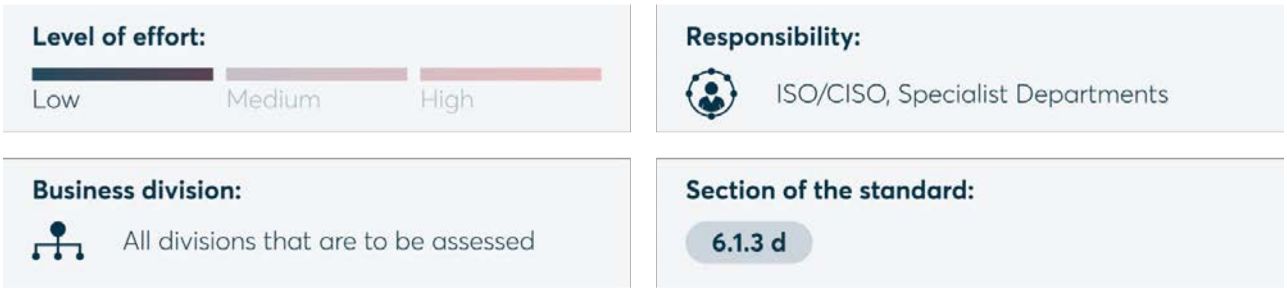
Section of the standard:

6.1.2

Preparing a declaration of applicability

As part of this step the ISO/CISO shall agree, with the respective specialist departments, which of the 93 controls stated in Appendix A of ISO 27001:2022 must be carried out or which are relevant for the company.

ISO 27001 has specified various areas such as cryptography, HR security or operational security. Companies may exclude some of these areas by providing appropriate justification. For example, if a business does not have a loading zone, it is simply not necessary to draw up rules for loading zones.



Level of effort:

Low Medium High

Responsibility:

ISO/CISO, Specialist Departments

Business division:

All divisions that are to be assessed

Section of the standard:

6.1.3 d

→ **Download our free E-Book to learn about all 22 documentation requirements.**

If you choose to work with experts such as DataGuard or an external consultant, you may receive documentation templates that will help cut down on your manual work significantly compared to creating them from scratch.

WHAT IS AN AUDIT, AND WHY IS IT IMPORTANT?

An audit is basically the process of checking that your ISMS meets the requirements and criteria of a standard. If you are certifying against ISO 27001, it will be the requirements of the ISO 27001 standard.

Audits ensure the success of your ISMS by identifying information security non-conformities and can be either internal or external. **Internal audits** can be carried out using the organisations' own resources — whether that's internal employees of the company or contracted independent consultants (2nd party auditors).

External audits are carried out by a certification body, external partners or customers who want to assess the ISMS on their own terms. The latter is rather the exception than the rule — when referring to an external audit, a certification body is meant in most cases.

Audits are incredibly important not only because they are:

- **A concrete requirement of the ISO 27001 standard.**
- The only way of **verifying whether you comply** with the standard.
- Necessary to **obtain your ISO 27001 certification.**

CONDUCTING INTERNAL AUDITS: HOW TO GO ABOUT IT

Internal audits are vital for long-term success in earning and keeping your ISO 27001 certification. They should be carried out on a regular basis by employees within the company, as opposed to external auditors coming into your company to assess your ISMS.

However, independency and qualification are a must for being an internal auditor. Another option is to perform internal audits with external consultants, like the experts at DataGuard, who also offer regular audits. Internal audits are your best bet for catching gaps in your documentation and improving it.

When you are getting certified for the first time, the internal audit ensures you have everything you need in place to pass your certification on the first try.

An internal audit checklist will help you keeping an overview of the necessary steps in that process. Here is an overview of the steps in an internal audit:

1. **Documentation Review**

- All documentation from the management and control system should be reviewed to ensure that it is complete, accurate, and up-to-date.

- A team should be assigned to perform this task.

- The team should be given a clear set of instructions to follow while they are performing the review.

- The documentation should be examined for completeness, accuracy, consistency, and suitability for its intended purpose.

- The auditor will then check to see if you have the required documents and that it complies with the standards.

2. **Management Review**

- The management review team should go through the documentation again to make sure that all relevant information has been recorded and that there are no omissions or missing information in any of the documents.

- Finally, management needs to look over the report and take the audit results into account. Make sure that any essential changes and corrective measures are put into place.

Get a full breakdown of how to conduct an internal audit.

UNDERGOING EXTERNAL AUDITS: WHAT TO EXPECT

You will be in touch with your auditor before the external audit takes place to agree on an audit that includes resources and timelines for the audit.

In general, there are four types of external audits:

- **Stage 1 Audit:** This is the documentation review audit, whereby the external auditor analyses if your organisation has all the necessary documentation in place for a fully functioning ISMS. Your documents need to cover the documentation required in the ISO/IEC 27001 standard. The certification body will take the time to gain a sufficient understanding of the ISMS design in the context of your organization, risk assessment and treatment (including the controls determined), information security policy and objectives. A large emphasis will also be put on your company's preparedness for the audit. This allows planning for stage 2.

- **Stage 2 Audit:** Based on documented findings in stage 1's audit report, the certification body will develop an audit plan to conduct stage 2 of the audit. In addition to evaluating the effective implementation of the ISMS, the aim of stage 2 is to confirm that your company adheres to its own policies, objectives and procedures.

To do this, the audit will focus on:

- Top management leadership and commitment to information security policy and the information security objectives.
- Documentation requirements listed in ISO/IEC 27001.
- Assessment of information security-related risks and that the assessments produce consistent, valid and comparable results if repeated.
- Determination of control objectives and controls based on the information security risk assessment Risk treatment processes.
- Information security performance and the effectiveness of the ISMS, evaluating against the information security objectives.
- Correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives.
- Implementation of controls (see Annex A), taking into account the external and internal context.
- And related risks, the organization's monitoring, measurement and analysis of information security.
- Processes and controls to determine whether controls are implemented and effective and meet their stated information security objectives.
- Programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.

Once you have completed stage two and passed the audit — you will receive your official certification.

- Surveillance/periodic audits: happen between certification and recertification audits focusing on specific areas of the ISMS. This is done every year.
- Recertification audit: This is necessary to keep your certification and covers all aspects of the standard and must be carried out every 3 years.

HOW LONG DOES IT TAKE TO GET READY FOR AN ISO 27001 EXTERNAL AUDIT?

Depending on the size of your company or organisation, you can be audit-ready in about 8 weeks. If you decide to go the manual route of building your documentation from scratch, it can take at least approximately 4 months.

There are a few main requirements you need to fulfil to obtain your ISO 27001. To help you with it, we've compiled a series of checklists which outline everything you'll need for your certification.

- **1 to 20 employees - Up to 3 months**
- **20 to 50 employees – 3 to 5 months**
- **50 to 200 employees - 5 to 8 months**
- **More than 200 employees - 8 to 20 months**

It is also important to take into account several other variables that may affect the time it takes for you to obtain the certification.

- The number of individuals on the ISMS implementation project (relative to the size of the business)
- The amount of time individuals are willing to spend on the project
- Engagement / endorsement / support from leadership
- The size of the company and complexity
- Auditor availability to conduct the external audit

When implementing your ISMS, you may experience unforeseen challenges which may delay certification as well.

WHAT YOU CAN EXPECT AT AN EXTERNAL AUDIT

Once you've successfully run through an internal audit, there's not much more you need to expect from an external auditor in terms of process. An auditor will come to your company premises, review your ISMS and speak with your employees.

Here's the overall process:

1. Document check

First, the external auditor will review all of your ISMS-related documentation. It has now also become the norm that auditors can do this remotely. But in fact, inviting them to physically come into your company so they can get to know your team builds trust early on.

2. On-site audit

In the second step, an on-site inspection is carried out. Some of your employees will be interviewed, and your systems will also be randomly checked. In addition to employees such as your CISO/ISB, who directly deal with the ISMS, your CFO or CEO should give the auditor confidence that the financial resources for operating the ISMS are firmly set up.

You will already know during the inspection whether you're going to pass the audit and receive the certification, as the auditor will directly address minor and perhaps even significant issues.

Afterwards, the certification body first has to prove all non-conformities addressed by the auditor, which usually gives you the chance to improve your documentation before an official result of the audit is confirmed.

Major non-conformance will lead to a failed audit. The only thing left is to set the date and conditions for a follow-up audit together.

3. Audit Report and ISO 27001 Certificate

Finally, you will receive an audit report and the certificate from your auditor. Many certification companies are currently busy, so this may take a few months.

"Our schedule was less than 6 months, and it would have been impossible without DataGuard."

WHAT HAPPENS IF YOU FAIL THE EXTERNAL AUDIT?

The external auditor will usually give you an indication during your external audit whether you are likely to pass or fail the audit. Major nonconformities may lead to a failed external audit — although this might seem like a major setback, it needs to be seen as an opportunity to improve.

When it comes to the 2022 version of ISO 27001, there are 93 Annex A controls that cover various areas of an organisation. These controls are segmented into 4 different categories (domains). Depending on which are relevant for your company, risks, industry and customers — you will fulfil the requirements in specific annexes.

You will receive an audit report; this will be your go-to to identify what you need to change in order to pass your next external audit. It is also recommended to speak with the auditors for further clarification on what precisely needs to be improved.

In general, nonconformities are classed as:

- Major non-conformities.
- Minor non-conformities.
- Opportunities for improvement.

There is no direct penalty for not passing an external audit, but not achieving certification may result in improper risk management, reputational damages and additional financial costs. Preparing thoroughly and undergoing internal audits significantly reduce the risk of failing. If you happen to have failed an audit in the past, we recommend the following:

- Assessing your audit report.
- Discussing the outcome with the external auditor.
- Communicating the outcomes and reasoning to all relevant stakeholders and ensuring internal alignment.
- Establishing an action plan with prioritized tasks, also sorted by due date and responsible persons.
- Initiating the entire process of setting and improving your ISMS again; ensuring enough relevant resources are available, especially for internal auditing.
- Once the scope of improving your ISMS is clear, set a date for your next external audit.

WHAT ARE THE ISO 27001 CERTIFICATION REQUIREMENTS?

The main requirements when it comes to the ISO 27001 certification are: documentation, undergoing audits and ensuring your employees adopt the processes.

Documentation includes the creation and maintenance of necessary documentation for your Information Security Management System (ISMS), such as policies, procedures, risk assessments, and controls.

Undergoing audits includes both the Stage 1 Audit, which reviews documentation and readiness, and the Stage 2 Audit, which assesses the practical implementation of your ISMS. Successful completion of these audits is necessary to achieve ISO 27001 certification. You will also be required to undergo internal audits and management reviews.

It's also crucial to **communicate the processes effectively.** This is to ensure that your organization's information security practices align with the ISO 27001 standards. You will need to have the documentation in place but also put the processes into action by ensuring employees are aware of and follow them.

⟶ **Learn "ISMS Documentation Checklist"**

The mandatory documents required for the ISO 27001 standard are listed below. All criteria must be followed and documented accordingly for an organisation to present during external audits. The standard requires you to undergo an internal audit before an external one. This will expose any gaps in your ISMS.

Once you have prepared the documentation and undergone an internal audit as well as a management review, you need to undergo an external audit by a certified body such as the UKAS.

The mandatory documents required for ISO 27001 are:

- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 The scope of the ISMS
- 4.4 Information Security Management System process
- 5.1 Commitment of the ISMS
- 5.2 Information security policy
- 5.3 Roles and their responsibilities (RACI/RASCI)
- 6.1.2 Information security risk assessment and treatment process
- 6.1.3 Information security risk treatment and assessment plan
- 6.1.3 The Statement of Applicability
- 6.2 Information security objectives
- 6.3 Change Management for the ISMS
- 7.1 Ressource planning
- 7.3 Awareness plan
- 7.4 Communication Plan
- 7.2 Evidence of competence
- 7.5 Document control policy
- 5.5.1 Documented information determined by the organisation as being necessary for the effectiveness of the ISMS
- 8.1 Operational planning and control
- 8.2 Results of the information security risk assessment
- 8.3 Results of the information security risk treatment
- 9.1 Evidence of the monitoring and measurement of results
- 9.2 A documented internal audit process
- 9.2 Evidence of the audit programmes and the audit results
- 9.3 Evidence of the results of management reviews
- 10.1 Evidence of the nature of the non-conformities and any subsequent actions taken
- 10.1 g) Evidence of the results of any corrective actions

To get a full breakdown of the ISO 27001 requirements, check the ISO 27001 requirements: A comprehensive list.

WHAT ARE ISO 27001 CONTROLS, AND HOW TO GO ABOUT IMPLEMENTATION?

A control is a measure that manages risk.

When it comes to the 2022 version of ISO 27001, there are 93 Annex A controls that cover various areas of an organisation. These controls are segmented into 4 different categories (domains). Depending on which are relevant for your company, risks, industry and customers — you will fulfil the requirements in specific annexes.

Standard controls include:

- 8 asset management
- 14 system acquisition development and maintenance
- 10 cryptography
- 18 compliance

Want more details on controls and their implementation? Take a deep dive here: ISO 27001 Annex A controls - A detailed guide.

THE COSTS OF ISO 27001 CERTIFICATION

The price or costs for getting ISO 27001 certified depends on many things. These are the most relevant influences on what you will need to invest in your ISO 27001 certification:

- The level of maturity reflected in the ISMS.
- The range of activities conducted within the defined boundaries of the ISMS.
- The extent of technology utilisation across the various facets of the ISMS.
- The degree of external sourcing and engagements with third-party entities covered by the ISMS.
- The variance between the current state and the intended state of the control environment.

- The internal capacity of the organisation to enhance the ISMS and address identified deficiencies.
- The requested timeline for getting certified.

This is why we cannot provide a one-size-fits-all answer — yet we can give indications that will help establish a budget.

How much does it cost to get ISO 27001 certified?

The cost of getting certified can be broken down into three phases: implementation (of your ISMS), internal auditing and certification.

Internal costs

These costs can include:

- Internal staff costs
- Consultation costs
- Management resources for reviews and communication
- Project management and awareness-building resources among staff
- Software tools to support the establishment of an ISMS

External costs

This generally refers to the auditor's cost; on average, the cost of auditing per day is £1000 — the number of days and whether you will have a remote or on-site audit will impact external costs.

Example breakdown of ISO 27001 certification cost

Below, you can find an example breakdown of costs you can expect in each phase:

Implementation

- Precertification Phase I (Scope, Definition, Risk Assessment, Risk treatment plan, Gap assessment), Phase II (remediation plan) - £15, 000.
- Precertification Phase II (Gap closure, Registrar Selection, ISMS artefact development, Risk management committee, Incident response, Internal ISMS audit, On-Site certification audit support) - £10,000.
- Average annual Compliance Manager salary (US) - £100,000 (depends on whether your organisation employs this position or not).
- Average annual cost of compliance software and tools - £15,000 to £100,000.

Internal auditing

- Compliance consultant cost - £140/hour, for about 24 to 160 consulting hours

Certification

- ISO 27001 Auditor cost - £5,500 to £18,000

Surveillance Audit Cost

- Annual Compliance Specialist salary - £75,000 to £90,000
- Cost of IS0 27001 audit - £5,500 to £12,000

The total cost of the ISO 27001 certification ranges from £10,000 to £48,000. To budget your own ISO 27001 certification, we recommend doing as much research as possible, getting quotes from different stakeholders and comparing prices. Tactics such as leveraging software tools that streamline the certification process can significantly trim your budget.

IS THE INVESTMENT WORTH IT?

According to Statista, the global average cost per data breach is USD 4.35 million as of 2022. If that's a hit your company or organisation can easily take — getting ISO certified might not be worth it.

Information security is bound to become more and more important and simply shouldn't be ignored. As ransomware and cyberattacks rise year after year, companies realise that a preventive approach might be better than cleaning up the reputational and financial mess once something does happen.

Of course, you will need to take your unique ROI of getting ISO 27001 certified into account. Speaking with an information security expert can give you an idea of what you can expect cost-wise and whether it's worth investing in.

At the same time, how you go about getting certified- e.g., using a process-driven platform backed by experts or hiring a compliance manager in-house — will have a significant impact on just how much you need to invest and whether it will be worth it in the long run.

HOW TO GET STARTED WITH ISO 27001 CERTIFICATION

As you can see, there are plenty of aspects you need to think about when it comes to achieving ISO 27001 certification. But the best time to get started is now. Let your ISMS grow and scale with you.

The recommended and common practice to start your ISO 27001 journey is to:

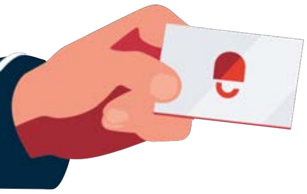
- Find a qualified consultant and/or platform to get an initial consultation so you can get clear on the scope, costs and timeline you can expect for your company.

- Develop a project plan and timeline where all the relevant stakeholders are named.

- Ensure a buy-in from management. Information security needs to be approached holistically to protect the entire company's assets, so have a game plan to get the whole team's green light and active involvement.

- Start defining your scope and work your way through the certification steps.

Get your free guide



DataGuard is a Compliance software company focused on Data Privacy and Information Security. As a European leader in the Compliance SaaS category, we enable over thousands of SMB and Corporate customers to automate and operationalise Privacy, InfoSec, and Compliance ("PIC") with ease. Our end-to-end SaaS solution drastically reduces the time and money companies spend to comply with privacy legislation such as GDPR, manage consents and preferences, and obtain infosec certifications such as ISO 27001. This enables our customers to focus on their core business, create value through trust and compliance, whilst mitigating risks and preventing breaches. We have offices globally in Munich, Berlin, London, and Vienna.

Let's talk about your challenges and define first steps on your compliance journey:

Contact us

You might also like:

→ **The ultimate guide to transitioning to ISO 27001:2022**

→ **ISO 27001 - Why Get Certified**

→ **Pitfalls To Avoid When Implementing ISO 27001**

dataguard.co.uk contact@dataguard.com +44 20 3514 65 57

DataGuard