GUIDE 2025/2026

ISO 27001 guide for mid-sized companies

Everything you need to know, explained plainly

iso-easy
ISO 27001

notivia GmbH

Edition 2025/2026

Contents

1 What is ISO 27001? 3

1.1 The standard in plain words 3

1.2 What is an ISMS? 3

1.3 ISO 27001:2022 — what has changed? 4

1.4 How it sits alongside other standards 4

2 Why would you need ISO 27001? 6

3 The road to certification — seven phases 8

4 What does ISO 27001 cost? 10

5 The ten most common mistakes 11

6 Readiness check: are you ready? 13

7 Glossary 15

8 Your next step 17

1 What is ISO 27001?

1.1 The standard in plain words

ISO 27001 is the internationally recognised standard for information security. Published by the International Organization for Standardization, it sets out how companies protect their information systematically — whether it is digital, on paper, or in people's heads.

Think of ISO 27001 as a construction kit: it gives you a frame within which you build your own security measures. It does not tell you which firewall to buy. What it asks is that you know your risks, make deliberate decisions, and record them so they can be followed.

> **The core idea:** ISO 27001 does not ask “do you have the best technology?” but “do you have a considered plan for protecting your information — and do you actually follow it?”

Certification is awarded by an independent, accredited certification body — TÜV, DEKRA or DQS, for example. It confirms that your company runs a working information security management system. The certificate is valid for three years and is checked each year by a surveillance audit.

1.2 What is an ISMS?

ISMS stands for **information security management system**. The term sounds unwieldy but means something very practical: the whole of the rules, processes, responsibilities and measures through which you organise information security in your company.

An ISMS covers three objectives:



Confidentiality

Information is accessible only to those authorised



Integrity

Information is correct and complete



Availability

Information is there when it is needed

An ISMS is not a one-off project but an ongoing process. It follows the **plan-do-check-act cycle** : you plan measures, put them in place, check whether they work and keep

improving. That cycle stops your level of security standing still and keeps it adapting to new threats.

1.3 ISO 27001:2022 — what has changed?

The current version dates from 2022 and replaces the 2013 edition. The most important changes affect Annex A, the collection of security controls:

- The number of controls was cut from **114 to 93** by merging and restructuring them.
- The former 14 categories became **4 themes** : organisational, people, physical and technological.
- **11 new controls** were introduced, among them threat intelligence, information security in cloud services, and data masking.
- Each control now carries attributes — preventive, detective, corrective — which make it easier to assign them precisely.

93	4	11
controls in the 2022 version	themes	new controls

Companies certifying for the first time have had to use the 2022 version since October 2023. Those already certified had to move across by October 2025.

1.4 How it sits alongside other standards

ISO 27001 is not the only security standard. Depending on your industry and what is asked of you, other frameworks come up:

Standard	Focus	Typical audience
ISO 27001	Information security as a whole	Every industry, recognised internationally
TISAX	Information security in the automotive industry	Suppliers and partners in the car industry
SOC 2	Controls for cloud providers (a US standard)	SaaS providers, especially with US customers
BSI IT-Grundschutz	A comprehensive IT security catalogue (Germany)	Public administration and critical infrastructure

> **Worth knowing:** ISO 27001 often forms the basis for other standards. If you hold it, you already meet a large part of the TISAX requirements. And the EU's NIS2 Directive points explicitly to ISO 27001 as suitable evidence of cybersecurity measures.

2 Why would you need ISO 27001?

We hear “do we really need this?” often. The honest answer is that it depends on your situation. But the reasons more and more mid-sized companies choose ISO 27001 are solid ones.

Customer requirements and tenders

The most common trigger: an important customer or partner asks for proof. Large companies and groups increasingly examine the information security of their supply chain. Without a certificate you will not even make the shortlist for many tenders.

> *A real example: a mid-sized IT provider with 35 staff loses a tender worth €400,000 a year, because the client made ISO 27001 certification a minimum requirement. Three months later the company starts its ISMS project.*

Regulatory duties

The regulatory landscape is tightening noticeably:

- **The NIS2 Directive (from 2024/2025):** the EU directive on network and information security covers far more companies than its predecessor — including many mid-sized firms in energy, health, digital infrastructure, food and machinery. ISO 27001 counts as recognised evidence of meeting its requirements.
- **DORA (the Digital Operational Resilience Act):** binding for the financial sector and its IT providers since January 2025. It requires robust IT security measures, and ISO 27001 covers most of them.
- **Synergies with the GDPR:** ISO 27001 and data protection overlap considerably. Running an ISMS automatically satisfies many of the technical and organisational measures the GDPR requires.

Competitive advantage

A certificate is a signal of trust. It tells customers, partners and investors: *this company takes security seriously.* For IT providers, SaaS companies and consultancies in particular, it can make the decisive difference.

Cyber insurance

Premiums for cyber insurance are rising — and so are insurers' demands on IT security. Companies with ISO 27001 often get better terms, because their risk profile is demonstrably lower. Some insurers already make an ISMS a precondition of cover.

3 The road to certification — seven phases

The road to certification is no great mystery, but it does take structure and discipline. Depending on your size and starting point, the whole process takes between **three and twelve months**.

1 Gap analysis — where do you stand today?

It starts with an honest stocktake: comparing where you are against what the standard requires. What do you already have? Where are the gaps? That analysis is the basis of your project plan and helps you judge the effort realistically. A gap analysis typically takes two to three weeks.

2 Set the scope and the structure

You define which parts of the company the ISMS covers. That can be every site and process, or just one line of business — your cloud hosting, say. You also settle the organisation: who is the information security officer, and how do they report to management?

3 Record the risks and the assets

The heart of the ISMS: you take an inventory of your information assets — servers, applications, databases, contracts, know-how — and assess the risks that go with them. For each risk you decide: treat it, accept it, avoid it or transfer it.

4 Build the policies and documentation

The standard requires certain documented information: an information security policy, a risk method, a statement of applicability and further policies. What matters is that the documents fit your company. Copied templates that nobody reads or understands are spotted immediately in the audit.

5 Training and awareness

Information security only works when everyone takes part. Your people have to understand why the rules exist and what is expected of them. That means general awareness training as well as role-specific sessions. Record attendance — the auditor will ask for it.

6

Internal audit and management review

Before the external auditor arrives, examine yourself. An internal audit uncovers weaknesses you can still fix. The management review makes sure leadership actually steers the ISMS. Both are mandatory.

7

External audit (stages 1 and 2)

The external audit comes in two stages. In **Stage 1** the auditor reviews your documentation. In **Stage 2** , on site, they check whether the ISMS works in practice: interviews, evidence, watching the processes. If no serious deviations come up, you receive your certificate.

> **Tip:** Allow at least four weeks between the two stages. That gives you time to put right anything stage 1 turns up.

4 What does ISO 27001 cost?

One of the questions we are asked most — and one too often answered with "it depends". Let us be concrete:

Company size	Total cost*	Timeframe	Internal effort
1–5 staff	**€15,000–19,000**	3–5 months	6–10 hrs/week
6–20 staff	**€22,000–28,000**	4–6 months	8–12 hrs/week
21–50 staff	**€32,000–40,000**	5–7 months	10–16 hrs/week
51–150 staff	**€48,000–60,000**	6–9 months	16–24 hrs/week
150+ staff	**€68,000–90,000**	8–12 months	½–1 FTE

* The total includes consulting and implementation support, the ISMS platform and tooling, and the certification audit by an accredited body.

What drives the cost?

- **Several sites:** allow 20 to 40 % more for each additional site in scope.
- **Regulated industries** (finance, health, critical infrastructure): additional requirements can add 10 to 15 %.
- **Where you start:** companies that already work in a structured way — documented processes, access management — get through more cheaply.

Costs after the first certification

The certificate is valid for three years, with a surveillance audit in years two and three and recertification in the third. For keeping it running, allow around **25 to 30 % of the initial cost per year**.

> **In the interest of transparency:** these figures come from watching the market and from our own experience of more than a hundred certification projects. Your own costs may differ. Use our free calculator at **iso-easy.de** for a first estimate.

5 The ten most common mistakes

From guiding a good many certification projects, we know the usual stumbling blocks. Avoid these and your road to certification will run far more smoothly.

1. **Starting too late**
   Many companies only begin when a customer or a deadline pushes them. Then there is no time to build it properly. Allow at least four to six months — better still, more.

2. **Treating it as an IT project**
   Information security concerns the whole company: HR, sales, management, facilities. Anchor it only in the IT department and the audit will go badly.

3. **Documentation nobody lives by**
   A perfectly written manual that nobody knows or follows fails the audit. Auditors ask staff directly: “do you know the password policy?”

4. **Risk management on paper only**
   The risk analysis is the foundation. Filled in for form's sake, without the risks it finds actually being treated, the whole system has no substance.

5. **No commitment from management**
   Leadership has to stand behind the ISMS visibly — not just with a signature but with resources, attention and by setting an example.

6. **A scope that is too wide or too narrow**
   Too wide and the project becomes needlessly complex. Too narrow and it looks implausible, and the auditor may reject it. Striking the balance matters.

7. **Forgetting to train the staff**
   The standard explicitly requires everyone to be made aware of information security. Missing training records are among the most common audit findings.

8 **Underestimating the internal audit**

The internal audit is mandatory, not a formality. It has to be independent and should uncover real room for improvement.

9 **Not planning for continual improvement**

Stop developing the ISMS once you are certified and the surveillance audit will go badly. Plan the capacity in from the start.

10 **Choosing the wrong consultant**

Look for demonstrable experience with companies of your size and in your industry. Be sceptical of promises like “certification in four weeks, guaranteed”.

6 Readiness check: are you ready?

The following ten questions let you judge quickly where your company stands today. Answer each one honestly, yes or no.

1. **Do you know which information assets are especially worth protecting?**
   Without understanding your critical assets you cannot target your measures.

2. **Is there someone responsible for information security?**
   Without a named officer there is nothing steering the ISMS centrally.

3. **Do you have documented security policies?**
   At least one overarching information security policy is mandatory.

4. **Do you carry out risk analyses regularly?**
   Risk management is the heart of it — at least yearly, and whenever something substantial changes.

5. **Are your staff aware of IT security risks?**
   Regular training and awareness work are explicitly required by the standard.

6. **Do you manage access in a structured way?**
   Is access withdrawn promptly when someone changes role or leaves?

7. **Is there a plan for IT security incidents?**
   A documented incident response plan with clear reporting routes is indispensable.

8. **Are security incidents documented and analysed?**
   Learning from incidents is a core principle of continual improvement.

9. **Do you review your suppliers and providers regularly?**
   Your security is only as strong as the weakest link in the chain.

10. **Has your management committed clearly to information security?**
    That commitment is explicitly required by the standard (clause 5).

Your yes answers	Assessment	Recommendation
0–3 × yes	New ground	Building up in a structured way, with outside help, is advisable. Expect six to twelve months.
4–6 × yes	Partly prepared	Focus on the gaps, above all risk management and documentation. Four to eight months is realistic.
7–10 × yes	A good basis	With targeted refinement and audit preparation you can be ready in three to five months.

> Whatever your result: **every company can achieve ISO 27001.** It is a question of planning properly, not of company size.

7 Glossary

The key ISO 27001 terms, explained plainly:

ISMS

Information security management system — the whole of the policies, processes, responsibilities and measures protecting your information.

SoA (Statement of Applicability)

A central document in which you record, for all 93 controls, whether and how each applies to your company.

Annex A

The normative annex of ISO 27001, defining 93 controls in four categories: organisational, people, physical and technological.

Controls

The security measures you implement to treat the risks you have identified: access control, encryption, physical security and so on.

Gap analysis

A comparison between where you are and what the standard requires. It shows where something has to be done.

Scope

What your ISMS covers — which sites, departments, systems and processes.

Stage 1 / Stage 2

The two stages of the external certification audit. Stage 1 is a document review, stage 2 an on-site check of how it works in practice.

Surveillance audit

The annual check by the certification body in the years after the first certification.

Recertification

Renewing the certificate after three years through a full re-audit.

Information security officer

The person responsible for the ISMS within the company. The role can be filled internally or brought in from outside.

plan-do-check-act cycle

Plan-do-check-act — the cycle of continual improvement the ISMS rests on.

Nonconformity

A finding in the audit that a requirement is not met. Major non-conformities block certification.

8 Your next step

You have read this guide — that is the first step already. Tackling information security systematically is an investment that pays off: in contracts won, in lower risk, and in the trust of your customers and partners.

A free first conversation

In 30 minutes, with no obligation, we work out together:

- ✓ Where does your company stand today?
- ✓ What scope makes sense?
- ✓ What timeframe and budget?
- ✓ Which next steps make sense?

No sales pitch, no pressure — just an honest assessment.

The quick calculator

At **iso-easy.de** you will find our free ISO 27001 calculator.
In a few clicks you get a first view of the cost, the timeframe and the effort.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de



iso-easy is part of notivia GmbH.
With more than 30 years of experience in IT consulting and information security we support mid-sized companies on their way to ISO 27001 certification —
pragmatically, transparently and as equals.

© 2025/2026 notivia GmbH — iso-easy.de | All rights reserved.