

GUIDE 2025/2026

NIS-2 guide for mid-sized companies

Everything you need to know, explained plainly

notivia GmbH

Edition 2025/2026

Contents

1 What is NIS-2? 3

1.1 The directive in plain words 3

1.2 The ten security measures (Art. 21) 3

1.3 NIS-2 vs. NIS-1 — what has changed? 4

1.4 How it sits alongside other rules 4

2 Are you in scope? 6

3 The road to compliance — seven phases 8

4 What does NIS-2 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 NIS-2?

1.1 The directive in plain words

NIS-2 is the revised EU directive on network and information security (**Network and Information Security Directive 2**, Directive (EU) 2022/2555). It obliges companies and organisations across many sectors to reach a minimum level of cybersecurity — and, when it matters, to show that they do.

Unlike an ISO standard, which you adopt voluntarily, NIS-2 is **binding law**. If you are in scope, you have to act. In Germany the directive is being written into national law through the NIS2 implementation act (NIS2UmsuCG). Supervision lies with the **Federal Office for Information Security (BSI)**.

> **The core idea:** NIS-2 does not ask "which security tools do you use?" but "can you show that you know your cyber risks, manage them, and can act quickly when it matters?"

Infringements are expensive: up to **€10 million or 2 % of worldwide annual turnover** for essential entities, €7 million or 1.4 % for important entities. On top of that, management is personally liable — something new in European cybersecurity regulation.

1.2 The ten security measures (Art. 21)

Article 21 of the directive sets out ten minimum measures that every company in scope has to implement:

1. **Risk analysis and security policies** for information systems
2. **Handling security incidents** (incident handling)
3. **Keeping the business running**: backup management, recovery, crisis management
4. **Supply chain security**, including the security aspects of relationships with direct suppliers and service providers
5. **Security in acquisition, development and maintenance** of information systems, including vulnerability management
6. **Policies and procedures for assessing the effectiveness** of the cybersecurity measures
7. **Basic cyber hygiene** and cybersecurity training
8. **Cryptography and encryption**, where appropriate
9. **Personnel security, access control and asset management**

10. **Multi-factor authentication** or continuous authentication, and secure voice, video and text communication

> **An easy way to remember it:** the ten measures cover the whole life of a cyber risk — from knowing it (1), through preventing it (4–5, 8–10) and detecting it (6), to responding (2–3) and learning (7).

1.3 NIS-2 vs. NIS-1 — what has changed?

The 2016 predecessor covered only a few dozen "operators of essential services" in Germany. NIS-2 widens the scope dramatically:

~30,000	18	24 h
companies in scope in Germany (estimated)	sectors, up from 7	maximum early-warning deadline after an incident

The most important changes:

- **Far broader sector coverage** — for the first time this includes the food industry, waste management, chemicals and parts of manufacturing (mechanical engineering, electrical engineering, automotive and others).
- **Personal liability of management** (Art. 20 and 23) — management commitment is no longer just good practice but a legal duty.
- **One set of reporting deadlines EU-wide**: 24-hour early warning, 72-hour notification, final report within one month.
- **Far higher sanctions** — ten times those under NIS-1.
- **A focus on the supply chain** — four of the ten mandatory measures concern supplier relationships.

1.4 How it sits alongside other rules

NIS-2 is part of a growing ecosystem of cybersecurity rules. Depending on your industry, several may apply at once:

Rules	Focus	Binding?
NIS-2	Cybersecurity in mandated sectors	EU law (binding)
ISO 27001	Information security in general	Voluntary (certification)

Rules	Focus	Binding?
DORA	IT resilience, financial sector	EU regulation (binding)
KRITIS Regulation	Protection of critical infrastructure	German law
BSI IT-Grundschutz	IT security (a methodology)	Voluntary

Worth knowing: An existing ISO 27001 ISMS covers around 80 % of the NIS-2 requirements. If you hold ISO 27001 you only have to add the NIS-2 specifics: the reporting duties, the supply chain requirements and registration with the BSI.

2 Are you in scope?

The question many companies ask is: “do we have to implement NIS-2 at all?” Three things decide it — your sector, your size, and the special rules.

A. Sector

NIS-2 distinguishes two categories, set out in Annexes I and II of the directive:

Essential entities (Annex I)

Stricter supervision, higher fines:

- Energy (electricity, district heating and cooling, oil, gas, hydrogen)
- Transport (air, rail, water, road)
- Banking and financial market infrastructure
- Health, including pharmaceuticals and medical devices
- Drinking water and waste water
- Digital infrastructure (DNS, TLD registries, data centres, cloud, CDN, trust services)
- ICT service management (managed services, managed security services)
- Public administration (federal and state, at certain levels)
- Space

Important entities (Annex II)

Lighter supervision, but the same full duty to implement:

- Postal and courier services
- Waste management
- Chemicals (manufacture, production, trade)
- Food (production, processing, distribution)
- Manufacturing: medical devices, computing equipment, electrical engineering, machinery, motor vehicles and other transport equipment
- Digital services (online marketplaces, search engines, social networks)
- Research

B. Size threshold

The rule is: **medium-sized companies and above** — defined by meeting at least one of these:

- 50 or more staff, **or**

- more than €10 million annual turnover and a balance sheet total above €10 million

> **An exception:** for certain entities NIS-2 applies whatever their size — DNS providers, TLD registries, qualified trust services and some public administration bodies.

C. Special cases

- Companies operating in **several sectors in scope**: the size figures are added together.
- **Group structures**: subsidiaries are assessed individually as a rule.
- **Cross-border activity**: the member state of your head office or main establishment is responsible.
- **Suppliers**: even if you are not in scope yourself, your customers can oblige you contractually to behave in a NIS-2-compliant way.

A real example: a mid-sized automation specialist with 120 staff and €25 million turnover supplies control technology to machine builders. As an important entity (machinery, Annex II) it falls under NIS-2 — and at the same time has to meet its customers' supply chain security requirements.

Implementing early is a competitive advantage

Large companies increasingly check their supply chain for NIS-2 conformity. Those who have already implemented it are preferred; those who have not lose orders or have to produce laborious one-off evidence.

3 The road to compliance — seven phases

Implementing NIS-2 is not an IT project but a management matter with IT in it. Depending on your size and starting point, the whole process takes **four to ten months**.

1 **Establish whether you are in scope**

It starts with settling the question: are we in scope — and if so, as an essential or an important entity? Sector, size and the special rules are all checked. One to two weeks.

2 **Gap analysis**

Compare your existing security measures with the Art. 21 requirements. If you already run ISO 27001 you will usually find 80 % of it is done. Two to four weeks.

3 **Governance and management commitment**

Management has to confirm formally that it takes on the NIS-2 duties. Roles and responsibilities are defined and a NIS-2 officer appointed. Management training (mandatory under Art. 20) is carried out. Two to three weeks.

4 **Implement the ten security measures**

The real operational work: technical and organisational measures are built, adapted or brought up to standard, prioritised by risk. Three to six months.

5 **Supplier management**

Critical suppliers are identified, security requirements written into contracts and audits agreed. Runs alongside phase 4. Two to four months.

6 **Incident response and reporting**

Processes for the 24-hour, 72-hour and 30-day reports to the BSI are set up and tested in tabletop exercises. When it matters, a working reporting process is vital. Two to four weeks.

7 **BSI registration and evidence**

Register with the BSI through the official portal and keep documented evidence to hand — the BSI can order an audit at any time. One week.

> **Tip:** If you are implementing NIS-2 from scratch, combine it with an ISO 27001 implementation. The extra effort is small and the benefit considerable — you end up with a certifiable ISMS that serves as evidence towards customers and insurers.

4 What does NIS-2 cost?

A question that is rarely answered honestly. Let us be concrete:

Company size	Total cost*	Timeframe	Internal effort
50–100 staff	**€25,000–40,000**	4–6 months	8–12 hrs/week
100–250 staff	**€40,000–70,000**	5–8 months	12–20 hrs/week
250–500 staff	**€65,000–110,000**	6–10 months	20–30 hrs/week
500–1,000 staff	**€95,000–160,000**	8–12 months	½–1 FTE
1,000+ staff	**from €150,000**	10–14 months	1+ FTE

* Includes external consulting, tooling (the ISMS platform), training, BSI registration and building the documentation. Excludes running costs.

What drives the cost?

- **An existing ISMS (ISO 27001):** cuts the cost by 30 to 50 %.
- **How complex your IT landscape is:** multi-cloud, many business applications and OT environments all add effort.
- **How many critical suppliers you have:** the more third parties matter to security, the more work supply chain management becomes.
- **A regulated sector:** energy, critical infrastructure and health bring additional requirements — a surcharge of 10 to 20 % is realistic.

Running costs after the first implementation

NIS-2 is not a one-off exercise. For keeping it running, allow **20 to 30 % of the implementation cost per year**. On top of that come one-off costs per reportable incident (30 to 80 person-hours) and, optionally, an external NIS-2 officer (from around €500 a month).

> **In the interest of transparency:** NIS-2 is not a certification but a legal duty. The effort is comparable to an ISO 27001 implementation, but what you end up with is not a certificate — it is registration with the BSI and a dependable body of evidence.

5 The ten most common mistakes

From guiding a good many NIS-2 projects, we know the usual stumbling blocks:

1. **Ruling yourself out too quickly**
   "We only build machines." Those are precisely the companies NIS-2 now covers. Every assessment should be documented — including a conclusion that you are not in scope.

2. **Waiting for the German implementation act**
   Starting only when it comes into force leaves you short of time. The requirements are already settled, and implementation takes as long as it takes.

3. **Management believing it is not personally affected**
   Art. 20 and 23 set out the personal responsibility and liability of the management body expressly — along with a duty to be trained.

4. **Ignoring the supply chain**
   Four of the ten mandatory measures concern the supply chain. Security requirements have to be written into contracts and made verifiable.

5. **Never rehearsing the reporting process**
   24 hours pass quickly when nobody knows who tells whom, and when. Tabletop exercises are not a formality.

6. **Treating NIS-2 as an IT project**
   Like ISO 27001, NIS-2 touches HR, procurement, legal, sales and management. Hide it in the IT department and the evidence will not hold.

7. **Underestimating the documentation**
   The BSI expects dependable evidence. "That is how we did it" is not enough — policies, records and audit trails have to exist.

8. **Forgetting to train management**
   The management body has to be demonstrably trained (Art. 20). Missing evidence is a ground for a fine in its own right.

9 **Missing the BSI registration**

Without registering on time you risk a fine, however good your cybersecurity is otherwise.

10 **Choosing on price alone**

“NIS-2-ready in four weeks” is not realistic if the work is done honestly. Look for demonstrable references at your size and in your industry.

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 whether you fall under Annex I or Annex II of the directive?**
   Without a documented scope assessment you risk getting it wrong.

2. **Do you have ISO 27001 or a comparable ISMS?**
   An existing ISMS shortens the road to NIS-2 by 40 to 60 %.

3. **Is there a documented information security policy?**
   The basis of any cybersecurity organisation — Art. 21(2)(a).

4. **Do you carry out risk analyses regularly?**
   At least yearly and whenever something substantial changes — not a box-ticking exercise.

5. **Is there an incident response plan with clear responsibilities?**
   Who detects, who reports, who decides — within 24 hours all three have to work.

6. **Are security incidents documented and analysed in a structured way?**
   Learning from incidents is an explicit NIS-2 requirement.

7. **Do you have an overview of your critical suppliers and their level of security?**
   Supply chain security is one of the directive's main concerns.

8. **Do you use multi-factor authentication for critical systems?**
   Art. 21(2)(j) explicitly requires MFA or comparable methods.

9. **Does management receive cybersecurity training at least once a year?**
   Art. 20 makes that training a duty of the management body.

10. **Do you know how quickly you would have to report a significant incident to the BSI?**
    24 hours for the early warning, 72 hours for the notification, one month for the final report.

Your yes answers	Assessment	Recommendation
0–3 × yes	**New ground**	Building this up in a structured way, with outside help, is advisable. Expect six to ten months.
4–6 × yes	**Partly prepared**	Focus on the gaps — above all the supply chain, reporting and documentation. Four to six months is realistic.
7–10 × yes	**A good basis**	You can finish, with targeted refinement, in two to four months.

Whatever your result: **every company in scope can reach NIS-2 compliance.** It is a question of planning and following through, not of company size.

7 Glossary

The key NIS-2 terms, explained plainly:

NIS-2

Network and Information Security Directive 2 — EU Directive 2022/2555 on cybersecurity.

NIS2UmsuCG

The German implementation act (the NIS2 Implementation and Cybersecurity Strengthening Act).

Essential entity

A company or organisation from Annex I of the directive. Stricter supervision, higher sanctions.

Important entity

A company or organisation from Annex II. Lighter supervision, but the same full duty to implement.

BSI

The German Federal Office for Information Security — the supervisory and reporting authority.

Art. 21

The article of the directive that sets out the ten minimum security measures.

Art. 23

The article on reporting duties after an incident (24 hours, 72 hours, one month).

Supply Chain Security

Securing the supply chain — one of the directive's central concerns.

Incident

A security incident. Once its effects are significant, it has to be reported.

24-hour early warning

The first notification to the BSI, within 24 hours of learning of the incident.

72-hour notification

A detailed notification with an initial assessment, within 72 hours.

Final report

The final report to the BSI, within one month of the 72-hour notification.

MFA

Multi-factor authentication — required explicitly as a minimum measure in Art. 21.

Cyber hygiene

The basic measures: patching, password hygiene, backup, MFA, awareness.

Critical infrastructure (KRITIS)

Critical infrastructure under the German BSI Act — not the same as NIS-2, but overlapping.

ISMS

Information security management system — the structured framework through which NIS-2 is implemented efficiently.

8 Your next step

You have read this guide — that is the first step already. Tackling NIS-2 systematically protects you from fines, from personal liability and from damage to your reputation. And it opens doors with customers who treat cybersecurity as a selection criterion.

A free first conversation

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

✓ Does NIS-2 apply to you?

✓ Where do you stand today — and where are the biggest gaps?

✓ What timeframe and budget are realistic?

✓ Which next steps make sense?

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

The NIS-2 scope check

At **iso-easy.de** you will find our free NIS-2 quick check. In a few minutes you will know whether you are in scope — and which category applies to you.

Contact

Web: iso-easy.de

Phone: +49 711 35 15 705

E-mail: feedback@iso-easy.de

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 in implementing NIS-2, ISO 27001 and neighbouring standards — pragmatically, transparently and as equals.

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