HOUSE OF CONTROL | A COMPANY IN VISMA

NIS2 requirements

A guide for affected organizations

Disclaimer: House of Control is a software company. We do not offer NIS2 compliance consulting services. Thus, **following this guidance does not guarantee compliance with all NIS2 legal requirements.**

The content of this article is based on our own research of the NIS2 requirements and our experience with regulatory compliance, and includes inspiration from various actors offering compliance services. We do not assume any responsibility or liability for any failure to comply with NIS2 requirements or resulting from the use of this guidance.

HOUSE OF CONTROL | A COMPANY IN VISMA

Table of contents

HOUSE OF
CONTROL

A COMPANY IN
VISMA

Digital security has evolved from being a purely IT responsibility to a clear leadership and organizational mandate. Today, cyberattacks, system failures, and supplier breaches can halt operations, damage reputations, and lead to direct financial consequences. With the NIS2 Directive, the EU is responding to this landscape by setting stricter requirements for how organizations approach cybersecurity, risk management, and incident handling.

This guide is designed for professionals working in IT, compliance, legal, or corporate governance. The purpose is to provide a practical understanding of what NIS2 actually requires. We have intentionally avoided unnecessary legal jargon and technical complexity. The goal is to clarify what is expected of your organization and what is needed to manage NIS2 in a structured and effective manner.

1. What is NIS2 and why is it important?

NIS2 is the EU's updated directive on network and information security, replacing NIS1 from 2016. The reasoning is simple: our society is more digital, more interconnected, and more vulnerable than ever before.

Today, organizations rely on:

- Stable IT systems
- Digital suppliers
- Cloud-based services
- Continuous availability

When something fails, the consequences often ripple far beyond the organization itself. This is precisely why NIS2 is not primarily about technology, but about **governance**.

NIS2 is not a technical manual; it is a framework for good management and control. It focuses less on which firewalls you use and more on:

- How you identify risk
- How you prioritize measures
- How you follow up on responsibilities
- How you document that the work is actually being performed

For many organizations, this is a clear signal that security can no longer be handled as a side project within the IT department.

2. Key differences between NIS1 and NIS2

If you are already familiar with NIS1, it is important to understand that NIS2 represents a significant tightening of the rules. Here are the most important changes:

More sectors are covered

NIS1 applied to a relatively limited number of organizations within critical infrastructure. NIS2 significantly expands this scope. New sectors now include:

- Manufacturing companies
- The healthcare and care sector
- Transport and logistics
- Energy and waste management
- Digital service providers

Many organizations that previously did not have to relate to these regulations are now directly covered.

Clearer leadership responsibility

NIS2 specifies that the organization's top management is responsible for compliance. This means:

- Security cannot be delegated away without follow-up.
- Management must approve and monitor security measures.
- Lack of compliance can have consequences at the leadership level.

This is a distinct change from NIS1, where responsibilities were often more vague.

Stricter risk management requirements

NIS2 sets concrete requirements for how risk should be assessed and managed. This applies not only to internal systems but also to the supply chain and third parties. It is no longer enough to assume that suppliers "have things under control."

Stricter sanctions

Authorities have been given stronger tools for enforcement. Maximum administrative fines depend on whether the organization is classified as "essential" or "important."

- **Essential entities:** Fines up to €10 million or 2% of total global annual turnover.
- **Important entities:** Fines up to €7 million or 1.4% of total global annual turnover.

Equally important is the power of authorities to issue binding instructions, perform audits, and demand improvements.

3. Who is covered by NIS2?

NIS2 divides organizations into two main categories:

1. **Essential entities**
2. **Important entities**

Both categories must meet the requirements of the directive, but supervision is stricter for essential entities. Furthermore, documentation requirements under Article 21 vary not only by sector but also by country. This makes the task particularly demanding for companies operating across multiple EU nations.

Classification depends on factors such as:

- The sector the organization belongs to.
- The size of the organization.
- The role the organization plays in society and value chains.

A key point regarding suppliers

Even if your organization is not directly subject to NIS2, you may be affected indirectly. If your customers are covered by the directive, they will impose requirements on you as a supplier. This particularly applies to IT services, operations, software, infrastructure, and other critical support functions.

4. Article 21: Risk management and security measures

Article 21 is the "engine room" of NIS2. It describes the measures an organization must have in place to manage risks related to network and information systems.

The core of the article is simple: The organization shall implement technical, operational, and organizational measures that are proportionate to the risks faced.

What does this mean in practice? The following list provides examples of measures that are often relevant:

Risk analysis: Have you identified which assets are critical and which threats could affect them?

Security policies: Are there written guidelines for information security, and are they known throughout the organization?

Incident handling: Do you have a plan for what to do when (not if) something goes wrong?

Continuity and contingency plans: How do you maintain operations during a major IT outage or security breach?

Supply chain security: Have you assessed risks related to subcontractors and third parties?

Training and awareness: Do employees and management receive training in digital security and risk understanding?

Data protection: Do you use encryption where necessary?

Secure system development and procurement: Do you have routines to ensure security during the development, purchase, and maintenance of IT systems, including vulnerability management?

Evaluation of security measures: Do you have mechanisms to check if security measures work as intended, and are these assessments used for improvement?

Basic cyber hygiene: Are basic security routines followed, such as system updates, securing endpoints, and using secure default settings?

Access management and asset overview: Do you have an overview of which systems, data, and devices are in use, and is access limited to what is necessary for each role?

Authentication and secure communication: Do you use strong authentication mechanisms, such as multi-factor authentication (MFA), and secure your communications?

A common gap in many organizations

Most organizations already have some measures in place. The challenge is often that:

- Documentation is scattered across Excel sheets and emails.
- Responsibility is unclear.
- Follow-up is irregular.
- It is difficult to show the "big picture."

NIS2 requires you to prove compliance over time. This involves documenting what you actually do, not just what you plan to do.

5. Supply chain security: You are only as strong as your weakest link

One of the most discussed aspects of NIS2 is the requirement for supplier management. Previously, many have blindly trusted that providers maintained robust governance. Under NIS2, trust is no longer enough – it must be documented.

Most modern cyberattacks do not hit the target directly but occur via a subcontractor with weaker security. If a security incident at a supplier significantly impacts your services, your organization is responsible for determining if the incident is reportable under NIS2 and, if so, reporting it to the authorities.

How to follow up with suppliers in practice:

1. **Categorization:** Not all suppliers are equally important. Identify the critical ones – those whose absence would stop your ability to deliver services.

2. **Security requirements in contracts:** Include specific information security requirements in all new agreements, including the requirement that they notify you of any breaches.

3. **Continuous monitoring:** An annual email is not enough. While certifications like ISO 27001 or SOC 2 reports are not explicit NIS2 requirements, they are useful forms of documentation when assessing a supplier's security level.

6. Article 23: Reporting security incidents

When a serious incident occurs, there is rarely a lack of activity. What is often missing, however, is an overview. Article 23 is designed for these high-pressure situations where information is incomplete and consequences are potentially vast.

The core of Article 23 is that the organization must be able to **report quickly, in a structured manner, and accurately** to the authorities.

What counts as a "significant incident"?

An incident must be reported if it has a significant impact on:

- The availability of systems or services.
- The integrity of data or systems.
- The confidentiality of information.
- The delivery of the organization's services.

The NIS2 reporting timeline:

1. **Early warning (within 24 hours):** Confirmation that a serious incident has occurred.
2. **Update (within 72 hours):** More information on the nature, scope, and potential consequences of the incident.
3. **Final report (within one month):** A full review of the cause, handling, and measures implemented to prevent recurrence.

7. Other important NIS2 requirements

Management’s role and competence (Article 20)

The board and management must:

- Understand the risks the organization takes.
- Approve security measures and monitor compliance.
- Undergo mandatory cybersecurity training to make informed decisions.

Supervision and authority control

Authorities have expanded powers to conduct audits, demand documentation, and order specific improvements.

Alignment with other regulations

NIS2 must be seen in conjunction with **GDPR** (especially regarding personal data) and **DORA** (for financial entities). A coordinated management model provides a better overview and lower risk.

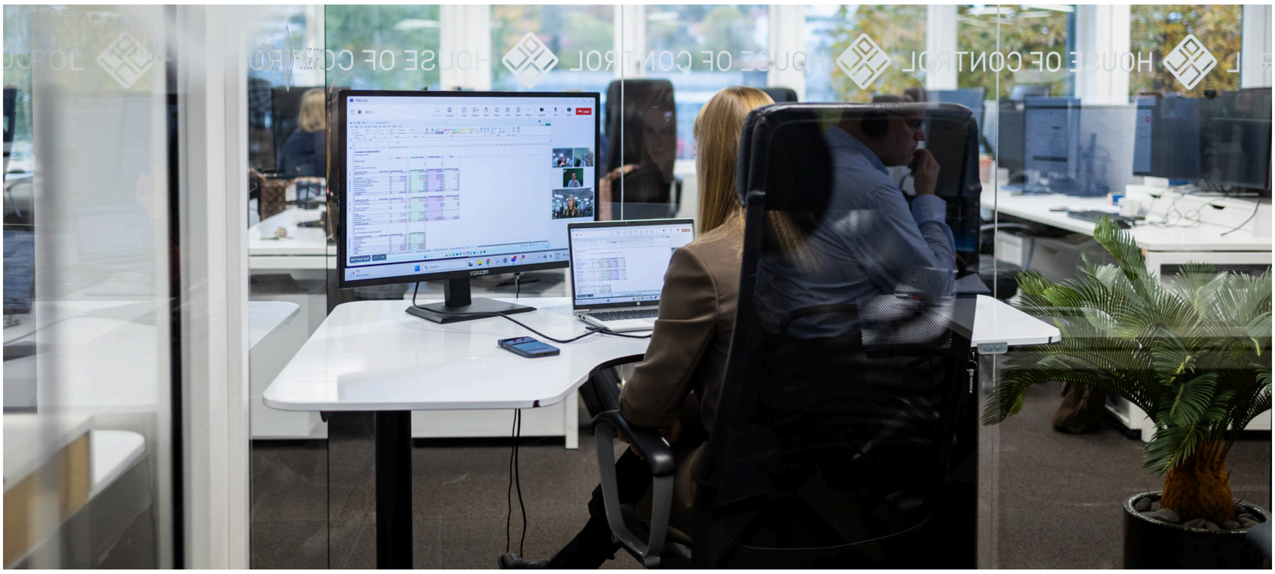
8. Common pitfalls

- Treating compliance as a one-time project.
- Unclear responsibility between IT, Legal, and Management.
- Assessing risk but failing to follow up with actions.
- Manual processes that are time-consuming and prone to error.

9. Building a structured NIS2 approach

Organizations that succeed with NIS2 work systematically. A structured approach typically looks like this:

1. **Map scope and responsibility:** Clarify which parts of the business are covered and who is responsible for what.
2. **Conduct a gap analysis:** Compare current practices with Article 21 and 23 requirements.
3. **Establish clear ownership:** Every control point must have an owner.
4. **Digitize the work:** Avoid manual spreadsheet dependency. Collect requirements, risks, and documentation in one place.
5. **Continuous improvement:** Update measures as risks evolve.



How to conduct an effective gap analysis

1. **Review Article 21:** Go through the ten minimum requirements in the article. For each point, you must ask: "Do we have a written policy for this? Is it implemented? Can we prove it?"

2. **Identify "paper compliance":** Many companies have excellent contingency plans that are merely "paper compliance", sitting in a drawer gathering dust. If the plan has not been updated or tested within the last year, it is considered a "gap" under NIS2.

3. **Assess technical vs. organizational:** A gap is not always the lack of a firewall. Often, the largest gap is a lack of documented employee training or unclear lines of responsibility between IT and management.

4. **Prioritization list:** Once the analysis is complete, you will be left with a list of gaps. Prioritize these based on risk: Which vulnerabilities are easiest for hackers to exploit, and which gaps would result in the most severe sanctions during an audit?

10. Why structure and tools are essential

NIS2 demands traceability and continuity. You must be able to:

- Show which assessments were made.
- Explain why specific measures were chosen.
- Document that follow-up occurs over time.

This is difficult to achieve without structure and the right tools. Effective digital solutions can organize and link risks, measures, and responsibilities. With built-in notifications, it becomes easier to document that NIS2 requirements are being met. On a more strategic level, a digital tool provides management with a clear overview and a solid basis for making informed decisions.

11. Conclusion: From regulation to resilience

NIS2 represents a clear shift in how digital risks are managed. While the requirements are stricter, the directive provides a clear path forward. Organizations that work structured with risk management and documentation will be better equipped, not just for audits, but against actual cyber threats.

Done correctly, NIS2 becomes a natural part of corporate governance, not as a burden, but as a framework for better control and safer operations.

HOUSE OF CONTROL | A COMPANY IN VISMA

Thank you for your interest in **House of Control!**

Contact

House of Control AS
O.H. Bangs vei 70 1363 Høvik, Norway
+47 815 66 355

www.houseofcontrol.com
mops@houseofcontrol.com
Follow us: Linkedin