NIS2 readiness report 2026

A Scandinavian market analysis for business leaders

Navigating the new European cybersecurity standard:
Trends, gaps, and strategic implementation

www.houseofcontrol.com

Table of Contents

1. Introduction: Adapting to the new regulatory landscape

The implementation of the EU's NIS2 Directive (Network and Information Security Directive) represents a fundamental shift in how European organisations manage digital risk.

NIS2 is a legal requirement for boardrooms and management, imposing a direct responsibility on leadership to oversee and approve the organisation's cybersecurity measures. Under the new Directive, management can be held personally liable for non-compliance, requiring them to actively participate in risk assessments, ensure the implementation of robust security frameworks, and undergo mandatory training to understand the evolving threat landscape.

This report is based on a market study conducted in February 2026 by Opinion on behalf of House of Control. With data collected from 462 relevant business leaders and decision influencers across Norway, Sweden and Denmark, this analysis highlights the specific gaps and trends in preparedness in Scandinavia.

In addition to the research data, we have included House of Control's reflections based on conversations with Nordic customers expected to be affected by NIS2. These sections are marked as "Our perspective" throughout the report.

Key research data

Purpose: To map market awareness and the strategic impact of NIS2, and to explore how companies plan to manage the upcoming regulatory requirements.

Methodology: Quantitative web-based survey conducted in February 2026 by Opinion.

Target group: Key decision-makers in Scandinavian companies with more than 50 employees.

Sample size: 462 respondents in total.

- Norway: 150
- Sweden: 218
- Denmark: 94

Respondent profile:

- Around six in ten respondents have decisive, high or fairly high influence over decisions in IT, reporting systems or compliance.
- Primary roles include IT Leaders/CTO (31%) and CEOs/Managing Directors (16%).
- The sample represents a broad range of sectors, including the public sector, digital infrastructure, and energy.

2. Summary of the key findings

The 2026 study reveals a Scandinavian market characterized by higher awareness than operational readiness.

The following findings highlight the current state of the region:

- Among respondents who know or have heard of NIS2, 62% say the Directive has or will likely have consequences for their company, corresponding to around half of the total market.

- 55% of respondents know the Directive well or somewhat. Among respondents who say NIS2 has or will likely have consequences for them, 15% have established systems and procedures for this work, and 45% rate their company as prepared for NIS2 requirements today.

- Manual compliance follow-up remains time-consuming. Among affected respondents who can estimate time use, organisations report an average of **54 hours per month** on manual follow-up, with Norway reporting the highest average at **83 hours per month.**

- NIS2 impact extends beyond directly regulated entities. Among organisations experiencing consequences from the Directive, 46% are indirectly affected only through customer or supplier requirements, while a further 14% are both directly and indirectly affected. House of Control interprets this as a sign that customer and supplier reporting requirements may create commercial documentation pressure in B2B relationships.

- Implementing security measures and documentation are the most resource-intensive activities. Among affected respondents, 52% point to implementing security measures, while 47% cite documenting and following up how they protect IT systems and data. Formalising supplier and subcontractor requirements is also significant at 30%.

3. Market awareness: High knowledge, low readiness

The study mapped the level of knowledge and perceived significance of NIS2 across Scandinavia.

3.1. Understanding the Directive

- **Market awareness:** Market awareness: 55% of respondents know the NIS2 Directive well or somewhat.
- **Deep knowledge:** 21% of total respondents state they know the Directive well.
- **Regional variation:** Sweden shows the highest level of deep knowledge at 24%, followed by Denmark at 23%, and Norway at 13%.
- **Leadership insight:** Among those with "significant" or "decisive" influence over IT and compliance, 34% know the Directive well.

3.2. The readiness gap

- **Preparation:** Among respondents who say NIS2 has or will likely have consequences for their company, 45% rate their company as prepared.
- **Current status:** Among respondents who say NIS2 has consequences for them, 15% have established systems and procedures to handle this work.

3.3. Our perspective: The gap between knowing and doing

While a majority are aware of NIS2, the survey shows that 55% know the Directive well or somewhat, 26% have only heard of it, and 19% had not heard of it.

In addition to the survey data, a clear trend stands out from House of Control's dialogues with Nordic companies who are preparing to report on NIS2. While many are aware of NIS2, many still lack a clear and operational plan for where to begin. The complexity of the new requirements often leads to a state of uncertainty, making it challenging for leaders to turn these legal demands into daily routines.

In House of Control's experience, a major obstacle is that supplier data is often scattered across different systems, meaning there is no single link between contracts and actual security risks. Additionally, many companies rely on generic questionnaires that act as simple check-the-box exercises without providing real insight into what a vendor actually delivers.

4. Scope and impact: Direct vs. indirect responsibility

NIS2 applies primarily to medium and large enterprises in critical sectors, but its reach extends far beyond direct regulation.

4.1. Critical sectors in the Scandinavian market

The survey targeted relevant leaders in companies with more than 50 employees. Many respondents represent NIS2-relevant sectors, while 31% selected "none of these" on the sector list.

- **Public sector:** 19% of the total sample.
- **Digital infrastructure:** 12% of the sample.
- **Energy and transport:** Both sectors represent 11% and 10% of the sample respectively.
- **Classification:** Among respondents asked this classification question, 56% say they are an "Important Entity" and 27% say they are an "Essential Entity".

4.2. The supply chain "ripple effect"

- **Indirect impact:** Among the companies that experience consequences from NIS2, 46% of companies affected by NIS2 believe they are indirectly affected because their customers or suppliers require NIS2-level reporting.
- **Regional peak:** Denmark has the highest share reporting indirect impact (61%), followed by Norway (50%) and Sweden (39%).
- **Strategic risk:** For many businesses, NIS2-related documentation may become increasingly important in B2B relationships, especially where customers or suppliers must report on NIS2-level requirements.

4.3. Our perspective: Supply chain visibility and compliance as a license to operate

While organisations may have control over their direct suppliers, they often lack visibility into sub-suppliers further down the supply chain. In our view, achieving true resilience requires a visual mapping of the entire supply chain that identifies interdependencies and criticality scores for every vendor. For suppliers affected indirectly, the ability to document their NIS2 status once in a portal and share it with all their customers will be a major advantage. This removes the need to fill out the same manual reports repeatedly.

Beyond the survey data, House of Control's dialogues with Nordic companies show that many are surprised by how NIS2 affects them indirectly. Even if your business is not directly regulated, customers may request more documentation from suppliers as part of NIS2-related supply-chain risk management.

We increasingly hear about companies facing strict documentation demands just to maintain their existing B2B contracts. In our experience, NIS2-related documentation is becoming a competitive qualifier in some B2B processes. Companies unable to document security maturity may face commercial disadvantages.

5. The compliance burden: Benchmarking manual effort

A major finding of the report is the high volume of manual labour currently dedicated to compliance.

5.1. Manual labour hours

Among affected companies where respondents could estimate manual compliance follow-up, reported averages are:

- **Regional average:** 54 hours per month.
- **Norway:** 83 hours per month.
- **Denmark:** 53 hours per month.
- **Sweden:** 45 hours per month.

5.2. High-resource activities

Among respondents who say NIS2 has consequences for their company, the most resource-intensive activities are:

- **Security measures:** 52% find implementing measures like risk assessments, access control, and encryption most demanding.
- **Documentation:** 47% cite documenting and following up on IT system protection as a major burden.
- **Vendor management:** 30% find formalizing requirements for suppliers and subcontractors highly resource-intensive.

5.3. Our perspective: The sustainability of manual processes

Among affected Norwegian respondents who could estimate manual compliance follow-up, the reported average is 83 hours per month. This is a challenge we recognise from our ongoing dialogues with the market. Relying on spreadsheets and manual follow-ups is not only expensive and time-consuming, but it also creates a significant risk of human error.

From House of Control's perspective, the clear takeaway is that manual processes are no longer sustainable. Under NIS2, where management faces personal liability, having a single source of truth becomes increasingly important for maintaining control, traceability and confidence.

6. Practical next steps for business leaders

Based on the findings from the Opinion survey and House of Control's dialogues with Nordic companies expected to be affected by NIS2, House of Control recommends that affected organisations prioritise four actions:

1. Clarify their NIS2 exposure
Determine whether the organisation is directly affected, indirectly affected through customer or supplier requirements, or both.

2. Map critical suppliers and sub-suppliers
Establish visibility into suppliers, services and dependencies that may create operational or compliance risk.

3. Establish documented compliance processes
Put in place structured processes for risk assessment, evidence collection, supplier follow-up and incident reporting.

4. Reduce dependency on manual spreadsheets and fragmented documentation
Move towards a more structured and traceable way of managing NIS2-related documentation and follow-up.

7. Looking ahead: Simplify NIS2 compliance with House of Control

House of Control's view is that affected companies have the knowledge but often lack the specialized tools required to meet the strict demands of the new Directive.

To bridge this gap, House of Control is currently developing the next generation of NIS2 compliance software. The solution is designed to transform complex legal requirements into a manageable operational reality, even for organisations without dedicated security experts.

This upcoming platform will serve as a single source of truth for the entire organisation. By automating essential documentation workflows, providing leadership with real-time visibility into digital risks, and streamlining supply chain oversight, we enable businesses to turn a significant regulatory burden into a competitive advantage.

We are now initiating dialogues with organisations that want to stay ahead of the curve. We offer detailed information about the concept and deep dives into how this survey data applies to your specific industry.

Contact House of Control for a non-binding discussion about your NIS2 readiness, supplier documentation needs and opportunities to reduce manual compliance work.

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

The content of this report is based on survey data collected by Opinion on behalf of House of Control, our own research into NIS2 requirements, and our experience with regulatory compliance and customer dialogues in the Nordic market.

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

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