HOUSE OF CONTROL | A COMPANY IN VISMA

NIS2 guide: Checklist for compliance

Risk management and incident reporting (Articles 20, 21 & 23)

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.

Table of contents

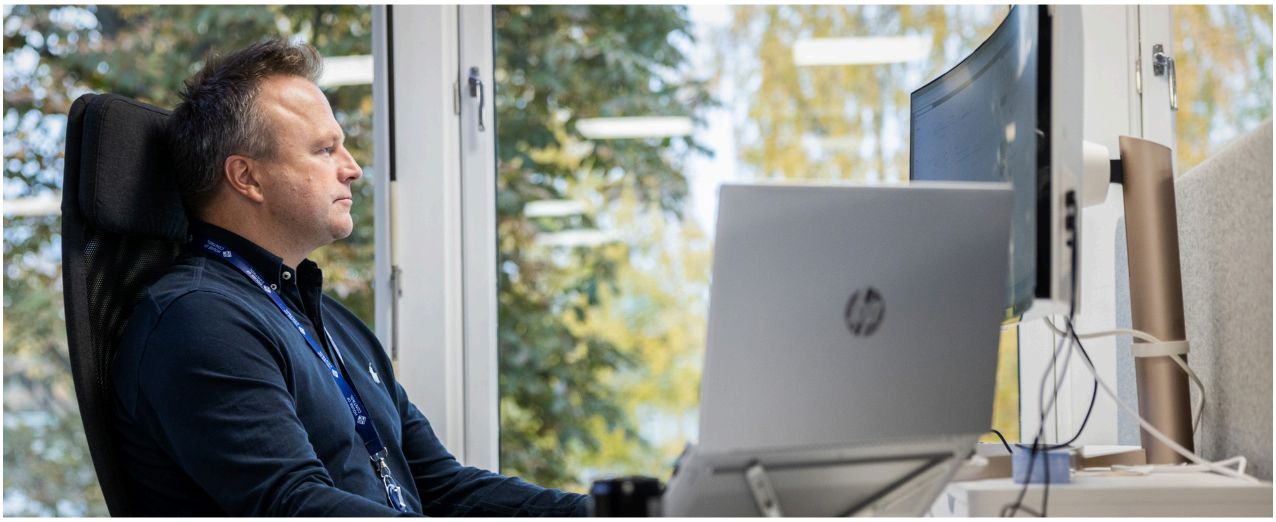
1. Introduction: From technical task to legal duty

The NIS2 Directive is the EU's response to an increasingly unpredictable digital world. It replaces the original NIS Directive by expanding the scope to more sectors and placing the burden of responsibility **directly on senior leadership.**

For many organizations, the shift from NIS1 to NIS2 is a jump from voluntary best practices to **mandatory legal requirements.** Regardless of your category, the goal is resilience and readiness. Organizations must now move beyond "best practices" into a regime of verifiable evidence.

This guide breaks down the complex legal language of Articles 21 and 23 into a clear and practical checklist.

Note that certain sectors may be subject to sector-specific Union legal acts (Lex Specialis) that provide for more stringent requirements, such as DORA for the financial sector or EU 2022/2557 (CER Directive) for critical entity resilience.



1.1. Essential and important entities: Quick comparison

Comparison point	Essential entities	Important entities
Audit type	Regular proactive checks	Primarily reactive checks (or if breach is suspected)
Proof needed	Must be ready at all times	Must be ready to show upon request
Management ban	Yes (leaders can be temporarily banned)	Depends on national implementation
Max fines	Up to €10M or 2% of global turnover	Up to €7M or 1.4% of global turnover

2. Governance and risk management (Articles 20 & 21)

Article 21 is the core of the Directive. It mandates that you take "appropriate and proportionate" steps to manage security risks. Implementation should be risk-based, considering the degree of the entity's exposure and the societal impact of its services.

2.1 Leadership and governance

NIS2 is unique because it makes senior leadership accountable for cybersecurity failures. Under Article 20 (Governance), executive leadership is required to approve security measures and oversee their implementation, including incident reporting and supply chain risk management.

While not directly responsible for a subcontractor's breach, management is accountable for ensuring such incidents are reported timely and that proper due diligence was conducted. Non-compliance can in some jurisdictions cause a temporary ban from management roles.

Executive training: Senior leadership has completed cybersecurity training tailored to their oversight duties.

Proof: Timestamped certificates and a record of the training curriculum.

Formal approval: The security strategy and risk-management measures have been formally approved by the board.

Proof: Signed board meeting minutes addressing the risk-management plan.

Budget and resources: There is a documented budget dedicated to maintaining NIS2 standards.

Proof: Financial records showing resource allocation for security tools and personnel.

2.2 The technical checklist for Article 21

The following 10 categories are mandatory under Article 21(2). While the specific implementation is risk-based, these examples represent best-practice "readiness":

1. Risk analysis and information security policies

The risk register: A live document listing digital assets and their specific threats.
All-hazards scope: Includes digital threats (ransomware) AND physical/environmental threats.
Version control: Security policies reviewed and updated regularly.

2. Incident handling

Detection capabilities: Systems that monitor for unusual activity.
Ticketing system: A central platform to log security events.

3. Business continuity and crisis management

Backup isolation: Backups are stored separately and are "immutable".
Recovery time objectives (RTO): Defined time limits for system restoration.
Best practice: A report from a "restore test" (e.g., every 6–12 months).

4. Supply chain security

Vendor risk map: Suppliers categorized by the risk they pose.
Contractual clauses: Agreements that facilitate your own compliance, such as breach notification.
Best practice: A completed "vendor assessment" form for critical suppliers.

5. Security in network and information systems

Vulnerability management: Systematic scanning for weaknesses.
Patch management: A risk-based policy for software updates.
Vulnerability disclosure: A policy allowing for the reporting of security flaws.

6. Evaluating the effectiveness of measures

Security audits: Regular internal or external audits to check policy adherence.

7. Cyber hygiene and training

Mandatory awareness: Staff training on phishing and reporting.

8. Cryptography and encryption

Data at rest & in transit: Use of encryption and secure protocols where appropriate.

9. HR security and access control

Access reviews: Periodic review of "who has access to what".
Principle of least privilege: Ensuring access is limited to what is strictly needed.

10. Multi-factor authentication (MFA) and secured comms

MFA: Required for remote access and administrative accounts (where appropriate).
Secured emergency comms: Secure voice, video, and text communication systems for use during an incident.

3. Article 23: The reporting obligations

Article 23 is the most time-sensitive part of the law. If an incident is "significant," the clock starts ticking the moment you become aware of it.

3.1 Defining "significant"

An incident is considered significant if it:

1. Has caused or is capable of causing severe operational disruption of the services or financial loss for the entity.

2. Has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

3.2 The reporting checklist

24-hour early warning: A notification to the national authority or CSIRT. It must include whether the incident is suspected of being caused by unlawful or malicious acts and whether it could have a cross-border impact.

72-hour incident notification: A detailed update updating the early warning and indicating initial findings, including severity and impact.

Intermediate report: Upon request by the authority or if the incident is ongoing.

1-month final report: A deep dive into the root cause, the duration, and the steps taken to prevent recurrence.

Recipient notification: If the incident affects your customers, you must notify them "without undue delay" and provide advice on mitigation.

Note: By 2026, most Member States have established centralized digital portals for incident reporting. Ensure your incident response team is registered and familiar with your specific national reporting interface.

4. The burden of proof: Beyond spreadsheets

The most common mistake organizations make is trying to track NIS2 compliance in a spreadsheet. This leads to "compliance friction", where the work of proving you are safe takes more time than actually being safe.

To stay ahead, organizations are moving toward centralized software solutions. A digital system ensures that your documentation is always ready for an audit and that your incident reporting happens with the click of a button.

5. Summary: The road to total readiness

1. Identify: Confirm if you are an essential or important entity.

2. Assign: Name a "compliance lead" to own the documentation process.

3. Gap analysis: Use the checklist above to find what evidence you are missing.

4. Remediate: Fix the gaps, starting with MFA, backups, and leadership training.

5. Centralize: Move your documentation into a single system of truth to ensure you are always audit-ready.

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