CORDEVO
FÖR ETT BÄTTRE LEDARSKAP

Cybersecurity

Board-Level Accountability for NIS2 Compliance

NIS2 (Directive (EU) 2022/2555) seeks to establish a high common level of cybersecurity across the EU. It extends the scope and responsibilities from the earlier NIS Directive to include more sectors and entities. The Directive emphasises that governance and accountability for cyber risk sit with the management body, often the board or equivalent, which must oversee implementation of security measures and may be held personally liable for infringements.

This whitepaper distils what leadership teams must do to meet NIS2 obligations, focusing on accountability, responsibility, authority and competence.

1. Governance Obligations for the Board

1.1 Accountability and Responsibility

Article 20 of NIS2 requires management bodies to approve cybersecurity risk-management measures, oversee their implementation and maintain effective management practices. If the organisation fails to comply, board members may be held liable. [Ref1] Leaders are therefore accountable for ensuring their organisation meets all NIS2 obligations. This includes:

- Approving the cybersecurity strategy and risk-management framework, ensuring it aligns with NIS2 and industry best practice.
- Overseeing implementation of appropriate technical, operational and organisational measures to manage risks to networks and information systems. [Ref2]
- Ensuring policies cover risk analysis and information system security, incident handling, business continuity, supply-chain security, secure development and acquisition, control effectiveness and basic cyber hygiene. [Ref3]
- Reviewing supply-chain risk management and ensuring that supplier vulnerabilities and cybersecurity practices are assessed before onboarding and throughout the relationship. [Ref4]
- Monitoring compliance with timely incident reporting: issuing an early warning within 24 hours, an incident notification within 72 hours and a final report within one month. [Ref5]

1.2 Authority

Boards must possess the authority to allocate resources, enforce policies and make strategic decisions required to achieve compliance. This includes budgeting for cybersecurity initiatives, appointing and empowering a competent Chief Information Security Officer (CISO) and delegating responsibilities while retaining oversight.

Boards should mandate contractual clauses requiring suppliers to meet equivalent security standards and grant management the authority to conduct audits and risk assessments across all departments and subsidiaries.

1.3 Competence and Training

NIS2 explicitly requires members of the management body to undergo training so they can identify risks and assess cybersecurity risk-management practices. [Ref1]

Leadership teams must cultivate competence in cybersecurity governance by:

- Undertaking regular cybersecurity awareness and risk-management training tailored for executives and board members.
- Ensuring specialised training for those with operational roles, including understanding of NIS2 reporting obligations and the organisation's incident response plan.
- Encouraging a culture of continuous learning and knowledge sharing throughout the organisation, with employees trained to recognise risks and assess cybersecurity practices. [Ref1]
- Aligning with ISO 27001 to establish a formal Information Security Management System (ISMS). ISO 27001 provides a framework for managing information security risk and emphasises continuous improvement and holistic controls across people, processes and technology. [Ref7]

2. Consequences of Non-Compliance

Ignoring NIS2 obligations exposes the organisation to financial, regulatory and reputational risks. Article 34 mandates that essential entities that infringe risk management or reporting obligations may face administrative fines of at least €10 million or 2 % of worldwide annual turnover, whichever is higher; important entities may be fined at least €7 million or 1.4 % of turnover. [Ref6] Supervisory authorities can also impose other corrective measures and require public disclosure of non-compliance. Moreover, inadequate governance may result in personal liability for directors and damage stakeholder trust.

3. Implementation Considerations for the Board

Leadership teams should embed cybersecurity into corporate governance structures and decision-making. Key steps include:

- Establish a governance framework with clear roles and responsibilities (RACI) covering the board, CISO, Data Protection Officer and operational teams.
- Institute a risk management process that identifies assets, assesses threats and vulnerabilities, quantifies financial impact and defines risk tolerances.
- Ensure security policies are comprehensive and are reviewed and approved annually. This includes incident response plans, regulatory reporting procedures, change management and supply-chain security policies.
- Implement technical and organisational controls based on NIS2 Article 21, including risk analysis, incident handling, business continuity, supply-chain security, secure development, control effectiveness assessment, basic cyber hygiene, encryption and multi-factor authentication. [Ref3]

- Integrate continuous monitoring and auditing to assess compliance and control effectiveness. Track key performance indicators such as mean time to detect and respond to incidents, vulnerability remediation timelines, training completion rates and supply-chain assessments.
- Develop a structured incident response and reporting plan aligned with NIS2 Article 23, ensuring early warning within 24 hours, detailed notification within 72 hours and final report within one month of incident detection. [Ref5]
- Undertake regular board-level reviews of cybersecurity posture, including audit findings, risk trends and progress against improvement plans.

4. Conclusion

NIS2 elevates cybersecurity to a board priority by imposing direct responsibility on management bodies to approve, oversee and continuously improve risk management.

Leadership teams must adopt a proactive and holistic approach encompassing governance, risk management, supply-chain oversight, incident reporting and training.

By embracing their accountability, exercising authority, investing in competence and aligning with frameworks such as ISO 27001, boards can not only meet regulatory requirements but also strengthen resilience and trust among customers, partners and regulators.

Contact us for more information

soren.rundgren@cordevo.se (070-519 03 40)
johan.mandelius@cordevo.se (070-595 04 82)

References:

1. Article 20 of Directive (EU) 2022/2555: Governance — Management bodies must approve cybersecurity risk-management measures, oversee their implementation and can be held liable; they must also undergo training and encourage employee training. [Ref1]
2. Article 21 of Directive (EU) 2022/2555: Cybersecurity risk-management measures — Entities must take appropriate and proportionate technical, operational and organisational measures to manage risks and prevent incidents. [Ref2]
3. Article 21(2) of Directive (EU) 2022/2555: Specific measures including risk analysis and security policies, incident handling, business continuity, supply-chain security, secure system acquisition, control effectiveness assessment, basic cyber hygiene, encryption policies, human resources security and multi-factor authentication. [Ref3]
4. Article 21(3) of Directive (EU) 2022/2555: Supply-chain security — Entities must consider vulnerabilities and the overall quality of products and cybersecurity practices of direct suppliers and service providers. [Ref4]
5. Article 23 of Directive (EU) 2022/2555: Reporting obligations — Significant incidents require early warning within 24 hours, incident notification within 72 hours and final report within one month. [Ref5]
6. Article 34 of Directive (EU) 2022/2555: Administrative fines — Essential entities may be fined at least €10 million or 2 % of worldwide turnover; important entities at least €7 million or 1.4 % of turnover. [Ref6]
7. ISO/IEC 27001:2022 – Information Security Management Systems standard: provides a framework for establishing, implementing, maintaining and improving an ISMS, emphasising risk-based controls, stakeholder confidence and continuous improvement. [Ref7]