COMPLIANCE GUIDE

NIS2 Directive — What Enterprises Must Do Now

Step-by-step breakdown of NIS2 obligations with mapped security controls, vendor recommendations, and audit-ready checklists for immediate compliance.

160K+	€10M	24hr
entities now in scope	maximum fines or 2% turnover	incident reporting deadline

Published by Mellivor Cybersecurity | February 2026 | 15 min read

What Is NIS2 and Why It Matters

The Network and Information Security Directive 2 (NIS2) is the European Union's updated cybersecurity legislation, replacing the original NIS Directive of 2016. It dramatically expands scope, strengthens requirements, and introduces personal liability for senior management — making cybersecurity a boardroom-level obligation rather than an IT department concern.

NIS2 applies to 'essential' and 'important' entities across 18 sectors including energy, transport, banking, health, digital infrastructure, public administration, and manufacturing. Organisations that fall within scope must implement risk management measures, report significant incidents within 24 hours, and demonstrate supply chain security — or face fines of up to €10 million or 2% of global turnover.

> *"NIS2 is not a checkbox exercise. It demands demonstrable, continuous risk management — and it holds leadership personally accountable for failures."*

Are You in Scope?

NIS2 classifies organisations into two categories. Both face the same core obligations, but essential entities face stricter supervisory regimes and higher penalties.

Category	Sectors	Supervision
Essential Entities	Energy, transport, banking, financial markets, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, space	Proactive: regular audits, on-site inspections, fines up to €10M or 2% turnover
Important Entities	Postal services, waste management, chemicals, food production, manufacturing, digital providers, research organisations	Reactive: investigation after incidents or evidence of non-compliance, fines up to €7M or 1.4% turnover

Core Obligations Mapped to Controls

NIS2 Article 21 defines ten categories of risk management measures. Below we map each obligation to practical security controls and relevant vendor capabilities.

1. Risk Analysis & Information System Security Policies

Maintain comprehensive risk assessments covering all information systems. Implement and regularly review security policies that reflect current threat landscape and business context.

> *Recommended: Nanitor provides continuous vulnerability remediation and exposure management, enabling risk-based prioritisation aligned to NIS2 requirements.*

2. Incident Handling

Establish incident detection, response, and recovery processes. Report significant incidents to the relevant CSIRT within 24 hours (early warning), 72 hours (full notification), and one month (final report).

> *Recommended: Lima Charlie delivers real-time endpoint visibility and threat detection at enterprise scale, while Cybereason XDR provides operation-centric detection across the full attack surface.*

3. Business Continuity & Crisis Management

Implement backup management, disaster recovery, and crisis management procedures to ensure operational resilience during and after security incidents.

> *Recommended: Mellivor's advisory team supports business continuity planning with architecture review and resilience testing across critical infrastructure.*

4. Supply Chain Security

Assess and manage cybersecurity risks in supplier and service provider relationships. Implement appropriate contractual and technical measures for supply chain assurance.

> *Recommended: Silent Push maps adversary infrastructure targeting your supply chain before attacks launch, while ZeroFOX monitors external threats across social media, dark web, and surface web.*

5. Network & Information System Security

Secure acquisition, development, and maintenance of network and information systems, including vulnerability handling and disclosure.

> *Recommended: Gatewatcher NDR provides deep network traffic analysis, 42Crunch secures APIs across the full lifecycle, and Corero delivers real-time DDoS protection for critical infrastructure.*

6. Cybersecurity Risk Assessment Effectiveness

Implement policies and procedures to assess the effectiveness of cybersecurity risk management measures. Conduct regular testing and auditing.

Recommended: Labyrinth Security deploys deception technology that validates detection effectiveness by generating high-fidelity intelligence from real adversary interactions.

7. Cyber Hygiene & Training

Implement basic cyber hygiene practices and provide regular cybersecurity awareness training for all staff, with specialist training for privileged users.

Recommended: Cynox enforces password hygiene across Active Directory in real time, blocking leaked and weak credentials without user friction or plaintext storage.

8. Cryptography & Encryption

Implement policies on the use of cryptography and, where appropriate, encryption to protect data in transit and at rest.

Recommended: Transfer Chain provides zero-knowledge encrypted file transfer, ensuring end-to-end data privacy without requiring users to manage encryption keys.

9. Human Resources & Access Control

Implement access control policies, asset management, and human resources security measures including least-privilege enforcement.

Recommended: Securden enforces privileged access management and least-privilege policies across the enterprise, with complete audit trails for compliance evidence.

10. Multi-Factor Authentication & Secure Communications

Deploy multi-factor authentication, continuous authentication where appropriate, and secured voice, video, and text communications.

Recommended: Beyond Guard delivers continuous zero-trust verification across the entire organisation, and SURF Security provides enterprise browser protection for all web-based communications.

NIS2 Compliance Checklist

Use this checklist to track your organisation's progress against NIS2 requirements.

■	Determine scope classification (essential / important entity)
■	Appoint a named security officer with board-level reporting
■	Complete comprehensive risk assessment across all information systems
■	Implement 24-hour incident reporting process to relevant CSIRT
■	Audit and document all supplier/third-party security arrangements
■	Deploy multi-factor authentication across all privileged and critical access
■	Implement network detection and monitoring capabilities
■	Establish vulnerability management with risk-based prioritisation
■	Implement data encryption policies for data in transit and at rest
■	Deploy endpoint detection and response across all managed devices
■	Conduct business continuity and disaster recovery testing
■	Deliver cybersecurity awareness training to all personnel
■	Implement supply chain security assessment process
■	Establish regular effectiveness testing and audit cycle
■	Document all policies, procedures, and evidence for regulatory review

Ready to build your security programme?

Mellivor works with 20+ specialist cybersecurity vendors across 12 security domains. Our advisory team can map the right technologies to your risk profile, compliance requirements, and operational environment — from initial assessment through deployment and ongoing optimisation.

Book a consultation: mellivorsecurity.com/contact

Explore our vendors: mellivorsecurity.com/vendors