AvePoint

INFOGRAPHIC

NIS2 Directive: Understanding EU's Cybersecurity Framework

The NIS2 Directive strengthens cybersecurity across the EU, covering 18 critical sectors with mandatory requirements for risk management, incident reporting, and business continuity. Understanding how NIS2 aligns with existing frameworks helps organizations build comprehensive compliance strategies that enhance operational resilience. Read on to discover what NIS2 means for your organization.

Key Requirements Overview

Risk Management Measures
- Conduct regular vulnerability assessments
- Maintain incident prevention protocols
- Implement multi-factor authentication and encryption

Incident Reporting
- Early warning within 24 hours of detection
- Detailed report within 72 hours
- Final comprehensive report within one month

Business Continuity
- Establish business continuity and disaster recovery plans
- Maintain crisis management procedures
- Ensure system recovery readiness

Corporate Governance
- Senior management accountability for cybersecurity
- Mandatory staff training programs
- Leadership oversight of compliance strategies

Who Must Comply

NIS2 categorizes organizations into essential and important entities. The affected sectors are grouped as follows:

NIS2's Classification of Affected Sectors

Essential Entities
- Energy; electricity, district heating and cooling; oil; gas
- Transport: air, rail, water, road
- Banking and financial market infrastructures, credit institutions
- Healthcare: hospitals, private clinics, other healthcare providers, and biotechnologies
- Drinking water supply and distribution
- Digital infrastructure: internet exchange points, domain name system (DNS) services
- Public electronic communications services
- Public administration at the central and regional levels

Important Entities
- Waste and wastewater management
- Manufacturing of critical products: chemicals, pharmaceuticals, medical devices, electronics, machinery
- Postal and courier services
- Space infrastructure and services
- Digital services: online marketplaces, online search engines, social networking services

Note that supply chain partners must align cybersecurity measures with NIS2 requirements.

How NIS2 Aligns with Other Frameworks

Understanding how NIS2 integrates with existing cybersecurity and data protection frameworks helps organizations streamline compliance efforts and avoid duplication.

How NIS2 Compares with GDPR

NIS2 Features	Alignment with GDPR	Differences from GDPR
Targets network and information system security	Both require incident reporting but on different types of incidents; NIS2 covers cybersecurity incidents affecting essential services, GDPR covers personal data breaches	NIS2 targets essential sectors; GDPR applies to any entity processing personal data
Mandates security measures and risk management	Both enforce third-party risk management practices	GDPR mandates explicit user consent for data processing; NIS2 mandates cybersecurity measures and risk reporting
Requires incident notification within 24 hours	GDPR requires data breach notification within 72 hours	Reporting criteria and incident types differ
Imposes fines up to €10 million or 2% global turnover	GDPR fines can reach €20 million or 4% of global turnover	GDPR fines are generally higher due to the data privacy focus

Key Takeaway: NIS2 focuses on network security across critical sectors, while GDPR centers on personal data protection. Both require incident reporting but with different timelines and scope. Coordinate your compliance efforts to address both frameworks efficiently.

How NIS2 Compares with DORA

NIS2 Features	Alignment with DORA	Differences from DORA
Directive requiring transposition into national law	Both aim to boost cybersecurity and operational resilience	NIS2 is a directive, requiring national implementation; DORA is an EU regulation, directly applicable, does not need transposition into national law
Focuses on enhancing cybersecurity across 18 critical sectors	Both require incident reporting, risk management, and governance	DORA uniquely emphasizes ICT risk management, security of third-party ICT providers, and resilience testing for entities in the financial sector.
Implementation deadline of October 2024	Implementation deadline of January 2025	Different timelines and legal effects across member states
Mandates cooperation between Member States' authorities	Both foster cross-border cooperation	Sectoral scope differs: NIS2 is broad; DORA is limited to finance and financial services

Key Takeaway: DORA targets financial sector ICT resilience with stricter testing requirements, while NIS2 provides broader cross-sector cybersecurity standards. Financial entities must comply with both, but NIS2's directive structure allows for national implementation flexibility.

How NIS2 Compares with the CRA

NIS2 Features	Alignment with CRA	Differences from CRA
Focuses on network and information system security for essential and important service providers	Both promote higher cybersecurity standards and risk management across the EU	CRA targets manufacturers and products with digital elements; NIS2 focuses on service providers and operators of essential services
Requires organizations to implement risk management, incident reporting, and resilience measures	Both require timely vulnerability reporting and continuous security updates	CRA regulates product design, production, and market distribution; NIS2 mandates organizational cybersecurity practices
Enforcement through Member State legislation transposing the directive	Both frameworks foster harmonized EU-wide cybersecurity practices and cooperation	NIS2 needs national transposition; CRA is a directly applicable EU regulation
Applies to sectors like energy, healthcare, transport, digital infrastructure	Both address security obligations impacting EU digital ecosystem trust	CRA enforces security-by-design and CE marking for products; NIS2 enforces operational cybersecurity controls

Key Takeaway: CRA regulates product security from manufacturers, while NIS2 governs operational cybersecurity for service providers. Together, they create comprehensive protection across the EU digital ecosystem—from products to services.

How NIS2 Compares with ISO 27001

NIS2 Features	Alignment with ISO 27001	Differences from ISO 27001
Mandatory directive with legal enforcement	Both emphasize risk management and security controls	ISO 27001 is voluntary, NIS2 is legally binding for specific sectors
Requires top management involvement and accountability	Both require involvement from top management	NIS2 enforces stricter C-level accountability, including penalties and management removal for non-compliance
Specifies incident notification and cooperation across member states	ISO 27001 includes incident management as part of ISMS	NIS2 has explicit cyber incident notification requirements, coordinated nationally and EU-wide
Sanctions include fines and enforcement powers	ISO 27001 penalties relate to loss of certification	NIS2 fines can reach €10 million or 2% global turnover

Key Takeaway: ISO 27001 certification provides a strong foundation for NIS2 compliance. Organizations with ISO 27001 can leverage existing controls while adding NIS2's mandatory incident reporting and EU-specific governance requirements.

How NIS2 Compares with SOC 2

NIS2 Features	Alignment with SOC 2	Differences from SOC 2
Mandatory directive with legal enforcement	Both frameworks focus on risk management and controls over security and availability	NIS2 is legally binding for specific sectors; SOC 2 is voluntary but commercially important
Applies to essential and important entities in EU sectors	Both require regular audits and assessments to verify controls	NIS2 includes specific incident reporting to national CSIRTs and EU cooperation; SOC 2 focuses on audit reports for clients
Mandates incident notification within 24 hours	Both emphasize timely detection and response to security events	SOC 2 does not mandate regulatory breach notifications or penalties
Enforces accountability at organizational leadership levels	Both frameworks require management oversight and responsibility	NIS2 includes penalties such as fines and potential removal of executives; SOC 2 penalties are market-driven and reputational
Requires comprehensive cybersecurity risk management programs	Both promote continuous monitoring, risk assessment, and improvement	SOC 2 aligns with Trust Services Criteria; NIS2 details EU-specific technical and organizational cybersecurity measures

Key Takeaway: SOC 2 builds market trust through voluntary audits, while NIS2 enforces legal cybersecurity obligations. EU organizations can pursue both — SOC 2 for customer assurance and NIS2 for regulatory compliance.

Implementation Success Tips

- **Assess Your Scope** — Determine if your organization qualifies as essential or important entity to align compliance efforts with regulatory requirements
- **Conduct Risk Assessments** — Evaluate vulnerabilities across networks, systems, and supply chains to prioritize mitigation efforts
- **Establish Clear Policies** — Develop comprehensive cybersecurity policies covering risk management, incident reporting, and business continuity
- **Assign Leadership Accountability** — Ensure senior management actively oversees cybersecurity strategy and mandatory training programs
- **Deploy Technical Controls** — Implement MFA, encryption, network monitoring, and vulnerability management tools to protect critical assets
- **Create Reporting Procedures** — Establish streamlined processes to report incidents within NIS2's strict deadlines
- **Plan for Continuity** — Prepare crisis management and disaster recovery plans to maintain essential functions during cyber incidents
- **Secure Your Supply Chain** — Make cybersecurity compliance mandatory for all vendors and partners
- **Train Continuously** — Provide regular, role-specific cybersecurity training aligned with NIS2 requirements
- **Audit Regularly** — Conduct frequent internal assessments to identify gaps and prepare for supervisory inspections

Ready to enhance your NIS2 compliance?

Download our comprehensive NIS2 Checklist to guide your organization through implementation systematically and strengthen your cybersecurity resilience.

DOWNLOAD NIS2 CHECKLIST