Network Information Systems 2 (NIS2)

Dr Diarmuid Ó Briain

19 June 2025

EU and Cybersecurity

- Common market, different OT Cybersecurity approaches.
- CNI risks, an incident in one state may impact in another.
- Network Information Security (NIS) Directive 2016/1148
  - Common level of security for all member states.
- NIS 2 Directive 2022/2555
  - Broadened the scope of the original directive.
  - Identifies 10 sectors of high criticality and 7 other critical services.

engineering the south east

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

NIS2 Directive (EU 2022/2555) seeks to further enhance the work started in the NIS Directive (EU 2016/1148) to build a high common level of cybersecurity across the EU.

Three main pillars of NIS2

Member State Responsibilities

- SPOC / NCA
- National Strategies
- CVD Frameworks
- Crisis Management
- Frameworks

Company Responsibilities

Risk Management

- Accountability for top management for non-compliance
- Essential and important companies are required to take security measures
- Companies are required to notify incidents within a given time frame

Co-operation and Information Exchange

- Cooperation Group
- CSIRTs Network
- CyCLONe
- CVD and European Vulnerability registry
- Peer-reviews
- Biennial ENISA cybersecurity report

Irish Competent Authorities

NCAs

CRU

IAA

CRR

NTA

HSE | eHealth Ireland

An Roinn Iompair
Department of Transport

SPOC

NCSC

enisa

engineering the south east

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

*Entities may be designated as "**Essential**" or "**Important**" depending on factors such as size, sector and criticality.*

Entities

Large Enterprise

- >= 250 employees, or
- > €50m revenue

Medium Enterprise

- 50-249 employees, or
- > €10m revenue

Small & Micro Enterprise

- < 50 employees

NIS2 Sectors of high criticality

Energy

Transport

Banking

Financial Markets

Digital Infrastructure

- **IXPs**
- **CSPs**
- **Data Centres**
- **CDNs**

Essential Entities

Important Entities

Drinking Water

Waste Water

Health

Space

NIS2 Sectors of high criticality

Digital Infrastructure

- **Qualified Trust Service Provider**
- **DNS Service Provider**
- **TLD registries**

Essential Entities

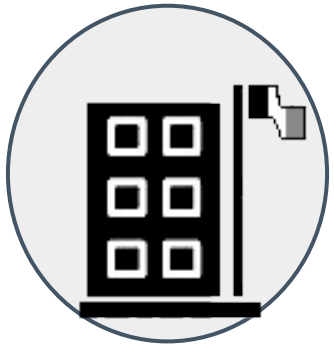
- **Providers of public electronic communications networks**

Essential Entities

Important Entities

- **Central Government**

Essential Entities



Public Administration

- **Regional Government**

Important Entities

NIS2 Other critical sectors

Postal & Courier

Waste Management

Chemicals

Food

Important Entities

Manufacturing

Digital Providers

Research Organisations

Supervision of Entities by NCAs

Essential Entities	Important Entities
Ex Ante & Ex Post	**Ex Post**
On-site inspections and off-site supervision	On-site inspections and off-site, ex post, supervision
Regular & Targeted Security Audits	Targeted Security Security Audits
Security Scans	Security Scans
Information Requests	Information Requests
Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned	Requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned
Ad hoc audits, for example after a significant incident	

engineering the south east

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

NIS2 applies to a wider and deeper pool of entities than covered by the original NIS Directive.

NIS2 Incident Reporting obligations

Time	Incident reporting
Within 24 hours	**Early Warning** should be communicated, as well as some first presumptions regarding the kind of incident
After 72 hours	**Official Incident Notification** A full notification report must be communicated, containing the assessment of the incident, severity and impact and indicators of compromise.
Upon Request	**Intermediate Status Report** At the request of CSIRT or relevant competent authority.
After 1 month	**Final report** must be communicated.
Every 3 months	Member states CSIRT (NCSC) reports incidents to ENISA.
Every 6 months	ENISA reports on all incidents EU wide.

engineering the south east

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Essential and Important Entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems.

Cyber Security Risk Management Measures

1) **Risk Assessment & Security**: Analyse risks and secure information systems.
2) **Incident & Crisis Management**: Handle security incidents and ensure business continuity.
3) **Supply Chain Security**: Secure external vendor relationships.
4) **System Lifecycle Security**: Integrate security into system acquisition, development, & maintenance.
5) **Policy & Compliance**: Implement policies to assess and improve cybersecurity.
6) **Basic Cyber Hygiene & Training**: Educate users on fundamental security practices.
7) **Cryptography & Encryption**: Use secure cryptographic methods.
8) **Access Control & Asset Management**: Secure human resources and manage access to assets.
9) **Secure Communications**: Utilise multi-factor authentication and secure communication channels.

Cyber Security Risk Management Measures

All measures must be:

- **Proportionate** to risk, size, cost, and impact & severity of incidents
- Take into account the **state-of-the-art**, and relevant **standards**.

To ensure risk management measures are in place the EU can:

- **Carry out risk assessments** of critical ICT services, systems or supply chains
- **Impose certification obligations** (delegated acts)
- **Adopt implementing acts** laying down technical requirements.

engineering the south east

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

*NIS2 provides NCAs with a **minimum** list of enforcement powers for non-compliance.*

NIS2 Penalties

- Strict penalties for non-compliance by entities.
- There are particularly high penalties for infringements of:
  - **Article 21 Cybersecurity risk-management measures**
  - **Article 23 Reporting obligations**
- Essential entities can be fined up to **€10,000,000** or at least **2%** of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.
- Important entities can be penalised by fines of up to **€7,000,000** or at least **1.4%** of the total annual worldwide turnover, whichever amount is higher.

engineering the south east

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Senior management have ultimate responsibility for cybersecurity risk management in Essential and Important Entities.

NIS2 Penalties

Management bodies of Essential and Important entities must:

- **Approve** cybersecurity risk management measures.
- **Oversee** implementation of these measures.
- **Undergo** cybersecurity training to assess risks and their impact.
- **Provide** regular cybersecurity training for employees.
- **Be accountable** for non-compliance.

engineering the south east

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

How does my company or organisation ensure compliance?

MITRE ATT&CK for ICS

- **Threat-informed framework** for manufacturing and CNI organisations.
- Helps meet NIS2 obligations by detailing OT/ICS adversary tactics and techniques.
- Enables precise risk analysis, threat modelling, and tailored security controls.
- Crucial for incident handling: improves detection, analysis, and response.
- Validates and refines cybersecurity measures for NIS2 compliance and effective protection.

https://attack.mitre.org/matrices/ics/

NIST SP 800-82 Guide to OT Security

- A key resource for securing ACS and OT environments.
- Aids in meeting NIS2 mandates for risk management, incident handling, business continuity, and supply chain security.
- Recommendations help organisations systematically identify, assess, and mitigate risks specific to OT systems.
- Implementation addresses NIS2 requirements for risk analysis, security policies, incident handling, and business continuity, building a strong cybersecurity posture for essential services.

https://csrc.nist.gov/pubs/sp/800/82/r3/final

ISA 62443 Security for IACS

- A comprehensive cybersecurity framework for IACS/OT.
- Addresses unique characteristics of OT such as real-time performance, safety, and legacy systems.
- Enables organisations to systematically manage cybersecurity risks and build robust security programmes.
- Directly aligns with NIS2 mandates for risk analysis, security policies, incident handling, and supply chain security.
- Ensures NIS2 compliance and significantly enhances operational resilience against cyber threats.

https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Framework Alignment with NIS2 Requirements

NIS2 Requirement Category	MITRE ATT&CK for ICS	NIST SP 800-82r3	ISA/IEC 62443 Series
Risk Management	Indirect/Reactive	Direct	Direct & Comprehensive
Incident Handling	Direct & Operational	Direct	Direct & Foundational
Business Continuity & Crisis Management	Indirect	Direct	Direct & Integrated
Supply Chain Security	Indirect	Indirect/Focus on Components	Direct & Comprehensive
Security in System Acquisition, Development, & Maintenance	Indirect	Direct	Direct & Strong
Awareness Training & Hygiene	Indirect	Direct	Direct
Access Control	Indirect/Informative	Direct	Direct & Detailed
MFA & Encryption	Indirect	Direct	Direct
Assessment of Effectiveness	Direct & Tool	Direct	Direct

Comparison between NIST SP 800-82 & ISA/IEC 62443

- **NIST SP 800-82r3**: Flexible, adaptable, potentially lower initial cost. Implementation cost varies with internal expertise.
- **ISA/IEC 62443**: Structured, prescriptive, potentially higher implementation/maintenance costs (certification). Leads to a more robust, auditable OT environment.
- Choosing the right fit depends on:
  - Organisation's security maturity.
  - Regulatory and certification needs.
  - Desired assurance level.
- Many organisations combine by using NIST guidance within a framework aligned with ISA/IEC 62443 principles or the NIST Cybersecurity Framework version 2.0 (CSF2.0).

Integrating Cybersecurity Standards for NIS2

- **ISO/IEC 27001**: High-level, organisation-wide Information Security Management System (ISMS). Ideal for overall cybersecurity governance and risk management, meeting broad NIS2 commitments.
- **NIST SP 800-82r3 & ISA/IEC 62443**: Domain-specific, providing detailed technical/operational guidance for OT/ICS security.
- **Key Difference**: ISO 27001 focuses on what an ISMS achieves, while OT-specific standards detail how to implement security in OT environments.
- **NIS2 Compliance**: Combine ISO 27001 for enterprise governance with NIST SP 800-82r3 or ISA/IEC 62443 for specialised OT security.

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

What's Next

Cyber Resilience Act (CRA)

- The CRA is a baseline cybersecurity standard for digital products sold in the EU, aiming to reduce vulnerabilities and cyber incidents.
- Products are categorised by risk level, dictating their conformity assessment requirements.
  - Entry into force: 10 Dec 2024.
  - Full enforcement: 11 Dec 2027.
  - Reporting obligations: 11 Sept 2026.

Cyber Resilience Act (CRA)

Category	Default "Unclassified"	Important "Class I"	Important "Class II"	Critical Products
Examples	Smart speakers, games, photo editing software, hard drives, mobile and desktops apps and everything else	IAM/PAM, OS, wearables, smart home, password managers, network management systems, microcontrollers, VPN, SIEM, anti-virus	Hypervisors & container runtimes, firewalls, Intrusion Detection / or Prevention, Tamper-resistant microprocessors & microcontrollers	Smart meter gateways smartcards or similar devices, including secure elements Hardware Security Modules
Conformance	**Self Assessment**	**Harmonised Standards**	**Third party assessment**	**EUCC**

Cyber Resilience Act (CRA) penalties

Non-compliance in relation to:

- **product security and vulnerability handling**
  - Up to **€15,000,000 or 2.5%** of the total worldwide annual turnover, whichever is higher
- **documentation or reporting requirements**
  - Up to **€10,000,000 or 2%** of the total worldwide annual turnover, whichever is higher
- provision of **incorrect, incomplete, or misleading information** to notified bodies and surveillance authorities
  - Up to **€5,000,000 or 1%** of the total worldwide annual turnover, whichever is higher

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Operational Technology Cybersecurity

Programmes

Operational Technology Cybersecurity Programmes

Semester	Level 9 Certificate award	Postgraduate Diploma award		Master of Science award		
1	Cybersecurity I	Industrial Control Systems Programming I Industrial Networks I Cybersecurity I	Work-based Project and Professional Development	Industrial Control Systems Programming I Industrial Networks I Cybersecurity I	Work-based Project and Professional Development	Research Methods for Engineering
2	Cybersecurity for Industrial Networks	Advanced Industrial Automation Programming II Industrial Networks II Cybersecurity for Industrial Networks		Advanced Industrial Automation Programming II Industrial Networks II Cybersecurity for Industrial Networks		
3				Dissertation		

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Thank you

engcore
advancing technology