Topic 3

NIS2 and CRA

Dr Diarmuid Ó Briain

28 Jan 2026

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

Version: 3.0.0

Licence

Learning objectives

- By the end of this topic you will:
  - Understand the key objectives of the NIS2 directive
  - Identify the key pillars of the NIS2 directive
  - Understand the categorisation of essential and important entities under the NIS2 directive
  - Recognise the incident notification obligations under the NIS2 directive
  - Evaluate the requirements of organisation to comply with the NIS2 directive
  - Understand the CRA's objectives, product categories, compliance, and penalties.

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

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

NIS2 seeks to further enhance the work started in the NIS Directive 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

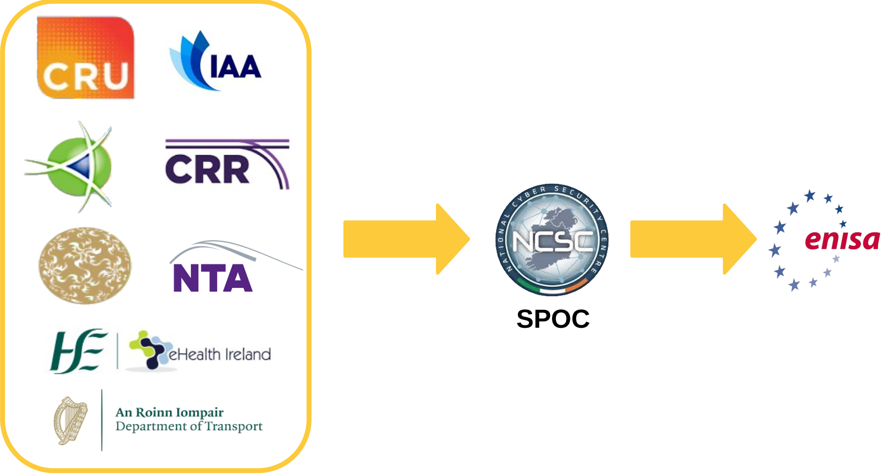
- Accountability for top management for non-compliance
- Essential and important companies are required to take security measures
- Companies are required to notify incidents within a given time frame

Co-operation and Information Exchange

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

Coordinated Vulnerability Disclosure (CVD)
European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)
European Network Information Security Agency (ENISA)

Irish Competent Authorities



SPOC

engineering the south east

SETU 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.*

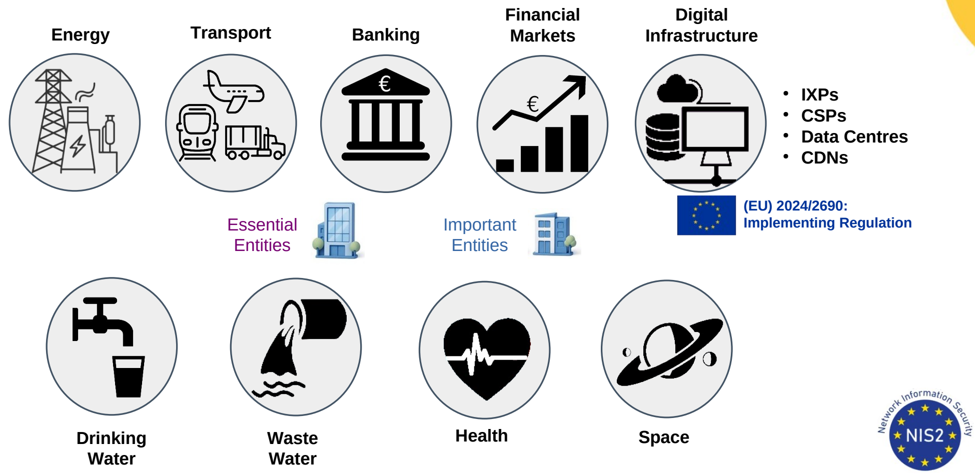
Entities

Large Enterprise	- ≥ 250 employees, or - > €50m revenue
Medium Enterprise	- 50-249 employees, or - €10-50m revenue
Small & Micro Enterprise	- < 50 employees, or - ≤ €10m revenue

Entities (Proposed changes 2026)

Large Enterprise	- ≥ 750 employees, or - > €150m revenue
Small Mid-Cap	- 250-749 employees, or - €50-150m revenue
Medium Enterprise	- 50-249 employees, or - €10-50m revenue
Small & Micro Enterprise	- < 50 employees, or - ≤ €10m revenue

NIS2 Sectors of high criticality



- IXPs
- CSPs
- Data Centres
- CDNs

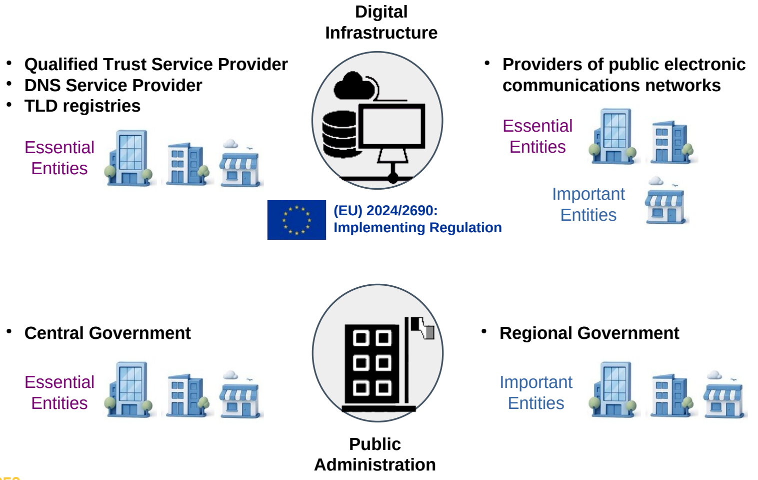
(EU) 2024/2690: Implementing Regulation

Essential Entities

Important Entities

https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

NIS2 Sectors of high criticality



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

Essential Entities

- Providers of public electronic communications networks

Essential Entities

Important Entities

(EU) 2024/2690: Implementing Regulation

- Central Government

Essential Entities

- Regional Government

Important Entities

NIS2 Other critical sectors

Postal & Courier

Waste Management

Chemicals

Food

Important Entities

Manufacturing

Digital Providers

Research Organisations

Network Information Security NIS2

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 Audits
Security Scans	Security Scans
Information Requests	Information Requests
Requests for information necessary to assess the cybersecurity Risk-Management Measures (RMM) adopted by the entity concerned	Requests for information necessary to assess, ex post, the cybersecurity RMMs adopted by the entity concerned
Ad hoc audits, for example after a significant incident	

engineering the south east

SETU 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 reports incidents to ENISA.
Every 6 months	ENISA reports on all incidents EU wide.

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

Cyber Security RMMs

- Risk Assessment & Security
- Incident & Crisis Management
- Supply Chain Security
- System Lifecycle Security
- Policy & Compliance
- Basic Cyber Hygiene & Training
- Cryptography & Encryption
- Access Control & Asset Management
- Secure Communications

Cyber Security RMMs

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 RMMs 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.

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

NIS2 Penalties that NCAs can impose

- Issue warnings for non-compliance.
- Give binding instructions.
- Order to cease non-compliant conduct.
- Mandate compliance with risk management or reporting.
- Order to inform affected parties of cyber threats.
- Require implementation of audit recommendations.
- Appoint a monitoring officer.
- Order public disclosure of non-compliance.
- Impose administrative fines.
- Suspend essential entity certification/authorisation.
- Temporarily prohibit C-level management from functions.

NIS2 Penalties

- Strict penalties for non-compliance by entities.
- There are particularly high penalties for infringements of:
  - **Article 21 Cybersecurity RMMs**
  - **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

SE TU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

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

NIS2 Penalties

- Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities.
- Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans and administrative fines as provided for in the implementing national legislation.

NIS2 Penalties

Management bodies of Essential and Important entities must:

- **Approve** cybersecurity RMMs.
- **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

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

How does my company 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.

MITRE ATT&CK™

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

Framework Alignment with NIS2 Requirements

NIS2 Requirement	MITRE ATT&CK	MITRE D3FEND
Risk Management	🟨 Indirect/Reactive	🟨 Strategic
Incident Handling	🟩 Direct & Operational	🟩 Direct & Operational
Business Continuity	🟥 Indirect	🟥 Functional
Supply Chain Security	🟨 Indirect	🟨 Structural
System Acquisition/ Main.	🟨 Indirect	🟨 Architectural
Awareness & Hygiene	🟥 Contextual	🟥 Operational
Access Control	🟩 Informative	🟩 Technical Control
MFA & Encryption	🟩 Tactical	🟩 Prescriptive
Effectiveness Assessment	🟩 Direct / Red Teaming	🟩 Direct / Purple Teaming

🟩 **Green**: Direct & Operational Strengths

🟨 **Amber**: Indirect Technical Support

🟥 **Red**: Significant Capability Gaps

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

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.

Introduction

- **NIS2 Directive Transposition**: Ireland National Cybersecurity Bill.
- Risk Management Measures (RMM), mandatory minimum baseline requirements for **ESSENTIAL** and **IMPORTANT** entities.
- **Recommended Compliance Tool**: Cyber Fundamentals 2025 (CyFun) Framework.
- The NCSC promotes both RMMs (the "***what you must do***") and CyFun (the "***how to do it and prove it***") to simplify compliance for organisations.

Risk Management Measures

CyFun® 2025

NIS2 Compliance Heatmap

NIS2 Requirement	NIST CSF 2.0	ISO 27001	ISA/IEC 62443	CyFun 2025
Risk Management	🟧 Strategic	🟩 Management	🟩 OT-Specific	🟩 RMM Match
Incident Handling	🟧 No Timelines	🟧 No Timelines	🟩 OT Recovery	🟩 24h/72h Focus
Business Continuity	🟧 Outcomes	🟩 ICT Focus	🟩 Safety Focus	🟩 All-Hazards
Supply Chain Security	🟩 New GV.SC	🟩 Annex A 5.19	🟩 Part 2-4	🟩 Contractual
System Acq/Maint.	🟧 High-level	🟩 SDLC Focus	🟩 Hardening	🟩 Patch Mandates
Awareness & Hygiene	🟩 Strong PR.AT	🟩 Annex A 6.3	🟧 Only OT	🟩 Hygiene Focus
Access Control	🟩 Strong PR.AA	🟩 Annex A 5.15	🟩 OT Physical	🟩 Least Privilege
MFA & Encryption	🟧 Goal-based	🟩 Annex A 8.24	🟩 Part 3-3	🟩 MFA Mandate
Effectiveness Assess.	🟧 No Audit	🟩 Certification	🟩 Maturity SL	🟩 Verification

🟩 **Green**: Direct & Operational Strengths   🟧 **Amber**: Indirect Technical Support   🟥 **Red**: Significant Capability Gaps

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.

Exercise

Exercise: Limerick Cheeses Limited

Exercise Scenario: Limerick Cheeses Limited

- Saint Patrick’s Day **Limerick Cheeses** was hit with a ransomware attack.
- The attack crippled its operations in Patrickswell.
- On the 1 April **Limerick Cheeses** was contacted by an officer of the NCSC who stated that **Amhain Transport** reported that they had suffered an attack and reported it on the 18 March.
- In the report the CTO of **Amhain Transport** stated that they believe the attack came through a VPN they had with **Limerick Cheeses** logistics system for processing movement orders.

Exercise Scenario: Limerick Cheeses Limited

- Additionally on the 19 March **Amhain Transport** reported that they had to rebuild each computer on their network and restore data to their business management system from backups.
- **Limerick Cheeses** responded by stating that they did have a minor issue and that they restored their systems after working to get the systems back up as quickly as possible as the attack was disrupting their production and shipping.
- Further questioning of the IT manager at **Limerick Cheeses** revealed that they had employed the services of **Echo Cyber**, a cybersecurity firm and the incident cost them €25,000 to get everything restored to pre-incident state.

NIS2

What jurisdiction did the NCSC have to contact Limerick Cheeses about their incident?

2

NIS2

What jurisdiction did the NCSC have to contact Limerick Cheeses about their incident?

- As a food producer ***Limerick Cheeses*** is part of a ***other critical sectors*** and they are therefore an ***important entity***.
- They are subject to ex-post supervision, meaning that as the CSIRT-IE receives evidence of non-compliance they had the right to take action.

NIS2

Were Limerick Cheeses and Amhain Transport in compliance with the NIS2?

⌛ 2

NIS2

Were Limerick Cheeses and Amhain Transport in compliance with the NIS2?

- ***Amhain Transport***, from a high criticality sector, is an essential entity, they reported the incident within 24 hours and followed up within 72 hours so they were in compliance.
- ***Limerick Cheeses*** did not report the incident, they were solicited by the NCSC because of information received from ***Amhain***, so they were not in compliance.

NIS2

Is there a case to answer by either Limerick Cheeses or Amhain Transport in case of either Article 21 or Article 23 of the NIS2?

⌛ 2

NIS2

Is there a case to answer by either Limerick Cheeses or Amhain Transport in case of either Article 21 or Article 23 of the NIS2?

- ***Amhain Transport***, In terms of Article 23, reporting obligations they have no case to answer; however, in the case of Article 21, Cybersecurity RMMs they may have.
- ***Limerick Cheeses*** infringed both Article 21 and Article 23, so they certainly have a case to answer.

Question 1

- **The NIS2 Directive focuses on:** (Select all that apply)

□ Protecting critical infrastructure and safeguarding the digital economy

□ Standardising data privacy regulations across the EU

□ Enhancing cybercrime investigation capabilities

□ Facilitating cross-border e-commerce

1

Question 1

- **The NIS2 Directive focuses on:** (Select all that apply)

☑ Protecting critical infrastructure and safeguarding the digital economy

☒ Standardising data privacy regulations across the EU

☒ Enhancing cybercrime investigation capabilities

☒ Facilitating cross-border e-commerce

Question 2

- **Which of the following sectors are NOT considered high criticality under NIS2?** (Select all that apply)

□ Healthcare

□ Transportation

□ Public administration

□ Manufacturing

1

Question 2

- **Which of the following sectors are NOT considered high criticality under NIS2?** (Select all that apply)

☒ Healthcare

☒ Transportation

☒ Public administration

☑ Manufacturing

Question 3

- **What is the minimum timeframe for essential entities to notify authorities of a significant cyber incident?** (Select all that apply)

□ Immediately

□ Within 24 hours

□ As soon as reasonably practicable

□ Within 72 hours

1

Question 3

- **What is the minimum timeframe for essential entities to notify authorities of a significant cyber incident?** (Select all that apply)

☒ Immediately

☒ Within 24 hours

☑ As soon as reasonably practicable

☒ Within 72 hours

Question 4

- **Which of the following is NOT included in the required RMMs for essential and important entities?** (Select all that apply)

□ Business continuity planning

□ Multi-factor authentication for all users

□ Patch management and vulnerability disclosure

□ Employee training and awareness programmes

1

Question 4

- **Which of the following is NOT included in the required RMMs for essential and important entities?** (Select all that apply)

☒ Business continuity planning

☑ Multi-factor authentication for all users

☒ Patch management and vulnerability disclosure

☒ Employee training and awareness programmes

Question 5

- **What is the minimum administrative fine for an essential entity that violates reporting obligations under NIS2?** (Select all that apply)

□ €500,000

□ €2,000,000

□ Up to the cost of the incident response

□ €10,000,000 or 2% of annual turnover (whichever is higher)

1

Question 5

- **What is the minimum administrative fine for an essential entity that violates reporting obligations under NIS2?** (Select all that apply)

☒ €500,000

☒ €2,000,000

☒ Up to the cost of the incident response

☑ €10,000,000 or 2% of annual turnover (whichever is higher)

Question 6

- **Who ultimately holds responsibility for cybersecurity risk management in essential and important entities?**
  (Select all that apply)

□ The CEO or legal representative

□ The IT security team

□ The data protection officer

□ The national cybersecurity authority

1

Question 6

- **Who ultimately holds responsibility for cybersecurity risk management in essential and important entities?**
  (Select all that apply)

☑ The CEO or legal representative

☒ The IT security team

☒ The data protection officer

☒ The national cybersecurity authority

Learning outcomes

- Understand the key objectives of the NIS2 directive ✓
- Identify the key pillars of the NIS2 directive ✓
- Understand the categorisation of essential and important entities under the NIS2 directive ✓
- Recognise the incident notification obligations under the NIS2 directive ✓
- Evaluate the requirements of organisation to comply with the NIS2 directive ✓

SE TU 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

SE TU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Thank you

engcore
advancing technology