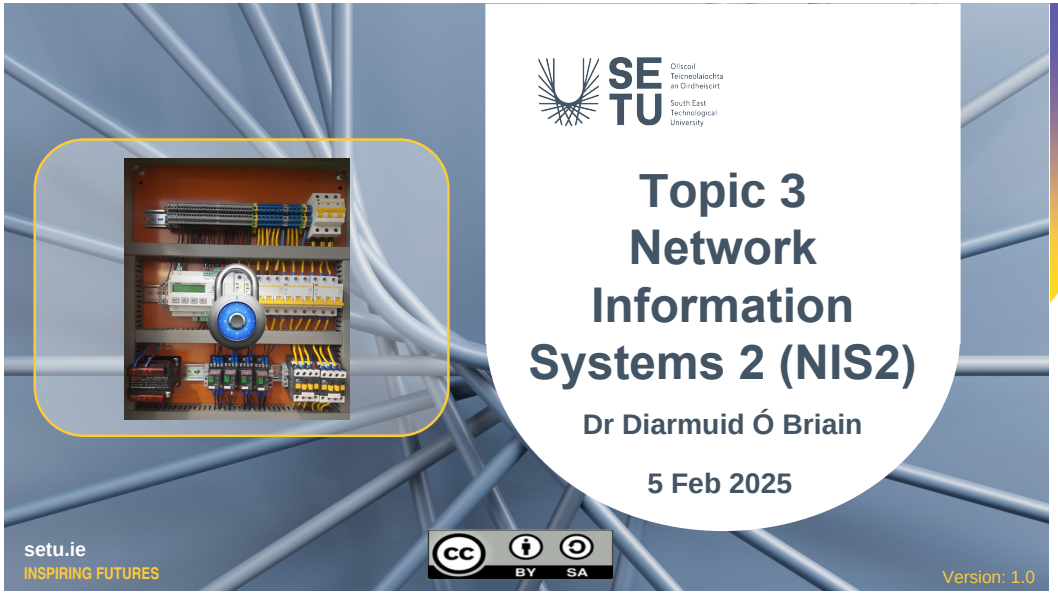


Topic 3 Network Information Systems 2 (NIS2)

Dr Diarmuid Ó Briain

5 Feb 2025

setu.ie
INSPIRING FUTURES

Version: 1.0

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.

EU and Cybersecurity

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

- National Authorities (NAI)
- National Strategies
- Cordinated Vulnerability Disclosure (CVD) Frameworks
- Crisis Management
- Frameworks

NIS2 seeks to further enhance the work started in the NIS Directive to build a high common level of cybersecurity across the European Union.

Three main pillars of NIS2

Member State Responsibilities

- National Authorities
- 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

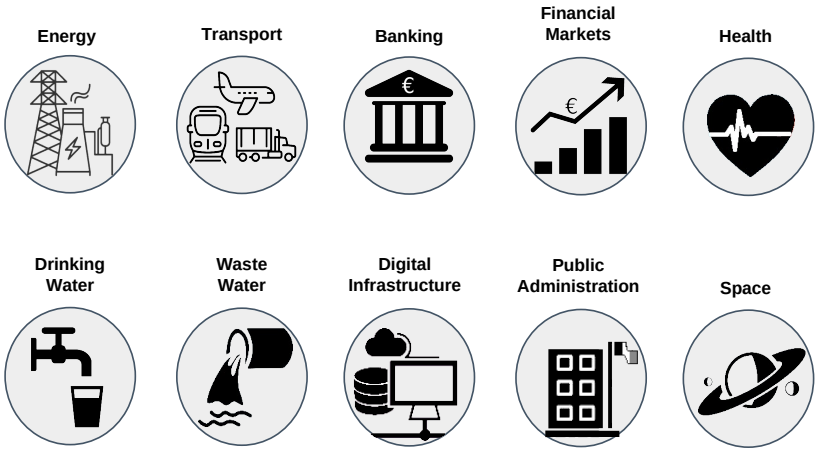
- Cooperation Group
- CSIRTs Network
- CyCLONe
- CVD and European Vulnerability registry
- Peer-reviews
- Biennial ENISA cybersecurity report

Coordinated Vulnerability Disclosure (CVD)
European Cyber Crises Liaison Organisation Network (EU-CyCLONe)
European Union Agency for Cybersecurity (ENISA)

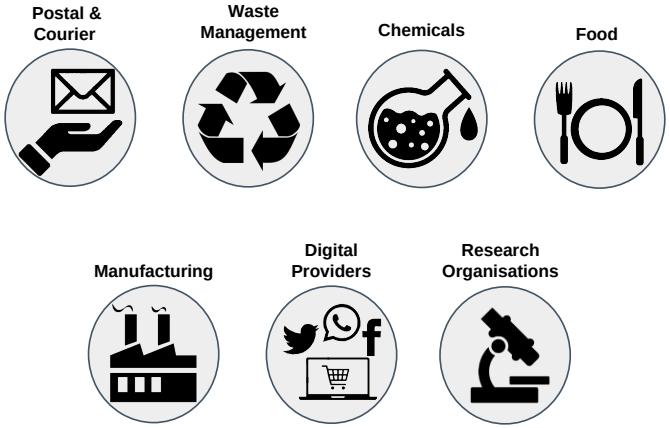
Entities may be designated as "Essential" or 'Important" depending on factors such as size, sector and criticality.

setu.ie
INSPIRING FUTURES

NIS2 Sectors of high criticality



NIS2 Other critical sectors



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

setu.ie
INSPIRING FUTURES

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 Risk Management Measures

1) Risk analysis & information system security
2) Incident handling
3) Business continuity measures (back-ups, disaster recovery, crisis management)
4) Supply Chain Security
5) Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6) Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7) Basic computer hygiene and training
8) Policies on appropriate use of cryptography and encryption
9) Human resources security, access control policies and asset management
10) Use of multi-factor, secured voice/video/text comm & secured emergency vulnerability handling and disclosure measures communication.

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 where applicable relevant European and international standards.

To ensure appropriate 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.

NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance.

setu.ie
INSPIRING FUTURES

NIS2 Penalties

NAIs can:

- Issue warnings for non-compliance
- Issue binding instructions
- Order to cease conduct that is non-compliant
- Order to bring risk management measures or reporting obligations in compliance to a specific manner and within a specified period
- Order to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat
- Order to implement the recommendations provided as a result of a security audit within a reasonable deadline
- Designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance
- Order to make public aspects of non-compliance
- Impose administrative fines
- An essential entities certification or authorisation concerning the service can be suspended
- C-level management can be temporarily prohibited from exercising managerial functions

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.

Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities.

setu.ie
INSPIRING FUTURES

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 the adequacy of the cybersecurity risk management measures taken by the entity.
- Supervise the implementation of the risk management measures.
- Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity.
- Offer similar training to their employees on a regular basis.
- Be accountable for the non-compliance.

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Exercise

setu.ie
INSPIRING FUTURES

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 risk-management measures they may have.
- ***Limerick Cheeses*** infringed both Article 21 and Article 23, so they certainly have a case to answer.

Revision

setu.ie
INSPIRING FUTURES

Question 1

- **The NIS2 Directive focuses on:**

☐ 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:**

☑ 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?**

☐ Healthcare

☐ Transportation

☐ Public administration

☐ Manufacturing


1

Question 2

- **Which of the following sectors are NOT considered high criticality under NIS2?**

☒ Healthcare

☒ Transportation

☒ Public administration

☑ Manufacturing

Question 3

- **What is the minimum timeframe for essential entities to notify authorities of a significant cyber incident?**

☐ Immediately

☐ Within 24 hours

☐ As soon as reasonably practicable

☐ Within 72 hours

Question 3

- **What is the minimum timeframe for essential entities to notify authorities of a significant cyber incident?**

☒ Immediately

☒ Within 24 hours

☑ As soon as reasonably practicable

☒ Within 72 hours

Question 4

- **Which of the following is NOT included in the required risk management measures for essential and important entities?**

☐ Business continuity planning

☐ Multi-factor authentication for all users

☐ Patch management and vulnerability disclosure

☐ Employee training and awareness programmes

Question 4

- **Which of the following is NOT included in the required risk management measures for essential and important entities?**

☒ 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?**

☐ €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 5

- **What is the minimum administrative fine for an essential entity that violates reporting obligations under NIS2?**

☒ €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?**

☐ The CEO or legal representative

☐ The IT security team

☐ The data protection officer

☐ The national cybersecurity authority

Question 6

- **Who ultimately holds responsibility for cybersecurity risk management in essential and important entities?**

☑ 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 ✓

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir

D +353 59 917 5426 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Thank you

engcore
advancing technology