engineering the south east

EU Directive 2022/2225
Network Information System v2 (NIS2)

Dr Diarmuid Ó Briain

Version: 1.3

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

1 Introduction

The Network Information Systems 2 (NIS2) Directive [1] seeks to further enhance the work started in the NIS Directive [2] to build a high common level of cybersecurity across the European Union (EU). It places obligations on Member States and individual companies in critical sectors. NIS2 adds more sectors, more entities, New methods of selection and registration, New incident notification deadlines and extra requirements based on the learnings from the implementation of the initial directive.

1.1 Objectives

By the end of this topic, you will be able to:

- 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
- Identify potential solutions for organisations to be compliant.

2 Network Information Security (NIS)

The open market nature of the EU facilitates organisations to operate across EU Member States within a single market. In terms of Cybersecurity organisations operated differing requirements and standards from member state to member state. As the cybersecurity requirement increased and lack of a standard approach by Member States, particularly in the case of Critical National Infrastructure (CNI), the European Union (EU) responded with the Network and Information Systems (NIS) Directive 2016/1148 [2] which was published in the Official Journal of the EU in July 2016. This was transposed into Member States law, in Ireland's case on 18/9/2018 via Statutory Instrument No. 360 of 2018. The directive is a framework that brings all entities to a common level of security no matter which state, or states, within the EU they operate in, therefore protecting CNI, the consumer, companies, states and the market alike. The directive focused on two specific groups; Operators of Essential Services (OES) and Digital Service Providers (DSP). However, this first NIS Directive had certain limitations. The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape. New challenges appeared, which required adapted and innovative responses.

The introduction of the NIS2 2022/2225 [1] directive broadened the scope of the original directive. It identifies 10 sectors of high criticality and 7 other critical services. Entities in both categories must meet the same requirements. However, the distinction is in the supervisory measures and penalties.

3 The three main pillars of NIS2

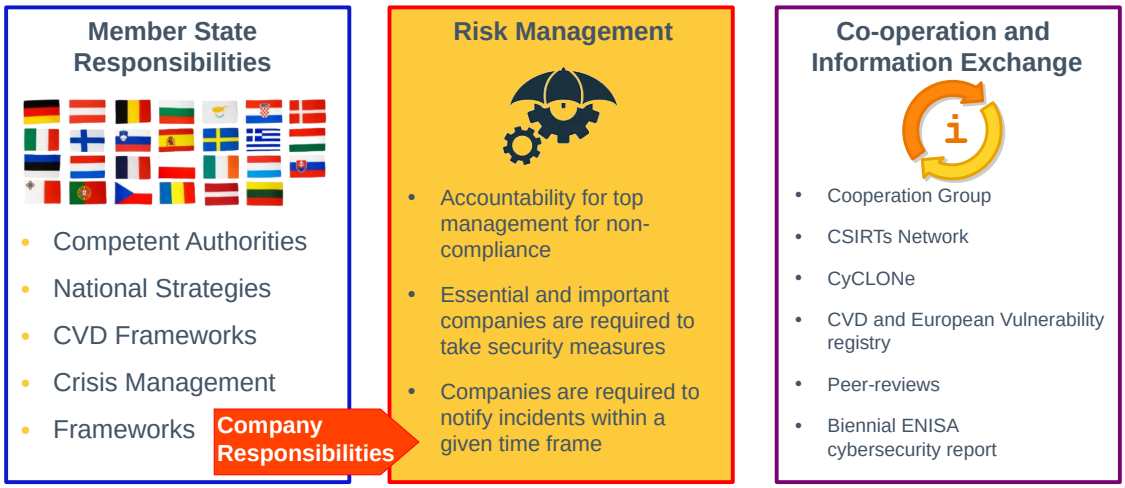

Figure 1: The three main pillars of NIS2

The three pillars of NIS2, as illustrated in Figure 1, support the EU collaborative approach to Cybersecurity. The figure depicts the shared responsibilities of Member States, National Competent Authorities (NCA), Essential Entities and Important Entities. It highlights the collaborative approach that is essential for achieving the directive's goal of enhancing cybersecurity in the EU.

Member States play a crucial role by implementing the NIS2 directive through designating and establishing individual NCA, such as the National Cyber Security Centre (NCSC) in Ireland and identifying and categorising both Essential and Important Digital Service Providers, as well as developing national cybersecurity strategies. They also monitor the cybersecurity performance of Essential and Important Entities and enforce the directive's requirements.

NCAs are the frontline enforcers of the NIS2 directive within their respective jurisdictions. They work closely with Member States to identify and categorise Essential and Important Entities, monitor their cybersecurity practices, and investigate any reported incidents.

Essential and Important Entities are the private sector entities that are subject to the NIS2 directive's requirements. They must conduct cybersecurity risk assessments, implement appropriate security measures, establish incident response plans, and notify NCAs of significant cybersecurity incidents.

The figure also emphasises that effective cybersecurity requires a collective effort from all stakeholders. Member States, NCAs, and Essential and Important Entities must work together to identify, assess, and mitigate cybersecurity risks, and to respond promptly and effectively to any incidents that occur.

By promoting collaboration and accountability in this way the NIS2 Directive aims to create a more resilient cybersecurity landscape that can protect critical infrastructure and safeguard the digital economy.

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

3.1 National Competent Authorities

Every Member State has a central point of contact for compliance with the Directive and a coordinating Computer Security Incident Response Team (CSIRT) for incident reporting. In Ireland, this is the role of the CSIRT Ireland (CSIRT-IE) within the NCSC. As the NCSC is Ireland's Lead NCA for the purpose of NIS2.

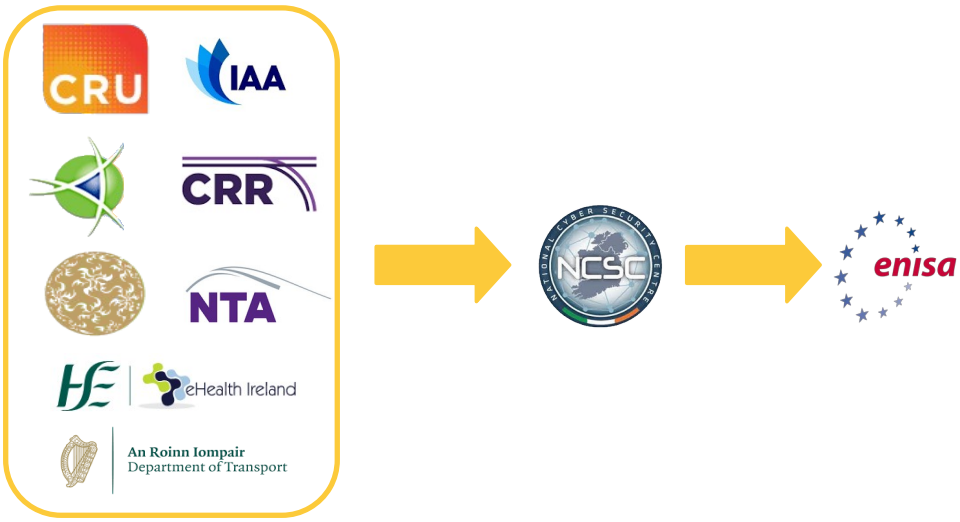

Figure 2: Competent Authorities and Reporting Relationships

As illustrated in Figure 2 a number of specialist NCAs have been appointed to handle specific NIS areas. The NCSC serves as the central pillar of the nation's cybersecurity framework and is the body that reports to ENISA, the EU agency tasked with achieving a high common level of cybersecurity across the Union. While the NCSC is specifically designated as the NCA for *all other sectors* not covered by the sectoral regulators, its overall responsibility extends far beyond this direct oversight. The NCSC is tasked with developing national cybersecurity strategies, providing overarching guidance, and acting as the national CSIRT-IE for incident detection and response. In this pivotal role, the NCSC actively supports the other designated sectoral NCAs (such as the Commission for the Regulation of Utilities (CRU), the Communications Regulator (ComReg), Central Bank of Ireland (CBI), Irish Aviation Authority (IAA), Commission for Railway Regulation (CRR), National Transport Authority (NTA), eHealth Ireland and the Minister for Transport) by sharing threat intelligence, offering operational advice, coordinating responses to significant cyber incidents, and ensuring a consistent national approach to cybersecurity resilience across all critical sectors covered by NIS2. This ensures a cohesive and robust national cybersecurity posture, leveraging the NCSC's expertise to uplift the capabilities of all NCAs and the entities under their supervision.

3.2 Sectoral NCAs

The government have designated specific sectoral regulators to act as NCAs for areas under their remit. For example:

3.2.1 Commission for the Regulation of Utilities (CRU)

The CRU is Ireland's independent energy and water regulator. It is the NCA for entities in the energy and water sectors. They take specific responsibility for:

- Energy (electricity, gas, oil)
- Drinking Water
- Waste Water

3.2.2 Commission for Communications Regulation (ComReg)

ComReg is the regulatory body for the electronic communications and postal sectors in Ireland. They are the NCA for entities within their regulated domains, such as telecommunications providers and Internet Service Providers (ISP). They take specific responsibility for:

- Digital Infrastructure
- ICT Service Management
- Space
- Digital Providers

3.2.3 Central Bank of Ireland (CBI)

The Central Bank is the NCA for the financial services sector, including credit institutions, investment firms, and financial market infrastructures. They oversee NIS2 compliance for:

- Banking
- Financial Market

3.2.4 Irish Aviation Authority (IAA)

The IAA is the statutory body responsible for the safety and economic regulation of the civil aviation industry in Ireland. They are the NCA for entities in the aviation transport sector. They take specific responsibility for:

- Transport - Aviation

3.2.5 Commission for Rail Regulation (CRR)

The CRR is the independent safety authority for railways in Ireland. They are the NCA for entities in the rail transport sector. They take specific responsibility for:

- Transport – Rail

3.2.6 The Department of Transport

The Minister and Department of Transport holds overall responsibility for national transport policy and infrastructure in Ireland. In the context of NIS2, the Minister is the NCA for entities in the maritime transport sector. They take specific responsibility for:

- Transport – Maritime

3.2.7 National Transport Authority (NTA)

The NTA is responsible for the planning and development of public transport and sustainable transport in Ireland. They are the NCA for entities in the road transport sector. They take specific responsibility for:

- Transport – Road

3.2.8 eHealth Ireland

eHealth Ireland, as part of the Health Service Executive (HSE), drives the digital transformation of healthcare services in Ireland. eHealth Ireland perform the NCA functions for the health sector. They take specific responsibility for:

- Health
- Pharmacy

4 Entities

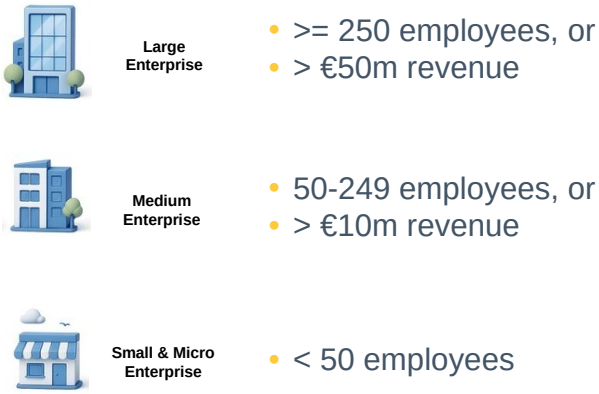

Figure 3: Entities defined in NIS2

Figure 3 illustrates the entities that NIS2 divides organisations. This division is primarily based on their size and this determines the type of supervision each receive, depending on the sector. Large Enterprises (LE) are defined by having 250 or more employees or a revenue exceeding €50 million, while Medium Enterprises (ME) have 50-249 employees or over €10 million in revenue, and Small & Micro Enterprises (SME) have fewer than 50 employees.

5 Essential and important entities

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

For the purpose of compliance with cybersecurity risk-management measures and reporting obligations entities are classified into two categories, essential entities and important entities that reflects the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. Essential Entities will be required to meet supervisory requirements, while important entities will be subject to ex-post supervision, meaning that in case authorities receive evidence of non-compliance, action is taken.

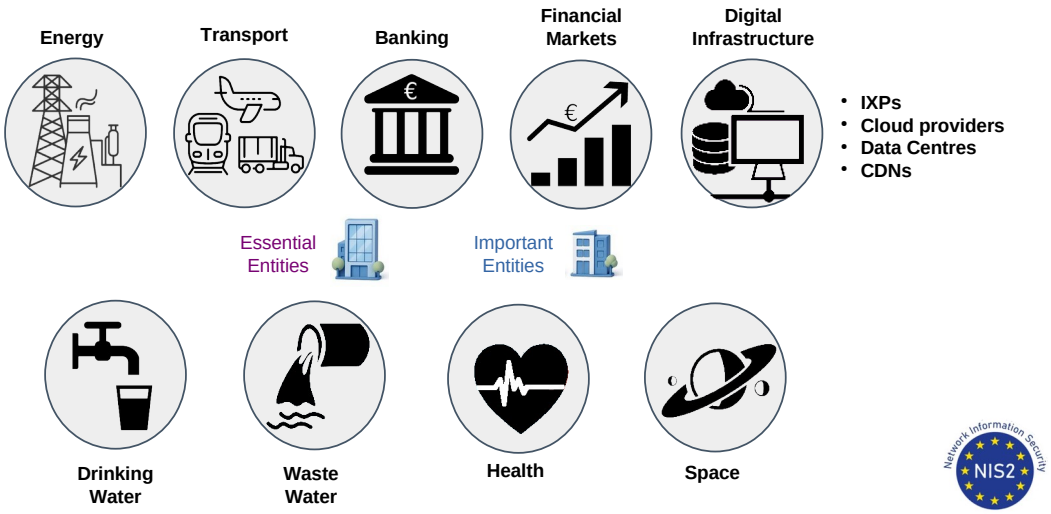

Figure 4: Sectors of High Criticality

5.1 Sectors of high criticality

As illustrated in Figure 4, energy, transportation, banking, and financial market infrastructure are among the sectors of high criticality identified by the NIS2 directive. These sectors are considered essential for the smooth functioning of the EU economy and society, and they are therefore subject to more stringent cybersecurity requirements under the NIS2 directive. These are detailed below:

1. **Energy**: Electricity, District heating and cooling, Oil, Gas and hydrogen
2. **Transport**: Air, Rail, Water, Road
3. **Banking**
4. **Financial market infrastructures**
5. **Health**: Manufacturers of pharmaceutical products including vaccines
6. **Drinking water**
7. **Waste water**
8. **Space**
9. **Digital infrastructure**
    - Internet eXchange Points (IXP)
    - Cloud computing Service Providers (CSP)
    - Data centre service providers
    - Content delivery networks (CDN)

In each of these cases LE are considered Essential Entities while ME are considered Important Entities. SMEs are considered out of scope of NIS2.

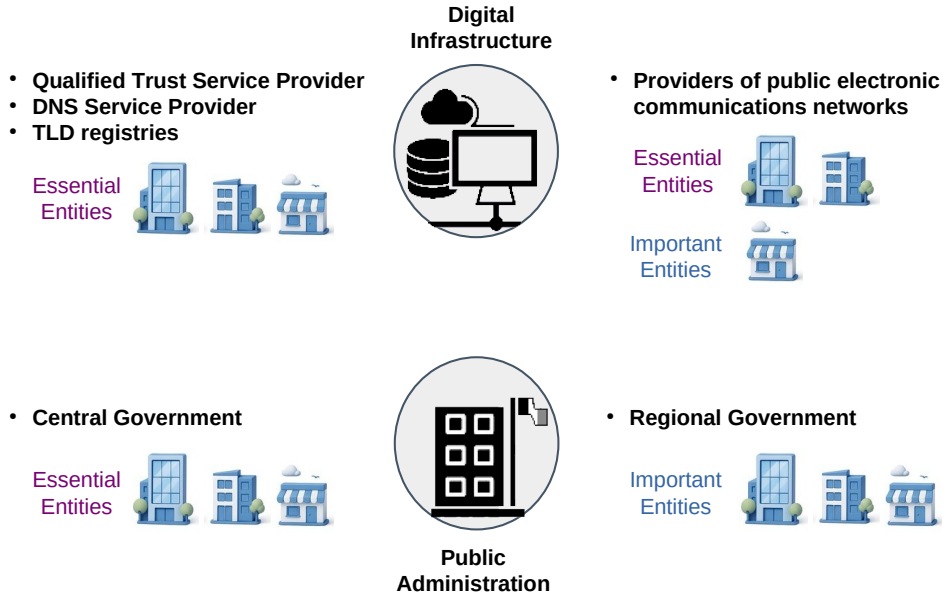

Figure 5: Digital Infrastructure and Public Administration

Some digital infrastructure and public administration are considered differently with NIS2 impacting on SMEs also.

As illustrated in Figure 5, **Digital infrastructure** providers such as Qualified Trust service providers (organisations that provide Electronic Signatures (QES), Electronic Seals (QESeal), Electronic Time Stamps (QTS), Electronic Registered Delivery Services (QERDS), Certificates for Website Authentication (QWAC), Preservation of Electronic Signatures, Seals, or Certificates), Domain Name Systems (DNS) service providers and Top Level Domain (TLD) name registries are considered Essential Entities no matter their size and LE and ME that provide public electronic communications networks and publicly available electronic communications services are consider Essential Entities while SMEs in this category are Important Entities.

Public administration is also different with central government functions considered Essential Entities while regional government are Important Entities.

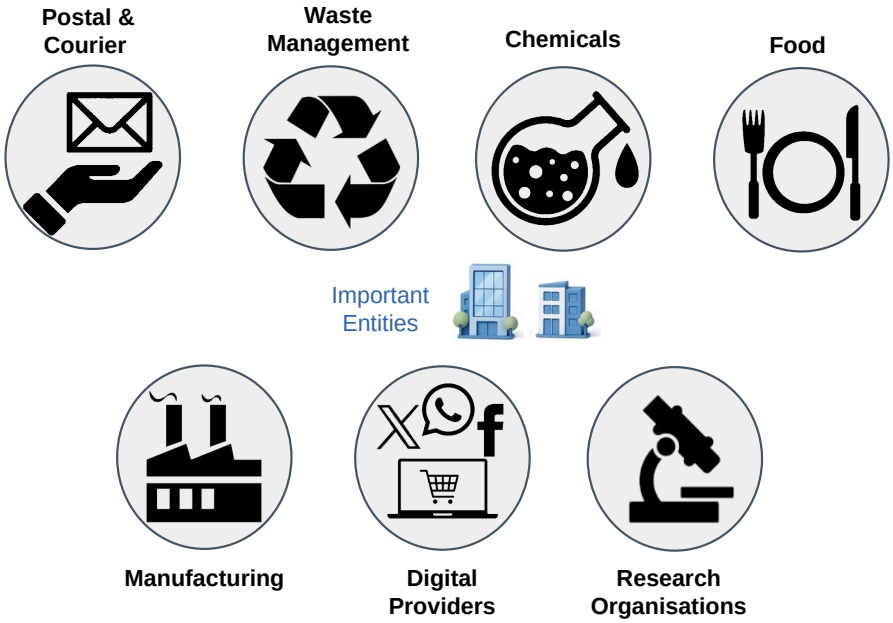

Figure 6: Other critical sectors

5.2 Other critical sectors

As illustrated in Figure 6, postal and courier services, waste management, manufacturing, production, and distribution of chemicals are among the Other critical sectors identified by the NIS2 directive. These sectors are considered to have a significant impact on the EU's security, public health, or economic and social well-being, and they are therefore subject to cybersecurity requirements under the NIS2 directive.

1. **Postal and courier services**
2. **Waste management**
3. **Chemicals**
4. **Food**
5. **Manufacturing**
   - Medical devices
   - Computers and electronics
   - Machinery and equipment
   - Motor vehicles
   - Trailers and semi-trailers
   - Other transport equipment
6. **Digital providers**
   - Online market places
   - Online search engines
   - Social networking service platforms
7. **Research organisations.**

5.3 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

Figure 7: Supervision of Entities by NCAs

The table in Figure 7 outlines two distinct approaches to oversight and risk management by NCAs, categorised by Essential Entities and Important Entities. The key differentiator lies in the timing and scope of their supervision methods. While Essential Entities are subject to a more comprehensive and proactive regime, encompassing both ex ante (before the event) and ex post (after the event) assessments, Important Entities primarily undergo ex post supervision. This distinction impacts aspects such as security audits, information requests, and the overall approach to assessing cybersecurity risk.

6 Incident Notification

NIS2 imposes notification obligations in phases, for incidents which have a ‘significant impact’ on the provision of their services. These notifications must be made to the relevant NCA CSIRT.

6.1 Incident reporting obligations

Every incident with significant impact should be notified by the Essential and Important Entities without undue delay. Organisations report to the appropriate NCA for their sector (such as CRU, ComReg, CBI, IAA, CRR, NTA, eHealth Ireland and the Department for Transport). These NCAs provide summary reports to the NCSC CSIRT-IE as lead NCA.

The NCSC acts as a single entry point for incidents to ENISA. This is to reduce the administrative burden, including for cross-Member State incidents. The NCSC reports to the ENISA on incidents in their jurisdiction every three months, using anonymised information. ENISA will consolidate the information in the form of a report to be published every six months on the EU incidents [3]. This reporting helps organisations and Member States to learn from other incidents and is a crucial change in the new NIS2 Directive.

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.

Figure 8: NIS2 Incident reporting deadlines

7 Cyber Security Risk Management Measures

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

Essential and Important Entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems which underpin their services, and prevent or minimise the impact of incidents on their and other services.

Such measures shall be based on an all-hazards approach that aims to protect the network and information systems and the physical environment of those systems from incidents, and must include at least the following:

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.

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.

8 Infringement Penalties

NIS2 introduces stricter penalties for non-compliance by entities. NCAs are granted a **minimum** list of enforcement powers for non-compliance through the directive, including:

- 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, if deadline for taking action is not met
- Those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily prohibited from exercising managerial functions (applicable to essential entities only, not important entities).

There are particularly high penalties for infringements of:

- Article 21 Cybersecurity risk-management measures
- Article 23 Reporting obligations

In these cases 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 while 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.

9 Management Responsibilities

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

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.

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.

10 Operationalising Compliance: Frameworks for OT Security

The NIS2 Directive mandates that Essential and Important Entities implement appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems. Key areas include:

- **Risk Management:** Policies on risk analysis and information system security.
- **Incident Handling:** Procedures for detection, management, and reporting of security incidents.
- **Business Continuity & Crisis Management:** Measures such as backup management and disaster recovery.
- **Supply Chain Security:** Cybersecurity in the procurement of network and information systems.
- **Security in System Acquisition, Development, and Maintenance:** Policies and procedures for vulnerability handling and disclosure.
- **Awareness Training & Hygiene:** Cybersecurity training and basic cyber hygiene.
- **Access Control:** Policies and procedures regarding access to network and information systems.
- **Multi-Factor Authentication (MFA) & Encryption:** Use of MFA and cryptographic solutions where appropriate.
- **Assessment of Effectiveness:** Policies and procedures for evaluating the effectiveness of cybersecurity risk management measures.

10.1 MITRE ATT&CK for Industrial Control Systems

MITRE ATT&CK for Industrial Control Systems (ICS) offers a threat-informed framework for manufacturing and CNI organisations to meet their NIS2 obligations. By detailing adversary tactics and techniques specific to OT/ICS environments, ATT&CK for ICS enables organisations to move beyond generic security measures, facilitating more precise risk analysis, threat modelling, and the implementation of tailored security controls. This knowledge base is especially crucial for incident handling, providing a common language to enhance detection capabilities, accelerate incident analysis, and streamline response efforts. Ultimately, integrating ATT&CK for ICS allows organisations to validate and refine their cybersecurity measures, ensuring both NIS2 compliance and highly effective protection for their critical operations.

The table in Figure 9 maps the NIS2 requirements with the level that the MITRE ATT&CK framework addresses each of them.

NIS2 Requirement	MITRE ATT&CK for ICS
Risk Management	**Indirect/Reactive**: Primarily focuses on understanding Tactics, Techniques and Procedures (TTP) to inform risk assessments. Helps identify what to defend against based on real-world attacks. Can inform threat modelling.
Incident Handling	**Direct & Operational**: Offers a structured taxonomy for detecting, analysing, and characterising adversary activity. Enables threat-informed incident response, better detection rules, and post-incident analysis by mapping observed events to specific TTPs.
Business Continuity & Crisis Management	**Indirect**: By understanding adversary persistence and impact tactics (e.g., Denial of Control, Impair Process Control), it helps anticipate potential disruptions and prioritise recovery efforts.
Supply Chain Security	**Indirect**: While not directly addressing supply chain management, understanding adversary techniques for initial access (for example, Supply Chain Compromise tactic) helps identify specific risks introduced through vendors and third parties.
Security in System Acquisition, Development, & Maintenance	**Indirect**: Provides insights into how adversaries exploit vulnerabilities (for example, Exploit Public-Facing Application, Software Development Lifecycle Compromise), which can inform secure coding practices and vulnerability management during development and maintenance.
Awareness Training & Hygiene	**Indirect**: By illustrating how adversaries use techniques such as Spearphishing Attachment or Drive-by Compromise, ATT&CK can inform and contextualise security awareness training, making it more impactful for employees.
Access Control	**Indirect/Informative**: Demonstrates how adversaries gain and maintain access (for example, Valid Accounts, Default Credentials, Maintain Persistence). This knowledge helps prioritise and implement robust access control measures.
MFA & Encryption	**Indirect**: While not prescribing specific controls, ATT&CK techniques (for example, Multi-Factor Authentication Bypass) highlight the importance of robust authentication and encryption, prompting organisations to implement these effectively.
Assessment of Effectiveness	**Direct & Tool**: Can be used as a framework for red teaming, purple teaming, and validating defensive capabilities. Organisations can test their security controls against known ATT&CK techniques to measure their effectiveness and identify gaps.

Figure 9: NIS2 Requirement - MITRE ATT&CK for ICS

10.2 NIST Special Publication 800-82

The NIS2 Directive places significant emphasis on enhancing the cybersecurity resilience of critical sectors, including manufacturing and CNI. For such organisations, where Automated Control Systems (ACS) and Operational Technology (OT) play a vital role in their operations, NIST Special Publication (SP) 800-82r3, Guide to OT Security, is a valuable resource [4]. NIS2 mandates comprehensive cybersecurity risk management measures, including those related to incident handling, business continuity, supply chain security, and security in system development and maintenance. NIST SP 800-82 provides specific, detailed guidance on how to secure the unique and often sensitive ACS/OT environments, which typically differ from traditional Information Technology (IT) systems in terms of performance, reliability, and safety requirements. By following the principles and recommendations within SP 800-82, manufacturing and CNI organisations can systematically identify, assess, and mitigate risks inherent to their OT systems, directly contributing to their ability to meet NIS2 obligations.

Implementing the recommendations of NIST SP 800-82 allows manufacturing and CNI organisations to address several key NIS2 requirements. For instance, NIS2 demands robust risk analysis and information system security policies; SP 800-82 provides a framework for conducting risk assessments tailored to ICS/OT environments, identifying specific threats and vulnerabilities, and recommending appropriate security countermeasures. Furthermore, the directive stresses the importance of incident handling and business continuity measures, areas where SP 800-82 offers guidance on developing tailored incident response plans for OT systems, ensuring operational resilience and recovery capabilities. By focusing on network segmentation, secure remote access, robust configuration management, and personnel security within their ICS/OT domains, organisations can demonstrate due diligence and build a strong cybersecurity posture that aligns with the *all-hazards approach* promoted by NIS2, ultimately safeguarding their essential services and minimising potential disruptions.

The table, in Figure 10, illustrates how the NIST SP 800-82r3 Guide to OT Security aligns with each of the NIS2 requirements.

NIS2 Requirement	NIST SP 800-82 r3
Risk Management	**Direct**: Provides comprehensive guidance on conducting risk assessments specifically for ICS/OT environments, identifying vulnerabilities, and recommending countermeasures. Establishes a foundation for a risk management programme.
Incident Handling	**Direct**: Provides detailed guidance on developing and implementing an ICS incident response plan, covering preparation, detection, analysis, containment, eradication, and recovery steps tailored for OT.
Business Continuity & Crisis Management	**Direct**: Addresses the critical importance of maintaining ICS availability and functionality during and after incidents, including considerations for system restoration, backups, and emergency procedures.
Supply Chain Security	**Indirect/Focus on Components**: Emphasises securing the OT supply chain throughout the lifecycle, including considerations for vendor risk management, secure procurement of OT systems and components, and continuous monitoring for supply chain vulnerabilities.
Security in System Acquisition, Development, & Maintenance	**Direct**: Addresses security considerations throughout the ICS lifecycle, from design and acquisition to implementation, operation, and decommissioning. Recommends incorporating security into system engineering processes and managing vulnerabilities.
Awareness Training & Hygiene	**Direct**: Stresses the importance of personnel training, security awareness, and adherence to security policies and procedures within ICS environments.
Access Control	**Direct**: Provides specific recommendations for implementing strong logical and physical access controls for ICS networks and devices, including authentication, authorisation, and least privilege principles.
MFA & Encryption	**Direct**: Recommends the use of secure communication protocols, encryption where feasible and appropriate for OT environments, and strong authentication mechanisms.
Assessment of Effectiveness	**Direct**: Encourages regular security audits, assessments, and continuous monitoring to evaluate the effectiveness of implemented ICS security controls and identify areas for improvement.

Figure 10: NIS2 Requirement - NIST SP 800-82 r3

10.3 ISA/IEC 62443 Series of Standards

The ISA/IEC 62443 series of standards, specifically designed for Industrial ACS (IACS) and OT cybersecurity [5] [6]. They provide a highly relevant and comprehensive framework for such organisations to meet their NIS2 commitments. Unlike general IT security standards, ISA/IEC 62443 addresses the unique characteristics of OT environments, such as real-time performance, safety implications, and the presence of legacy systems. By adopting a structured approach derived from these standards, organisations can systematically manage their cybersecurity risks, establish robust security programmes, and enhance the resilience of their critical industrial operations, which is a core tenet of NIS2.

The multi-part ISA/IEC 62443 series directly aligns with several key areas of NIS2. For instance, NIS2 mandates comprehensive risk analysis and security policies; ISA/IEC 62443-2-1 provides guidance on establishing an IACS security programme that includes tailored risk assessments for OT environments, while ISA/IEC 62443-3-2 details how to define security levels for zones and conduits within the industrial network. Furthermore, NIS2 emphasises incident handling, business continuity, and supply chain security. ISA/IEC 62443-2-1 and 62443-2-4 offer clear guidance on incident response and recovery planning for both asset owners and service providers, respectively, and the series as a whole promotes secure development lifecycles for products and systems (62443-4-1, 62443-4-2), thereby addressing supply chain security. By leveraging the ISA/IEC 62443 standards, manufacturing and CNI organisations can establish a mature, auditable cybersecurity posture that not only ensures compliance with NIS2 but also significantly enhances their overall operational resilience against cyber threats.

The table in Figure 11 compares the coverage of NIS2 requirements by the ISA/IEC 62443 Series of Standards.

NIS2 Requirement	ISA/IEC 62443 Series
Risk Management	**Direct & Comprehensive**: Central to the series, e.g., 62443-2-1 (IACS security programme) and 62443-3-2 (risk assessment for system design) provide detailed methodologies for risk assessment and defining security levels (SL-T).
Incident Handling	**Direct & Foundational**: Covers incident response procedures in 62443-2-1 (IACS security programme) and continuous monitoring (62443-3-3). Helps establish processes for detection, analysis, and recovery, aligning with NIS2's reporting mandates.
Business Continuity & Crisis Management	**Direct & Integrated**: Emphasises resilience and continuity within IACS design and operation (e.g., 62443-3-3 on system requirements). Encourages secure recovery and business continuity planning as part of a holistic security programme (62443-2-1).
Supply Chain Security	**Direct & Comprehensive**: Integral to the series, especially 62443-2-4 (service provider requirements) and 62443-4-1 (secure product development lifecycle) and 62443-4-2 (technical security requirements for components). Provides explicit requirements for securing products and services throughout their lifecycle.
Security in System Acquisition, Development, & Maintenance	**Direct & Strong**: A core strength of the series. 62443-4-1 focuses on secure product development lifecycle requirements for vendors, and 62443-3-3 specifies technical security requirements for the system itself, ensuring security is baked into design and operation.
Awareness Training & Hygiene	**Direct**: 62443-2-1 includes requirements for cybersecurity training and awareness programmes for personnel involved in IACS operations, ensuring a strong security culture.
Access Control	**Direct & Detailed**: 62443-3-3 defines technical requirements for identity and access management, including Role-Based Access Control (RBAC), authentication, and authorisation, ensuring only authorised personnel and systems have appropriate access.
MFA & Encryption	**Direct**: 62443-3-3 includes requirements for data confidentiality (e.g., encryption), communication integrity, and strong authentication to protect IACS communications and data at rest and in transit.
Assessment of Effectiveness	**Direct**: The series emphasises ongoing security assessments, audits, and reviews (e.g., 62443-2-4 provides guidelines for service providers to conduct audits) to ensure the effectiveness and continuous improvement of the IACS security programme.

Figure 11: NIS2 Requirement - ISA/IEC 62443 Series

10.4 Comparison between NIST SP 800-82r3 and ISA/IEC 62443

In general, NIST SP 800-82r3 offers greater flexibility and potentially lower initial barriers to entry, making it suitable for organisations that prefer to adapt guidance to their unique circumstances. Its cost is more influenced by internal expertise and the chosen level of implementation. ISA/IEC 62443, while potentially more expensive to implement and maintain due to its structured and prescriptive nature (especially if certification is sought), often leads to a more robust, auditable, and systematically secure OT environment. The choice often depends on the organisation's existing security maturity, regulatory drivers (for example, is certification required in the future), and the desired level of assurance. Many organisations find value in using NIST SP 800-82r3 as a practical guide for implementation within an overall programme that may be aligned with the principles of ISA/IEC 62443 or a broader framework such as the NIST Cybersecurity Framework (CSF).

10.5 ISO/IEC 27001 and Domain-Specific OT Frameworks

ISO/IEC 27001, provides a high-level, management system approach to information security, establishing requirements for an Information Security Management System (ISMS) across an entire organisation [7]. This makes it ideal for establishing overall cybersecurity governance and risk management to meet broad NIS2 commitments.

In contrast, NIST SP 800-82r3 and the ISA/IEC 62443 series are highly domain-specific frameworks offering detailed technical and operational guidance for securing industrial (OT/ICS) environments. While ISO 27001 focuses on *what* an ISMS should achieve, the OT-specific standards detail *how* to implement robust security within the unique constraints of operational technology. Therefore, for NIS2 compliance, organisations in manufacturing and CNI can effectively layer an ISO 27001-based ISMS for enterprise-wide governance with the specialised, practical security measures from either NIST SP 800-82r3 or ISA/IEC 62443 to protect their critical OT systems.

11 What is Next: Cyber Resilience Act (CRA)

The EU's Cyber Resilience Act (CRA)[8], effective December 2024, establishes 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.

The act came into force on December 10, 2024, and will be fully enforced on December 11, 2027. Manufacturers therefore have a three-year grace period to comply with its requirements. Some obligations, such as mandatory incident reporting, will apply from September 11, 2026.

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

Figure 12: CRA Conformance by Category

11.1 Product Categories and Assessment Requirements

As listed in Figure 12, all products are categorised and each category has particular conformance requirements.

11.1.1 Default “unclassified”

The low risk category handles ~90% of products and delf-assessment is allowed if the product aligns with a Harmonised Standard, Common Specification, or a European Cybersecurity Certification scheme.

11.1.2 Important “Class I” and “Class II”

Important products are those with higher cybersecurity risk compared to default products, encompassing essential digital elements such as operating systems, browsers, and network equipment, and requiring more stringent conformity assessments.

Class I products must meet Harmonised Standards, meaning European technical specifications that, when applied, allow manufacturers to self-assess their product's compliance with the Act's essential cybersecurity requirements, presuming conformity and simplifying the certification process. For this the CRA leverages the existing CE marking system.

Class II are higher risk and require a mandatory third-party conformity assessment, even if harmonised standards or certifications apply. These are carried out by Conformity Assessment Bodies (CAB), which are independent organisations accredited by Member States to assess product compliance with the CRA.

11.1.3 Critical

Critical products represent the highest cybersecurity risk, including highly sensitive hardware and security devices, and always require the most rigorous European Cybersecurity Certification Scheme on Common Criteria (EUCC) by a conformity assessment body.

11.2 Penalties

Like NIS2, the CRA imposes significant penalties for non-compliance, designed to be effective, proportionate, and dissuasive. These administrative fines can be substantial:

- Up to €15,000,000 or 2.5% of the total worldwide annual turnover, whichever is higher, for non-compliance in relation to product security and vulnerability handling.
- Up to €10,000,000 or 2% of the total worldwide annual turnover, whichever is higher, for non-compliance with obligations such as documentation or reporting requirements.
- Up to €5,000,000 or 1% of the total worldwide annual turnover, whichever is higher, for providing incorrect, incomplete, or misleading information to notified bodies and market surveillance authorities.

It's important to note that these fines can be applied in addition to other corrective or restrictive measures, such as market withdrawal or product recalls. Member States are responsible for laying down the specific rules on penalties and ensuring their implementation.

SMEs have largely identical reporting obligations to larger entities, there are some derogations for certain deadlines to ease the administrative burden.

12 OT Cybersecurity Programmes

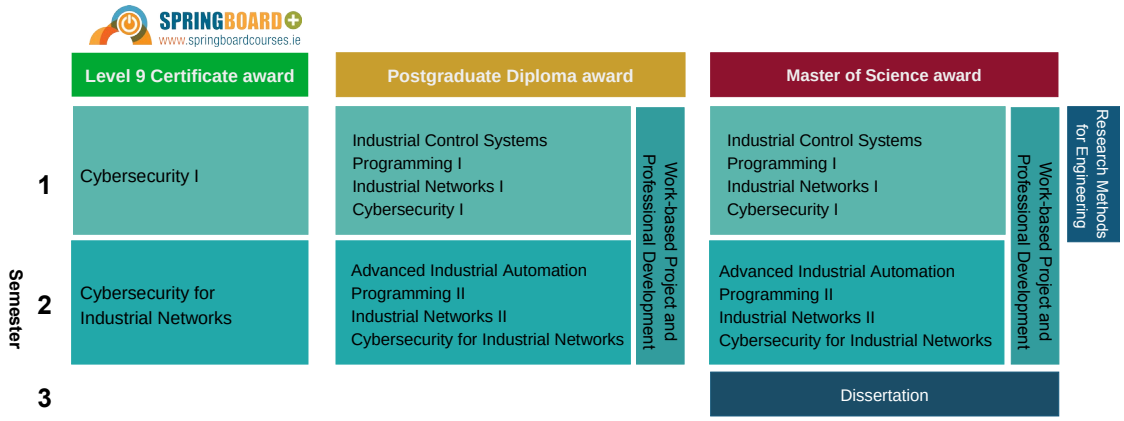

Figure 13: OT Cybersecurity Programmes

Figure 13 illustrates three Level 9 programmes offered by SETU Carlow Campus, progressing from a specialised Certificate to a comprehensive Master of Science, all centered on industrial networks and cybersecurity.

The level 9 **Certificate in Cybersecurity for Indusrial Networks** is a concise, Springboard-funded two-semester blended programme designed to tackle the urgent need for specialised cybersecurity in OT and CNI. With a focus on OT, participants gain the knowledge to distinguish OT from traditional IT security and visualise these systems across sectors such as manufacturing, energy, and transport.

Designed for professionals safeguarding essential infrastructure, this programme empowers engineers to design, build, and manage Cyber Security Management Systems (CSMS) for OT or CNI environments, backed by robust business cases for OT-specific cybersecurity investment.

The **Postgraduate Diploma (PGDip) in Industrial Networks and Cybersecurity** represents a significant expansion on the foundational Certificate. This two-semester award offers a robust curriculum that delves into the core components of industrial operations and their security. Students gain a comprehensive understanding of IACS through the **Industrial Control Systems** and **Advanced Industrial Automation**, modules which are vital for managing critical infrastructure and manufacturing processes. The inclusion of **Programming I & II** ensures that graduates have the necessary coding skills to interact with and secure these complex systems. Furthermore, the programme covers **Industrial Networks I & II**, providing in-depth knowledge of how these specialised networks function and how to protect them. Crucially, it integrates the essential **Cybersecurity I** and **Cybersecurity for Industrial Networks** modules from the Certificate, ensuring a continuous focus on OT-specific cybersecurity challenges. A distinguishing feature of the PGDip is the **group work-based project**, which provides practical, real-world experience in applying theoretical knowledge to solve industry-relevant problems, fostering collaboration and professional development. This diploma is designed to equip professionals with a strong, skills-based knowledge of industrial networking and

cybersecurity, enabling them to design, build, and troubleshoot industrial networks while identifying and mitigating unique security challenges.

The **Master of Science (MSc) in Industrial Networks and Cybersecurity** builds directly upon the PGDip, extending the programme to three semesters to offer the highest level of specialisation and research capability. It incorporates all the content of the PGDip, providing a comprehensive grounding in IACS, programming, industrial networks, and cybersecurity. The added value of the MSc lies in its emphasis on advanced academic and research skills. The inclusion of **Research Methods for Engineering** prepares students to critically analyse existing research, design their own investigations, and contribute to the body of knowledge in the field. The culmination of the MSc is the **Dissertation**, an independent research project that allows students to delve deeply into a specific area of industrial cybersecurity. This dissertation provides an opportunity to develop advanced problem-solving skills, conduct in-depth analysis, and propose innovative solutions to complex cybersecurity challenges in industrial environments. The MSc aims to develop both theoretical and applied skills, positioning graduates as leaders capable of working in operational roles, collaborating with IT managers and Chief Information Security Officers (CISO), and focusing specifically on the cybersecurity aspects of industrial networks.

13 Bibliography

[1] Directive (EU) 2022/2555, *EU Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] Directive (EU) 2016/1148, *EU Measures for a high common level of security of network and information systems across the Union*. 2016, p. 30. Accessed: Jun. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[3] ENISA, 'ENISA Incident Reporting', NIS Incident Reporting. Accessed: Aug. 12, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/incident-reporting/

[4] K. Stouffer *et al.*, *Guide to Operational Technology (OT) Security*, NIST SP 800-82 Rev. 3, Sep. 28, 2023. doi: 10.6028/NIST.SP.800-82r3.

[5] ISA/IEC 62443, 'Industrial communication networks - IT security for networks and systems'. International Society of Automation/International Electrotechnical Commission, Jul. 20, 2009.

[6] P. Kobes, *Guideline Industrial Security: IEC 62443 is Easy*. HEYER, 2017. [Online]. Available: https://books.google.ie/books?id=uQEjtAEACAAJ

[7] ISO/IEC27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, Standard ISO/IEC 27001:2022, Oct. 25, 2022.

[8] Regulation (EU) 2024/2847, *EU Cyber Resilience Act (CRA)*. 2024. Accessed: Jun. 13, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

This page is intentionally blank