Cybersecurity in Manufacturing

engineering the south east

South East Automation Group

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Dr Diarmuid Ó Briain

CEng, FIEI CISSP®

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

Table of Contents

Illustration Index

Index of Tables

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 presentation, you will be able to:

- Understand the key objectives 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
- Understand the CRA's objectives, product categories, compliance, and penalties.

2 Network Information Security

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

3.1.1 The Three Pillars of NIS2

The three pillars of NIS2 support a collaborative EU approach to cybersecurity, defining the shared responsibilities of Member States, National Competent Authorities (NCA), and Essential/Important Entities. This framework is vital for enhancing collective resilience across the digital economy.

3.1.1.1 Member States

Member States implement the directive by developing national cybersecurity strategies and designating a Single Point of Contact (SPOC), such as the National Cyber Security Centre (NCSC) in Ireland as well as National Competent Authorities (NCA) who serve as the frontline enforcers within their jurisdictions. They are responsible for categorising entities, monitoring overall national performance, and enforcing compliance.

3.1.1.2 Essential and Important Entities

These private and public sector organisations must adhere to strict security mandates. Their obligations include conducting risk assessments, implementing robust security measures, establishing incident response plans, and notifying NCAs of any significant disruptions.

3.1.2 A Collective Effort

The NIS2 framework emphasises that effective security requires a unified effort. By mandating cooperation between states, regulators, and private entities to identify and mitigate risks, the directive creates a more resilient landscape to protect critical infrastructure and safeguard the digital economy. 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)

3.2 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.

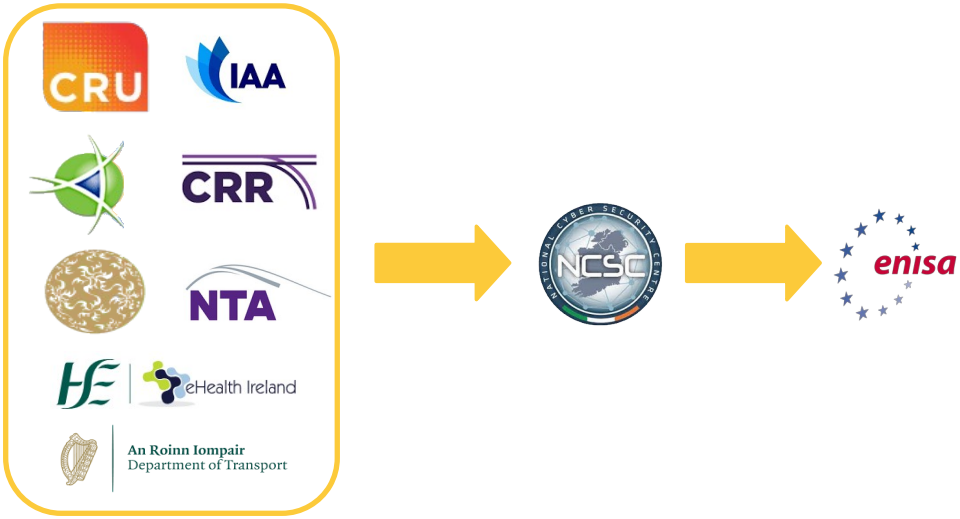

Figure 1: Competent Authorities and Reporting Relationships

As illustrated in Figure 1 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.

3.3 Sectoral NCAs

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

3.3.1 Commission for the Regulation of Utilities

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

3.3.2 Commission for Communications Regulation

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

3.3.3 Central Bank of Ireland

The CBI 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

3.3.4 Irish Aviation Authority

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

3.3.5 Commission for Rail Regulation

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

3.3.6 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

3.3.7 National Transport Authority

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

3.3.8 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

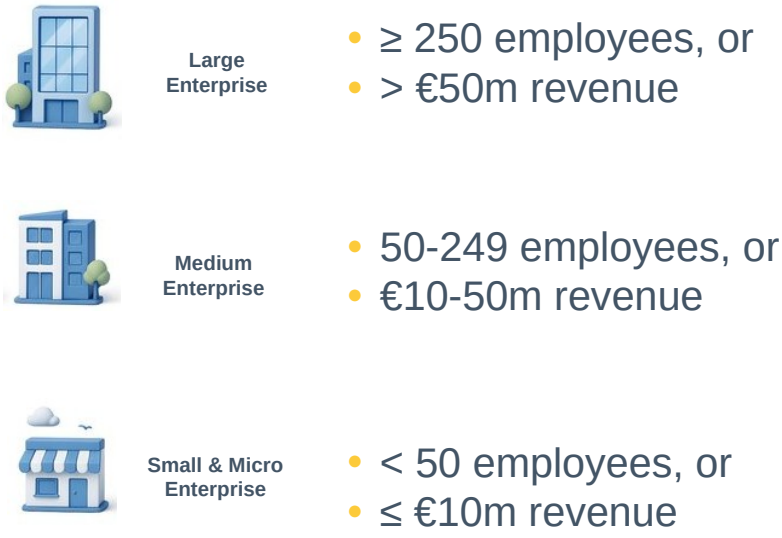

Figure 2: Entities defined in NIS2

Figure 2 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 (RMM) 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.

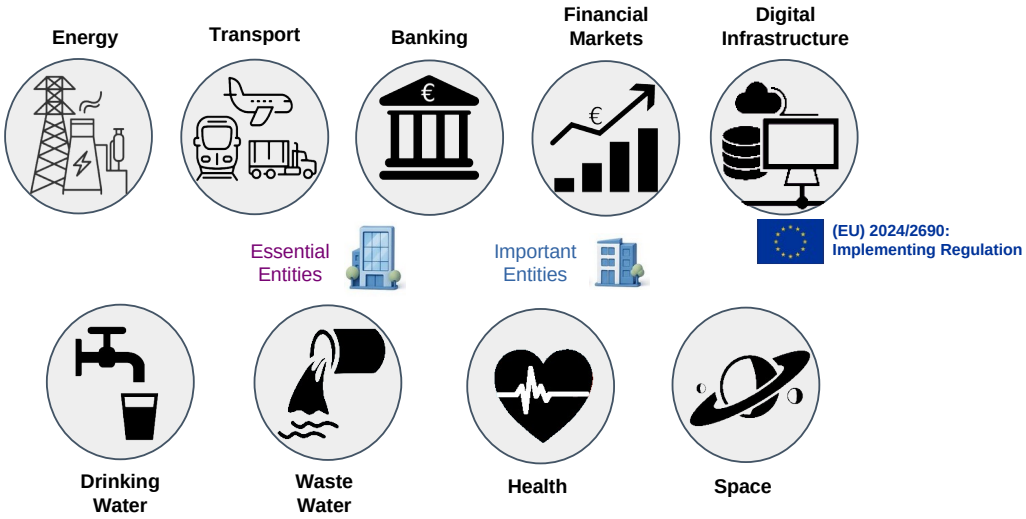

Figure 3: Sectors of High Criticality

5.1 Sectors of high criticality

As illustrated in Figure 3, 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.

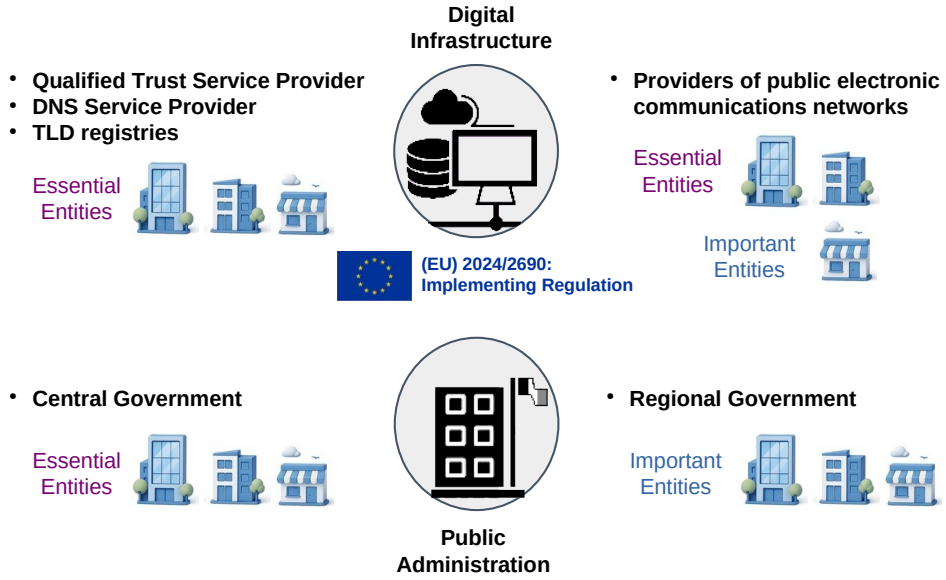

Figure 4: Digital Infrastructure and Public Administration

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

As illustrated in Figure 4, 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.

Taking account of the cross-border nature of the activities of Digital Providers specifically and in order to ensure a coherent framework for them, the EU added Regulation (EU) 2024/2690 Implementing Regulation[3] to lay down the technical and the methodological requirements of the measures referred to in Article 21(2) of Directive (EU) 2022/2555 and to further specify the cases in which an incident should be considered to be significant as referred to in Article 23(3) of Directive (EU) 2022/2555.

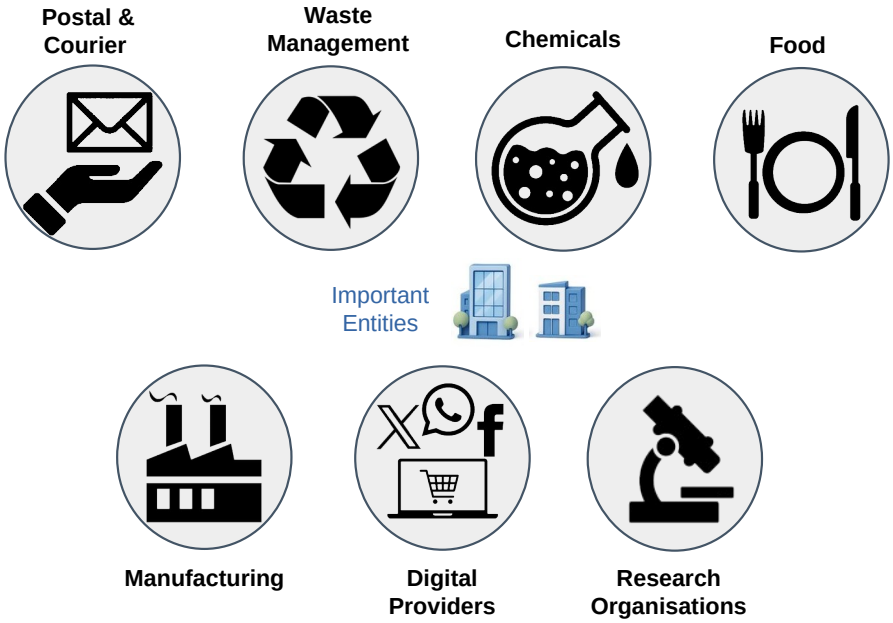

Figure 5: Other critical sectors

5.2 Other critical sectors

As illustrated in Figure 5, 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

Table 1: 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 RMMs adopted by the entity concerned	Requests for information necessary to assess, ex post, the cybersecurity RMMs adopted by the entity concerned

Table 1 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 [4]. This reporting helps organisations and Member States to learn from other incidents and is a crucial change in the new NIS2 Directive.

Table 2 lists the various NIS2 incident reporting deadlines, by whom, and to whom.

Table 2: NIS2 Incident reporting deadlines

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.

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 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, and 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.

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 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.

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 RMMs 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 RMMs
- 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 RMMs taken by the entity.
- Supervise the implementation of the RMMs.
- 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 RMMs.

10.1 ISO/IEC 27001 Information Security Management System

ISO/IEC 27001:2022 provides a high-level, management system approach to information security, establishing the requirements for a strategic Information Security Management System (ISMS) across an entire organisation. A core component of this standard is the Statement of Applicability (SoA), which serves as a critical document justifying the selection (or exclusion) of specific security measures. The standard utilises a risk-based approach to target threats through 93 Annex A controls, categorised into organisational, people, physical, and technological themes. By mandating rigorous documentation and continuous improvement through management reviews and audits, ISO 27001 ensures that security remains a boardroom priority and meets broad NIS2 compliance benchmarks.

In contrast, the ISA/IEC 62443 series and the CyberFundamentals (CyFun) 2025 framework are domain-specific, offering granular technical and operational guidance for securing industrial (OT/ICS) environments. While ISO 27001 focuses on the governance of *what* an ISMS should achieve, these specialised standards detail *how* to implement robust security within the unique constraints of operational technology.

Therefore, for comprehensive NIS2 compliance, organisations in manufacturing and Critical Infrastructure can effectively layer an ISO 27001-based ISMS for enterprise-wide governance with the specialised, practical security measures from CyFun® 2025 or ISA/IEC 62443 to safeguard their critical OT systems.

10.2 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.

10.3 Risk Management Measures

Figure 6: Risk Management Measures

The RMMs, issued by the NCSC, define the *What* of the NIS2 directive for Irish entities. They represent a comprehensive set of sixteen distinct requirements that establish the necessary security baseline for Essential and Important entities. By categorising these measures into Foundational and Supporting Actions, the NCSC provides a clear framework of the specific security outcomes that must be achieved to meet national compliance standards.

10.4 Cyber Fundamentals® 2025

CyFun® 2025

CyFun® 2025 serves as the *How*. Originally developed by the Centre for Cybersecurity Belgium (CCB) in Belgium and now an internationally collaborative standard co-owned by the NCSC (Ireland), CyFun® 2025 provides the concrete, step-by-step methodology for implementation. The standard is also adopted in Romania and Malta with Portugal and Croatia currently observing or partially adopting the framework as it moves toward becoming a de facto European standard for NIS2 compliance.

It offers a practical path for organisations to operationalise the RMMs, helping them reduce risk and enhance their ability to withstand and recover from common cyber-attacks through a structured, iterative process. Together, these two elements allow an organisation to move from high-level regulatory obligations to a functional, resilient security posture.

10.5 Comparison between Frameworks

Table 3 illustrates how the three distinct cybersecurity frameworks, ISO/IEC 27001, IEC 62443, and CyFun® 2025, address the core requirements of the NIS2 directive. It highlights a strategic gap and overlap reality: while ISO 27001 is *Optimised* for high-level governance, risk policies, and hygiene, it is often rated as only *Sufficient* in more technical, operational areas such as incident handling and supply chain security when compared to the specialised demands of NIS2. Conversely, IEC 62443 provides *Optimised* technical depth for industrial OT environments but may only reach *Sufficient* levels for general corporate hygiene and training. Notably, CyFun® 2025 emerges as the most consistently *Optimised* framework across all categories, reflecting its design as a dedicated, modern *how-to* tool specifically built to operationalise the NIS2 and NCSC RMMs.

- **ISO/IEC 27001** focus on Management Enterprise Governance & Policies, elevating security to a boardroom priority by establishing formal policies, risk ownership, and a culture of continuous improvement across the entire enterprise.
- **ISA/IEC 624443** focus on OT Machine & Network Security by addressing the security of the factory floor, securing the Programmable Logic Controllers (PLC), industrial networks, and legacy systems that standard IT security often overlooks.
- **CyFun® 2025** focus on Compliance through fast-track Audit for EU Regulators through a structured, tiered methodology that translates technical and management efforts into a format that regulators recognise as credible evidence of NIS2 compliance.

Table 3: Alignment with NIS2 Requirements: Manufacturing

NIS2 Requirements	ISO 27001 (ISMS)	IEC 62443 (OT)	CyFun 2025
Risk & Policies	Optimised	Optimised	Optimised
Incident Handling	Sufficient	Optimised	Optimised
Continuity & Recovery	Sufficient	Optimised	Optimised
Supply Chain	Sufficient	Optimised	Optimised
Hygiene & Training	Optimised	Sufficient	Optimised
Crypto & MFA	Optimised	Optimised	Optimised

Focus Area	Management	Technology	Compliance
Manufacturing Role	Enterprise Governance & Policies	OT Machine & Network Security	Fast-track Audit for EU Regulators

11 Cyber Resilience Act

The EU's Cyber Resilience Act (CRA) [7], 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.

11.1 Scope: Who is Affected and Excluded

The CRA applies to manufacturers, importers, and distributors of products with digital elements sold within the EU. This includes everything from smart home devices, wearables, industrial systems, network equipment, and software applications.

Certain products are explicitly excluded, such as medical devices already regulated under specific EU medical device regulations, motor vehicles, aviation systems, and some Software as a Service (SaaS) products covered by other regulations such as the NIS2 Directive.

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 7: CRA Conformance by Category

11.2 Product Categories and Assessment Requirements

As listed in Figure 7, all products are categorised and each category has particular conformance requirements.

11.2.1 Default “unclassified” (Low Risk)

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

11.2.2 Important “Class I” and “Class II” (Higher Risk)

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.

11.2.3 Critical (Highest Risk)

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.

11.3 Mandatory Product Security Requirements

The CRA introduces a set of mandatory requirements that manufacturers must meet to enhance cybersecurity resilience:

- **Risk Management**: Manufacturers must perform risk assessments on their digital products and implement appropriate security measures.
- **Secure by Design**: Products should be designed with cybersecurity as a priority, ensuring secure configurations by default and protecting data confidentiality, integrity, and availability.
- **Incident Preparedness**: Organisations must build resilience against cyberattacks, mitigate potential impacts, and ensure efficient security event logging.

- **Security Updates and Maintenance**: Manufacturers are required to provide free and secure updates to fix vulnerabilities promptly and notify users about security patches.
- **Vulnerability Handling Requirements**: Organisations must maintain a Software Bill of Materials (SBOM), conduct regular security testing, and implement CVD policies.
- **Product Information & Guidance**: Clear documentation must be provided to users, including manufacturer contact details, product identification, cybersecurity guidelines, and decommissioning procedures.

11.4 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, product recalls, and restrictions on market access, along with significant reputational damage that can erode stakeholder trust. 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.

11.5 Preparing for CRA Compliance

To prepare for CRA compliance, organisations should:

- **Determine Scope and Applicability**: Identify all products subject to CRA compliance.
- **Perform CRA Conformity Assessment**: Evaluate current security controls against CRA requirements (Gap Analysis) to determine gaps and areas requiring improvement.
- **Build & Execute a Roadmap**: Develop a detailed roadmap outlining specific steps and timelines needed to achieve CRA conformity, including risk management strategies and security policies.
- **Continuously Improve**: Establish a process for ongoing evaluation and enhancement of cybersecurity measures, including regular security audits and updates to security protocols.
- **Audit and Certify**: Achieve certification under recognised certification schemes such as EUCC or other alternatives when available, ensuring long-term compliance and enhanced market credibility.

12 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] Regulation (EU) 2024/2690, *EU rules for the application of EU 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures.* 2024. Accessed: Jun. 30, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

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

[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] 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