Workshop Notes

Cybersecurity in the Maritime Domain

Dr Diarmuid Ó Briain

Version: 1.0.2

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

Table of Abbreviations

ACS	Automation and Control Systems
AGV	Automated Guided Vehicles
BESS	Battery Energy Storage Systems
BYOD	Bring Your Own Devices
CAB	Conformity Assessment Bodies
CCB	Centre for Cybersecurity Belgium
CDN	Content delivery networks
CIS	Centre for Internet Security’s
CMS	Cargo Management System
CNI	Critical National Infrastructure
CRA	Cyber Resilience Act
CRU	Commission for the Regulation of Utilities
CSC	Critical Security Controls
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CSIRT-IE	CSIRT Ireland
CSMS	Cybersecurity Management System
CSP	Cloud computing Service Providers
CVD	Coordinated Vulnerability Disclosure
CyFun	Cyber Fundamentals 2025
DCS	Distributed Control System
DE	Detect
DNS	Domain Name Systems
DNSC	Romanian National Cyber Security Directorate
DPA	Designated Person Ashore
DSP	Digital Service Providers
ENISA	European Network Information Security Agency
EU	European Union
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
EUCC	European Cybersecurity Certification Scheme on Common Criteria
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
GV	Govern
HMI	Human-Machine Interfaces
IA&CS	Industrial Automation and Control Systems
IACS	International Association of Classification Societies
ICS	Industrial Control Systems
ICT	Information and Communications Technology
ID	Identify
IEC	International Electrotechnical Commission
IG	Implementation Groups
IMO	International Maritime Organisation
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISPS	International Ship and Port Facility Security

IT	Information Technology
IXP	Internet eXchange Points
LE	Large Enterprises
ME	Medium Enterprises
MFA	Multi-Factor Authentication
MITA	Malta Information Technology Agency
NCA	National Competent Authorities
NCSC-IE	Irish National Cyber Security Centre
NIS	Network and Information Systems
NIS2	Network and Information Systems version 2
NIST	National Institute of Standards and Technology
OES	Operators of Essential Services
OT	Operational Technology
PLC	Programmable Logic Controllers
PCS	Port Community Systems
PR	Protect
QERDS	Electronic Registered Delivery Services
QES	Qualified Trust service providers
OEM	Own Equipment Manufacturers
QESeal	Electronic Seals
QTS	Electronic Time Stamps
QWAC	Certificates for Website Authentication
RC	Recover
RMM	Risk Management Measures
RS	Respond
SaaS	Software as a Service
SAIC	Safety, Availability, Integrity and Confidentiality
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SME	Small & Micro Enterprises
SMS	Safety Management System
SoA	Statement of Applicability
SPOC	Single Point of Contact
TLD	Top Level Domain
UR	Unified Requirements
VTS	Vessel Traffic Services

1 Introduction

As the maritime and industrial sectors undergo a rapid digital transformation, the traditional *ship-centric* safety model is being superseded by a complex landscape of interconnected Information Technology (IT) and Operational Technology (OT) systems. This workshop provides a roadmap for navigating this shift, focusing on the mandatory transition to the Network and Information Security Directive 2 [1] and the implementation of Ireland’s CyFun 2025 framework [2]. By harmonising global standards such as ISO/IEC 27001 [3] for governance and ISA/IEC 62443 [4] for industrial safety, organisations can move beyond checkbox exercises to achieve operational resilience. In an era where a single cyber incident can compromise vessel propulsion or port logistics, this workshop serves as a pathway for leadership and technical teams to secure the future of the maritime supply chain.

1.1 Objectives

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

- Contextualise the maritime cyber-physical landscape.
- Navigate the regulatory transition to NIS2.
- Operationalise defence via cybersecurity frameworks.
- Harmonise global standards for technical resilience.

2 The Maritime Cyber domain: The story so far

2.1 Introduction

The maritime industry is currently navigating a period of unprecedented regulatory convergence. Historically, maritime security was defined by physical barriers and the safe navigation of individual vessels, governed by a ship-centric philosophy that isolated the ship from the shore. However, as the maritime economy undergoes rapid digitalisation, this isolation has vanished, replaced by an interconnected web of OT and global data networks. This section explores the evolution of the maritime cyber landscape, from the foundational safety-first mandates of the International Maritime Organisation (IMO) and International Association of Classification Societies (IACS) to the rigorous, entity-wide governance required by the NIS2 directive. By analysing the interplay between management layers and technical standards, a roadmap is established for moving beyond mere compliance towards organisational resilience.

2.2 The Legacy of Safety and the "Ship-Centric" Mindset

For decades, the maritime industry has operated under a clear, singular mandate *Safety and Seaworthiness*. Traditionally, cybersecurity was viewed primarily through this lens, preventing a ship from being *taken over* or crashing to avoid loss of life and environmental disaster.

Historically, this has been managed through a patchwork of standards rather than a unified digital policy. The International Ship and Port Facility Security (ISPS) Code [5] for physical and digital security, IMO guidelines for management processes, and IACS requirements for technical systems. These were governed by Class Societies and Flag States, not national cybersecurity agencies. While effective for individual vessels, this framework was never intended to protect the broader European Digital Single Market, a gap that NIS2 is now designed to bridge.

2.3 The Management and Technical Layers

The current landscape is built on two distinct pillars:

- management processes
- technical design.

2.3.1 The Management Layer (ISPS & MSC-FAL.1)

Every commercial vessel today operates under the *Management Layer*. Since 2021, the IMO has mandated that cyber risks be addressed within a ship's Safety Management System (SMS).

This is anchored by the ISPS code. This code was originally a post-9/11 response to terrorism, it now treats cyber as a direct threat to the Ship Security Plan.

Additionally, guidelines such as IMO Guidelines on Maritime Cyber Risk Management [6], act as the source document for this integration. They do not dictate which firewall to buy; instead, they use the language of the United States (US) National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 [7] framework (*Govern, Identify, Protect, Detect, Respond, Recover*) to ensure the organisation has a plan for when systems fail.

2.3.2 The Technical Layer (IACS UR E26 & E27)

The IACS has added security at the shipyard level through the following Unified Requirements (UR) which are mandatory standards for any vessel contracted for construction on or after 1 July 2024.

- **UR E26 Cyber Resilience of Ships** applies to the System Architect. It treats the entire ship as a single entity, ensuring that the integration of bridge, engine room, and shore office does not create any single point of failure.
- **UR E27 Cyber resilience of on-board systems and equipment** [8] forces vendors to ensure individual parts, such as Global Positioning System (GPS) or engines, are *secure by design*.

However, these are only mandatory for new builds contracted after July 1, 2024. This leaves a legacy fleet of thousands of older ships that lack these native technical protections.

2.4 The Shift from Maritime Rules to NIS2

Within the European Union (EU) there is a cultural shift from self-regulation to one of state oversight. The differences between the status quo and the NIS2 Directive are stark and laid out in Table 1.

Table 1: The Shift from Maritime Rules to NIS2

Feature	Current Maritime (IMO/IACS)	NIS2 Directive Requirements
Enforcement	**Port State Control/Class Surveys:** Fines are rare; *deficiencies* are the norm.	**Heavy Penalties:** Up to €10M or 2% of global turnover.
Incident Reporting	**No strict timeline**: Focus on reporting to Flag State/Owner.	**Strict Timelines**: *Early Warning* within 24 hours; full report in 72 hours to national authorities.
Supply Chain	E27 covers hardware, but not service providers (Security as a Service (SaaS), remote monitoring).	**Total Supply Chain**: Deep audits of all digital service providers and software vendors.
Governance	**Technical/Designated Person Ashore (DPA)** responsibility.	**C-Suite Liability**: Management is personally liable for cybersecurity failures.

2.5 Conclusion: The Roadmap Ahead

The transition to NIS2 represents a fundamental shift in responsibility. Cybersecurity is no longer just an IT problem or a Captain’s problem, it is a core business risk.

A switch in thinking from ship-centric to organisation-centric is required, stop considering vessels in isolation and start viewing the entire company as an Entity within the NIS2 infrastructure.

This does not mean that NIS2 replaces ISPS Code and IACS requirements and guidelines, they are technical base layer upon which the NIS2 reporting and governance requirements are layered on top.

The biggest hurdle will be the older ships. While they may be exempt from newer UR E27 technical standards, they are not exempt from NIS2 operational resilience requirements. Maritime organisations must now prove that even its oldest vessels can operate securely within a modern digital network.

Additionally, under NIS2, Port Authorities are also classified as Entities, moving them beyond the physical focus of the ISPS Code into a regime of proactive, mandatory digital oversight. They are now legally responsible for the cyber-cleanliness of the entire port ecosystem, including Vessel Traffic Services (VTS), automated terminal hardware, and Port Community Systems (PCS). Crucially, the Port Authority’s management now faces personal liability for the security of their entire supply chain, meaning they must audit the digital resilience of every third-party vendor and service provider operating within their infrastructure.

3 The Maritime Threat Context

As the energy and maritime sectors undergo rapid digitalisation, they face a more hostile and sophisticated threat landscape. Table 2 outlines how geopolitical tensions, supply chain complexity, and systemic software vulnerabilities have escalated the risk to critical infrastructure in 2026.

Table 2: Escalated Threat Context

Threat Trend	Details from Recent Reports
Increased Frequency	The number of cyberattacks in the energy sector has increased ten to twenty times since the war in Ukraine.
Focus on OT	While past attacks often targeted IT systems, the industry recognises that State-sponsored actors are engaging in *pre-positioning* or *silent attacks* to gain access to OT systems, waiting for the right moment to strike and cause disruption.
Vulnerable Supply Chain	The complex and long supply chain in offshore wind, with many parties (Own Equipment Manufacturers (OEM), data analysts, etc.), makes it harder to maintain oversight and spot deviations.
Human/ System Error	Major power disruption can still be caused by human and system errors with cascading digital effects: • ***2024 Crowdstrike Incident***: A faulty software update inadvertently crashed around 8.5 million computer systems globally, affecting critical services such as airports. • ***2023 Sungrow Incident***: The Chinese inverter and Battery Energy Storage Systems (BESS) manufacturer sent a *bad update*, causing around 800 energy storage systems to go down.
Focus on Solar/BESS	There is significant recent concern regarding vulnerabilities in solar inverters and BESS across Europe, which are rapidly integrating into the grid and often rely on components with known security weaknesses.

3.1 Cyberattacks on offshore wind farms

Cyberattacks on offshore wind farms across Europe have resulted in serious consequences, including power outages, environmental damage, and leaks of sensitive data.

The under-reporting of incidents due to fear of financial and reputational damage continues to create an intelligence gap, meaning attacks are likely still occurring but are not publicly attributed or detailed.

Attacks on the office environments of wind companies, often with ransomware, still happen, though these may not directly affect the turbines.

In summary, and as illustrated in the list of attacks in Table 3, the threat is higher and more pervasive than ever, but the specific, high-profile incident disclosure rate remains low due to industry practice.

Table 3: Cyber attacks on Offshore Wind

Company	Date	Attack Type	Impact Overview	Operational Consequence
Vestas	01/11/21	Direct Ransomware	Targeted the Danish wind manufacturer's IT systems, resulting in sensitive data leaks and production issues.	Multiple business units and locations had to shut down IT systems, causing production delays. Company shares decreased by 3%.
Enercon	01/02/22	Indirect (ViaSat satellite attack)	Targeted satellite communications infrastructure (attributed to Russian actors). Enercon wind farms were collateral damage, losing remote control access.	Loss of remote monitoring access to over 5,800 turbines in Germany. Some turbines took two months to come back online.
Deutsche Windtechnik	01/04/22	Direct Ransomware (Conti group)	Targeted the German maintenance company's IT system, resulting in the disabling of remote connectivity.	Approximately 2,000 out of 7,500 turbines across Germany were shut down to prevent further damage.
Nordex	01/03/22	Direct Ransomware	Targeted the German turbine manufacturer's control centre.	The company disabled the platform and IT systems.

Beyond offshore energy, the vulnerability of the global supply chain is underscored by a history of attacks on land-side maritime infrastructure and vessel navigation systems. These incidents demonstrate that a breach in a single port’s cargo management system or fleet software can have immediate, cascading effects on international trade, safety, and national security. Table 4 outlines key historical and recent attacks that have shaped the current maritime cybersecurity landscape.

Table 4: Cyberattacks on other Maritime Infrastructure

Attack/ Incident	Year	Target	Type of Attack	Primary Impact on Operations	Estimated Cost/Scope
Port of Antwerp Cyber-Operation	2011 – 2013	Cargo Management Systems (CMS) (Port of Antwerp)	Espionage and System Manipulation (via phishing and keyloggers)	Allowed drug traffickers to track specific containers and illegally remove them from the port before the legal owners arrived.	Enabled drug-trafficking for over two years.
Maersk NotPetya Attack	2017	A.P. Moller-Maersk (Global Shipping Giant)	*Wiper* Malware (spread via supply chain, disguised as ransomware)	Crippled global IT network, shut down container tracking, and froze operations at 17 APM Terminals worldwide.	Over $300 million in damages and recovery costs.
Black Sea GNSS Spoofing	2017	Global Navigation Satellite Systems (GNSS) on vessels	GPS Spoofing (sending false signals)	Caused the navigation systems on over 20 ships to incorrectly report their location as being miles inland (at an airport).	Major safety and navigation risk, likely state-sponsored electronic warfare test.
Port of Lisbon Ransomware Attack	2022	Port of Lisbon Administration (APL)	Ransomware (claimed by the LockBit group)	Temporarily shut down the port's website and internal computer systems for four days.	Exfiltration of sensitive data, including financial reports and ship logs. Ransom demand of $1.5 million.
DNV Ransomware Attack	2023	DNV (Maritime Classification Society)	Ransomware	Forced DNV to shut down servers for its Ship Manager software, which is critical for fleet operations.	Impacted the operations of up to 1,000 vessels belonging to 70 customers globally.

To understand the risks addressed by the NIS2 Directive, it is essential to distinguish between the systems that manage business data and those that control physical systems and devices. While IT failure typically results in financial or data loss, a compromise of OT on a ship or in a port can lead to immediate physical catastrophe.

Table 5: What is Operational Technology (OT)

Feature	IT	OT
Primary Function	Manages data and information (Emails, billing, HR, payroll, logistics scheduling).	Controls and monitors physical processes (Propulsion, steering, cargo cranes, valves).
Where does it exist	Shore offices, personal devices, and port administrative centres.	**On the Ship**:The Bridge and Engine Room. **In the Port**: Automated gantry cranes, Automated Guided Vehicles (AGV), VTS, and terminal gates.
Impact of failure	Financial loss, stolen data, inconvenience.	A loss of control, a collision, an engine failure, or a physical accident.

3.2 Operational Technology Terms

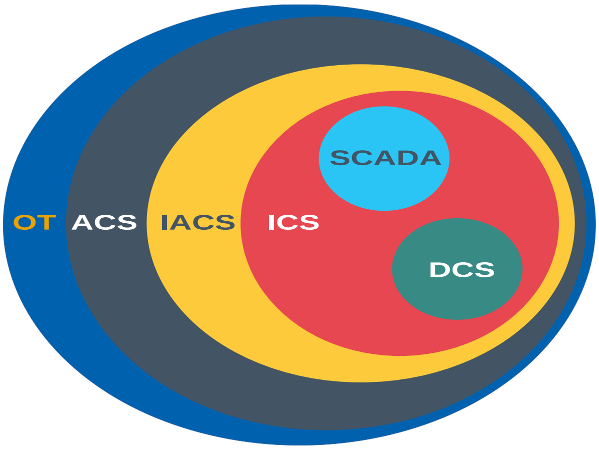


Figure 1: OT Terms

Figure 1 illustrates the relationship between various OT terms:

- **Operational Technology (OT):** The hardware and software used to change or monitor the physical state of assets, such as engines, pumps, or valves.
- **Automation and Control Systems (ACS):** The broad category of technologies that use control loops to manage equipment without human intervention.
- **Industrial Automation and Control Systems (IA&CS):** A more formal designation for the collection of personnel, hardware, and software that affects the safe and secure operation of an industrial process.
- **Industrial Control Systems (ICS):** The integrated hardware and software units, such as Programmable Logic Controllers (PLC) and sensors, that perform specific control functions within a ship or port terminal.
- **Supervisory Control and Data Acquisition (SCADA):** High-level software used to gather data from multiple remote sites and provide a central interface for operators to monitor and control large-scale processes.
- **Distributed Control System (DCS):** A decentralised control architecture where controllers are distributed throughout a system (such as an engine room) to ensure there is no single point of failure.

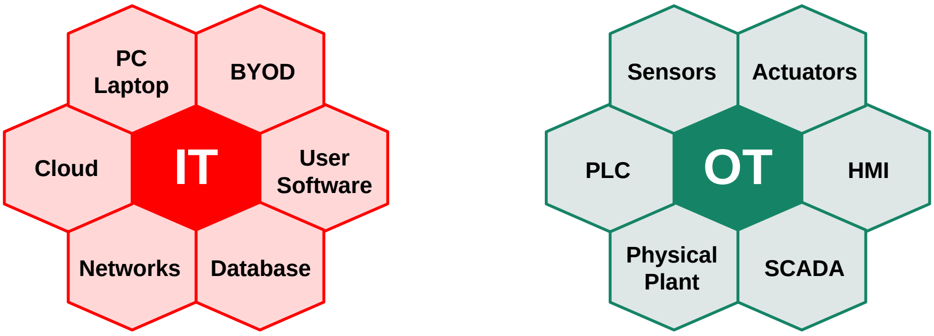


Figure 2: IT vs OT

Figure 2 illustrates the distinct components that define IT and OT within an industrial or maritime environment. The IT cluster (red) represents the data-centric side of the organisation, encompassing elements such as cloud services, hardware (PC/Laptops), user software, databases, and general networks. In contrast, the OT cluster (green) focuses on the physical execution and monitoring of assets, featuring components like sensors, actuators, PLC, and Human-Machine Interfaces (HMI). By grouping SCADA and the Physical Plant under OT, the diagram emphasises that these systems are responsible for controlling the tangible processes, such as steering a ship or operating port cranes, whereas IT handles the administrative and digital infrastructure.

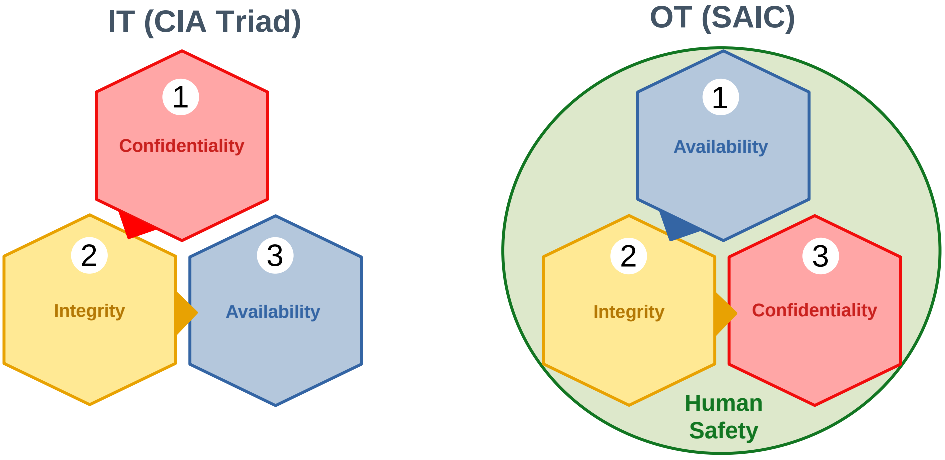


Figure 3: IT/OT Priorities

Figure 3 illustrate the core priority differences between IT and OT, highlighting their distinct components and conflicting security priorities. The first image categorises IT as data-centric, involving cloud services, Bring Your Own Devices (BYOD), and databases, while OT is defined by physical execution through sensors, actuators, and PLC. The second image demonstrates the fundamental shift in priorities: IT follows the Confidentiality, Integrity and Availability (CIA) Triad, where Confidentiality is the primary concern to protect sensitive data. Conversely, OT prioritises the Safety, Availability, Integrity and Confidentiality (SAIC) model, placing Safety and Availability at the top to ensure continuous operation, all while being underpinned by a critical foundation of Human Safety, a factor rarely present in standard IT environments.

Table 6: IT/OT Priorities

Priority	**IT**	**OT**
Top Priority	**Confidentiality**: Protecting data from unauthorised access.	**Availability**: Ensuring the system never stops running.
Secondary	**Integrity**: Ensuring data hasn't been tampered with.	**Integrity**: Ensuring commands to hardware are accurate.
Tertiary	**Availability**: Keeping systems online for users.	**Confidentiality**: Protecting system configuration data.
Ultimate Goal	Data Privacy & Financial Security	Human Safety & Physical Reliability

4 Network Information Security

The open market nature of the EU facilitates organisations to operate across 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 EU responded with the Network and Information Systems (NIS) Directive 2016/1148 [9] 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:

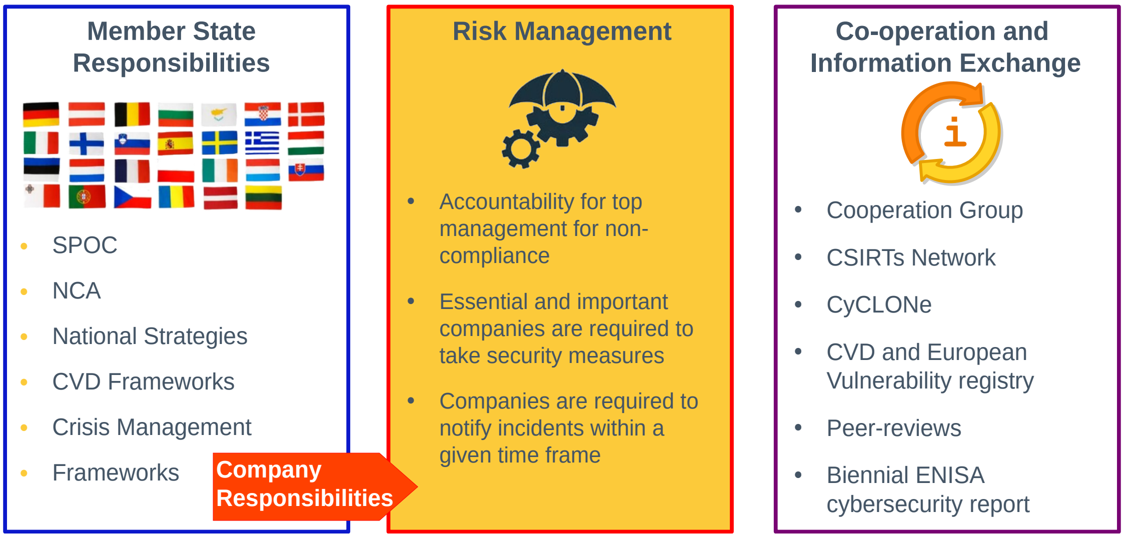
- Operators of Essential Services (OES)
- Digital Service Providers (DSP).

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 version 2, the NIS2 Directive 2022/2225 broadened the scope of the original version. 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.

4.1 The three main pillars of NIS2

The three pillars of NIS2, as illustrated in Figure 4, support the EU collaborative approach to Cybersecurity. The figure depicts the shared responsibilities of Member States, National Competent Authorities (NCA), Essential and Important entities. It highlights the collaborative approach that is essential for achieving the directive's goal of enhancing cybersecurity in the EU.



Member State Responsibilities

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

Company Responsibilities

Risk Management

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

Co-operation and Information Exchange

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

Figure 4: The three main pillars of NIS2

Member States play a crucial role by implementing the NIS2 directive through designating and establishing a Single Point of Contact (SPOC), such as the Irish National Cyber Security Centre (NCSC-IE), individual NCAs, and the identification and categorisation of both Essential and Important DSPs, 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 the SPOC and NCAs in other EU 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, SPOC, NCAs, 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)

4.2 National Competent Authorities

Every member state has a SPOC 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) housed within NCSC-IE, as it is Ireland's SPOC for the purpose of NIS2.

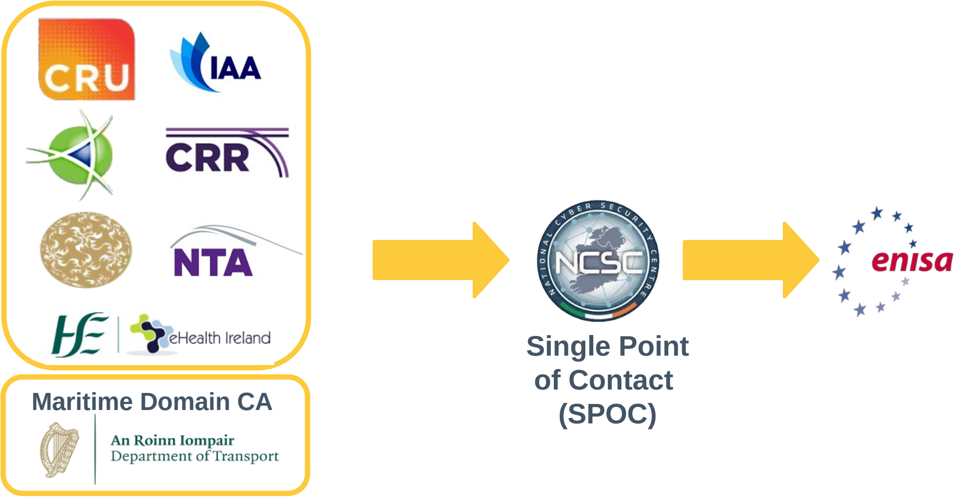
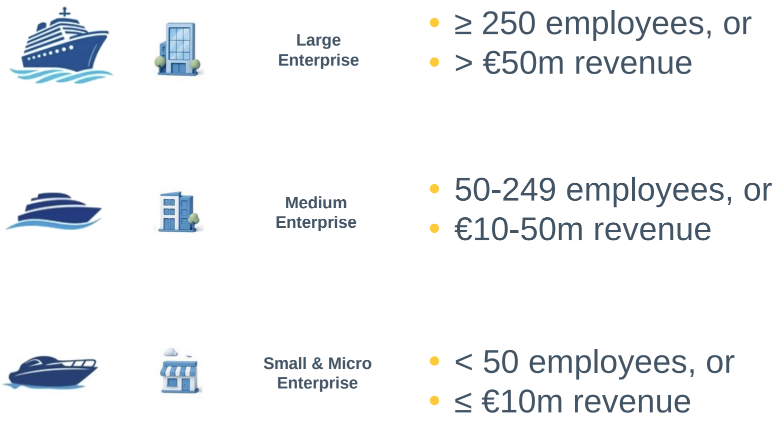


Figure 5: Competent Authorities and Reporting Relationships

As illustrated in Figure 5 a number of specialist NCAs have been appointed to handle specific NIS2 sectors. The NCSC-IE 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 NCSC-IE 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-IE 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, NCSC-IE actively supports the other designated sectoral NCAs (such as the Department of Transport, responsible for the Maritime Domain and the Commission for the Regulation of Utilities (CRU), responsible for Energy Utilities), who in the case of offshore wind also have some responsibilities associated with the maritime domain. In this way NCSC-IE shares 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 NCSC-IE's expertise to uplift the capabilities of all NCAs and the entities under their supervision.

4.3 Entities



Large Enterprise
- ≥ 250 employees, or
- > €50m revenue

Medium Enterprise
- 50-249 employees, or
- €10-50m revenue

Small & Micro Enterprise
- < 50 employees, or
- ≤ €10m revenue

Figure 6: Entities defined in NIS2

Figure 6 illustrates the entity groupings as defined in NIS2. 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.

4.4 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
- Important

These entity categorisations reflect 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.

4.5 Sectors of high criticality

As illustrated in Figure 7, 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.

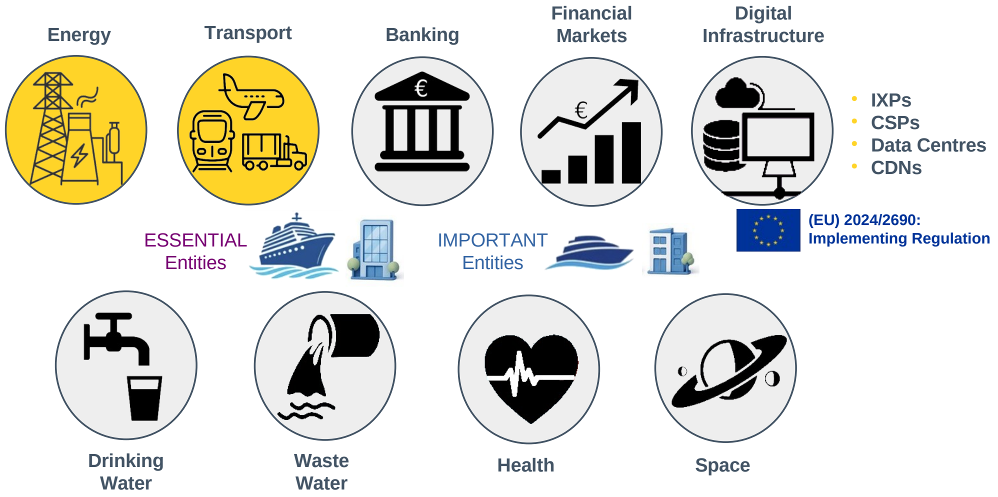


Figure 7: Sectors of High Criticality

These sectors are detailed in the following list:

1. Transport: Air, Rail, Maritime, Road
2. Energy: Electricity, District heating and cooling, Oil, Gas and hydrogen
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. Some digital infrastructure and public administration are considered differently and in these cases NIS2 can impact on SMEs also.

As illustrated in Figure 8, *Digital infrastructure* providers such as Qualified Trust service providers (QES) [organisations that provide Electronic Signatures], 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.

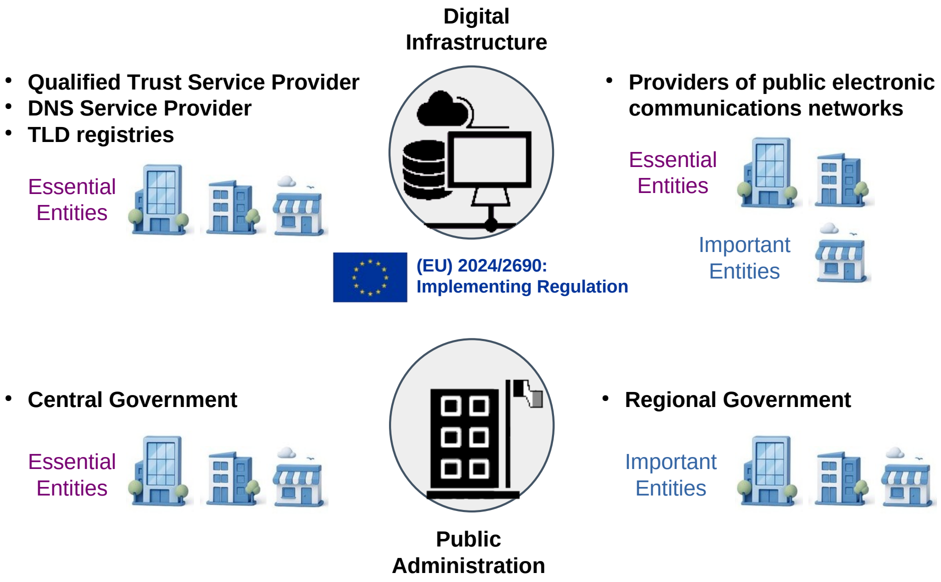


Figure 8: Digital Infrastructure and Public Administration

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 [10] 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.

4.6 Other critical sectors

As illustrated in Figure 9, 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.

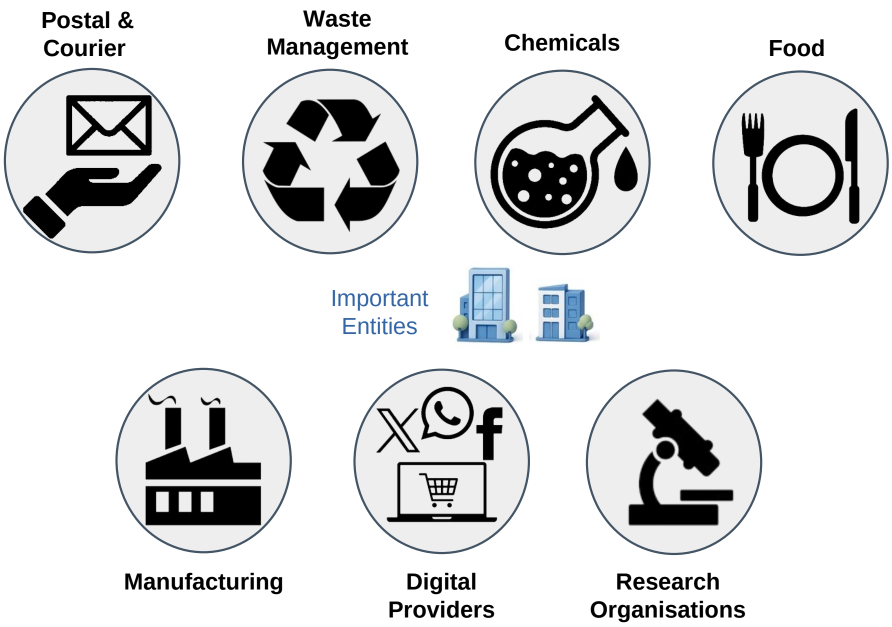


Figure 9: Other critical sectors

4.7 Supervision of Entities by NCAs

Table 7: Supervision of Entities by NCAs

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

Table 7 outlines two distinct approaches to oversight and risk management by NCAs, categorised by Essential 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.

4.8 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.

4.8.1 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 and the Department for Transport). These NCAs provide summary reports to the CSIRT-IE as lead NCA.

The NCSC-IE acts as the SPOC for incidents to ENISA. This is to reduce the administrative burden, including for incidents crossing member states. The NCSC-IE reports to the ENISA on incidents within the Irish jurisdiction every three months, using anonymised information. ENISA consolidates the information in the form of a report to be published every six months on the EU incidents [11]. This reporting helps organisations and member states to learn from other incidents and is a crucial change in the new NIS2 Directive.

Table 8 lists the various NIS2 incident reporting deadlines, by whom, and to whom.

Table 8: 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.

4.9 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 risk management measures are in place the EU can:

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

4.10 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 (RMM)
- 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.

4.11 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.

5 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.

5.1 NIST Cybersecurity Framework v2.0

A Cybersecurity Framework, such as the NIST CSF, describes essential cybersecurity outcomes that can help an organisation reduce its cybersecurity risk. The CSF is a base framework that is incorporated into many other frameworks, in fact it forms the base of the IMO Guidelines on MSC-FAL.1/Circ.3/Rev.3 Maritime Cyber Risk Management that has been discussed already as well as the Cyber Fundamentals 2025 framework that will be discussed later.

5.1.1 Framework Core

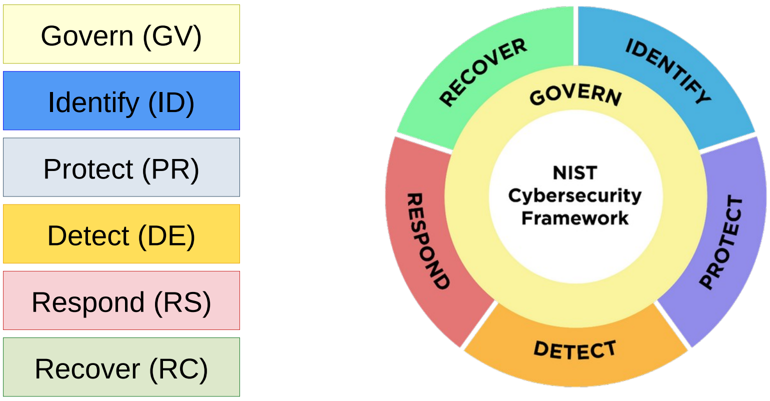


Figure 10: CSF Framework Functions

The Framework Core, illustrated in Figure 10, provides a set of cybersecurity outcomes, arranged by Function, Category, and Subcategory, implementation examples of how those outcomes might be achieved as well as references to additional guidance on how to achieve those outcomes.

5.1.2 Functions

Govern (GV)

Establish and monitor the organisation’s cybersecurity risk management strategy, expectations, and policy. This is a cross-cutting function and provides outcomes to inform how an organisation will achieve and prioritise the outcomes of the other five functions in the context of its mission and stakeholder expectations. GV directs the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy.

Identify (ID)

A function to determine the current cybersecurity risk to the organisation. Understanding the assets as well as the related cybersecurity risks enables an organisation to focus and prioritise effort in a manner consistent with its risk management strategy and the mission needs identified under GV. This function includes the identification of improvements needed for the organisation’s policies, processes, procedures, and practices supporting cybersecurity risk management to inform efforts under all six functions.

Protect (PR)

Use safeguards to prevent or reduce cybersecurity risk. Once assets and risks are identified and prioritised, PR supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events. This function includes outcomes such as awareness and training; data security; identity management, authentication, and access control; platform security as well as the resilience of technology infrastructure.

Detect (DE)

Find and analyse possible cybersecurity attacks and compromises. DE enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring.

Respond (RS)

Action related to a detected cybersecurity incident. RS supports the ability to contain the impact of cybersecurity incidents and outcomes include incident management, analysis, mitigation, reporting, and communication.

Recover (RC)

Restore assets and operations that were impacted by a cybersecurity incident. RC supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts.

Figure 10 illustrates the CSF Functions in a wheel as all framework functions are related to each other. GV is in the centre of the wheel considering how it informs the organisation on the implementation of the other five functions.

5.1.3 Categories and Sub-categories

CSF functions listed in Table 9 are subdivided into categories of related outcomes and subcategories are a further division of each category into specific outcomes of technical and management activities.

Table 9: Categories and their identifiers

Function	Category	Category ID
Govern (GV)	Organisational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

5.2 Centre for Internet Security – Critical Security Controls

The Centre for Internet Security's (CIS) Critical Security Controls (CSC), established by US Government and private sector experts in 2008, serve as a technical *gold standard* designed to provide organisations with a prioritised roadmap for cyber defence [12]. Version 8.1 reflects a modern, activity-based approach that streamlines the framework into 18 essential controls, specifically optimised for cloud and hybrid environments. Guided by the principle that *offence informs defence*, the framework focuses on feasibility, measurability, and alignment with other global standards. This ensures that organisations are not just performing good security tasks, but are specifically targeting the most prevalent and damaging attacker behaviours with practical, data-driven safeguards.

To ensure these controls are accessible to organisations of all sizes, the framework utilises Implementation Groups (IG) as a tiered adoption model. IG1 represents *Essential Cyber Hygiene* for small businesses, while IG2 and IG3 progressively add complexity to support larger enterprises and critical infrastructure facing sophisticated threats. Each of the 18 controls contains specific safeguards, detailed sub-steps that are assigned to different IGs. For example, a foundational control such as *Asset Inventory* may require only two basic safeguards for an IG1 organisation, but scales up to all five safeguards for an IG3 entity, ensuring that security maturity grows in tandem with an organisation's risk profile and resources.

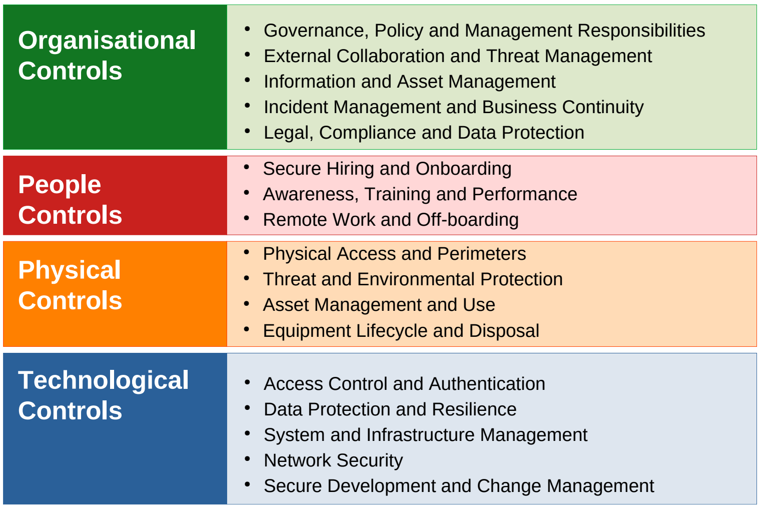
5.3 ISO/IEC 27001 Information Security Management System

The International Organisation for Standardisation (ISO) provides globally recognised frameworks to enhance quality, safety, and efficiency across various industries. Developed by global experts, these standards, including ISO 9001 (Quality) [13], ISO 14001 (Environment) [14], and ISO/IEC 27001 Information Security, Cybersecurity and Privacy Protection [15], establish a common language for best practices.

By adopting these standards, organisations demonstrate a commitment to continuous improvement and global benchmarks. This helps businesses build consumer trust, ensure regulatory compliance, and compete more effectively in the international marketplace.

5.3.1 ISO/IEC 27000 Series

The ISO/IEC 27000-series is a comprehensive set of information security standards developed jointly by the ISO and the International Electrotechnical Commission (IEC). Together, they provide best-practice recommendations for managing security, risks, and controls within an Information Security Management System (ISMS). By implementing a formal ISMS, organisations can move beyond reactive fixes to a proactive, risk-based culture championed by senior management at board level. This systematic approach relies on a clear hierarchy of standards, from the core requirements of ISO/IEC 27001 (Requirements) and ISO/IEC 27701 (Privacy) [16] to specialised guidance on risk management and incident response, ensuring that every stakeholder understands their shared responsibility in defending the organisation's most critical assets.



Organisational Controls

- Governance, Policy and Management Responsibilities
- External Collaboration and Threat Management
- Information and Asset Management
- Incident Management and Business Continuity
- Legal, Compliance and Data Protection

People Controls

- Secure Hiring and Onboarding
- Awareness, Training and Performance
- Remote Work and Off-boarding

Physical Controls

- Physical Access and Perimeters
- Threat and Environmental Protection
- Asset Management and Use
- Equipment Lifecycle and Disposal

Technological Controls

- Access Control and Authentication
- Data Protection and Resilience
- System and Infrastructure Management
- Network Security
- Secure Development and Change Management

Figure 11: ISO/IEC 27001 Annex A Themes

The practical strength of this framework lies in the Statement of Applicability (SoA), which bridges high-level policy with tangible operational defences. By selecting relevant safeguards from the 93 Annex A controls, spanning the Organisational, People, Physical, and Technological themes, as listed in Figure 11, an organisation creates a customised security roadmap tailored to its specific environment. This is supported by a rigorous audit trail of mandatory documentation, ranging from risk treatment plans to evidence of staff competence. The core documentation is listed in Table 10. This structured evidence not only ensures regulatory compliance, and consumer trust, but also fuels a cycle of continuous improvement, allowing the organisation to evolve alongside a volatile global threat landscape.

Table 10: ISO/IEC 27001 Core Mandatory Documents

Document Type	Clause	Purpose
ISMS Scope	4.3	Defines the boundaries of the security system.
ISMS Policy & Objectives	5.2 / 6.2	Sets the strategy and measurable security goals.
Risk Assessment & Treatment	6.1.2 / 6.1.3	Details how risks are identified and managed.
Statement of Applicability	6.1.3 (d)	The master list of implemented security controls.
Internal Audit Results	9.2	Proof of regular self-assessment.

5.4 ISA/IEC 62443 Series of Standards

The ISA/IEC 62443 series of standards, specifically designed for IA&CS and OT cybersecurity [17]. They provide a highly relevant and comprehensive framework for such organisations to meet their NIS2 commitments through the development of a Cybersecurity Management System (CSMS). 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. At its heart, the series is built upon the core principles of *Security by Design*, *Defence in Depth*, *Security throughout the Lifecycle* and *Security Risk Management* ensuring that protections are layered across every level of the industrial architecture. 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.

This multi-part series directly aligns with NIS2 mandates through a comprehensive focus on organisational maturity. While NIS2 requires robust risk analysis and security policies, ISA/IEC 62443-2-1 and 62443-3-2 provide the specific blueprints for establishing security programmes and defining security levels for network zones and conduits.

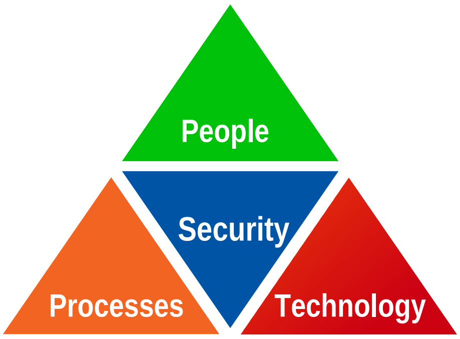


Figure 12: ISA/IEC 62443: Pillars of a CSMS

As illustrated in Figure 12, these standards emphasise that practical resilience is not found in software alone, but in the balanced integration of *People, Process, and Technology*, ensuring that staff are trained, procedures are rigorous, and hardware is secure. By integrating secure development lifecycles and service provider requirements, the series addresses NIS2's emphasis on supply chain security and incident handling. Leveraging these standards allows manufacturing and critical infrastructure organisations to establish an auditable posture that ensures legal compliance while significantly hardening their operational defences.

5.5 Cyber Fundamentals Framework

RMMs CyFun 2025

The NCSC-IE have responded to the National Cybersecurity Bill, an Irish transposition of the EU Directive 2022/2555 NIS2, by releasing RMM [18] while at the same time supporting the Cyber Fundamentals 2025 (CyFun) Framework.

These serve two distinct but complementary functions necessary for compliance with the NIS2 Directive:

- **RMMs**: represent the substance of the legal obligation, a formal guidance on the minimum baseline requirements that Essential and Important entities must meet under Article 21, Cybersecurity RMMs, define what cybersecurity areas must be addressed (e.g., governance, supply chain security, incident reporting).

1. **CyFun**: is the recommended tool to demonstrate compliance. It is a voluntary, structured, and risk-based framework that NCSC-IE recommends to entities to use to practically implement, organise, and evidence their compliance with the RMMs. It provides a roadmap for assessing cybersecurity maturity and applying the necessary controls.

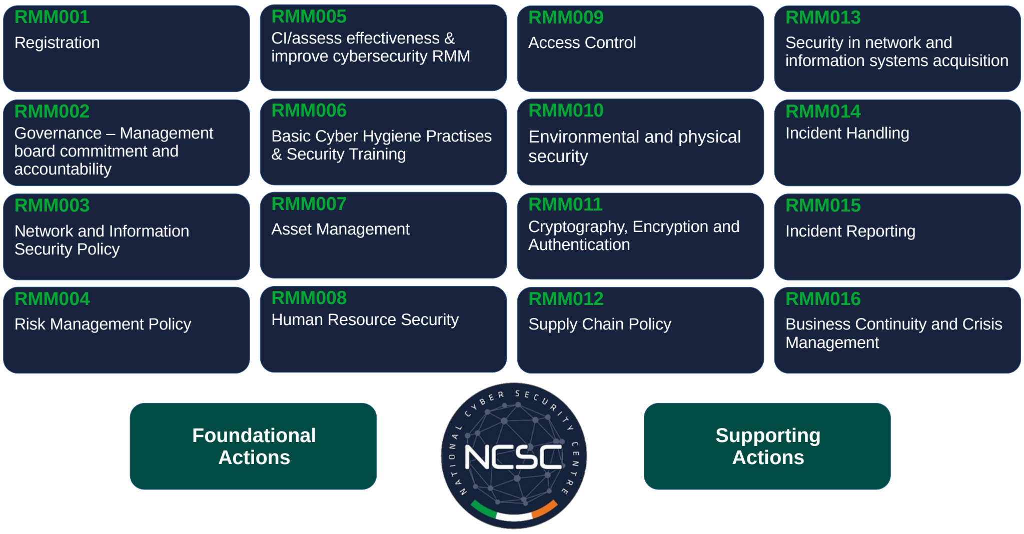
The NCSC-IE provides both the mandatory list of requirements (RMMs) [the *what you must do*] and a recommended compliance tool (CyFun) to simplify the process for organisations [the *how to do it and prove it*]. It is promoting both to ensure entities not only know what they must achieve but also have a practical, endorsed method how to achieve and prove it.

5.5.1 Risk Management Measures

The 18 RMMs are the bridge between the NIS2 Directive and daily operations for Irish entities, translating the high-level NIS2 text into a concrete roadmap for compliance. By defining the official minimum cybersecurity posture required under NIS2 Article 21, Cybersecurity RMMs, these measures remove the guesswork for organisations, establishing a clear baseline for digital resilience.

This framework is structured around a dual-tier approach: *Foundational Actions* establish the mandatory minimum that every entity must adopt, while *Supporting Actions* provide additional, risk-dependent controls to address specific vulnerabilities.

Each RMM emphasises that security is a governance priority rather than a IT exercise. Implementation must be both appropriate and proportionate to the organisation's risk profile, with management boards held directly accountable for the approval and ongoing oversight of these defensive strategies.



RMM001 Registration	RMM005 CI/assess effectiveness & improve cybersecurity RMM	RMM009 Access Control	RMM013 Security in network and information systems acquisition
RMM002 Governance – Management board commitment and accountability	RMM006 Basic Cyber Hygiene Practises & Security Training	RMM010 Environmental and physical security	RMM014 Incident Handling
RMM003 Network and Information Security Policy	RMM007 Asset Management	RMM011 Cryptography, Encryption and Authentication	RMM015 Incident Reporting
RMM004 Risk Management Policy	RMM008 Human Resource Security	RMM012 Supply Chain Policy	RMM016 Business Continuity and Crisis Management

Figure 13: Risk Management Measures (RMM)

5.5.2 CyFun 2025

The CyFun 2025 Framework, is a powerful tool for organisations seeking to elevate their cyber resilience in line with NIS2 requirements. This is not just a domestic standard; it's a collaborative international effort owned by four national Cybersecurity agencies, the Centre for Cybersecurity Belgium (CCB) (Primary Scheme Owner), NCSC-IE, the Romanian National Cyber Security Directorate (DNSC) and the Malta Information Technology Agency (MITA).

At its core, the framework provides a set of concrete measures combined with a clear, step-by-step approach. It is designed to help organisations protect their valuable data, significantly reduce their risk of the most common cyber-attacks, and ultimately enhance their overall ability to withstand and recover from incidents.

The CyFun 2025 framework is structured to be both practical and globally aligned. It achieves this by incorporating and synthesising insight from several globally respected standards and frameworks:

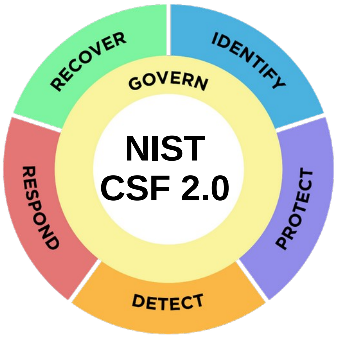
- **NIST CSF 2.0**: Provides the foundational lifecycle structure.
- **ISO/IEC 27001 and 27002**: Offers comprehensive guidance on the establishment, implementation, maintenance, and continual improvement of an ISMS [19].
- **ISA/IEC 62443**: Provides specific guidance relevant to securing IA&CS.
- **CIS CSCs**: Contributes practical, prioritised security actions for defending against current threats.

5.5.3 CyFun and Operational Technology

The CyFun 2025 Framework chose to draw from ISA/IEC 62443 as this series of standards offers a comprehensive and technically detailed standard specifically tailored to IA&CS.

As an internationally recognised and certifiable framework, it aligns best with European regulatory strategies and facilitates harmonisation across sectors and EU member states. This choice supports CyFun’s maturity-based model and enhances its applicability in European industrial contexts.

5.5.4 CyFun Core Structure



GOVERN (GV)	Organisational Context (GV.OC)
	Risk Management Strategy (GV.RM)
	Roles, Responsibilities, and Authorities (GV.RR)
	Policy (GV.PO)
	Oversight (GV.OV)
	Supply Chain (GV.SC)
IDENTIFY (ID)	Asset Management (ID.AM)
	Risk Assessment (ID.RA)
	Improvement (ID.IM)
PROTECT (PT)	Identity Management, Authentication, and Access Control (PR.AA)
	Awareness and Training (PR.AT)
	Data Security (PR.DS)
	Platform Security (PR.PS)
	Technology Infrastructure Resilience (PR.IR)
DETECT (DE)	Continuous Monitoring (DE.CM)
	Adverse Event Analysis (DE.AE)
RESPOND (RS)	Incident Management (RS.MA)
	Incident Analysis (AN)
	Incident Response Reporting and Communication (RS.CO)
	Incident Mitigation (RS.MI)
RECOVER (RC)	Incident Recovery Plan Execution (RC.RP)
	Incident Recovery Communications (RC.CO)

Figure 14: CyFun 2025 Core Structure

The CyFun structure is anchored by the six core functions of the NIST CSF 2.0: *Govern, Identify, Protect, Detect, Respond,* and *Recover*. By adopting this standardised language, the framework fosters seamless communication between technical teams and non-technical leadership, ensuring that cyber risk is integrated into broader business strategy rather than being treated as an isolated IT issue. This alignment allows organisations to move from reactive defence to a mature, risk-informed posture where every department shares a common understanding of security objectives.

To transform these high-level functions into actionable defence, the CyFun 2025 framework maps specific controls directly to each of these six categories. These controls are harmonised from leading international standards, such as ISO/IEC 27001, ISA/IEC 62443 and the CIS CSCs, ensuring that the technical and procedural safeguards an organisation implements are always tethered to a strategic core function. This mapping ensures that every operational task, from identity management to incident recovery, serves a clear purpose within the overarching governance and risk management strategy.

5.5.5 CyFun Assurance Levels

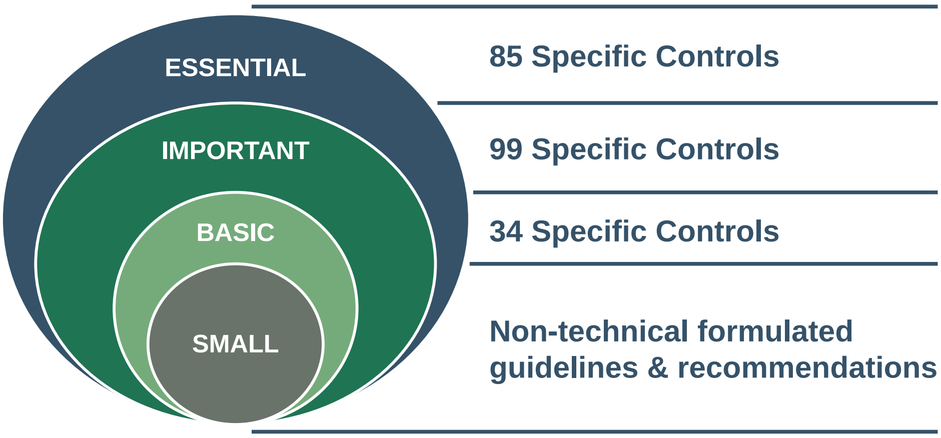


Figure 15: CyFun Assurance Levels

The CyFun 2025 control distribution represents a strategic escalation in defensive depth, designed to meet the rising sophistication of modern threat actors. At the ***BASIC*** level, the framework establishes a foundation of 34 controls centred on essential security hygiene to defend against untargeted, opportunistic attacks. Furthermore, the framework offers a streamlined ***SMALL*** subset of these ***BASIC*** controls, specifically developed to provide micro-enterprises with a high-impact, manageable starting point for their security journey.

As an organisation moves to the ***IMPORTANT*** level, the defensive library expands significantly with 99 additional controls, creating a barrier defence against common targeted threats by integrating deeper governance and technical safeguards.

Finally, the ***ESSENTIAL*** level adds 85 sophisticated controls, focusing on the elite maturity and auditable certification necessary to detect and respond to advanced, high-skilled adversaries. This tiered structure ensures that the volume of controls is highest when moving from basic hygiene to a comprehensive programme, while the final tier shifts the focus toward the extreme precision required for high-level operational resilience.

5.5.6 Self Assessment Tools

The CyFun *Self-Assessment Tools* designed to bridge the gap between high-level frameworks and daily operations by providing organisations with a structured, spreadsheet-based roadmap to evaluate their security posture. The process begins with a *Selection Tool* that helps an organisation determine its appropriate assurance level, ***SMALL***, ***BASIC***, ***IMPORTANT***, or ***ESSENTIAL***, based on its size, sector, and risk profile. Once a level is selected, the primary *Self-Assessment Tool* allows teams to score themselves across the six core functions, assessing both *documentation maturity* (is there a policy?) and *implementation maturity* (is it actually happening?). The tool automatically generates visual spider diagrams, as illustrated in Figure 16, and gap analyses, transforming technical audit data into clear, management-ready reports that highlight exactly where improvements are needed to meet the baseline for digital trust.

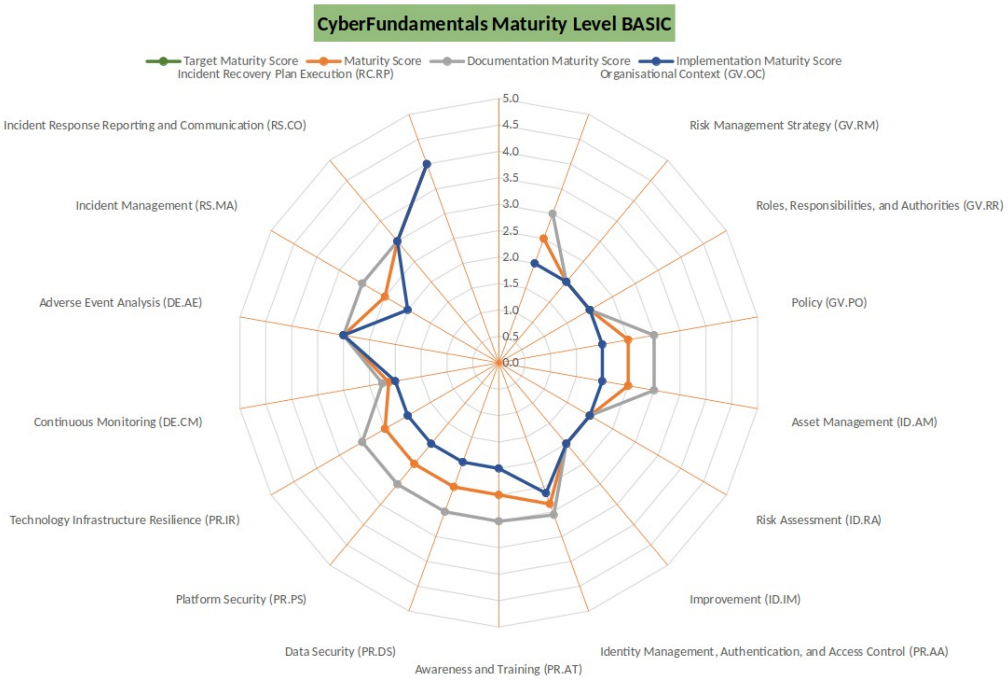


Figure 16: CyFun Self-Assessment Tools

5.5.7 Verification and Certification

CyFun offers a dual-track assurance model where ***BASIC*** and ***IMPORTANT*** levels undergo independent verification to earn a compliance label, while the ***ESSENTIAL*** level requires a formal audit for full certification. These assessments, performed by accredited third-party bodies, Conformity Assessment Bodies (CAB), provide a validated audit trail that organisations can use to demonstrate their cybersecurity maturity and *presumption of conformity* to NIS2 regulators and supply chain partners.

6 Meeting the NIS2 Requirements

Table 11 presents a visualisation of how these frameworks function as a unified defence for a shipping or industrial operation, mapping each standard against the core mandated requirements of the NIS2 Directive.

Table 11: Comparison of Frameworks in the context of NIS2

NIS2 Requirement	NIST CSF 2.0 (Strategy)	ISO/IEC 27001 (Management)	ISA/IEC 62443 (OT/Industrial)	CyFun 2025
Risk Management	🟧 GV & ID High-level risk strategy.	🟩 Cl 6.1.2 Formal ISMS risk process.	🟩 62443-3-2 Detailed OT risk & zone/conduit design.	🟩 Foundational: Mandatory risk register & impact assessments.
Incident Handling	🟧 RS Triage and communication.	🟧 A 5.24 Incident policy & logs.	🟩 62443-2-1 OT-specific emergency response.	🟩 Mandate: Hardwired 24h/72h NCSC-IE reporting workflows.
Business Continuity	🟧 RC Restoring services.	🟩 A 5.29 ICT readiness.	🟩 62443-2-1 IACS continuity & safety recovery.	🟩 Essential: Mandatory disaster recovery testing.
Supply Chain Security	🟩 GV.SC Third-party risk.	🟩 A 5.19 Supplier agreements.	🟩 62443-2-4 Requirements for OT service providers.	🟩 Important+: Nth-party risk mapping in contracts.
System Acquisition/ Maint.	🟧 PR.PS Platform security.	🟩 A 8.25 Secure SDLC.	🟩 62443-4-1 & 4-2 Secure dev & component hardening.	🟩 Technical Pillar: Secure config & patching cycles.
Awareness & Hygiene	🟩 PR.AT Staff outcomes.	🟩 A 6.3 Awareness programmes.	🟧 62443-2-1 Specialised IACS/OT training.	🟩 Foundational: Phishing simulations & basic hygiene.
Access Control	🟩 PR.AA Identity outcomes.	🟩 A 5.15 Logical access.	🟩 62443-3-3 OT least privilege & physical keys.	🟩 Maturity 3+: Strict *Least Privilege* audits.
MFA & Encryption	🟧 PR.IR Data protection.	🟩 A 8.24 Crypto management.	🟩 62443-3-3 Secure comms & remote access MFA.	🟩 Mandatory: Universal MFA for remote access.
Effectiveness Assessment	🟧 GV.OV Oversight.	🟩 Cl 9.1 Internal audit.	🟩 62443-2-1 (4.4.3) Continuous CSMS improvement.	🟩 Verification: Maturity scoring & external audits.

🟩 Green: Excellent alignment; the framework contains the specific language, timelines, or technical depth required by NIS2.

🟧 Amber: Partial alignment; the framework covers the concept but lacks the specific European legal precision (e.g., missing 24h/72h reporting or board liability).

7 What is Next: Cyber Resilience Act

The EU's Cyber Resilience Act (CRA) [20], 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.

7.1 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 like the NIS2 Directive.

Table 12: CRA Conformance by Category

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**

7.2 Product Categories and Assessment Requirements

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

7.2.1 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.

7.2.2 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 CABs, which are independent organisations accredited by Member States to assess product compliance with the CRA.

7.2.3 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 CAB.

7.3 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.

7.4 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.

8 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] 'Cyber Fundamentals 2025 (CyFun)', Cyber Fundamentals. Accessed: Oct. 18, 2025. [Online]. Available: https://cyfun.eu/en/cyfun-2025

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

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

[5] IMO, *International Code for the Security of Ships and Port Facilities (ISPS)*. International Maritime Organisation, 2003.

[6] IMO, *IMO Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3/Rev.3, Apr. 04, 2025. Accessed: Dec. 20, 2025. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.3.pdf

[7] NIST, 'NIST CSWP 29 Cybersecurity Framework 2.0 (CSF2.0)', National Institute of Standards and Technology, NIST CSWP 29, Feb. 2024. Accessed: Mar. 01, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[8] IACS, *IACS UR E27 Cyber resilience of on-board systems and equipment*, UR E27, Apr. 04, 2025.

[9] 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

[10] 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

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

[12] 'CIS Critical Security Controls'. Center for Internet Security. Accessed: Jun. 03, 2025. [Online]. Available: https://www.cisecurity.org/controls/v8-1

[13] *ISO 9001: 2015 Quality management systems — Requirements*, Sep. 2015. Accessed: Sep. 10, 2023. [Online]. Available: https://www.iso.org/standard/62085.html

[14] *ISO 14001: 2015 Environmental management systems — Requirements with guidance for use*, Sep. 2015. Accessed: Sep. 10, 2023. [Online]. Available: https://www.iso.org/standard/60857.html

[15] *ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, Jan. 10, 2022. Accessed: Sep. 10, 2023. [Online]. Available: https://www.iso.org/standard/27001

[16] *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*, Aug. 2019. Accessed: Sep. 10, 2023. [Online]. Available: https://www.iso.org/standard/71670.html

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

[18] 'Risk Management Measures (RMM)'. NCSC-IE, Jun. 04, 2025. Accessed: Oct. 10, 2025. [Online]. Available: https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf

[19] *ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection — Information security controls*, Feb. 2022. Accessed: Sep. 10, 2023. [Online]. Available: https://www.iso.org/standard/75652.html

[20] 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