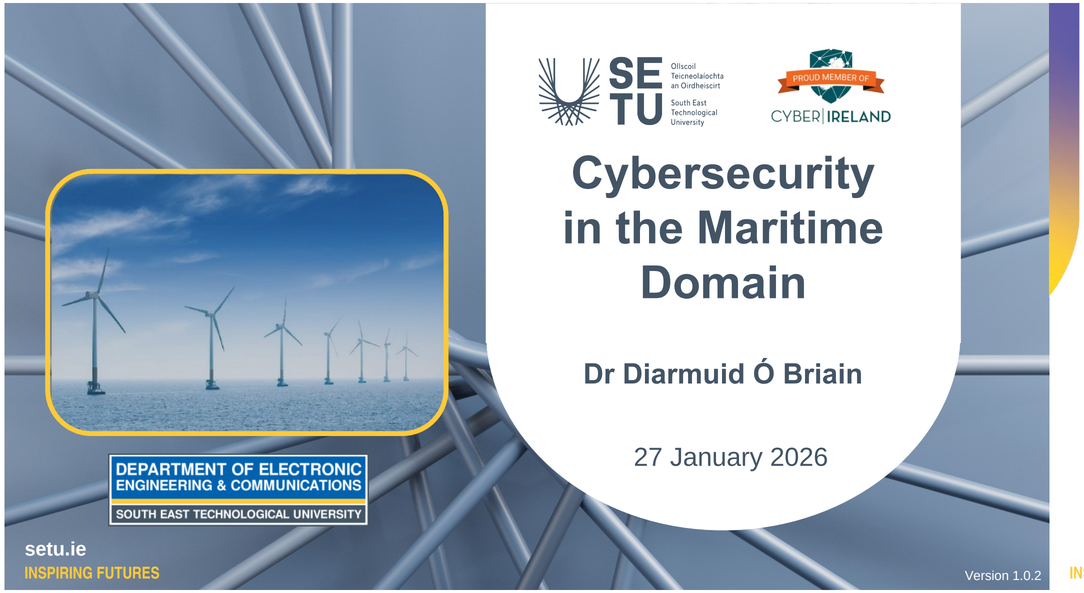


# Cybersecurity in the Maritime Domain

Dr Diarmuid Ó Briain

27 January 2026

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

setu.ie
INSPIRING FUTURES

Version 1.0.2

## Objectives

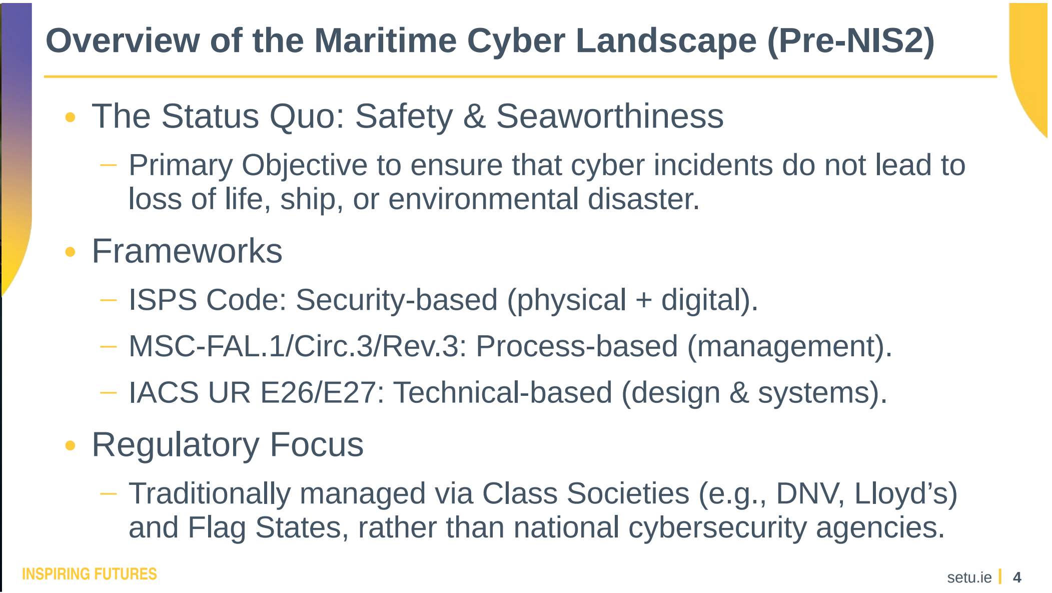
By the end of this workshop, you will be able to:

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

INSPIRING FUTURES

## The Maritime Cyber domain: *The story so far*

INSPIRING FUTURES



## Overview of the Maritime Cyber Landscape (Pre-NIS2)

- The Status Quo: Safety & Seaworthiness
  - Primary Objective to ensure that cyber incidents do not lead to loss of life, ship, or environmental disaster.
- Frameworks
  - ISPS Code: Security-based (physical + digital).
  - MSC-FAL.1/Circ.3/Rev.3: Process-based (management).
  - IACS UR E26/E27: Technical-based (design & systems).
- Regulatory Focus
  - Traditionally managed via Class Societies (e.g., DNV, Lloyd’s) and Flag States, rather than national cybersecurity agencies.

INSPIRING FUTURES

## ISPS Code & MSC-FAL.1/Circ.3/Rev.3

- **The Management Layer**
  - ***International Ship and Port Facility Security (ISPS) Code***:
    - Mandatory under SOLAS. Originally for physical "piracy/terrorism," it now includes cyber as a threat to the Ship Security Plan (SSP).
  - ***MSC-FAL.1/Circ.3/Rev.3: Guidelines on Maritime Cyber Risk Management***
    - Encourages companies to integrate cyber risk into existing Safety Management Systems (SMS).
    - Govern, Identify, Protect, Detect, Respond, and Recover (NIST CSF2.0).
    - Focuses on the "Company" and the "Ship" as a functional unit.

IMO

## IACS UR E26 & UR E27

IACS International Association of Classification Societies

- **The Technical Layer** (Design & Integration)
  - ***UR E26: Cyber Resilience of Ships***
    - Treats the entire ship as a single entity.
    - Requires secure integration of OT and IT during design, construction, and commissioning.
  - ***UR E27: Onboard Systems & Equipment***
    - Focuses on Third-Party Suppliers.
    - Ensures individual components (engines, ECDIS, GPS) are "hardened" by the manufacturer before they ever reach the shipyard.
    - Mandatory for newbuilds contracted after July 1, 2024.

## How the Current Domain Falls Short of NIS2

IMO

Network Information Security 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 (SaaS, remote monitoring). | **Total Supply Chain**: Deep audits of all digital service providers and software vendors. |
| **Governance** | Technical/DPA responsibility. | **C-Suite Liability**: Management is personally liable for cybersecurity failures. |

## Summary – The "Shift" to NIS2

- From "Safety" to "Business Continuity"
  - IMO cares if the ship sinks; NIS2 cares if the supply chain stops.
- Legacy Fleet Problem
  - IACS UR E26/E27 mostly applies to new ships. NIS2 applies to the entire organisation, including older vessels in the fleet, if they operate in EU waters.
- Centralisation
  - Security is moving away from the Ship's Master and into the hands of the National Cybersecurity Centres.

SETU

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

# The Maritime Threat Context

## 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 Operational Technology (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 (OEMs, 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:<br>• *2024 Crowdstrike Incident*: A faulty software update inadvertently crashed around 8.5 million computer systems globally, affecting critical services such as airports.<br>• *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. |

## Cyberattacks on offshore wind

- 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, the threat is higher and more pervasive than ever, but the specific, high-profile incident disclosure rate remains low due to industry practice.

## Cyberattacks on offshore wind

| Company | Date | Attack Type | Impact Overview | Operational Consequence |
|---|---|---|---|---|
| **Vestas** | Nov 2021 | 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** | Feb 2022 | 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** | Apr 2022 | 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** | Mar 2022 | Direct Ransomware | Targeted the German turbine manufacturer's control center. | The company disabled the platform and IT systems. |

# 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 (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. |

# Cyberattacks on other Maritime Infrastructure

| Attack/Incident | Year | Target | Type of Attack | Primary Impact on Operations | Estimated Cost/Scope |
|---|---|---|---|---|---|
| **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 ShipManager software, which is critical for fleet operations. | Impacted the operations of up to 1,000 vessels belonging to 70 customers globally. |

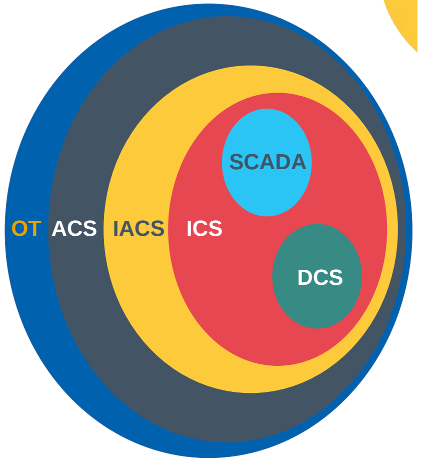
# The Maritime Industry is built on OT

- What is Operational Technology (OT)

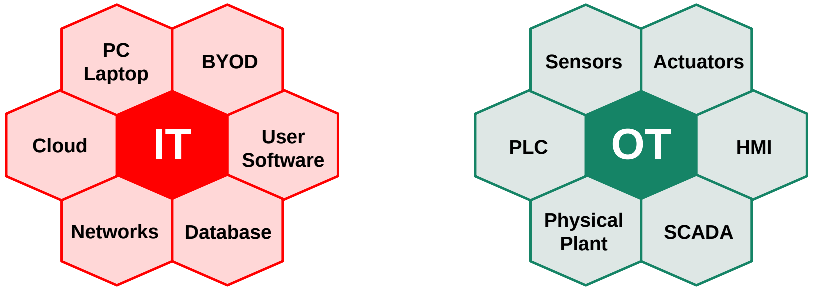
| Feature | IT | OT |
|---|---|---|
| **Primary Function** | Manages data and information (Emails, billing, HR, payroll, logistics scheduling). | Controls and monitors physical processes (Propulsion, steering, cargo cranes, valves). |
| **Where does in exist** | Shore offices, personal devices, and port administrative centers. | **On the Ship**<br>The Bridge and Engine Room.<br>**In the Port**<br>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. |

# Some OT Terms

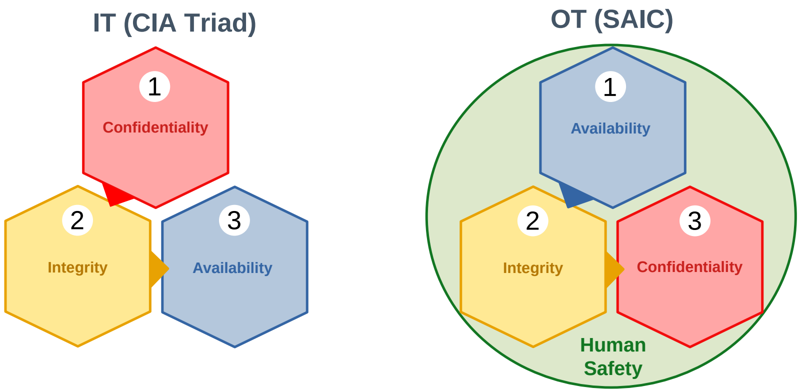
- Operational Technology (OT)
- Automation and Control Systems (ACS)
- Industrial Automation and Control Systems (IACS)
- Industrial Control Systems (ICS)
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control System (DCS)



## Information Technology -v- Operational Technology



## Core IT/OT Priorities



SE TU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University
NIS-2

## EU and Cybersecurity

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

Ref: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

## Three main pillars of NIS2

### Member State Responsibilities

- Competent Authorities
- National Strategies
- CVD Frameworks
- Crisis Management
- Frameworks

**Company Responsibilities**

### Risk Management

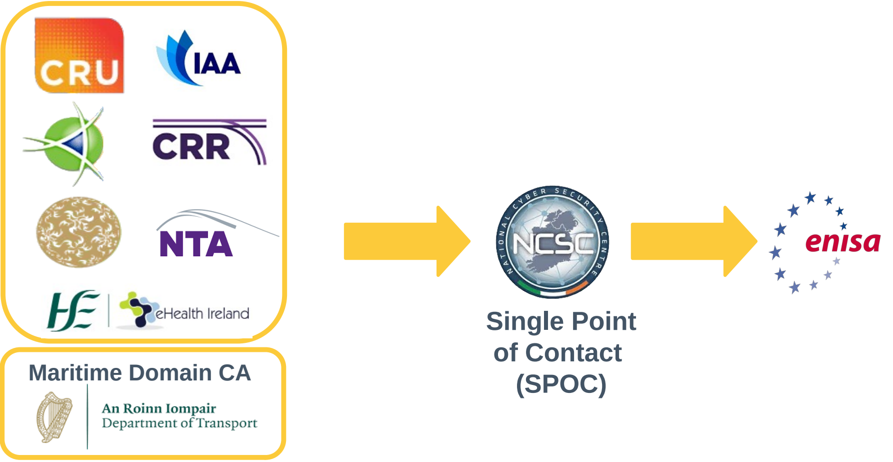
- Accountability for top management for non-compliance
- ESSENTIAL and IMPORTANT companies are required to take security measures
- Companies are required to notify incidents within a given time frame

### Co-operation and Information Exchange

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

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

## Irish Competent Authorities (CA)



Maritime Domain CA

Single Point of Contact (SPOC)

## Entities

**Large Enterprise**

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

**Medium Enterprise**

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

**Small & Micro Enterprise**

- < 50 employees, or
- ≤ €10m revenue

## Entities (Proposed changes 2026)

**Large Enterprise**

- ≥ 750 employees, or
- > €150m revenue

**Small Mid-Cap**

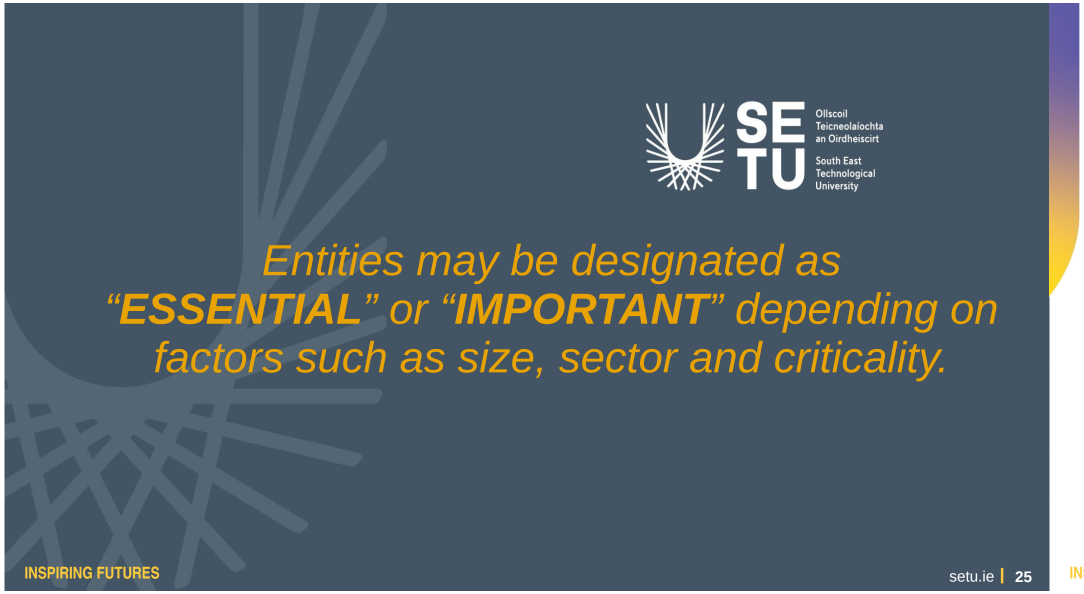
- 250-749 employees, or
- €50-150m revenue

**Medium Enterprise**

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

**Small & Micro Enterprise**

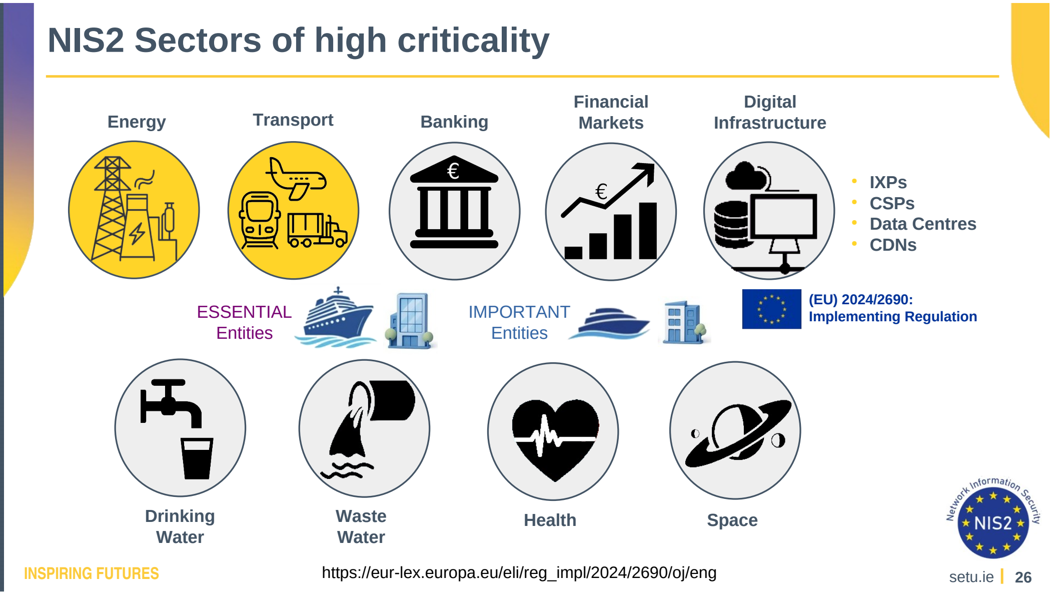
- < 50 employees, or
- ≤ €10m revenue



Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

*Entities may be designated as “**ESSENTIAL**” or “**IMPORTANT**” depending on factors such as size, sector and criticality.*



## NIS2 Sectors of high criticality

Energy

Transport

Banking

Financial Markets

Digital Infrastructure

- IXPs
- CSPs
- Data Centres
- CDNs

ESSENTIAL Entities

IMPORTANT Entities

**(EU) 2024/2690: Implementing Regulation**

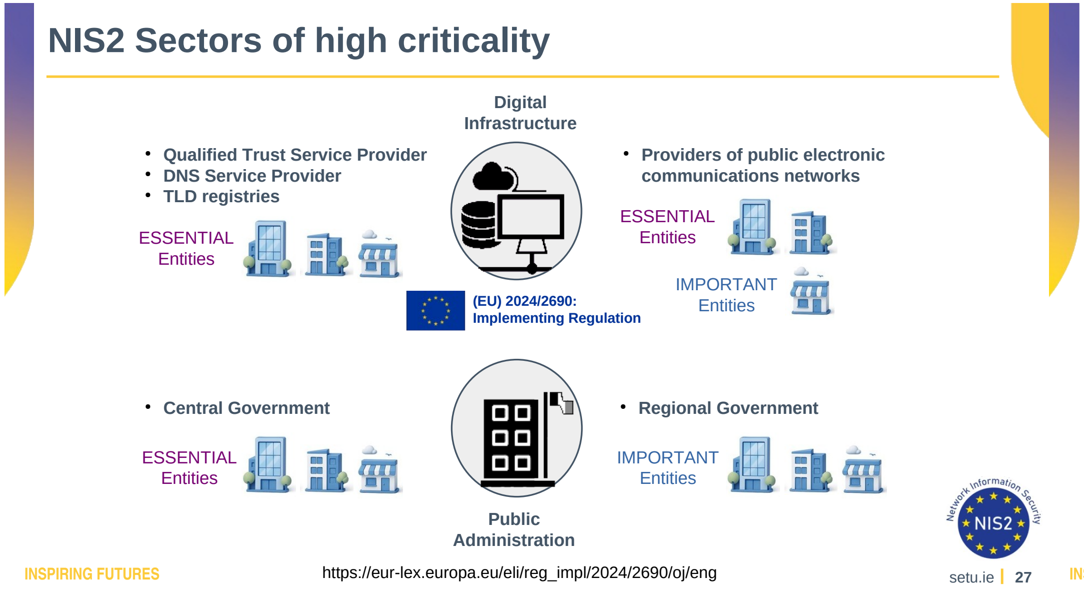
Drinking Water

Waste Water

Health

Space

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



## NIS2 Sectors of high criticality

Digital Infrastructure

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

ESSENTIAL Entities

- Providers of public electronic communications networks

ESSENTIAL Entities

IMPORTANT Entities

**(EU) 2024/2690: Implementing Regulation**

- Central Government

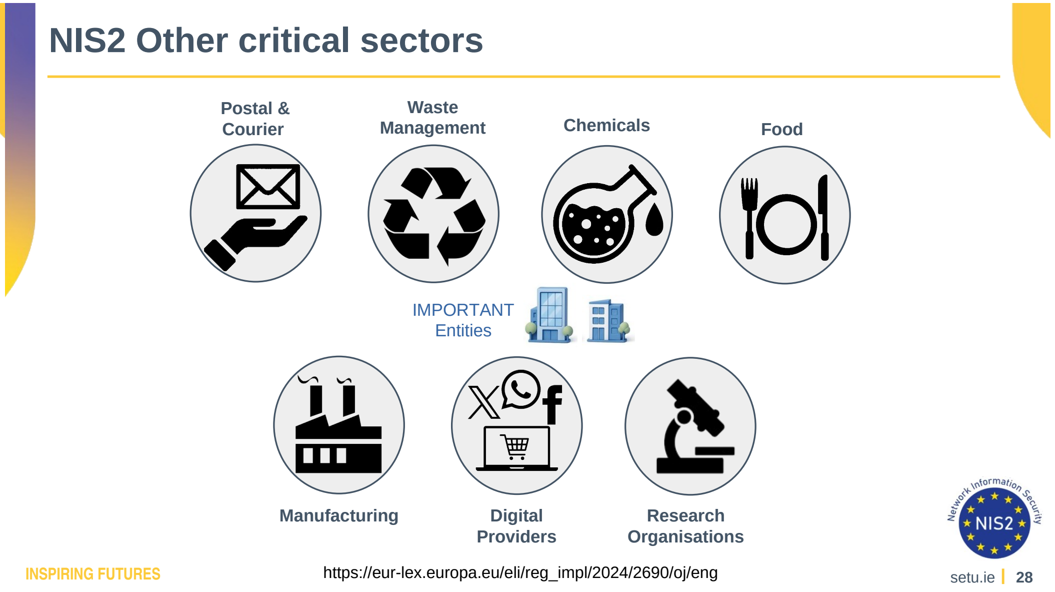
ESSENTIAL Entities

- Regional Government

IMPORTANT Entities

Public Administration

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



## NIS2 Other critical sectors

Postal & Courier

Waste Management

Chemicals

Food

IMPORTANT Entities

Manufacturing

Digital Providers

Research Organisations

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

## Supervision of Entities by NCAs

| ESSENTIAL Entities | IMPORTANT Entities |
|---|---|
| **Ex Ante & Ex Post** | **Ex Post** |
| On-site inspections and off-site supervision | On- & off-site inspections, 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 |
| Ad hoc audits, for example after a significant incident | |

## NIS2 Incident Reporting obligations

| Time | Incident reporting |
|---|---|
| **Within 24 hours** | **Early Warning** should be communicated, as well as some first presumptions regarding the kind of incident |
| **After 72 hours** | **Official Incident Notification** A full notification report must be communicated, containing the assessment of the incident, severity and impact and indicators of compromise. |
| **Upon Request** | **Intermediate Status Report** At the request of CSIRT or relevant competent authority. |
| **After 1 month** | **Final report** must be communicated. |
| **Every 3 months** | Member states CSIRT reports incidents to ENISA. |
| **Every 6 months** | ENISA reports on all incidents EU wide. |

SETU
Ollscoil Teicneolaíochta an Oirdheisceirt
South East Technological University

***ESSENTIAL and IMPORTANT entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems.***

## Cyber Security Risk Management Measures (RMM)

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

## Cyber Security RMMs

All measures must be:

- **Proportionate** to risk, size, cost, and impact & severity of incidents
- Take into account the **state-of-the-art**, and relevant **standards**.

To ensure risk management measures are in place the EU can:

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

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

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

## NIS2 Penalties

- Strict penalties for non-compliance by entities.
- There are particularly high penalties for infringements of:
  - **Article 21 Cybersecurity RMMs**
  - **Article 23 Reporting obligations**
- **ESSENTIAL entities** can be fined up to **€10,000,000** or at least **2%** of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.
- **IMPORTANT entities** can be penalised by fines of up to **€7,000,000** or at least **1.4%** of the total annual worldwide turnover, whichever amount is higher.

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

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

# ***Operationalising Compliance**: Frameworks for OT Security*

*How does my company ensure compliance?*

## Operationalising Compliance

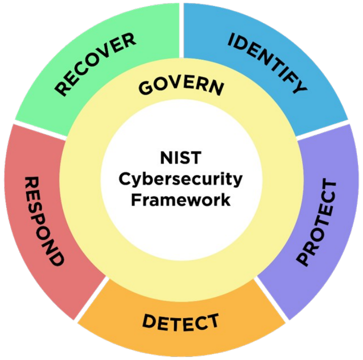
- Risk Management
- Incident Handling
- Business Continuity & Crisis Management
- Supply Chain Security
- Security in System Acquisition, Development, and Maintenance
- Awareness Training & Hygiene
- Access Control
- Multi-Factor Authentication (MFA) & Encryption
- Assessment of Effectiveness

# NIST Cybersecurity Framework (**CSF**) v2.0

## NIST Cybersecurity Framework (CSF) v2.0

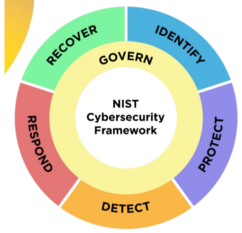
- CSF Functions

| |
|---|
| Govern (GV) |
| Identify (ID) |
| Protect (PR) |
| Detect (DE) |
| Respond (RS) |
| Recover (RC) |



Ref: https://www.nist.gov/cyberframework

## Categories and Sub-categories



| 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 |

SE TU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

CIS

Center for Internet Security

CIS Controls

## Centre for Internet Security (CIS)

- 2008 - collaboration between representatives from the U.S. government and private sector security research organisations.
- Current version 8.1 – Released June 2024
- Prioritised set of safeguards to mitigate the most prevalent cyber-attacks against systems and networks.
- They are considered the gold standard for cybersecurity best practices and are widely used by organisations of all sizes to improve their security posture.

https://www.cisecurity.org/controls

SE TU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University
ISO

ISO

27001

ISMS

## ISO/IEC 27001 – ISMS

- A **strategic cybersecurity framework** that moves security from a technical issue to a boardroom priority via an ISMS.
- It has a **Risk-Based Approach**, focusing defences on critical threats using the 93 Annex A controls, inder the heading of Organisational, People, Physical, and Technological.
- A required **Statement of Applicability (SoA)** provides a customised roadmap justifying which specific security safeguards apply to each environment.
- Through **mandatory documentation** the framework builds a rigorous audit trail through defined policies, risk treatment plans, and evidence of staff competence.
- A cycle of **continuous improvement** ensures the system is never static, evolving through internal audits and management reviews to meet new threats.
- Establishes a **common language** for best practices to build consumer trust and meet international regulatory benchmarks.

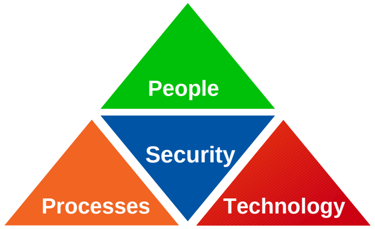
Ref: https://www.iso.org/standard/27001

## ISA/IEC 62443

Cybersecurity for operational technology in automation and control systems

## ISA/IEC 62443 Series of Standards

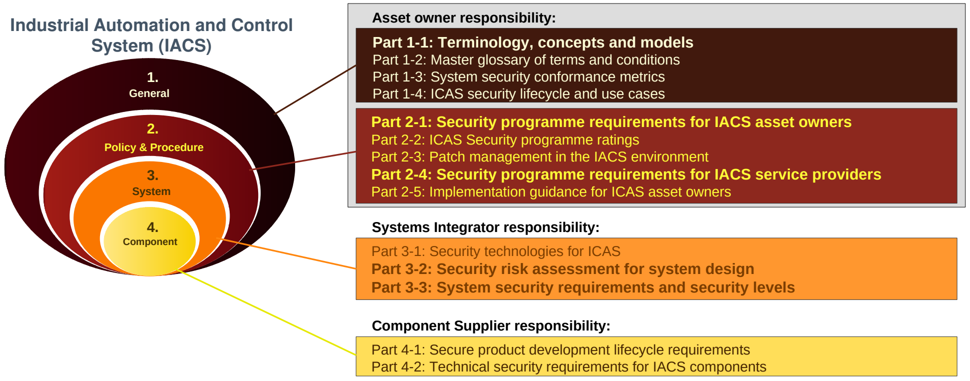
- A series of standards is a comprehensive and internationally recognised framework for securing IACS.
- It provides a holistic approach to cybersecurity, addressing all aspects of IACS security throughout their lifecycle, from design and development to operation and maintenance.



- Core Principles
  - Security by design
  - Security by default
  - Security throughout the lifecycle
  - Security risk management

Ref: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

## ISA/IEC 62443 Series of Standards



Asset owner responsibility:

**Part 1-1: Terminology, concepts and models**
Part 1-2: Master glossary of terms and conditions
Part 1-3: System security conformance metrics
Part 1-4: ICAS security lifecycle and use cases

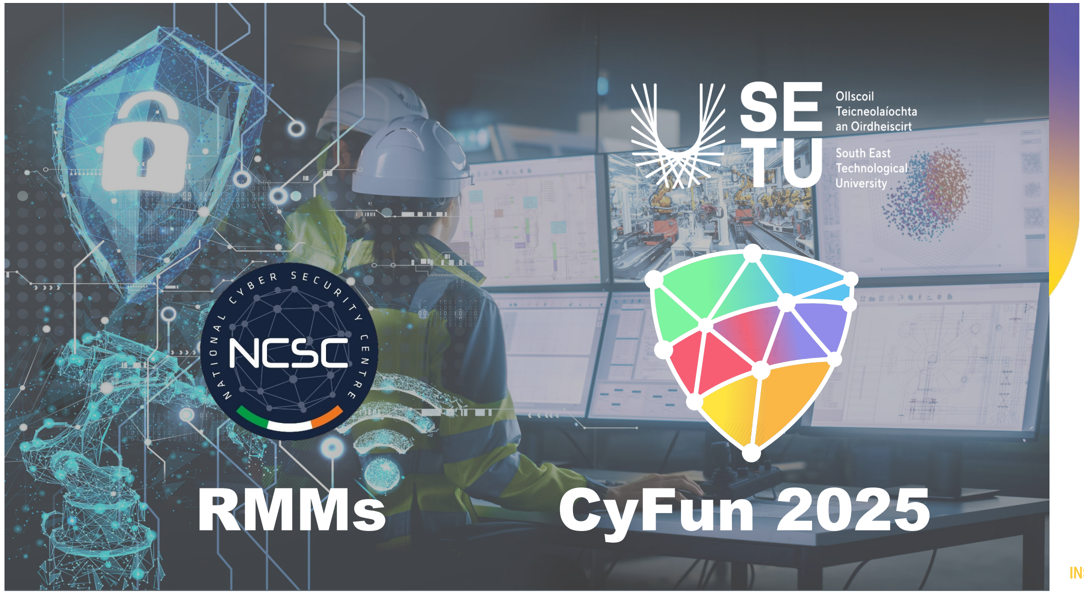
**Part 2-1: Security programme requirements for IACS asset owners**
Part 2-2: ICAS Security programme ratings
Part 2-3: Patch management in the IACS environment
**Part 2-4: Security programme requirements for IACS service providers**
Part 2-5: Implementation guidance for ICAS asset owners

Systems Integrator responsibility:

Part 3-1: Security technologies for ICAS
**Part 3-2: Security risk assessment for system design**
**Part 3-3: System security requirements and security levels**

Component Supplier responsibility:

Part 4-1: Secure product development lifecycle requirements
Part 4-2: Technical security requirements for IACS components



RMMs

CyFun 2025

## Introduction

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

**Risk Management Measures**

CyFun® 2025

## Risk Management Measures (RMM)

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

**Foundational Actions**

**Supporting Actions**

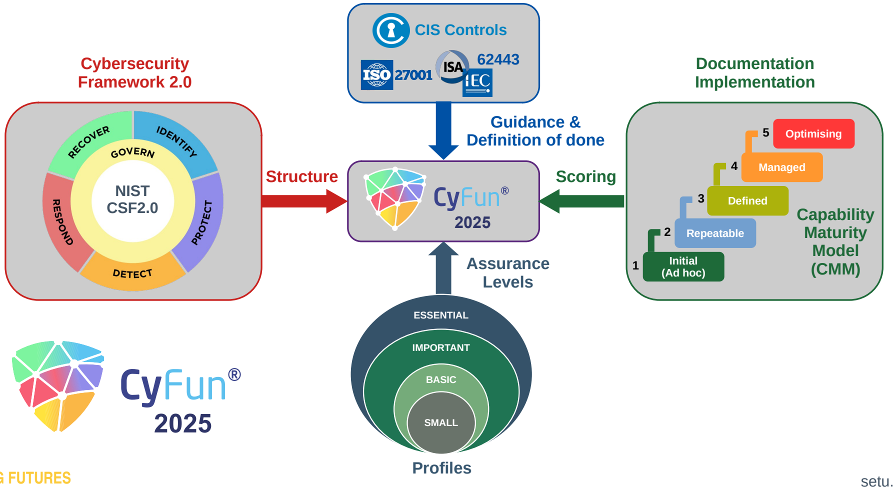
Ref: https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf

## Cyber Fundamentals 2025 (CyFun 2025)

- CyFun 2025 is a powerful, internationally collaborative Framework to elevate organisational cyber resilience.
- Joint International Standard co-owned by the CCB (Belgium) [Primary Scheme Owner], NCSC (Ireland), DNSC (Romania) and MITA (Malta).
- Concrete measures and a clear, step-by-step approach for implementation.
- Helps organisations reduce risk, protect data, and enhance ability to withstand/recover from common cyber-attacks.

CyFun® 2025

## CyFun 2025 Framework



Cybersecurity Framework 2.0

Structure

CIS Controls

Guidance & Definition of done

CyFun® 2025

Scoring

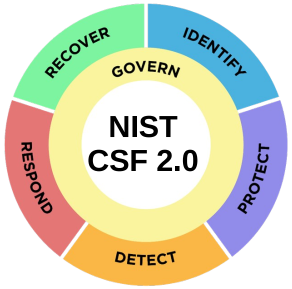
Documentation Implementation

Capability Maturity Model (CMM)

Assurance Levels

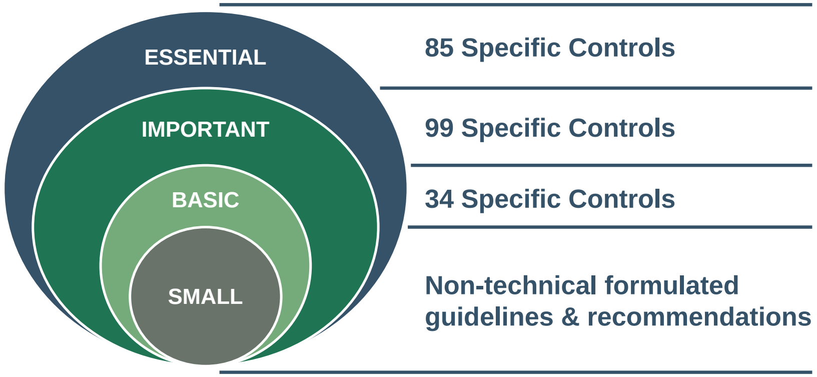
Profiles

## CyFun 2025 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) |

## CyFun 2025 Assurance Levels



ESSENTIAL — 85 Specific Controls

IMPORTANT — 99 Specific Controls

BASIC — 34 Specific Controls

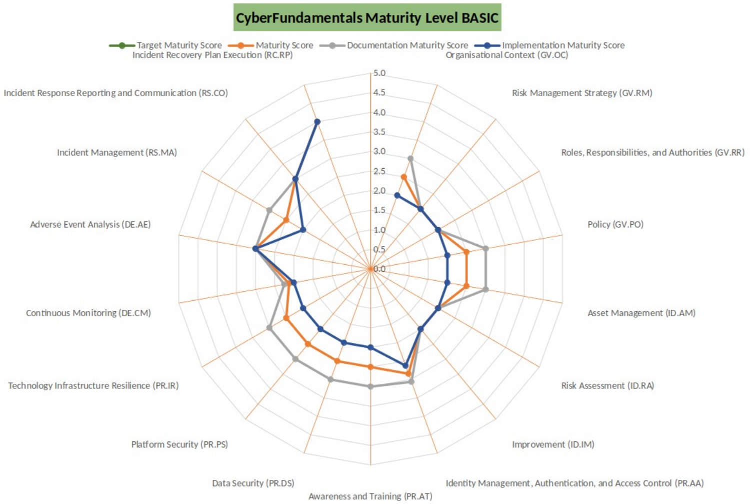
SMALL — Non-technical formulated guidelines & recommendations

Ref: https://cyfun.eu/en/cyfun-2025

## CyFun 2025 Self-Assessment Tools

- Spreadsheet based tools.
- CyFun **BASIC**
  - Outlines the standard information security measures expected for all enterprises.
- CyFun **IMPORTANT**
  - Builds directly upon the foundational security established in CyFun **BASIC**.
  - Introduces enhanced requirements across all six CSF functions to limit the impact of targeted attacks carried out by threat actors with limited resources and skills.
- CyFun **ESSENTIAL**
  - Further strengthens all measures from the **IMPORTANT** to withstand sophisticated cyber-attacks carried out by threat actors with significant resources and expertise.

# A Spider Chart of the category summaries



# CyFun 2025 Verified || Certified

| Term | VERIFIED (CyFun BASIC & IMPORTANT) | CERTIFIED (CyFun ESSENTIAL) |
|---|---|---|
| Meaning | The organisation's implementation of the required security measures has been externally checked and confirmed to meet the CyFun standard for that level. | The organisation has implemented a full CSMS and its continuous operation has been formally audited and approved by a third-party CAB. |
| Focus | **Implementation**: Focuses on whether the required technical and organisational controls are in place (e.g., "Do you have controls on critical systems?"). | **Management System**: Focuses on whether the organisation maintains and continuously improves the controls (e.g., "Do you have policies, evidence, and an audit cycle to ensure controls is always working and documented?"). |
| Assurance Level | **Good assurance**. Suitable for most medium-risk entities. | **Highest assurance**. Required for high-risk, critical entities (like many maritime or offshore operators). |
| Action | Receive a Verification Statement. | Receive a formal Certificate. |

# NIS2 Compliance Heatmap

| NIS2 Requirement | NIST CSF 2.0 | ISO 27001:2022 | ISA/IEC 62443 | CyFun 2025 |
|---|---|---|---|---|
| Risk Management | Strategic | Management | OT-Specific | RMM Match |
| Incident Handling | No Timelines | No Timelines | OT Recovery | 24h/72h Focus |
| Business Continuity | Outcomes | ICT Focus | Safety Focus | All-Hazards |
| Supply Chain Security | New GV.SC | Annex A 5.19 | Part 2-4 | Contractual |
| System Acq/Maint. | High-level | SDLC Focus | Hardening | Patch Mandates |
| Awareness & Hygiene | Strong PR.AT | Annex A 6.3 | Only OT | Hygiene Focus |
| Access Control | Strong PR.AA | Annex A 5.15 | OT Physical | Least Privilege |
| MFA & Encryption | Goal-based | Annex A 8.24 | Part 3-3 | MFA Mandate |
| Effectiveness Assess. | No Audit | Certification | Maturity SL | Verification |

# When to Choose CyFun 2025 over ISA/IEC 62443

- When the priority is speed, compliance, and foundational maturity:
  - **NIS2 Compliance is Mandated**: If organisation is an IMPORTANT or ESSENTIAL Entity under the NIS2 Directive and operates in a country that officially recognises CyFun as a clear path to compliance.
  - **Establishing a Baseline**: A simple, tiered roadmap to quickly raise the organisation's cybersecurity maturity from a low level without overwhelming limited staff or resources.
  - **Executive Buy-in and Reporting**: A framework is required that is easy to communicate to non-technical management using clear assurance levels and quantifiable metrics.
  - **Integrating IT and OT**: A framework that addresses organisational fundamentals holistically across both IT and OT management functions, rather than solely focusing on the deep technical aspects of the control systems.

## When to Choose ISA/IEC 62443 over CyFun 2025

- Priority is deep technical security and supply chain rigour:
  - **New System Design (Greenfield)**: When designing a brand-new IACS/OT network and need the detailed, prescriptive requirements for Zones and Conduits, secure architecture, and component Security Levels (SL).
  - **Vendor/Supply Chain Requirements**: Original Equipment Manufacturer (OEM), System Integrator, or Component Supplier and must adhere to specific technical standards (such as 62443-4-1 for secure product development) to sell components into the global OT market.
  - **Detailed Risk Assessment**: Risk assessment requires the granularity and depth of the ISA/IEC 62443 risk assessment process (62443-3-2) to determine the necessary Target Security Levels for high-risk, mission-critical equipment.
  - **Global Standard and Certification**: Require an internationally recognised, vendor-neutral standard that is universally accepted in regulatory and procurement contracts worldwide.

## What's next from EU

## Cyber Resilience Act (CRA)

- The CRA is a baseline cybersecurity standard for digital products sold in the EU, aiming to reduce vulnerabilities and cyber incidents.
- Products are categorised by risk level, dictating their conformity assessment requirements.
  - Entry into force: 10 Dec 2024.
  - Full enforcement: 11 Dec 2027.
  - Reporting obligations: 11 Sept 2026.

## Cyber Resilience Act (CRA)

| Category | Default "Unclassified" | Important "Class I" | Important "Class II" | Critical Products |
|---|---|---|---|---|
| **Examples** | Smart speakers, games, photo editing software, hard drives, mobile and desktops apps and everything else | IAM/PAM, OS, wearables, smart home, password managers, network management systems, microcontrollers, VPN, SIEM, anti-virus | Hypervisors & container runtimes, firewalls, Intrusion Detection / or Prevention, Tamper-resistant microprocessors & microcontrollers | Smart meter gateways smartcards or similar devices, including secure elements Hardware Security Modules |
| **Conformance** | **Self Assessment** | **Harmonised Standards** | **Third party assessment** | **EUCC** |

## Cyber Resilience Act (CRA) penalties

Non-compliance in relation to:

- **Product security and vulnerability handling**
  - Up to **€15,000,000 or 2.5%** of the total worldwide annual turnover, whichever is higher.
- **Documentation or reporting requirements**
  - Up to **€10,000,000 or 2%** of the total worldwide annual turnover, whichever is higher.
- Provision of **incorrect, incomplete, or misleading information** to notified bodies and surveillance authorities
  - Up to **€5,000,000 or 1%** of the total worldwide annual turnover, whichever is higher.

## Exercise #4
## Wind of Change Offshore Wind Farm (WOC)

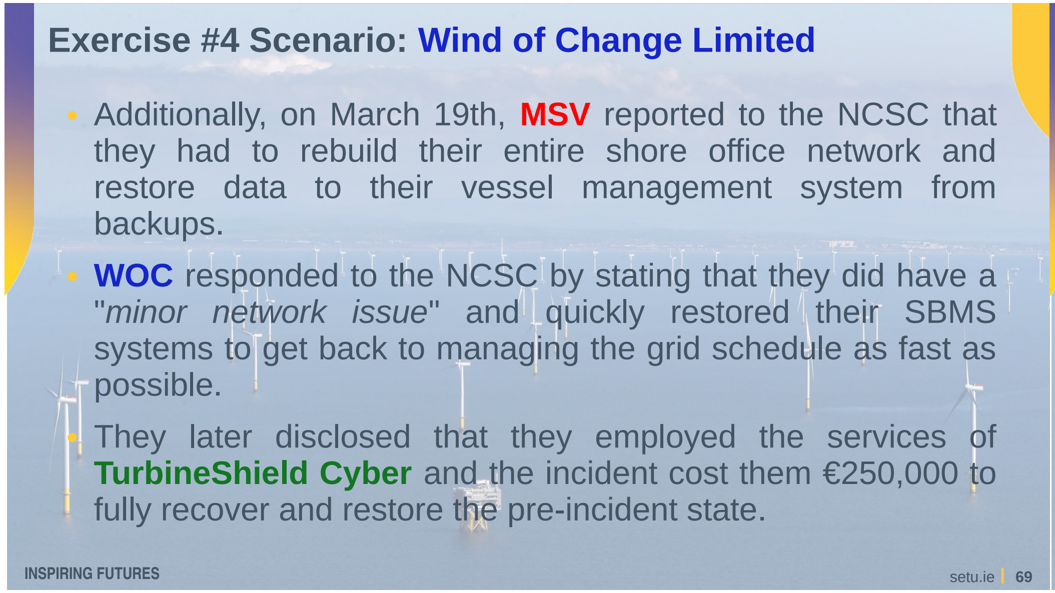
SETU
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

## Exercise #4 Scenario: Wind of Change Limited

- **Wind of Change Offshore Wind Farm (WOC)**, a major energy producer based in Ireland, was hit with a ransomware attack on Saint Patrick's Day (March 17th).
- The attack encrypted their Shore-Based Management System (SBMS), crippling all remote monitoring, performance tracking, and maintenance scheduling for their offshore turbines.

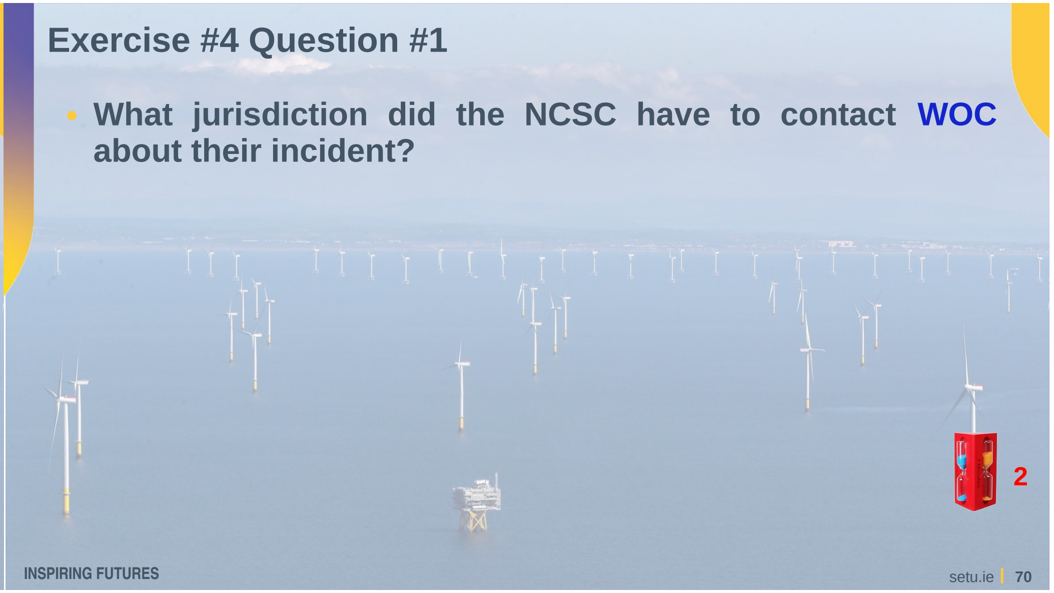
## Exercise #4 Scenario: Wind of Change Limited

- On April 1st, WOC was contacted by an officer of the National Cyber Security Centre (NCSC) who stated that **Maritime Service Vessels Ltd. (MSV)**, a key vessel operator responsible for ferrying technicians and parts, had suffered an attack and reported it on March 18th.
- In their report, the CTO of **MSV** stated they believe the attack came through a VPN they utilise for securely downloading daily work orders and vessel routes from **WOC**'s SBMS.



## Exercise #4 Scenario: Wind of Change Limited

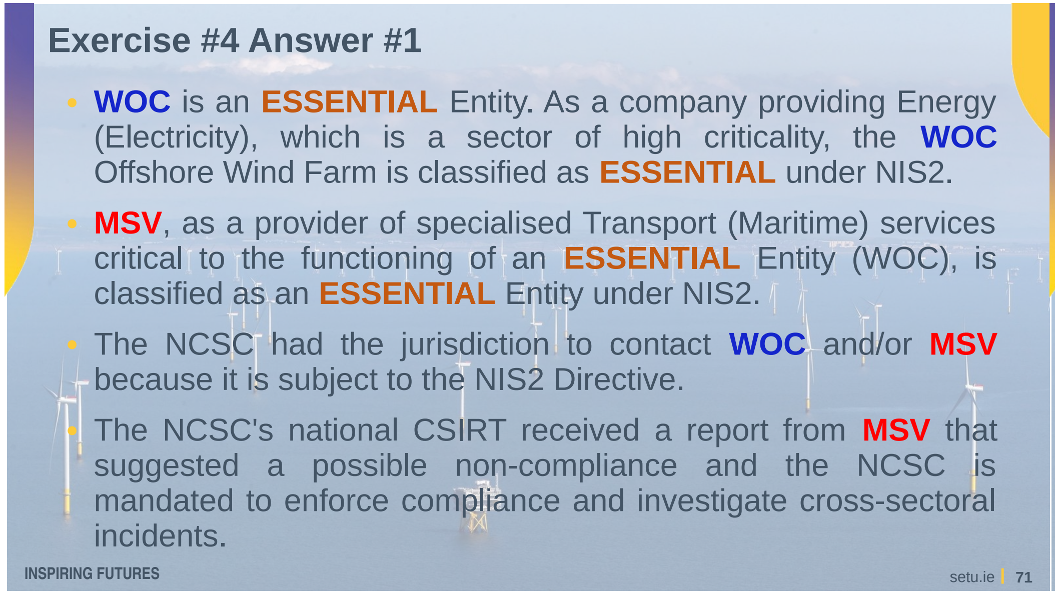
- Additionally, on March 19th, **MSV** reported to the NCSC that they had to rebuild their entire shore office network and restore data to their vessel management system from backups.
- **WOC** responded to the NCSC by stating that they did have a "*minor network issue*" and quickly restored their SBMS systems to get back to managing the grid schedule as fast as possible.
- They later disclosed that they employed the services of **TurbineShield Cyber** and the incident cost them €250,000 to fully recover and restore the pre-incident state.



## Exercise #4 Question #1

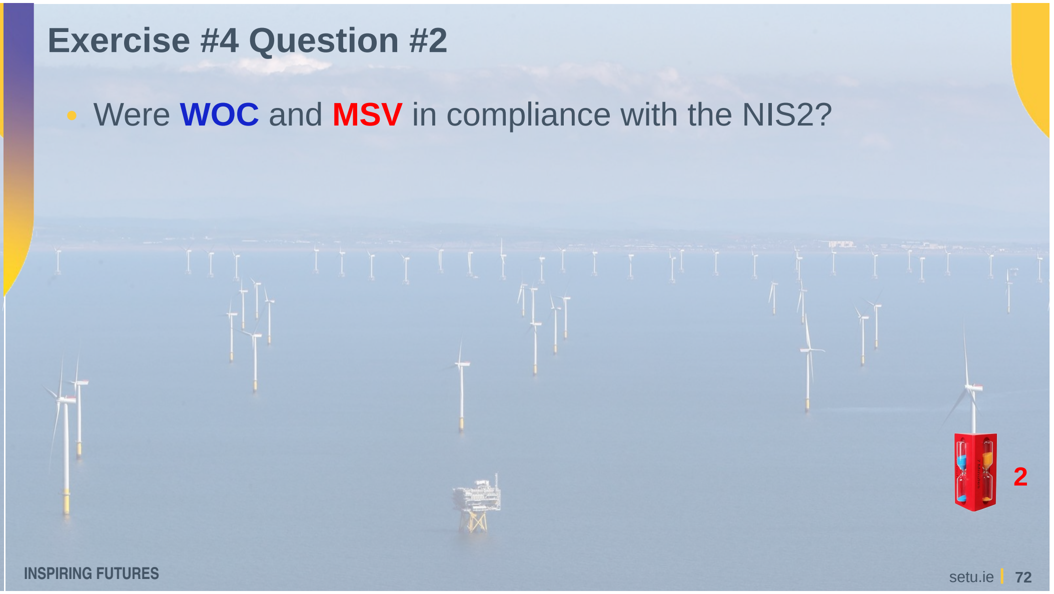
- **What jurisdiction did the NCSC have to contact WOC about their incident?**

2



## Exercise #4 Answer #1

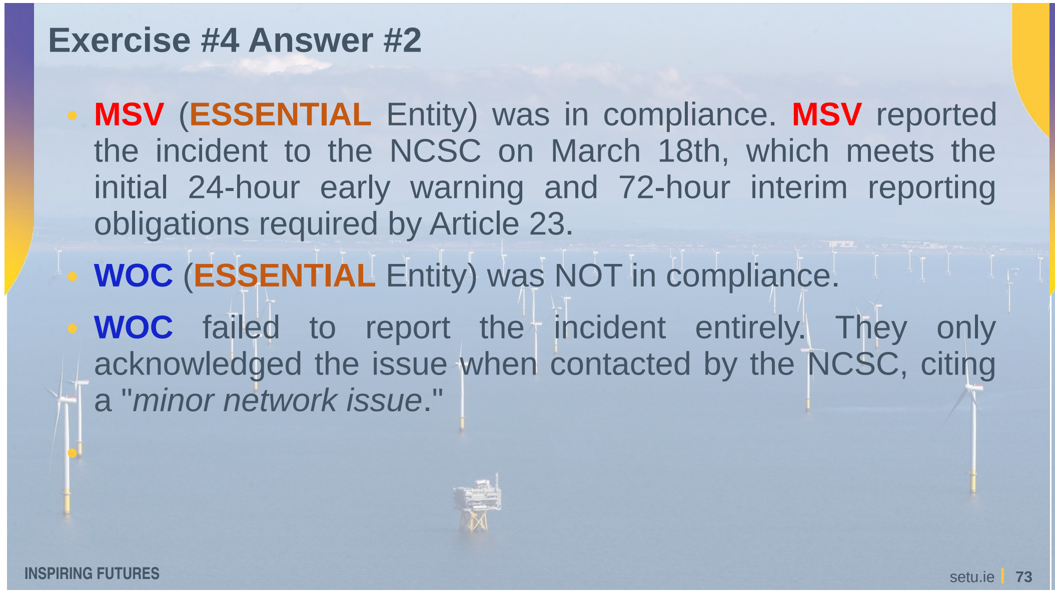
- **WOC** is an **ESSENTIAL** Entity. As a company providing Energy (Electricity), which is a sector of high criticality, the **WOC** Offshore Wind Farm is classified as **ESSENTIAL** under NIS2.
- **MSV**, as a provider of specialised Transport (Maritime) services critical to the functioning of an **ESSENTIAL** Entity (WOC), is classified as an **ESSENTIAL** Entity under NIS2.
- The NCSC had the jurisdiction to contact **WOC** and/or **MSV** because it is subject to the NIS2 Directive.
- The NCSC's national CSIRT received a report from **MSV** that suggested a possible non-compliance and the NCSC is mandated to enforce compliance and investigate cross-sectoral incidents.



## Exercise #4 Question #2

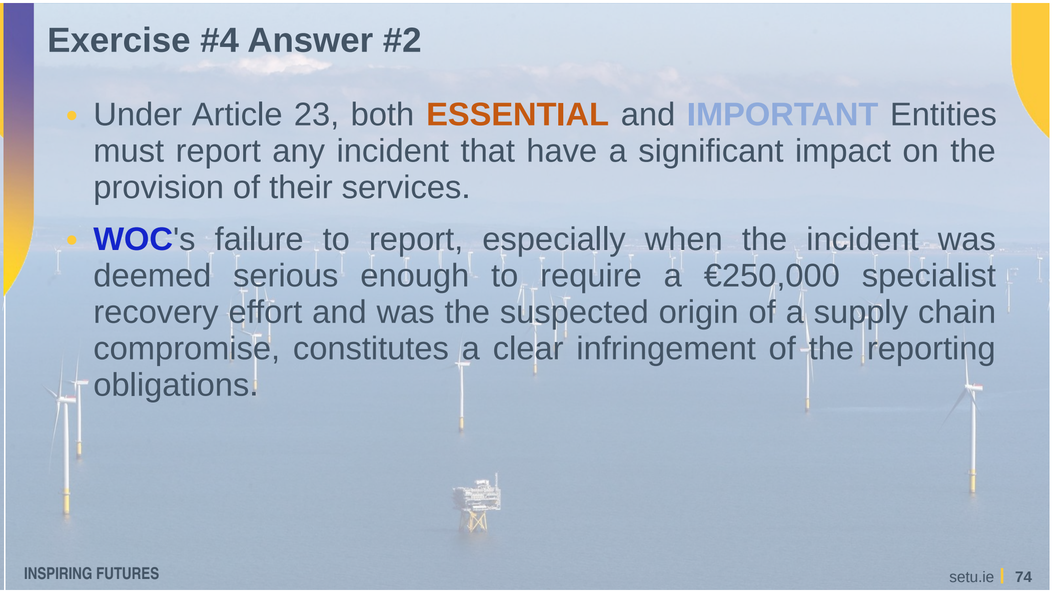
- Were **WOC** and **MSV** in compliance with the NIS2?

2



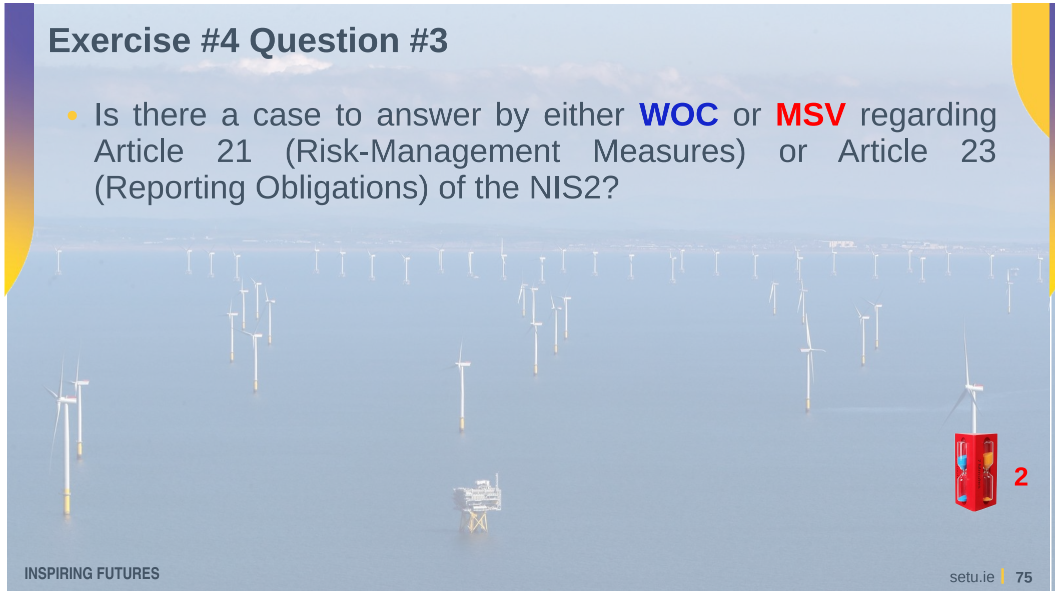
## Exercise #4 Answer #2

- **MSV** (**ESSENTIAL** Entity) was in compliance. **MSV** reported the incident to the NCSC on March 18th, which meets the initial 24-hour early warning and 72-hour interim reporting obligations required by Article 23.
- **WOC** (**ESSENTIAL** Entity) was NOT in compliance.
- **WOC** failed to report the incident entirely. They only acknowledged the issue when contacted by the NCSC, citing a "*minor network issue*."



## Exercise #4 Answer #2

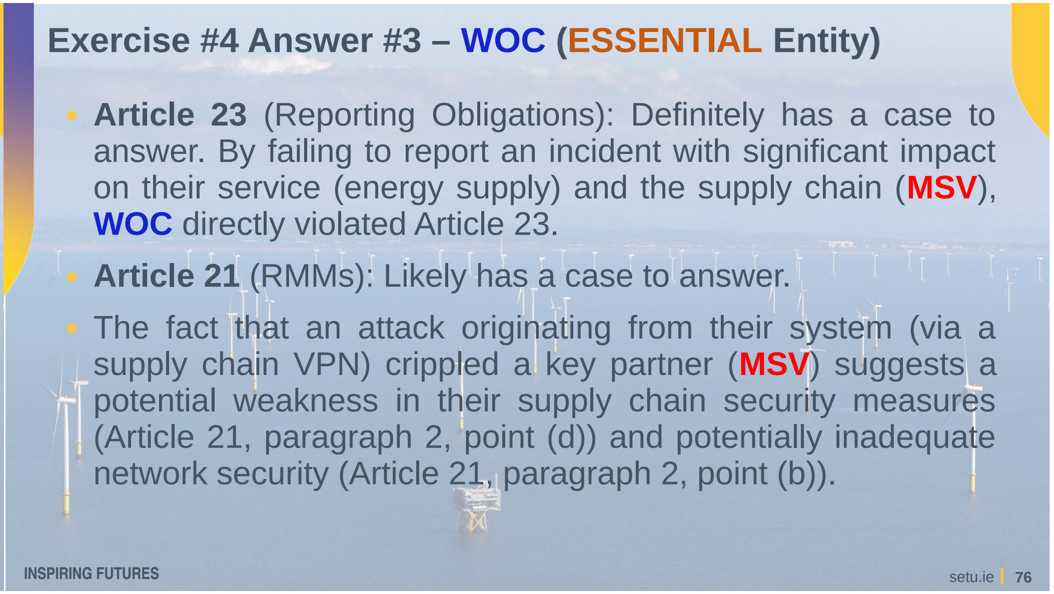
- Under Article 23, both **ESSENTIAL** and **IMPORTANT** Entities must report any incident that have a significant impact on the provision of their services.
- **WOC**'s failure to report, especially when the incident was deemed serious enough to require a €250,000 specialist recovery effort and was the suspected origin of a supply chain compromise, constitutes a clear infringement of the reporting obligations.



## Exercise #4 Question #3

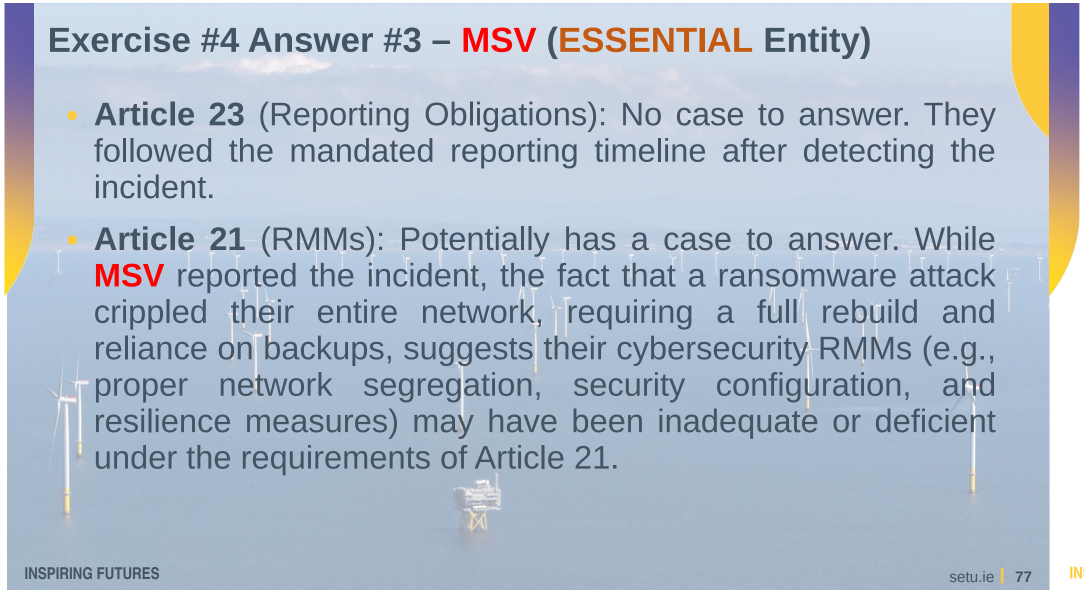
- Is there a case to answer by either **WOC** or **MSV** regarding Article 21 (Risk-Management Measures) or Article 23 (Reporting Obligations) of the NIS2?

2



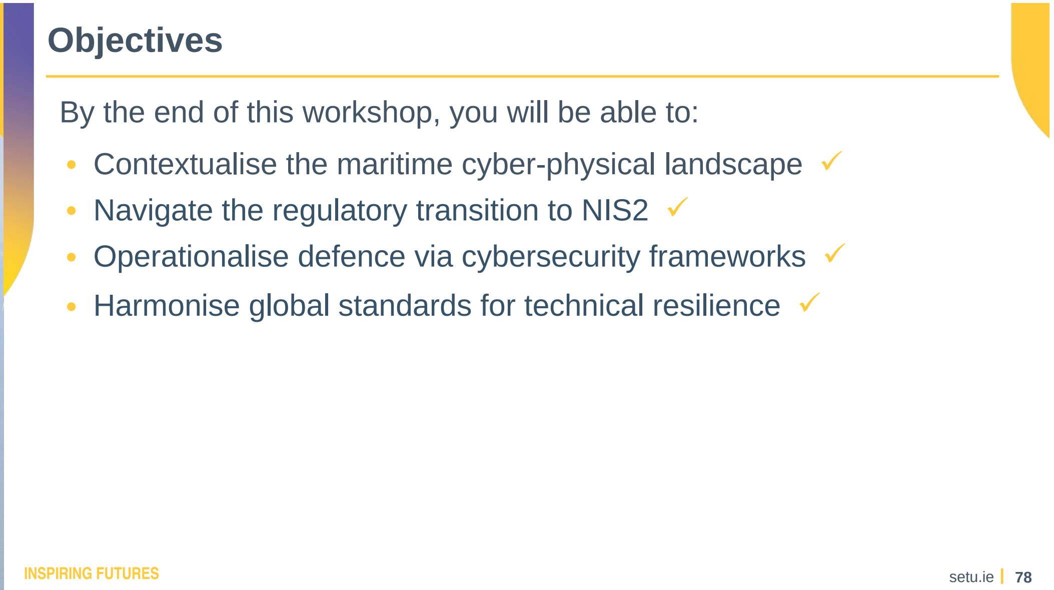
## Exercise #4 Answer #3 – WOC (ESSENTIAL Entity)

- **Article 23** (Reporting Obligations): Definitely has a case to answer. By failing to report an incident with significant impact on their service (energy supply) and the supply chain (**MSV**), **WOC** directly violated Article 23.
- **Article 21** (RMMs): Likely has a case to answer.
- The fact that an attack originating from their system (via a supply chain VPN) crippled a key partner (**MSV**) suggests a potential weakness in their supply chain security measures (Article 21, paragraph 2, point (d)) and potentially inadequate network security (Article 21, paragraph 2, point (b)).



## Exercise #4 Answer #3 – MSV (ESSENTIAL Entity)

- **Article 23** (Reporting Obligations): No case to answer. They followed the mandated reporting timeline after detecting the incident.
- **Article 21** (RMMs): Potentially has a case to answer. While **MSV** reported the incident, the fact that a ransomware attack crippled their entire network, requiring a full rebuild and reliance on backups, suggests their cybersecurity RMMs (e.g., proper network segregation, security configuration, and resilience measures) may have been inadequate or deficient under the requirements of Article 21.



## 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 ✓

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach
D +353 59 917 5000 | E diarmuid.obriain@setu.ie | setu.ie
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Thank you

engcore
advancing technology