engineering the south east
South East Automation Group

SETU Ollscoil Teicneolaíochta an Oirdheiscirt / South East Technological University

NIS2

CRA Cyber Resilience Act

**Dr Diarmuid Ó Briain**

**24 February 2026**

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY



setu.ie
INSPIRING FUTURES

Version: 3.0

## The EU Cybersecurity Response

- **Unified Defence for a Common Market**
  - Incidents in one state threaten the entire common market.
  - **NIS2**: Sets a high baseline for infrastructure security & resilience.
    - Scope 10 high-critical + 7 other critical sectors.
  - **CRA**: Security-by-Design for digital products & software.
    - Mandatory CE marking for cyber-secure hardware.
  - Shared Goal to eliminate "weak links" in both operations and supply chains.



engineering the south east

SETU Ollscoil Teicneolaíochta an Oirdheiscirt / South East Technological University

*NIS2 Directive (EU 2022/2555) seeks to further enhance the work started in the NIS Directive (EU 2016/1148) to build a high common level of cybersecurity across the EU.*

setu.ie
INSPIRING FUTURES

## Irish Competent Authorities

**NCAs**

CRU
IAA
CRR
NTA
HSE | eHealth Ireland
An Roinn Iompair / Department of Transport

**SPOC**

NCSC

enisa

engineering the south east

SETU 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.*

setu.ie
INSPIRING FUTURES

## Entities

| | |
|---|---|
| Large Enterprise | • >= 250 employees, or<br>• > €50m revenue |
| Medium Enterprise | • 50-249 employees, or<br>• > €10m revenue |
| Small & Micro Enterprise | • < 50 employees |

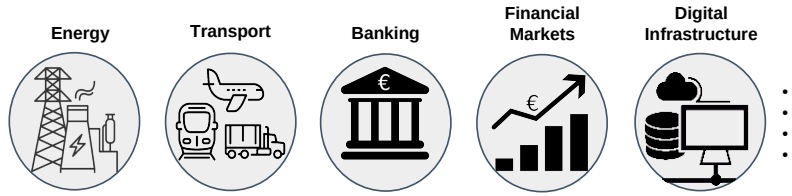


## Entities (Proposed changes 2026)

| | |
|---|---|
| Large Enterprise | • ≥ 750 employees, or<br>• > €150m revenue |
| Small Mid-Cap | • 250-749 employees, or<br>• €50-150m revenue |
| Medium Enterprise | • 50-249 employees, or<br>• €10-50m revenue |
| Small & Micro Enterprise | • < 50 employees, or<br>• ≤ €10m revenue |



## NIS2 Sectors of high criticality



## 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

- **Central Government**

Essential Entities

**Public Administration**

- **Regional Government**

Important Entities



## NIS2 Other critical sectors

**Postal & Courier**

**Waste Management**

**Chemicals**

**Food**

Important Entities

**Manufacturing**

**Digital Providers**

**Research Organisations**



engineering the south east

SETU Ollscoil Teicneolaíochta an Oirdheisceart 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.*



## Supervision of Entities by NCAs

- **Essential Entities (Ex-Ante)**
  - High-criticality sectors (e.g., Energy, Health) face proactive supervision, where authorities conduct regular audits and inspections to verify compliance before any incident occurs.
- **Important Entities (Ex-Post)**
  - Other critical sectors (e.g., Food, Manufacturing) are subject to reactive supervision, meaning authorities typically only investigate or take enforcement action after evidence of a breach or non-compliance surfaces.

## 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 (NCSC) reports incidents to ENISA. |
| **Every 6 months** | ENISA reports on all incidents EU wide. |



engineering the south east

SETU 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 risk-management measures**
  - **Article 23 Reporting obligations**
- Essential entities can be fined up to **€10,000,000** or at least **2%** of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher.
- Important entities can be penalised by fines of up to **€7,000,000** or at least **1.4%** of the total annual worldwide turnover, whichever amount is higher.



engineering the south east

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

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

setu.ie
INSPIRING FUTURES

## NIS2 Penalties

Management bodies of Essential and Important entities must:

- **Approve** cybersecurity risk management measures.
- **Oversee** implementation of these measures.
- **Undergo** cybersecurity training to assess risks and their impact.
- **Provide** regular cybersecurity training for employees.
- **Be accountable** for non-compliance.



engineering the south east

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

*How does my company or organisation ensure compliance?*






## ISO/IEC 27001 – ISMS

ISO IEC 27001

- Boardroom Priority elevates security to a strategic ISMS.
- Risk-Based, target threats using 93 Annex-A controls.
- Statement of Applicability (SoA) justifies each control.
- Mandatory documentation creates a rigorous trail for audit.
- Continuous Improvement via audits and management reviews.
- Build trust and meet regulatory benchmarks.

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




## ISA/IEC 62443 Security for IACS

- Comprehensive framework for IACS/OT environments.
- Operational focus prioritises safety, performance, and legacy systems.
- Systematic risk management of cybersecurity via robust security programmes.
- NIS2 aligned through the mapping of risk, policy, and incidents.
- Enhanced uptime against industrial cyber threats.
- Technical Compliance vital for "Security by Design" requirements.

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




## Risk Management Measures (RMM)

| | | | |
|---|---|---|---|
| **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 |

**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



## Alignment with NIS2 Requirements: Manufacturing

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



## Integrating Cybersecurity Standards for NIS2

- Comparison Summary for Automation

| Standard | Focus Area | Manufacturing Role |
|---|---|---|
| ISO 27001 | Management | Enterprise Governance & Policies |
| IEC 62443 | Technology | OT Machine & Network Security |
| CyFun 2025 | Compliance | Fast-track Audit for EU Regulators |

ISO 27001 ISA IEC 62443 CyFun® 2025



SETU Oliscoil Teicneolaíochta an Oirdheiscirt South East Technological University

CRA Cyber Resilience Act

setu.ie
INSPIRING FUTURES

## Cyber Resilience Act (CRA) Objectives

- Address the low level of cybersecurity in digital products and the insufficient information available to consumers.
- It is the first EU-wide legislation to impose mandatory cybersecurity requirements on **Products with Digital Elements (PDE)**.
- Key Objectives:
  - Reduce vulnerabilities throughout the product lifecycle.
  - Ensure "Secure by Design" and "Secure by Default" principles.
  - Empower users with transparent security information via CE Marking.



## CRA Implementation Timeline

- **Dec 10, 2024**: Act officially entered into force.
- **Sept 11, 2026**: **Early Deadline**: Mandatory incident and vulnerability reporting begins.
- **Dec 11, 2027: Full Enforcement**: All products must meet essential requirements and carry the CE mark to stay on the market.
- Manufacturers given a 3-year grace period for technical compliance, but only 21 months for reporting setup.



## CRA Scope

- Any software or hardware product with a direct or indirect data connection to a device or network.
  - Examples: Smart home devices, wearables, routers, OS, and B2B software.
- Explicit Exclusions:
  - Sector-Specific: Medical devices, Motor vehicles, Aviation (already regulated).
  - Services: Most SaaS (covered by NIS2).
  - Open Source: Non-commercial open-source software is generally excluded.



## CRA Product Categorisation (The Risk Matrix)

- CRA uses a risk-based approach to determine how a product is certified.

| 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** |

## CRA Mandatory Security Requirements

- Manufacturers must demonstrate:
  - **Secure by Design**: Minimal attack surface and encryption by default.
  - **Vulnerability Management**:
    - Mandatory Software Bill of Materials (SBOM).
    - Free security updates for the "support period" (typically 5 years).
  - **Transparency**: Clear documentation on how to decommission products and where to find patches.
  - **Reporting**: Notify ENISA of ***actively exploited*** vulnerabilities within 24 hours.



## CRA Enforcement and Penalties

- Non-compliance carries heavy financial and operational risks:
  - **Security Breaches**: Up to €15M or 2.5% of global turnover.
  - **Reporting Failures**: Up to €10M or 2% of global turnover.
  - **Deceptive Information**: Up to €5M or 1% of global turnover.
  - **Market Sanctions**
    - Authorities can order product recalls or ban sales across the entire EU.



## CRA Summary and Next Steps

- Audit Your Portfolio
  - Determine which of your products fall into Class I, II, or Critical.
- Update Contracts
  - Ensure third-party components (libraries/hardware) are CRA-compliant.



SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

**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

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

# Thank you

engcore
advancing technology