Kilkenny Chamber Cybersecurity Event

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Navigating the EU cyber landscape, regulatory expectations and operational risk

Dr Diarmuid Ó Briain

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

23 September 2026

Regulatory Context

Regulatory Context

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Network and Information Systems v2 (NIS2) *(Directive (EU) 2022/2555) addresses the* ***risks of a fragmented market and cross-border Critical National Infrastructure incidents*** *by encompassing ten sectors of high criticality and seven other critical services, ensuring a unified and enhanced common level of cybersecurity across the EU.*

Regulatory Context

Critical Entities Resilience

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

*CER (Directive (EU) 2022/2557) seeks to strengthen the **physical and operational resilience of essential services** across the EU, ensuring they can withstand and recover from all-hazards, including natural, human-made, and hybrid threats, to maintain vital societal and economic functions.*

Regulatory Context

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

CRA (Regulation (EU) 2024/2847) establishes ***mandatory security requirements for all products with digital elements*** *across the EU, ensuring they are designed, developed, and maintained securely throughout their lifecycle to protect critical infrastructure and consumers from cyber threats and systemic digital vulnerabilities.*

NIS2, CRA & CER Directives

Law	EU Directive Cyber Security Bill 2024	EU Regulation (EU) 2024/2847	EU Directive S.I. No. 559
Focus Area	Entity Cyber Security	Physical Resilience	Product Security
Objective	Organisational cyber-risk management.	All-hazards operational continuity.	Secure-by-design hardware/software.
Organisation Role	**Operations**: Implement risk-management & report incidents.	**Governance**: Map dependencies & resilience planning.	**Procurement**: Require CE-marked, compliant digital products.

Regulatory Context

Entity Definitions

Large Enterprise (LE)

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

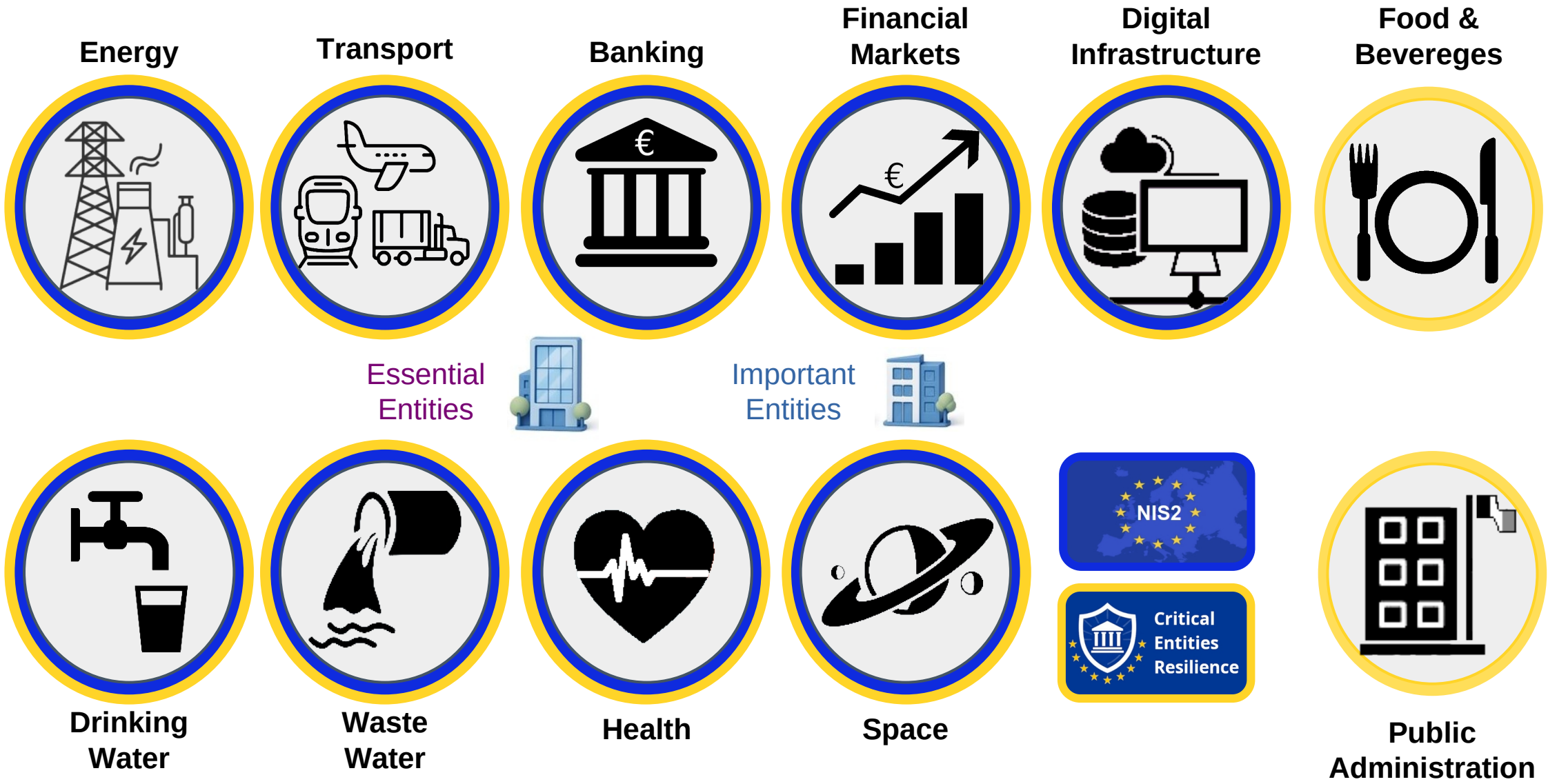
Medium Enterprise (ME)

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

Small & Micro Enterprise (SME)

- < 50 employees, or
- ≤ €10m revenue

NIS2/CER: Sectors of high criticality



https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng

NIS2 Sectors of high criticality

Digital Infrastructure

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

Essential Entities

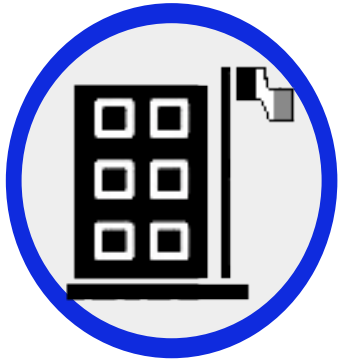
- **Providers of public electronic communications networks**

Essential Entities

Important Entities

- **Central Government**

Essential Entities



Public Administration

- **Regional Government**

Important Entities

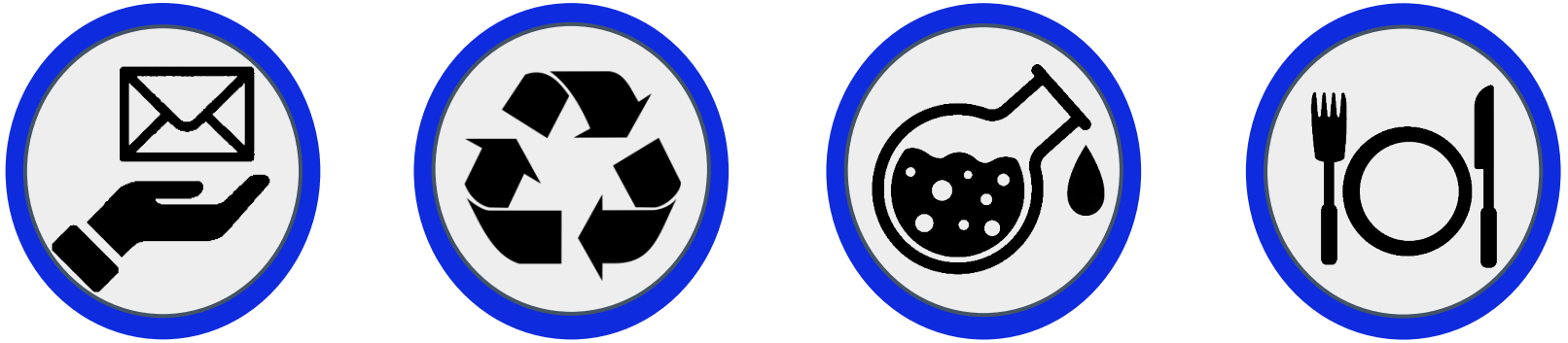
NIS2: Other critical sectors

Postal & Courier

Waste Management

Chemicals

Food



Important Entities

Manufacturing

Digital Providers

Research Organisations

Threat Vectors in Ireland

Unaddressed security weaknesses and social engineering account for over 90% of cybercrime entry points in organisational networks

- **Phishing & Social Engineering**
  - Spear-phishing attachments and drive-by compromises
  - Targeted Reconnaissance
  - Credential Infiltration
- **Ransomware & Operational Impact**
  - High-Impact Disruption
  - Lateral Supply-Chain Spread
  - Multi-Stage Lifecycle
- **Software Vulnerabilities**
  - Exploiting Public-Facing Apps
  - Software weakness the root cause of breaches
  - Mandatory Scanning & Patching

Board Governance & Director Liability

- NIS2
  - Mandatory Board Training
  - Personal Executive Liability
  - Heavy Administrative Fines
    - Essential: €10M / 2%
    - Important: €7M / 1.4%
- CRA
  - Digital Lifecycle Oversight
  - Supply Chain Audits
  - Market Sanctions
    - €15M / 2.5%
- CER
  - All-Hazards Governance
  - Statutory Enforcement
  - Legal Sanctions

Supply Chain & Vendor Risk

- **Vendor Due Diligence** (NIS2 & CyFun)
  - **Mandatory Due Diligence**: Pre-contract risk assessments and due diligence required before establishing supplier relationships.
  - **Contractual Mandates**: Supply chain policies must mandate vendor security controls, security in system acquisition, and ongoing monitoring.
  - **Incident Integration**: Third-party vendors must be integrated into organisational incident response and continuity plans.
- **Digital Product Procurement** (CRA)
  - **Products with Digital Elements (PDE)**: with CE-marked hardware and software meeting EU security-by-design standards.
  - **Software Bill of Materials (SBOM)**: Must be provided by Vendors detailing software components and open-source libraries.
  - **Lifecycle Patching**: Manufacturers must guarantee free security updates throughout the product support lifecycle.

Incident & Vulnerability Reporting Timelines

Time	Incident reporting
Within 24 hours	**NIS2/CRA: Early Warning** should be communicated, as well as some first presumptions regarding the kind of incident.
After 72 hours	**NIS2/CRA: Official Incident/Vulnerability Notification** A full notification report must be communicated, containing the assessment of the incident, severity and impact and indicators of compromise.
Upon Request	**NIS2/CRA: Intermediate Status Report** At the request of CSIRT or relevant competent authority.
Within 14 Days	**CRA: Final Vulnerability Report** is submitted no later than 14 days after a corrective/mitigating measure (patch) is available.
After 1 month	**NIS2/CRA: Final report** must be communicated.
Every 3 months	**NIS2/CRA:** Member states CSIRT reports incidents to ENISA.
Every 6 months	**NIS2/CRA:** ENISA reports on all incidents EU wide.

Risk Management Measures

RMM001
Registration

RMM002
Governance – Management board commitment and accountability

RMM003
Network and Information Security Policy

RMM004
Risk Management Policy

RMM005
CI/assess effectiveness & improve cybersecurity RMM

RMM006
Basic Cyber Hygiene Practises & Security Training

RMM007
Asset Management

RMM008
Human Resource Security

RMM009
Access Control

RMM010
Environmental and physical security

RMM011
Cryptography, Encryption and Authentication

RMM012
Supply Chain Policy

RMM013
Security in network and information systems acquisition

RMM014
Incident Handling

RMM015
Incident Reporting

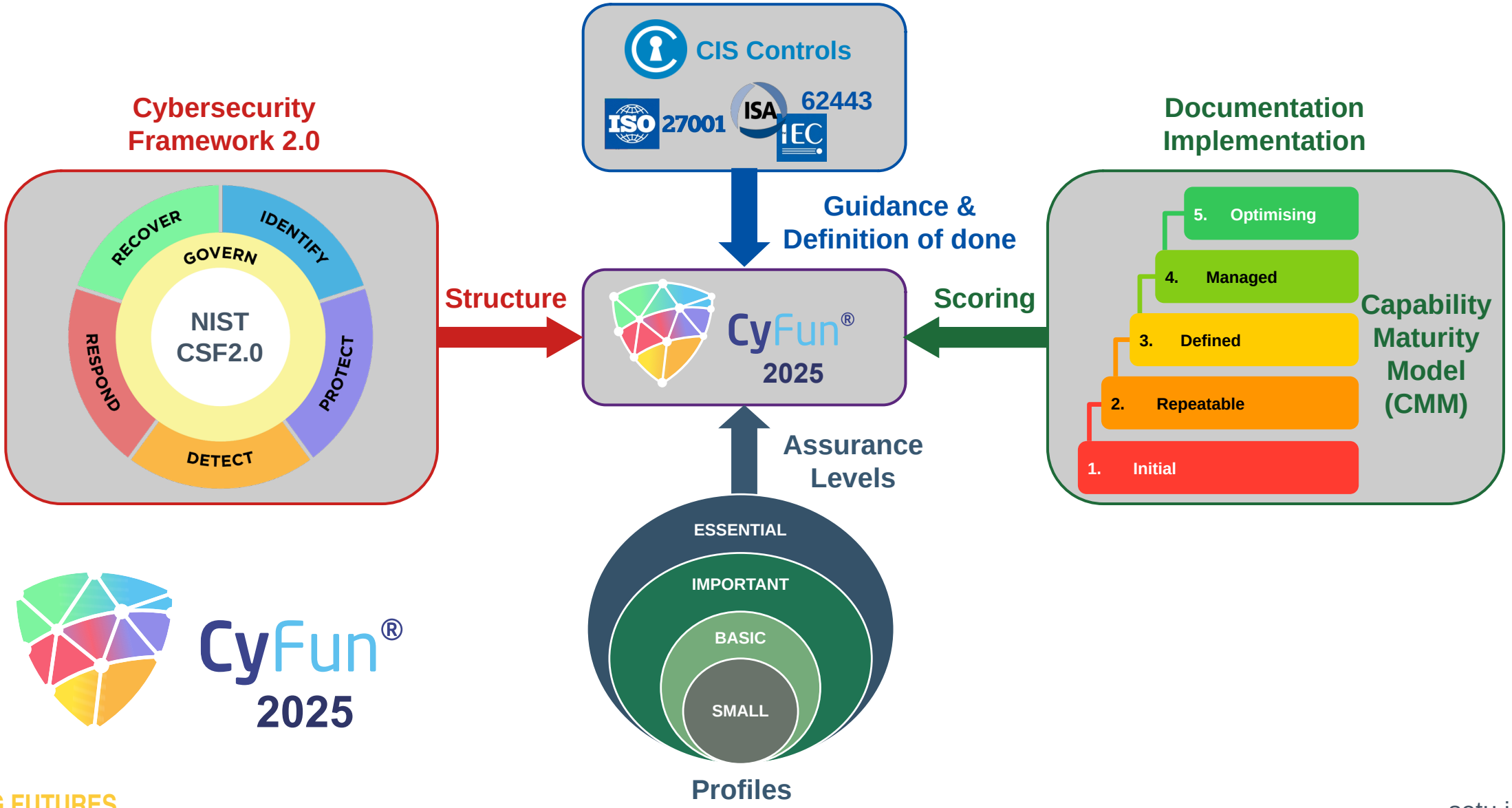
RMM016
Business Continuity and Crisis Management

Foundational Actions

Supporting Actions

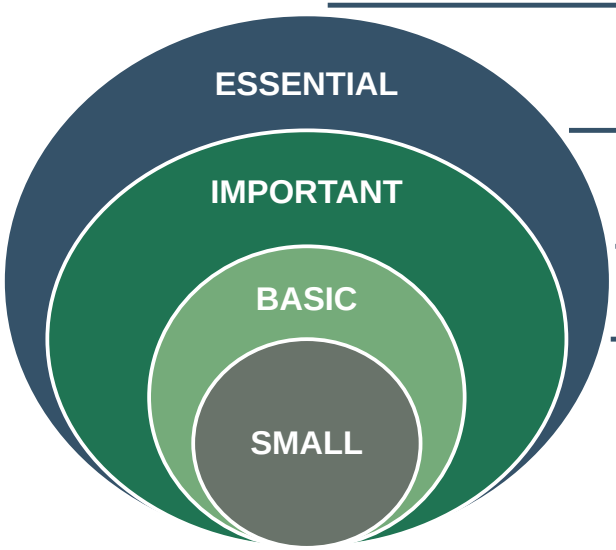
Ref: https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf

Cyber Fundamentals



Cyber Fundamentals

Assurance Levels



90 Specific Controls

69 Specific Controls

28 Specific Controls

Non-technical formulated guidelines & recommendations

Road to Operational Readiness

Preliminary Phase

- Determine the target level (**BASIC**, **IMPORTANT**, and **ESSENTIAL**).
- Internal audit of security maturity.
- Implementing corrective measures.

Path A: Verification

- An authorised CAB reviews evidence and conducts on-site checks to verify the self-assessment.
- Awarded an official Verification Report and the CyFun label.

Path B: Certification

- Two-stage audit incl. technical testing (Pen-testing, etc..) and in-depth process analysis.
- Awarded a formal Certificate of Conformity.
- Independent evidence of compliance with NIS2.

Pragmatic Cyber Resilience

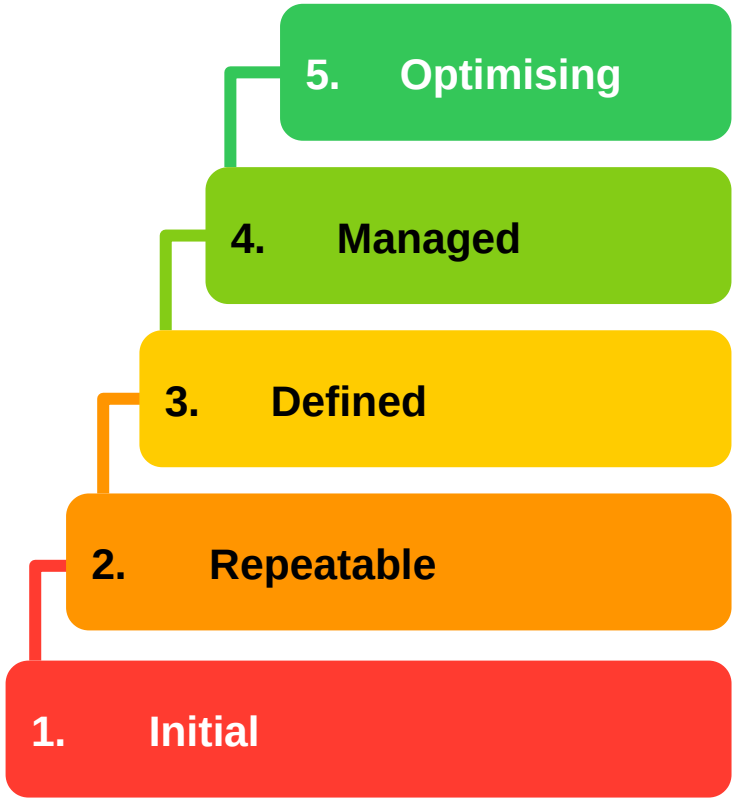
The Shift in Focus

- **Beyond Checklists**: Audits prove policy existence, not crisis survival during an active breach.
- **Cross-Functional Ownership**: Shifting responsibility from purely IT/Security to Legal, PR, and C-Suite.
- **Realistic Constraints**: Validating decision velocity under fog-of-war conditions and tight reporting windows.

Tabletop Exercises

- **Scenario Injects**: Ransomware, supply chain outages, and operational disruptions.
- **Decision Stress-Testing**: Rehearsing notification timelines (NIS2/CRA 24h/72h) and escalation thresholds.
- **Feedback Loops**: Translating post-exercise debriefs into actionable playbook updates.

Capability Maturity Model



Summary

- **Governance & Liability**:
  - Board-level oversight, mandatory training, and C-level personal liability across NIS2, CER, and CRA.
- **Supply Chain & Sourcing**:
  - Binding vendor contracts, SBOMs, and CE-marked digital procurement.
- **Operational Readiness**:
  - Shift from static paper checklists to active tabletop drills and CyFun baseline controls.

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