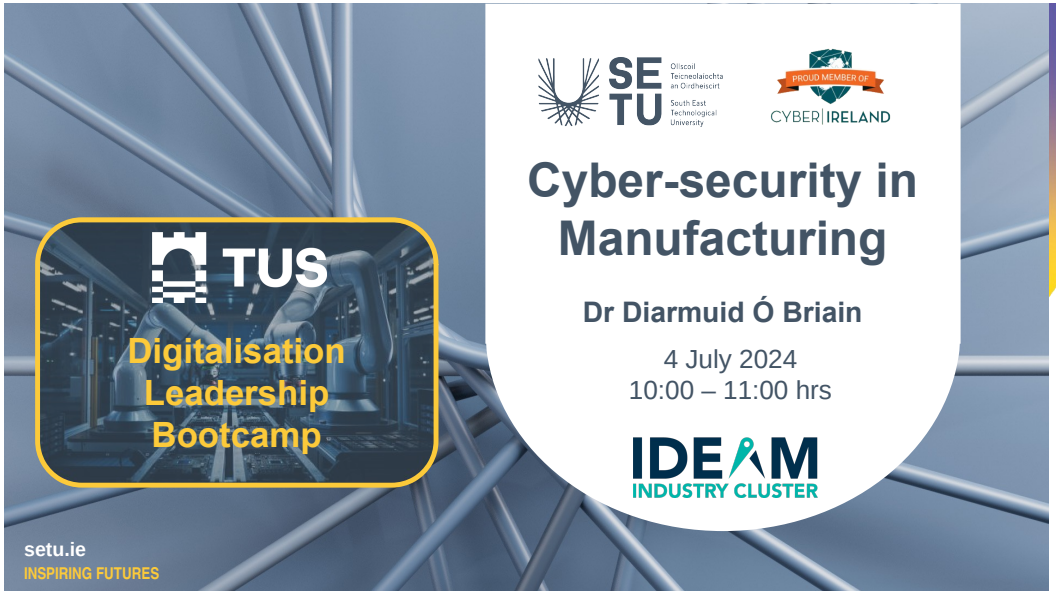


Topics

- What is Operational Technology?
- The Purdue Enterprise Reference Architecture
- NIST Cybersecurity Framework (CSF) v2
- CIS Critical Security Controls (CSC)
- NIST SP 800-82 Guide to Operational Technology Security
- ISA/IEC 62443 Securing Industrial Systems
- Network Information Systems 2 (NIS-2)
- Risk Management Measures (RMM) and CyFun

Information Technology —v— Operational Technology

- **IT**

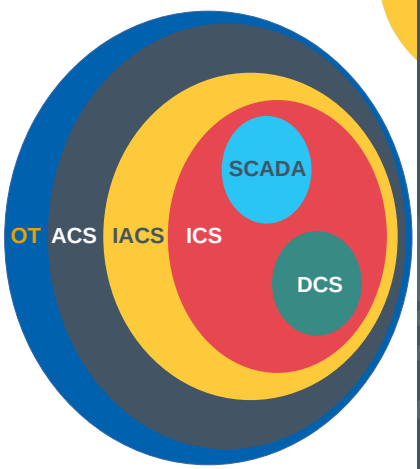
  Any equipment or interconnected system used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organisation or by a 3rd party on the organisations behalf.

- **OT**

  Programmable systems or devices that interact with the physical environment, or manage devices that interact with the physical environment. These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.

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)



Exercise #1

Exercise #1

- What is different about this power station and a typical office environment in terms of computing?

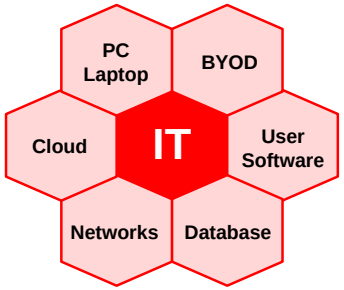
ESB Aghada, Cork, Ireland

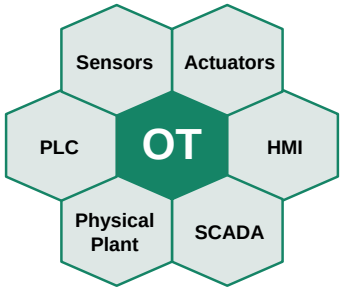
Exercise #1

- What is different about this power station and a typical office environment in terms of computing?
  - Computing interacts with physical processes.
  - There is the potential for physical damage.
  - The size of such facilities and the concerns for operations and security.
  - There is a real risk to human life.
  - Wider implications for society if the station is disrupted.

ESB Aghada, Cork, Ireland

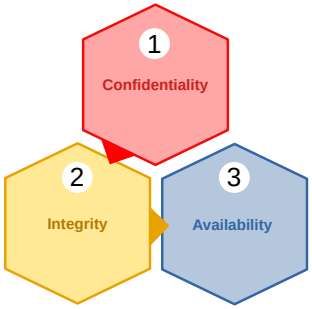
Information Technology -v- Operational Technology



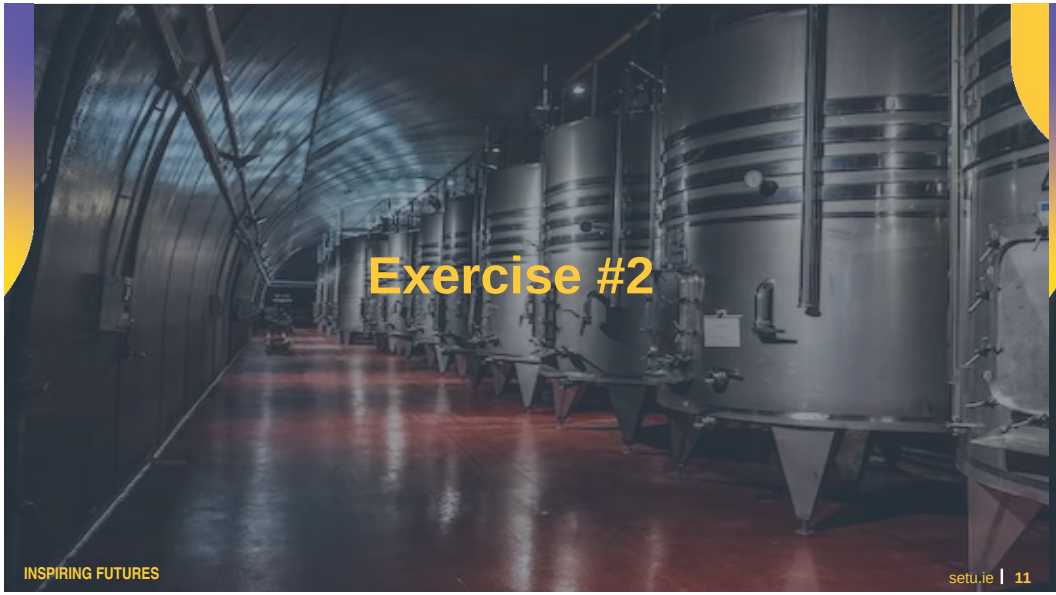


Core Principles IT/OT

IT (CIA Triad)



OT (SAIC)



Exercise #2

- **A breweries main Production Management Software (PMS), actually running outside of the IACS, in the enterprise network, was affected by malware.**

What are the implications?

Exercise #2

- **A breweries main Production Management Software (PMS), actually running outside of the IACS, in the enterprise network, was affected by malware.**
  - Because the PMS was down, the production line had to be halted.
  - Because the production line was stopped, no product was coming off the line that could be packed and shipped.
  - The resulting logjam, then also means that goods coming in cannot be unloaded, and production line employees are unable to do their jobs.

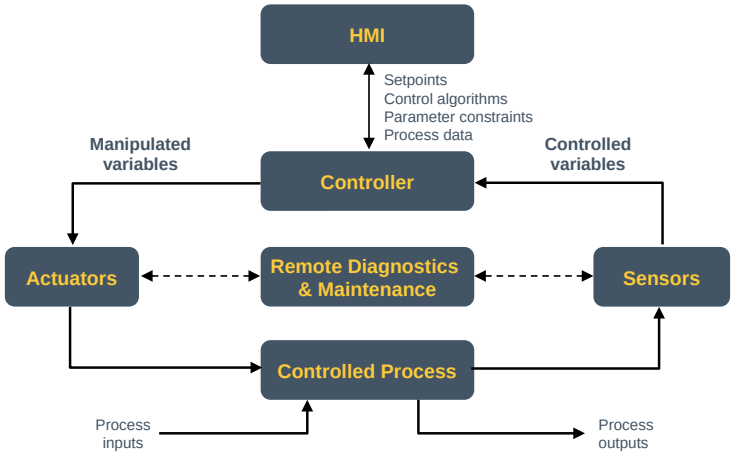
Exercise #2

- This is why **Availability** is more important than **Confidentiality** in OT.
- Data is still very important within OT as proprietary knowledge and confidential product information can all be stored and transmitted as part of a OT network.
  - Storage of brewery recipes, process timings, security controls as well as Intellectual Property (IP).

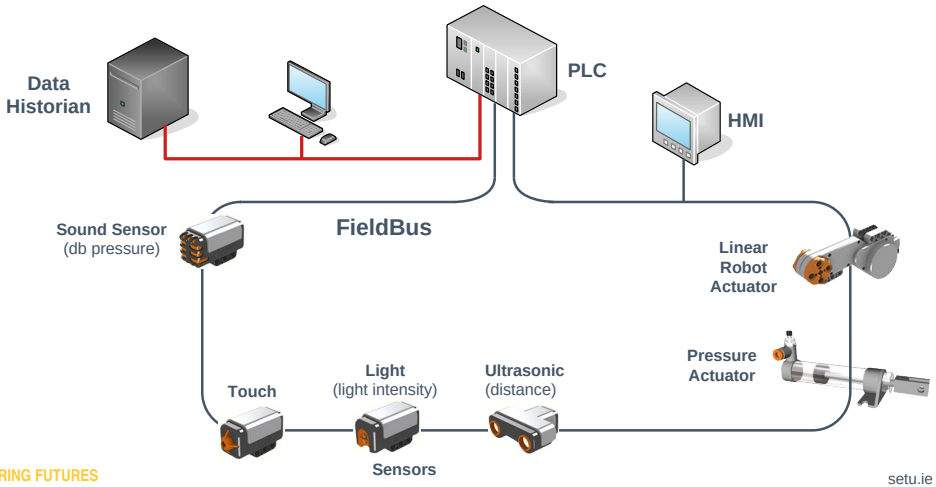
Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Purdue Enterprise Reference Architecture (PERA)

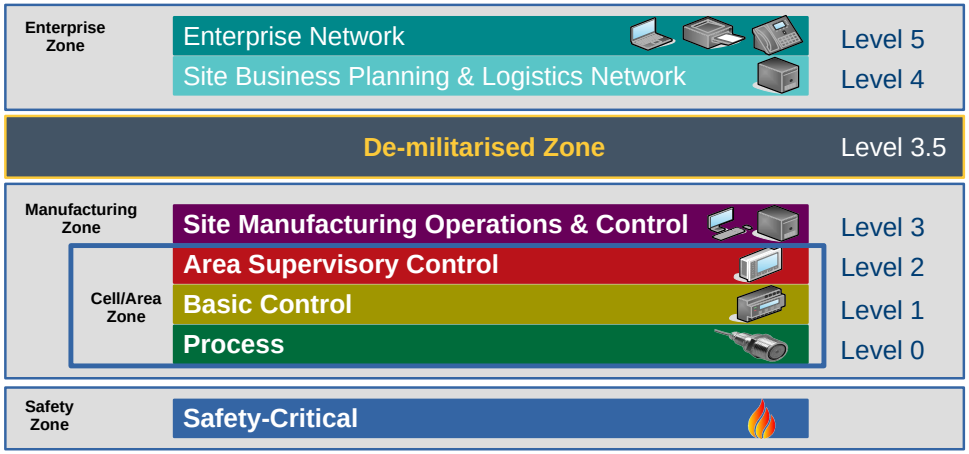
Typical OT System



PLC Control in OT System



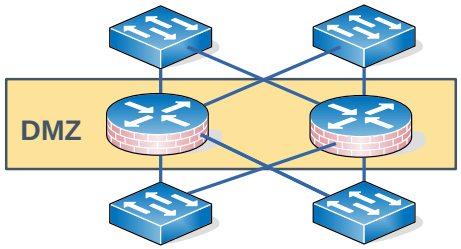
Functional manufacturing levels

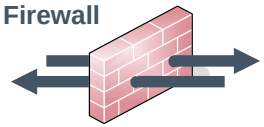


Ref: https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-14_FINAL.pdf

Purdue Model

- **Industrial DMZ** (Level 3.5)
  - This first line of defence in isolating the IACS from IT network.





Exercise #3

- **Scenario**: Take a computer parts assembly line:
  - At the end of each line there is packer **robot #1** that takes flat-packed boxes and assembles them, bends the sides, closes the 4 bottom flaps, tapes the base.
  - Another packer **robot #2** packs parts off the assembly line into the boxes and when full allows the box to continue.
  - Packer **robot #3** that inserts the manual and warranty information closes the lid, tapes the lid and affixes the product specification sticker to the box.
  - The box passes on to a sorter robot who places it in a large box along with 99 others until the large box is full, seals it and it is moved to a distribution warehouse.

Exercise #3

- **Task**: Consider that a software patch was applied to packer **robot #1** that rendered it unworkable.
  - List the consequences that you can foresee for the business, the plant and the employees if this robot is offline for two to three hours as a result.

Exercise #3

- **Business**
  - Production Slowdown, missed deadlines, production quotas not being met, and potential loss of revenue.
- **Increased Costs**
  - Overtime
  - Expedited Shipping
  - Customer Dissatisfaction
- **Plant**
  - Production Line Inefficiency
  - Inventory Buildup
  - Equipment Wear and Tear
- **Employees**
  - Downtime
  - Frustration and boredom
  - Increased Workload
  - Safety Concerns

The impact can be lessened if there are **mitigation strategies** in place.

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

Center 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

Implementation Groups

- **IG1** - Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks.
- **IG2** (Includes IG1) - An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission.
- **IG3** (Includes IG1 and IG2) - An IG3 enterprise employs security experts that specialise in the different facets of cybersecurity. IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight.

Critical Security Controls (CSC)

Critical Security Controls (CSC)

CSC Safeguards example

- CSC 1 - Inventory and Control of Enterprise Assets

Safeguard 1.1 - Establish and Maintain Detailed Enterprise Asset Inventory
- Security function: Identify

Safeguard 1.2 - Address Unauthorised Assets
- Security function: Respond

Safeguard 1.3 - Utilise an Active Discovery Tool
- Security function: Detect

Safeguard 1.4 - Use DHCP Logging to Update Enterprise Asset Inventory
- Security function: Identify

Safeguard 1.5 - Use a Passive Asset Discovery Tool
- Security function: Detect

ISO/IEC 27001 – Management Requirement

- ISO/IEC 27001 provides and ISMS that allows the organisation to:
  - Systematically **identify security risks**, considering threats, vulnerabilities, and impacts.
  - Design and deploy comprehensive **security controls** or other risk treatments.
  - Maintain an ongoing process to ensure **controls remain effective**.
  - Use a coherent, **all-encompassing suite of controls**.
  - **Continuously monitor and adjust** security measures.

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

Control Points (CP) in ISO27001:2022

Technical	• Firewalls • Intrusion detection systems • Data encryption • Password management
Organisational	• Information security policies and procedures • Training for employees • Incident response plan • Risk Assessment • Access Control • Data Security • Business Continuity
Change Management	• Offsite backup • Asset management

Systematic approach to implementation of ISMS

- Get top management **commitment and support**.
- **Involve all stakeholders** in the implementation process.
- Use a **risk-based approach** to identify and mitigate risks.
- Choose the **right tools and technologies** to support the ISMS.
- **Monitor and review** the ISMS on an ongoing basis.
- Make **continuous improvement** a part of the ISMS.

NIST SP 800-82 Rev. 3

- Guidance on how to secure OT while addressing their unique performance, reliability, and safety requirements.
- Identifies common threats and vulnerabilities to OT.
- Recommends security countermeasures to mitigate associated risks.
- Provides OT-tailored security control overlay that customises controls for the unique characteristics of the OT domain.

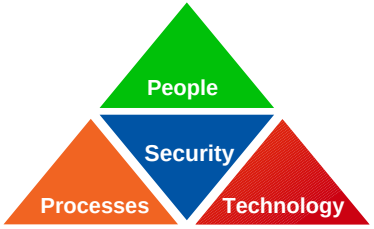
https://csrc.nist.gov/pubs/sp/800/82/r3/final

NIST SP 800-82 Rev. 3

- Establish OTSec governance.
- Build and train a cross-functional team to implement an OTSec programme.
- Define the OTSec strategy.
- Define OT-specific policies and procedures.
- Establish a OT specific cybersecurity awareness training programme.
- Implement a Risk Management Framework for OT.
- Develop a maintenance tracking capability.
- Develop an incident response capability.
- Develop a recovery and restoration capability.

ISA/IEC 62443 Series of Standards

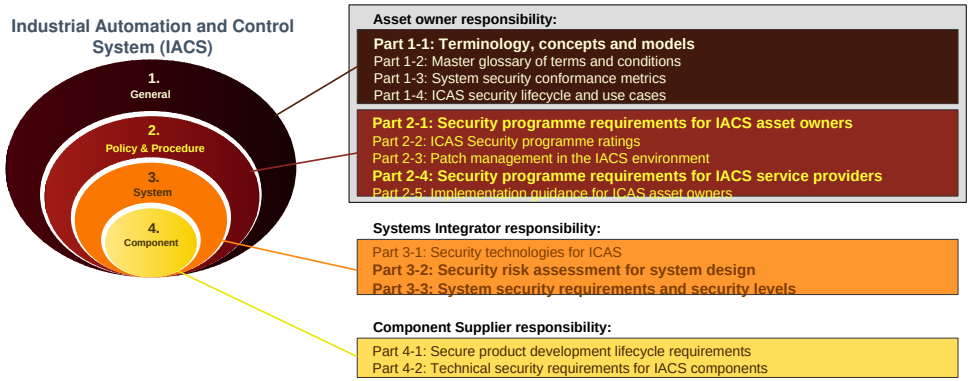
- A series of standards is a comprehensive and internationally recognised framework for securing IACS.
- It provides a holistic approach to cybersecurity, addressing all aspects of IACS security throughout their lifecycle, from design and development to operation and maintenance.



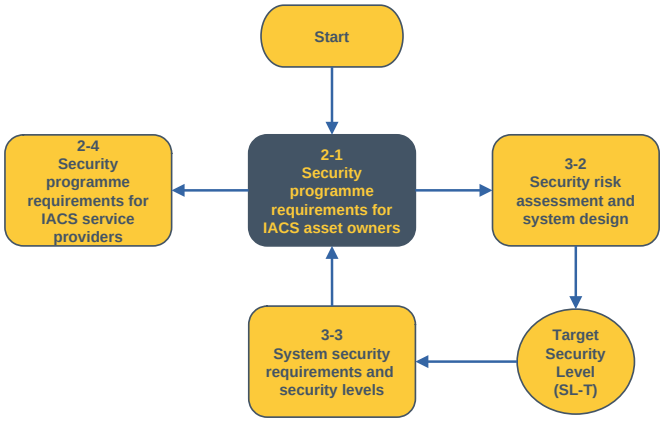
- **Core Principles**
  - Security by design
  - Security by default
  - Security throughout the lifecycle
  - Security risk management

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

ISA/IEC 62443 Series of Standards



ISA/IEC 62443 Relationship Between Parts



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

Essential and Important entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems.

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

CRU

IAA

CRR

NTA

HSE | eHealth Ireland

An Roinn Iompair
Department of Transport

NCSC

SPOC

enisa

*Entities may be designated as "**Essential**" or "**Important**" depending on factors such as size, sector and criticality.*

Entities

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

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

Small & Micro Enterprise
- < 50 employees

NIS2 Sectors of high criticality

Energy | **Transport** | **Banking** | **Financial Markets** | **Digital Infrastructure**

- **IXPs**
- **CSPs**
- **Data Centres**
- **CDNs**

Essential Entities | Important Entities

Drinking Water | **Waste Water** | **Health** | **Space**

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**

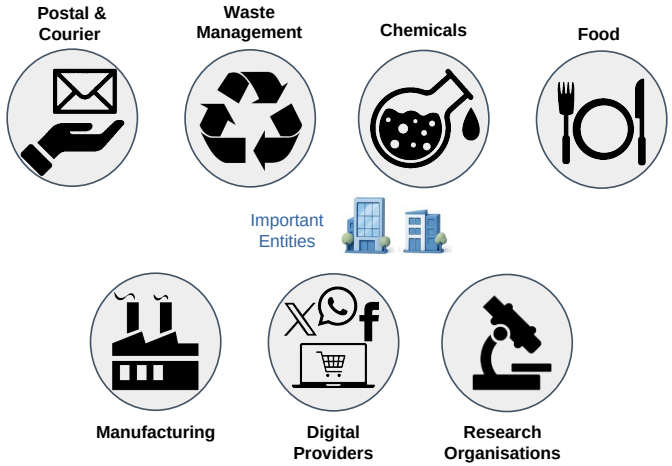
Essential Entities

Public Administration

- **Regional Government**

Important Entities

NIS2 Other critical sectors



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 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 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.

NIST SP 800-82 ‖ ISA/IEC 62443

NIS2 Requirement Category	NIST SP 800-82r3	ISA/IEC 62443 Series
Risk Management	Direct	Direct & Comprehensive
Incident Handling	Direct	Direct & Foundational
Business Continuity & Crisis Management	Direct	Direct & Integrated
Supply Chain Security	Indirect/Focus on Components	Direct & Comprehensive
Security in System Acquisition, Development, & Maintenance	Direct	Direct & Strong
Awareness Training & Hygiene	Direct	Direct
Access Control	Direct	Direct & Detailed
MFA & Encryption	Direct	Direct
Assessment of Effectiveness	Direct	Direct

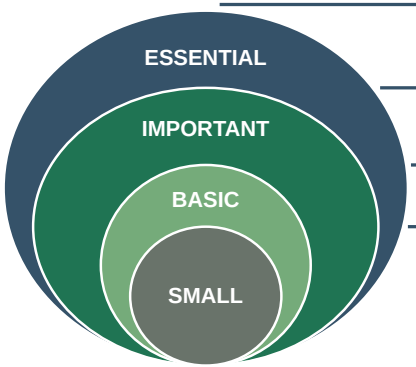
Risk Management Measures (RMM)

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

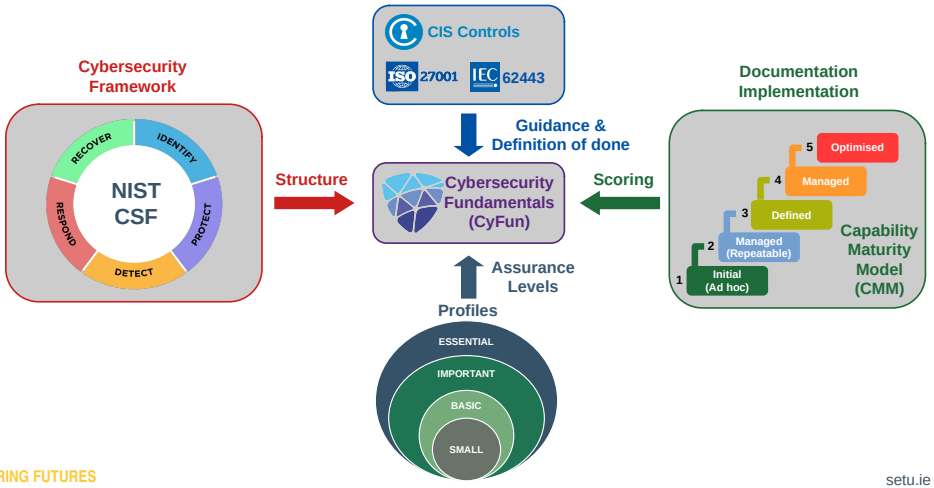
CyberFundamentals Framework (CyFun)



- **ESSENTIAL** — 140 Controls
- **IMPORTANT** — 117 Controls
- **BASIC** — 34 Controls
- **SMALL** — Non-technical formulated guidelines & recommendations

Ref: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

CyFun Framework



Exercise #4 Limerick Cheeses Limited

Exercise #4 Scenario: Limerick Cheeses Limited

- Saint Patrick's Day **Limerick Cheeses** was hit with a ransomware attack.
- The attack crippled its operations in Patrickswell.
- On the 1 April **Limerick Cheeses** was contacted by an officer of the NCSC who stated that **Mótar Transport** reported that they had suffered an attack and reported it on the 18 March.
- In the report the CTO of **Mótar Transport** stated that they believe the attack came through a VPN they had with **Limerick Cheeses** logistics system for processing movement orders.

Exercise #4 Scenario: Limerick Cheeses Limited

- Additionally, on the 19 March, **Mótar Transport** reported that they had to rebuild each computer on their network and restore data to their business management system from backups.
- **Limerick Cheeses** responded by stating that they did have a minor issue and that they restored their systems after working to get the systems back up as quickly as possible as the attack was disrupting their production and shipping.
- Further questioning of the IT manager at **Limerick Cheeses** revealed that they had employed the services of **Echo Cyber**, a cybersecurity firm, and the incident cost them €175,000 to get everything restored to pre-incident state.

Exercise #4 Scenario: Limerick Cheeses Limited

What jurisdiction did the NCSC have to contact Limerick Cheeses about their incident?

Exercise #4 Scenario: Limerick Cheeses Limited

What jurisdiction did the NCSC have to contact Limerick Cheeses about their incident?

- As a food producer ***Limerick Cheeses*** is part of a ***other critical sectors*** and they are therefore an ***important entity***.
- They are subject to ex-post supervision, meaning that as the CSIRT-IE received potential evidence of non-compliance they had the right to take action.

Exercise #4 Scenario: Limerick Cheeses Limited

Were Limerick Cheeses and Mótar Transport in compliance with the NIS2?

Exercise #4 Scenario: Limerick Cheeses Limited

Were Limerick Cheeses and Mótar Transport in compliance with the NIS2?

- ***Mótar Transport***, from a high criticality sector, is an essential entity, they reported the incident within 24 hours and followed up within 72 hours so they were in compliance.
- ***Limerick Cheeses*** did not report the incident, they were solicited by the NCSC because of information received from ***Mótar Transport***, so they were not in compliance.

Exercise #4 Scenario: Limerick Cheeses Limited

Is there a case to answer by either Limerick Cheeses or Mótar Transport in case of either Article 21, risk-management measures, or Article 23, reporting obligations, of the NIS2?

2

Exercise #4 Scenario: Limerick Cheeses Limited

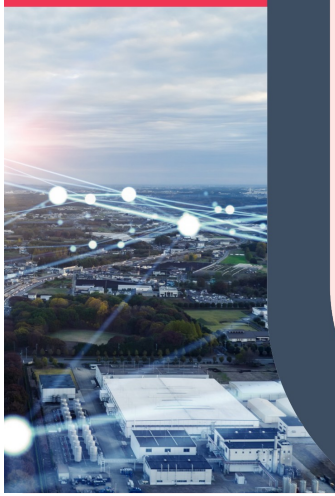
Is there a case to answer by either Limerick Cheeses or Mótar Transport in case of either Article 21, risk-management measures, or Article 23, reporting obligations, of the NIS2?

- ***Mótar Transport***, In terms of Article 23, reporting obligations they have no case to answer; however, in the case of Article 21, Cybersecurity risk-management measures they may have.
- ***Limerick Cheeses*** infringed both Article 21 and Article 23, so they certainly have a case to answer.

Topics

- What is Operational Technology? ✓
- The Purdue Enterprise Reference Architecture ✓
- NIST Cybersecurity Framework (CSF) v2 ✓
- CIS Critical Security Controls (CSC) ✓
- NIST SP 800-82 Guide to Operational Technology Security ✓
- ISA/IEC 62443 Securing Industrial Systems ✓
- Network Information Systems 2 (NIS-2) ✓
- Risk Management Measures (RMM) and CyFun ✓

CARLOW
CW-ESCIN-A
Level 9



SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Certificate in Cybersecurity for Industrial Networks

This programme offers comprehensive OT/IACS cybersecurity training, covering foundational concepts, IT/OT distinctions, risk management, and business case development. It also delves into advanced topics such as penetration testing, CSMS frameworks, and business continuity, equipping learners with technical, and managerial skills for critical infrastructure protection.

SPRINGBOARD+ www.springboardcourses.ie
Rialtas na hÉireann Government of Ireland
Có-mhaoinithe ag an Aontas Eorpach Co-funded by the European Union
HEA HIGHER EDUCATION AUTHORITY AN tÚDARÁS um ARD-OIDEACHAS

Follow @setuireland on

CARLOW
CW-ESCIN-A
Level 9

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Certificate in Cybersecurity for Industrial Networks

https://www.setu.ie/CW_ESCIN_A

SPRINGBOARD+ www.springboardcourses.ie
Rialtas na hÉireann Government of Ireland
Có-mhaoinithe ag an Aontas Eorpach Co-funded by the European Union
HEA HIGHER EDUCATION AUTHORITY AN tÚDARÁS um ARD-OIDEACHAS

Follow @setuireland on

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

INSPIRING FUTURES