The NIS2 Directive

What do you need to know?

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre


SMART
TARGETING
PHONE
GLOBAL
EXPLOITS
WWW
HIGH-TECH
ESPIONAGE
PIRACY
ANALYTICS
DETECTION
SERVICES
RISKS
HACKING
ENCRYPTION
MALICIOUS
INTELLIGENCE
AGENCY
TROJAN
CYBER
VIRUS
JAVASCRIPT
PRIVACY
SOLUTIONS
CYBER CRIME
SECURE CODING
PROTECTION
ATTACK
SOFTWARE
COMPUTER SYSTEM
TOOLS
TARGET
MALWARE
APPS
OFFENSIVE
MONEY
USER
INTERNET
GLOBAL
WEB
SSL
RANSOMWARE
PHISHING
CYBER WAR

Maybe we can pass a law to solve that?

Critical Infrastructure

NIS Directive (2016)

First EU-wide cyber directive which aimed to enhance the cybersecurity of critical infrastructure obliging operators of essential services to manage security risks and report significant incidents.

Cyber Certificatio

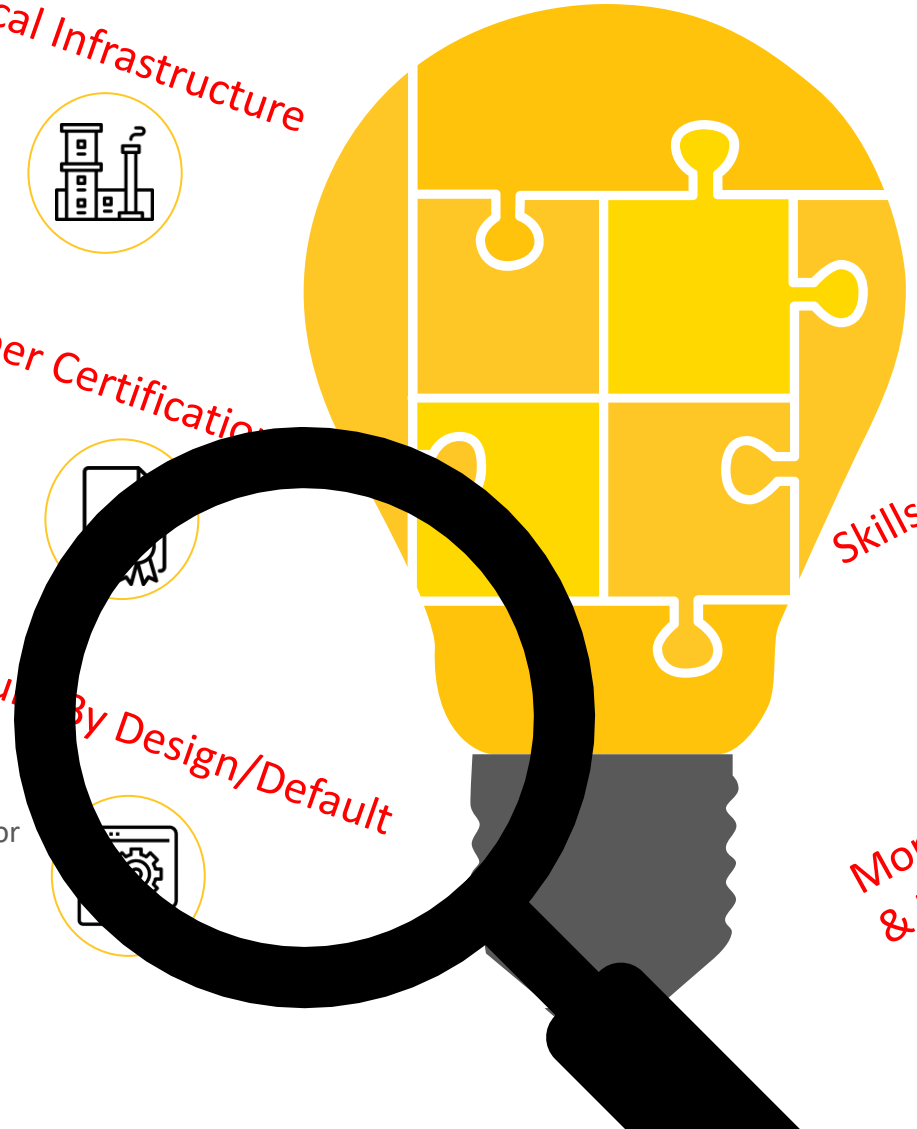
Cyber Security Act (2019)

Establishes a framework for EU-wide cybersecurity certification schemes for ICT products, services, and processes.

Secu By Design/Default

Cyber Resilience Act (2024)

Mandatory cybersecurity requirements for products with digital elements, aiming to ensure that hardware and software products are designed, developed, and maintained with robust cybersecurity features throughout their lifecycle.



Wider Economy

NIS2 Directive (2022)

NIS2 expands the scope to more sectors, strengthens security requirements, and introduces stricter supervisory measures and enforcement.

Skills, Research, Industry

ECCC Regulation (2021)

This regulation creates a central EU Cybersecurity Competence Centre to pool resources and expertise, drive research and innovation, and enhance the EU's cybersecurity industrial base and competitiveness.

Monitoring, Detection & Response

Cyber Solidarity Act (2024)

Creating a European Cyber Alert System for detecting and responding to threats, establishing a Cybersecurity Emergency Mechanism with a reserve of incident response companies, and setting up an EU-wide alert system.

What is the NIS2 Directive?

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

46 Articles, 142 Recitals & 3 Annexes , 41,696 words.

What is the NIS2 Directive?

Article 1
Subject matter

Article 2
Scope

Article 3
Essential and important entities

Article 4
Sector-specific Union legal acts

Article 5
Minimum harmonisation

Article 6
Definitions

Article 7
National cybersecurity strategy

Article 8
Competent authorities and single points of contact

Article 9
National cyber crisis management frameworks

Article 10
Computer security incident response teams (CSIRTs)

Article 11
Requirements, technical capabilities and tasks of CSIRTs

Article 12
Coordinated vulnerability disclosure and a European vulnerability database

Article 13

Article 14
Cooperation Group

Article 15
CSIRTs network

Article 16
European cyber crisis liaison organisation ne… CyCLONe)

Article 17
International cooperation

Article 18
Report on the state of cybersecurity in the U…

Article 19
Peer reviews

Article 20
Governance

Article 21
Cybersecurity risk-management measures

Article 22
Union level coordinated security risk assessm… critical supply chains

Article 23
Reporting obligations

Article 24
Use of European cybersecurity certification schemes

Article 25
Standardisation

Article 26
Jurisdiction and territoriality

…data

…angements

…rmation

…n and enforcement

…es in relation to

…es in relation to

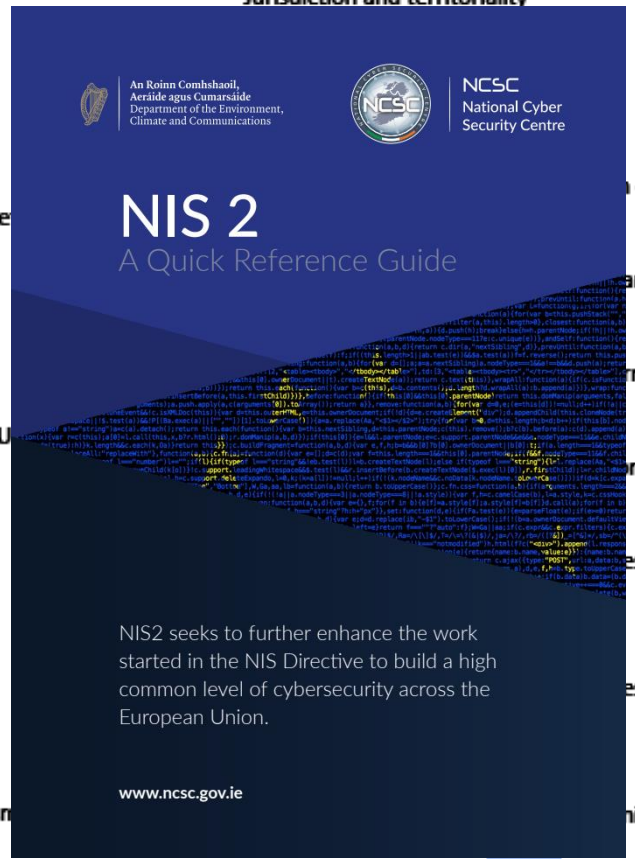
…nistrative fines on

Article 35
Infringements entailing a personal data breach

Article 36
Penalties

Article 37
Mutual assistance

NOT ENOUGH TIME…



I don’t like the sound of all that…

Am I in scope of the Directive?

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

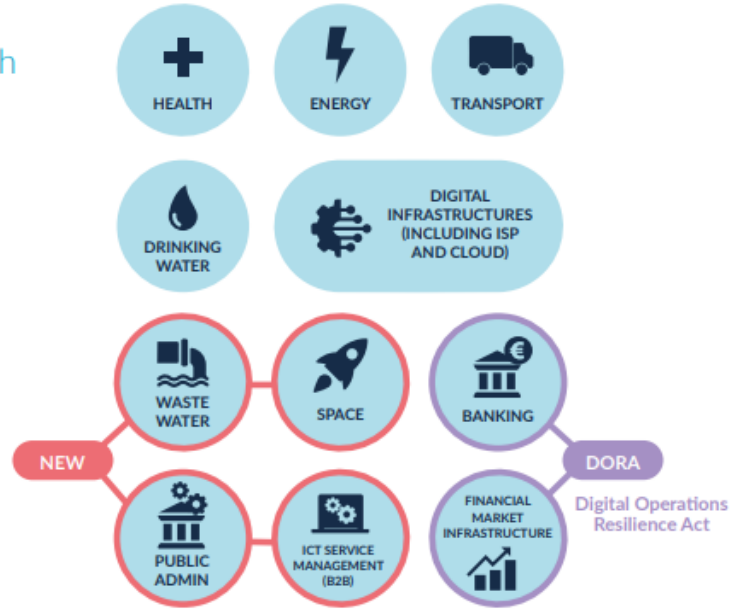
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Do I operate in one of the sectors listed in Annex I or Annex II?

YES!

- Pay close attention the definitions in NIS2 and Annex I & II
- You may need to refer to definitions in other directives
- You may need legal advice
- You know your business best

Annex 1 - Sectors of High Criticality



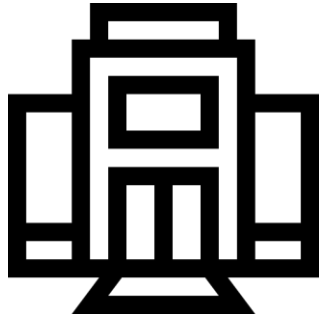
Annex 2 - Other Critical Sectors

What size is my business?

MICRO/SMALL

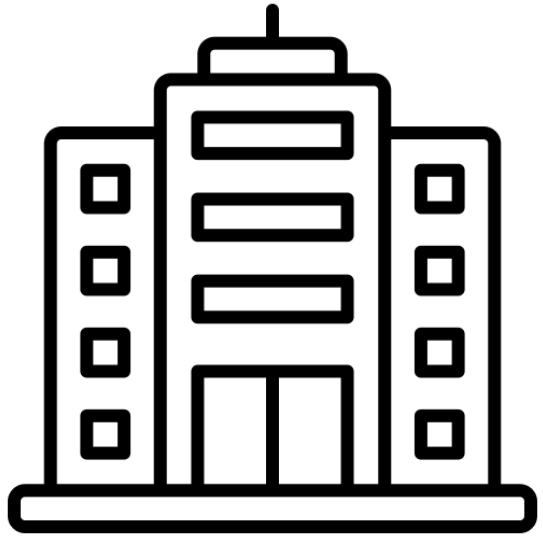
< 50 people employed
< €10m revenue/€10m balance sheet

MEDIUM



< 250 people employed
< €50m revenue/ €43 balance sheet

LARGE



250+ people employed
€50m+ revenue/ €43+ balance sheet

Annex I: Sectors of high criticality

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: public transport: ***only*** if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
BANKING	Credit institutions **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
HEALTH	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: entities holding a distribution authorization for medicinal products: ***only*** if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
WASTE WATER	(***only*** if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
	TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
	Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
	Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Of regional governments: risk based.(Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10 million revenue)	SMALL & MICRO ENTITIES

Annex II: other critical sectors

POSTAL AND COURIER SERVICES		IMPORTANT	IMPORTANT	NOT IN SCOPE
WASTE MANAGEMENT	(***only*** if principal economic activity)	IMPORTANT	IMPORTANT	NOT IN SCOPE
CHEMICALS	Manufacture, production, distribution	IMPORTANT	IMPORTANT	NOT IN SCOPE
FOOD	Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT	NOT IN SCOPE
MANUFACTURING	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)	IMPORTANT	IMPORTANT	NOT IN SCOPE
DIGITAL PROVIDERS	online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT	NOT IN SCOPE
RESEARCH	Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT	NOT IN SCOPE
ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES	All sizes, but only subject to Article 3(3) and Article 28			

Essential vs Important

- Same obligations – supervision requirements are different.

ESSENTIAL ENTITIES	IMPORTANT ENTITIES
✓ Ex Ante & Ex Post Supervision	✓ Ex Post Supervision
✓ On-site inspections and off-site supervision	✓ On-site inspections and off-site ex post supervision
✓ Regular & Targeted Security Audits	✓ Targeted Security Audits
✓ Security Scans	✓ Security Scans
✓ Information Requests	✓ Information Requests
✓ Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned.	✓ Requests for information necessary to assess, ex post, the cybersecurity risk-management measures adopted by the entity concerned.
✓ Ad hoc audits, for example after a significant incident	✗

Authorities can take a risk based approach to prioritise supervisory tasks.

Okay, pretty sure we're in scope …

What do I need to do to comply?

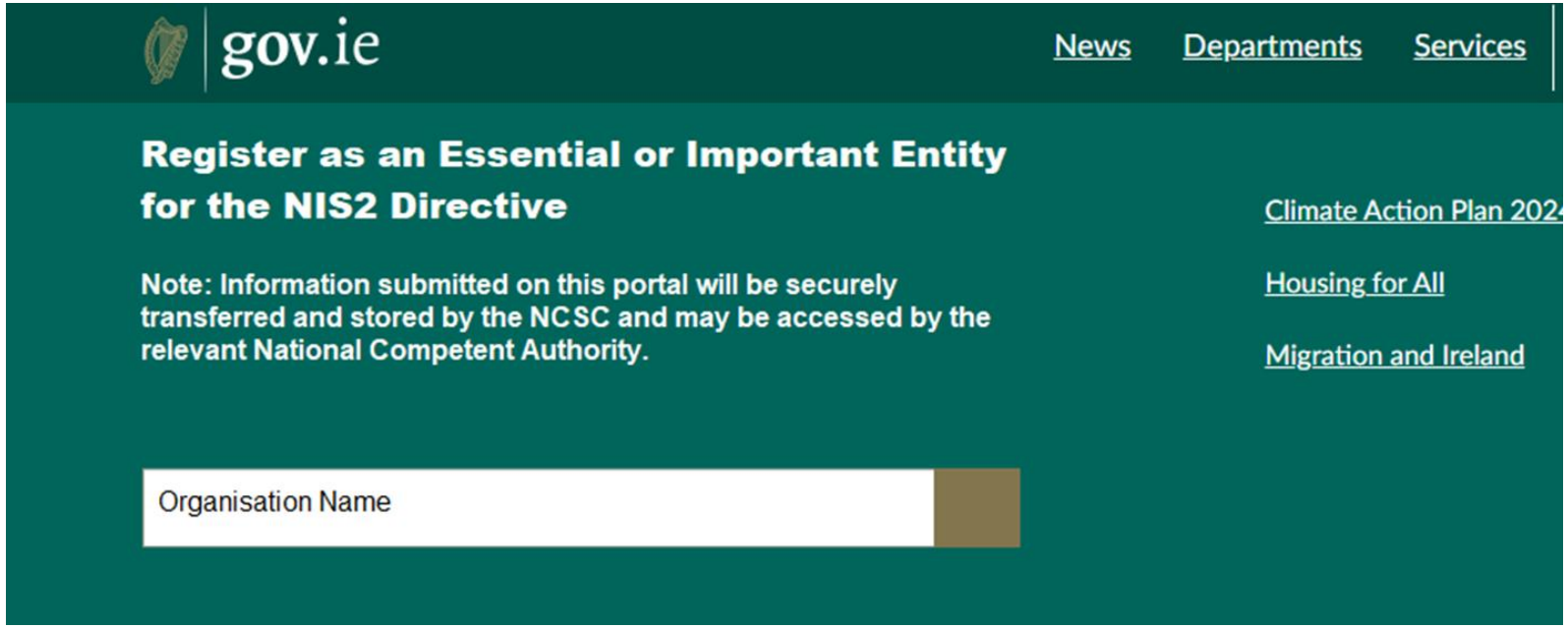
02

Register as an Essential/Important Entity

NCSC will provide a single national platform

You need to submit after 17 Oct 2024:

- Sector/Subsector
- Name
- Address
- Up to date contact details (email, telephone, IP ranges)



Oversight and Accountability

Cybersecurity is the board's responsibility

- Member States shall ensure that the management bodies of essential and important entities **approve the cybersecurity risk-management measures** taken by those entities in order to comply with Article 21, **oversee its implementation** and **can be held liable for infringements by the entities** of that Article.

- Training to gain knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices.

Most important sentence in the Directive

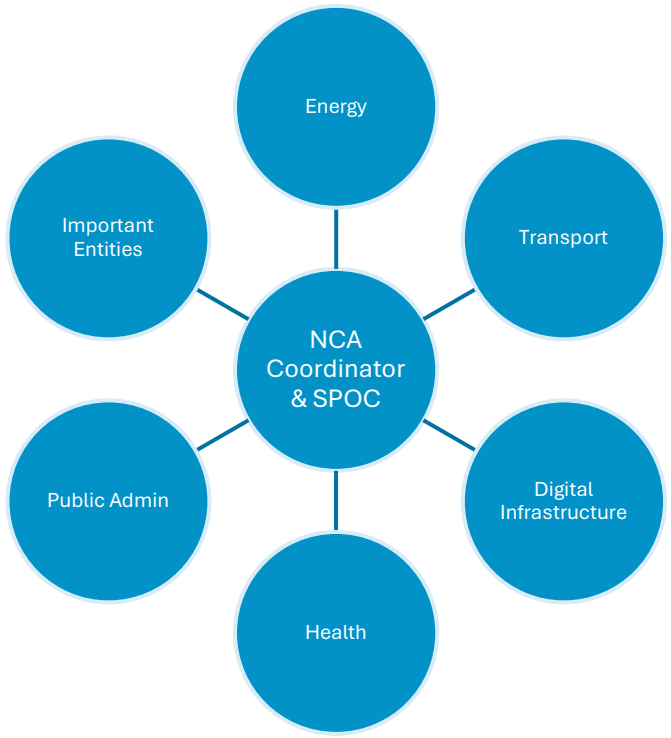
Risk Management Measures

- *Article 21 - "Cybersecurity risk-management measures" including at least the following...*

Assess your current cyber security posture and maturity

National Competent Authorities (NCA)

Federated Model



NCSC will be NCA Coordinator.

- Act as National Single Point of Contact (SPOC)
- Establish and chair an NCA Forum.
- Assist new NCAs to build capacity.
- Standardise guidance on Security Measures, Audit Methodology and Incident Reporting.

Supervision and Enforcement

More robust powers, larger fines.

Supervision Measures.

- On site inspections, off-site supervision, random checks
- Regular & targeted security audits, ad hoc audits
- Security scans, where necessary with the cooperation of the entity concerned
- Access to documentation, policies, data, security audit results.

Enforcement Measures

- To issue warnings, binding instructions, orders to cease conduct/implement recommendations
- To designate a monitoring officer
- Order entities to make public aspects of infringements
- To notify those potentially affected by a cyber threat, and remedial measure they can take
- To impose administrative fines

Further sanctions include – temporary suspension of service authorisation / temporary suspension of CEO or legal representative – where enforcement measures are ineffective

What about when things go wrong…

How do I report incidents, and what can I expect?

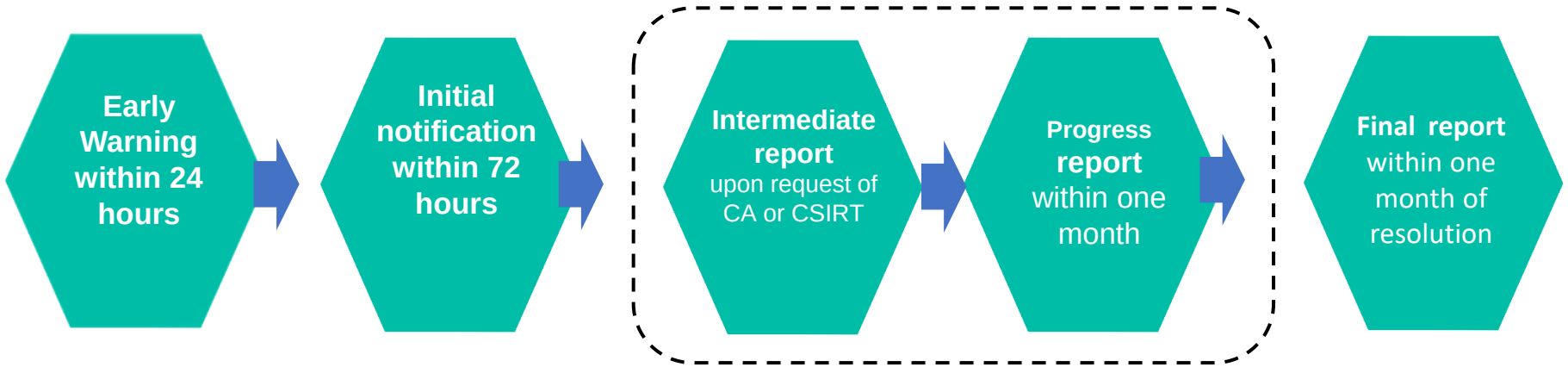
3

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Incident Reporting (Art 23)

- *All **significant** incidents must be reported to NCSC within 24hrs.*
- *Significant Incident:*
  - *Anything which affects or is capable of affecting operations or causing financial loss.*
  - *It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage*



Significant Incidents

- *'incident' means an event compromising the **availability**, **authenticity**, **integrity** or **confidentiality** of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems;*
- *Guidance on how to determine a significant incident will be provided (e.g a total outage of the service for >10 mins, or more than 5% of users cannot access the service for more than an hour etc.).*
- *Sector and organisation specific context is very important. If in doubt – report.*
- *"Initial Assessment: Importance of system affected to service, severity and technical characteristics of the cyber threat and underlying vulnerabilities that are exploited."*

Type of event	Definition
Availability (Total service outage)	The incident has caused complete unavailability of the services provided
Availability (Partial service outage)	There is an incident that has caused or is capable of causing a service degradation, or one or more services are not available, or services are intermittent available for more than a specific number of hours.
Confidentiality/integrity /authenticity (Compromised data and/or systems)	The incident has caused or is capable of causing the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, stored, transmitted or processed data[2].
Material/non-material damage to individuals and legal entities	The incident has caused or is capable of causing material or non-material damage for the entity

What information is required?

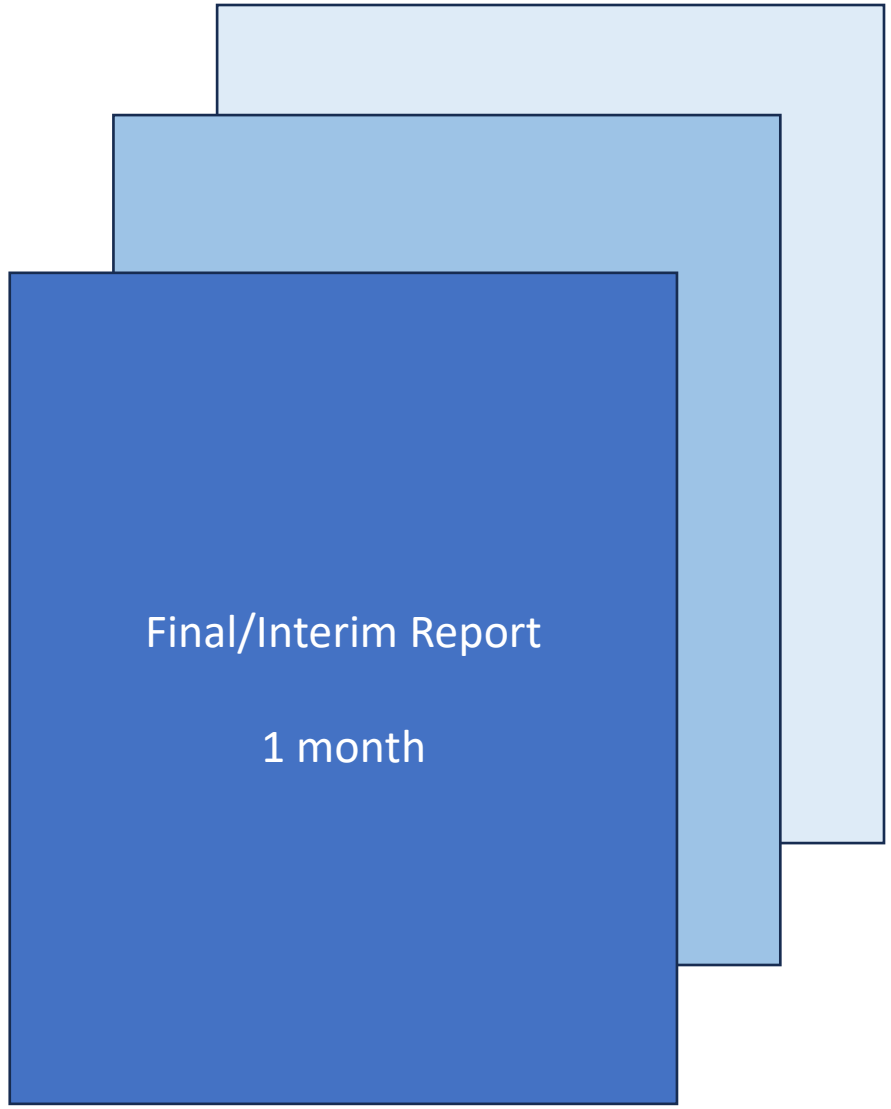
- *A **warning** that a suspected significant incident has occurred. Whether it was caused by unlawful/malicious actions and whether it has a cross-border impact.*
- *A **notification** that updates earlier information and also provides an initial assessment of the severity and impact and Indicators of Compromise (IOCs).*
- *A **final report** that provides*

— *A detailed description of the incident, including its severity and impact.*

— *The type of threat and root cause likely to have triggered the incident*

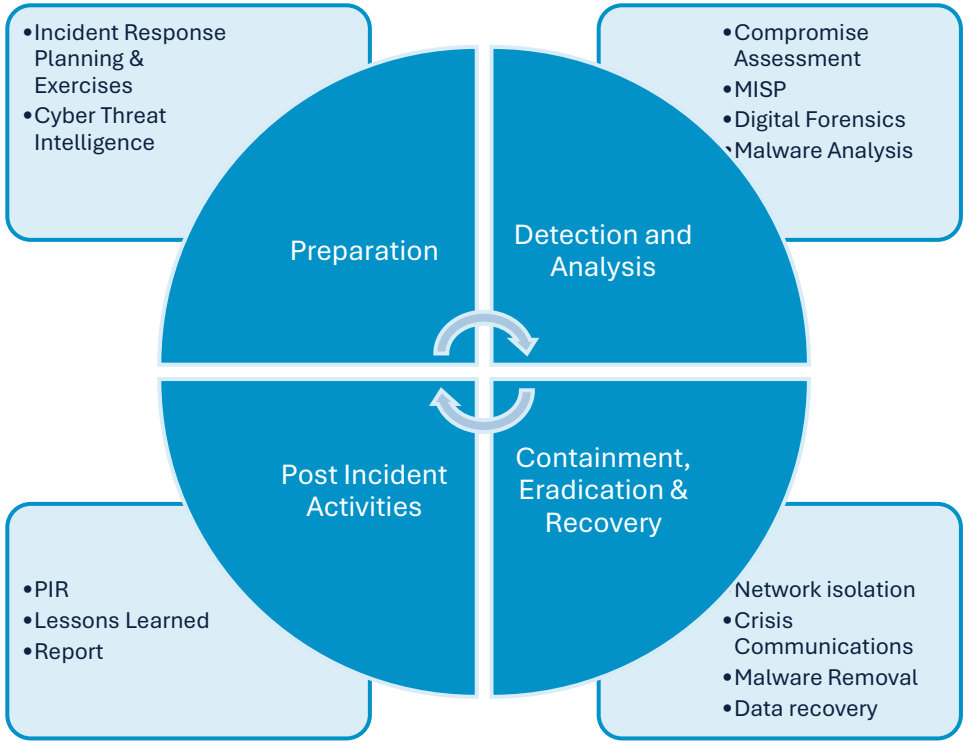
— *Applied and ongoing mitigation measures*

— *The cross-border impact (if applicable)*



NCSC and Incident Response

What services are available as an essential/important entity?



NCSC CSIRT can support before during and after an incident alongside your security team or MSSP.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

What next...

What can I expect for the remainder of 2024?

04

Milestones

Q3/Q4 2024

- All NCA designations confirmed – July
- NCA Forum Meeting 3 – July
- General Scheme brought to Government for Approval - July
- Draft Security Measures Framework published for consultation – September
- National Cyber Security Bill enacted– October
- EU-wide cross-border entities security measures and incident notification implementing act published – October
- National guidelines on incident reporting and security measures – Q4
- Cross-border entities list sent to ENISA – 17 Jan 2025

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Thank you!

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre