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

NCSC
National Cyber
Security Centre

NIS 2

A Quick Reference Guide

NIS2 seeks to further enhance the work started in the NIS Directive to build a high common level of cybersecurity across the European Union.

www.ncsc.gov.ie

Table of Contents

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

NCSC
National Cyber
Security Centre

NIS 2
Introduction

NIS2 seeks to further enhance the work started in the NIS Directive to build a high common level of cybersecurity across the European Union.

1

www.ncsc.gov.ie

1

NIS 2 Introduction

NIS2 will further enhance the work started in the NIS Directive in building a high common level of cybersecurity across the European Union.

It places obligations on Member States AND individual companies in critical sectors.

New in NIS2

- ✔ More Sectors
- ✔ More entities
- ✔ New methods of selection and registration
- ✔ New incident notification deadlines
- ✔ Extra requirements

Three Main Pillars of NIS2

MEMBER STATE RESPONSIBILITIES

National 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 INFO EXCHANGE

Cooperation Group

CSIRTs Network

CyCLONe

CVD and European Vulnerability registry

Peer-reviews

Biennial ENISA cybersecurity report

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

NCSC
National Cyber Security Centre

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

NCSC
National Cyber
Security Centre

NIS 2
Essential and Important Entities

Entities may be designated as “Essential” or ‘Important” depending on factors such as size, sector and criticality.

2

www.ncsc.gov.ie

2

Essential and Important Entities

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			

Notes:

Entities designated as Critical entities under Directive (EU) 2022/2557, (CER Directive) shall be considered Essential entities under NIS2.

Lex Specialis may apply where sectoral regulations are at least equivalent.

There are certain exceptions to the above guide, please consult the text of the Directive for a full and comprehensive list of all exceptions.

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

NCSC National Cyber Security Centre

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

NCSC
National Cyber
Security Centre

NIS 2
Sectors in scope

NIS2 will apply to a wider and deeper pool of entities than currently covered by the NIS Directive.

3

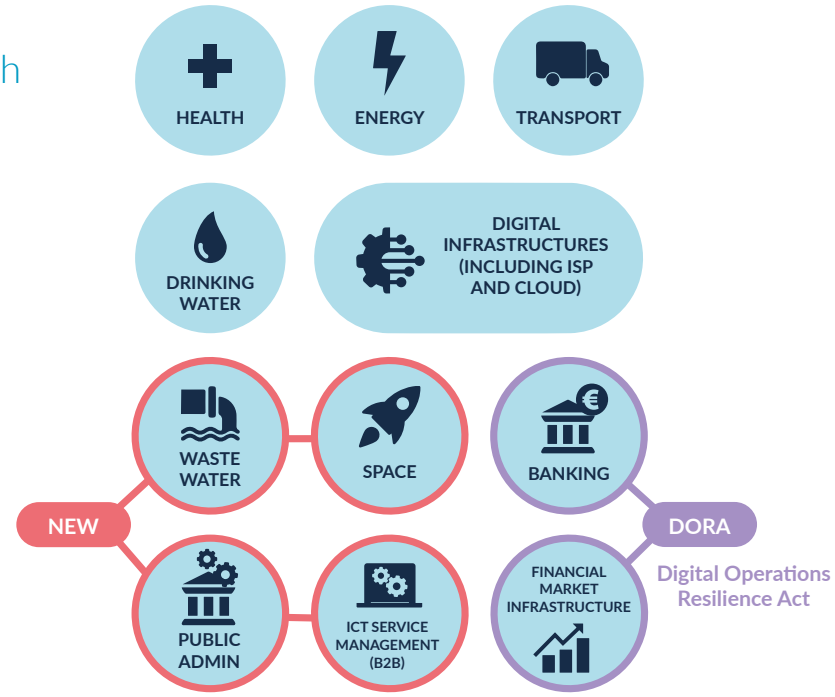
www.ncsc.gov.ie

3

Sectors in scope

NIS2 will apply to a wider and deeper pool of entities than currently covered by the NIS Directive. NIS2 includes new sectors whilst broadening the criteria for inclusion of entities, categorised as essential or important, within existing sectors. The sectors are divided into two groups: “Sectors of High Criticality” and “Other Critical Sectors”.

Annex 1 - Sectors of High Criticality



Annex 2 - Other Critical Sectors

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications
NCSC National Cyber Security Centre

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

NCSC
National Cyber
Security Centre

NIS 2
Incident Notification

4

www.ncsc.gov.ie

4

Incident Notification

NIS2 imposes notification obligations in phases, for incidents which have a 'significant impact' on the provision of their services. These notifications must be made to the relevant competent authority or CSIRT (Computer Security Incident Response Team).

Where appropriate, entities shall notify the recipients of their services of significant incidents.

When in the public interest, the CSIRT or relevant competent authority may inform the public about the significant incident or may require the entity to do so.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications
NCSC National Cyber Security Centre

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

NCSC
National Cyber
Security Centre

NIS 2
Cyber Security Risk Management Measures

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

5

www.ncsc.gov.ie

5

Cyber Security Risk Management Measures

Essential and Important entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems which underpin their services, and prevent or minimise the impact of incidents on their and other services.

Such measures shall be based on an all-hazards approach that aims to protect the network and information systems and the physical environment of those systems from incidents, and must include at least the following:

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

All measures must be:

- Proportionate to risk, size, cost, and impact & severity of incidents
- Take into account the state-of-the-art, and where applicable relevant European and international standards

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

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

NCSC
National Cyber Security Centre

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

NCSC
National Cyber
Security Centre

NIS 2
Essential and Important Entities - Supervision

The former distinction between “operators of essential services” (OES) and “digital service providers” (DSP) in the original NIS Directive is replaced by a distinction between “essential” and “important” entities.

6

www.ncsc.gov.ie

6

Essential and Important Entities - Supervision

The former distinction between "operators of essential services" (OES) and "digital service providers" (DSP) in the original NIS Directive is replaced by a distinction between "essential" and "important" entities.

No more categorisation of OES and DSP

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.

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

NCSC National Cyber Security Centre

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

NCSC
National Cyber
Security Centre

NIS 2
Enforcement and Penalties

NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance

7

www.ncsc.gov.ie

7

Enforcement and Penalties

NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance, including:

A	Issue **warnings** for non-compliance
B	Issue **binding instructions**
C	Order to **cease conduct** that is non-compliant
D	Order to **bring risk management measures** or reporting obligations in compliance to a specific manner and within a specified period
E	Order to **inform the natural or legal person(s)** to whom they provide services or activities which are potentially affected by a significant cyber threat
F	Order to **implement the recommendations** provided as a result of a security audit within a reasonable deadline
G	**Designate a monitoring officer** with well-defined tasks over a determined period of time to oversee the compliance
H	Order to **make public** aspects of non-compliance
I	Impose administrative **fines**
J	An essential entities **certification or authorisation concerning the service can be suspended**, if deadline for taking action is not met
K	And those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily **prohibited from exercising managerial functions** (applicable to essential entities only, not important entities).

NIS2 makes provision to impose administrative fines for infringements.

A maximum of **at least 10,000,000 EUR or up to 2% of the total worldwide annual turnover** of the undertaking to which the **ESSENTIAL ENTITY** belongs in the preceding financial year, whichever is higher.

A maximum of **at least 7,000,000 EUR or 1,4% of the total worldwide annual turnover** of the undertaking to which the **IMPORTANT ENTITY** belongs in the preceding financial year, whichever is higher.

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

NCSC National Cyber Security Centre

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

NCSC
National Cyber
Security Centre

NIS 2
Management Responsibilities

Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities.

8

www.ncsc.gov.ie

8

Management Responsibilities

Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities. Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans and administrative fines as provided for in the implementing national legislation.

Management bodies of essential and important entities must:

Approve the adequacy of the cybersecurity risk management measures taken by the entity;

Supervise the implementation of the risk management measures;

Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity

Offer similar training to their employees on a regular basis;

Be accountable for the non-compliance

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

NCSC
National Cyber Security Centre

Contact Us

National Cyber Security Centre,
Department of the Environment, Climate and Communications,
29-31 Adelaide Road, Dublin, D02 X285, Ireland.

info@ncsc.gov.ie

+353 1 6782333

https://twitter.com/ncsc_gov_ie

www.ncsc.gov.ie

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

NCSC
National Cyber
Security Centre