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

1  Introduction
2  Essential and Important Entities
3  Sectors in scope
4  Incident Notification
5  Cyber Security Risk Management Measures
6  Essential and Important Entities - Supervision
7  Enforcement and Penalties
8  Management Responsibilities
NIS2 seeks to further enhance the work started in the NIS Directive to build a high common level of cybersecurity across the European Union.
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.

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

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

<table>
<thead>
<tr>
<th>SECTOR</th>
<th>SUB-SECTOR</th>
<th>LARGE ENTITIES</th>
<th>MEDIUM ENTITIES</th>
<th>SMALL &amp; MICRO ENTITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENERGY</td>
<td></td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>TRANSPORT</td>
<td></td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>BANKING</td>
<td></td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>FINANCIAL MARKET INFRASTRUCTURE</td>
<td></td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>HEALTH</td>
<td></td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>DRINKING WATER</td>
<td></td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>WASTE WATER</td>
<td></td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>DIGITAL INFRASTRUCTURE</td>
<td>Qualified trust service providers</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
</tr>
<tr>
<td></td>
<td>DNS service providers (excluding root name servers)</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
</tr>
<tr>
<td></td>
<td>TLD name registries</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
</tr>
<tr>
<td></td>
<td>Providers of public electronic communications networks</td>
<td>ESSENTIAL ESSENTIAL IMPORTANT</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
</tr>
<tr>
<td></td>
<td>Non-qualified trust service providers</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td></td>
<td>Internet exchange point providers</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td></td>
<td>Cloud computing service providers</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td></td>
<td>Data centre service providers</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td></td>
<td>Content delivery network providers</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>ICT-SERVICE MANAGEMENT (B2B)</td>
<td>Managed service providers, managed security service providers</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
<tr>
<td>PUBLIC ADMINISTRATION ENTITIES</td>
<td>Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
<td>ESSENTIAL ESSENTIAL ESSENTIAL</td>
</tr>
<tr>
<td></td>
<td>Of regional governments: risk based.(Optional for Member States: of local governments)</td>
<td>IMPORTANT IMPORTANT IMPORTANT</td>
<td>IMPORTANT IMPORTANT IMPORTANT</td>
<td>IMPORTANT IMPORTANT IMPORTANT</td>
</tr>
<tr>
<td>SPACE</td>
<td>Operators of ground-based infrastructure (by Member State)</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
<td>ESSENTIAL IMPORTANT NOT IN SCOPE</td>
</tr>
</tbody>
</table>

## Annex I: Sectors of high criticality

- **ENERGY**: Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.
- **TRANSPORT**: Air (commercial carriers; airports; Air traffic control [ATC]; rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)
  - **Special case**: public transport: only if identified as CER (see notes on page 2)
- **BANKING**: Credit institutions
  - **Attention**: DORA lex specialis – see note on page 2
- **FINANCIAL MARKET INFRASTRUCTURE**: Trading venues, central counterparties
  - **Attention**: DORA lex specialis – see note on page 2
- **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
  - **Special case**: entities holding a distribution authorization for medicinal products: only if identified as CER (see note on page 2)
- **DRINKING WATER**: (only if it is an essential part of their general activity)
- **WASTE WATER**: (only if it is an essential part of their general activity)
- **DIGITAL INFRASTRUCTURE**: Qualified trust service providers
  - **DNS service providers (excluding root name servers)**
  - **TLD name registries**
  - **Providers of public electronic communications networks**
  - **Non-qualified trust service providers**
  - **Internet exchange point providers**
  - **Cloud computing service providers**
  - **Data centre service providers**
  - **Content delivery network providers**
- **ICT-SERVICE MANAGEMENT (B2B)**: Managed service providers, managed security service providers
- **PUBLIC ADMINISTRATION ENTITIES**: Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).
- **Of regional governments: risk based.** (Optional for Member States: of local governments)
- **SPACE**: Operators of ground-based infrastructure (by Member State)
<table>
<thead>
<tr>
<th>SECTOR</th>
<th>SUB-SECTOR</th>
<th>LARGE ENTITIES</th>
<th>MEDIUM ENTITIES</th>
<th>SMALL &amp; MICRO ENTITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>POSTAL AND COURIER SERVICES</td>
<td></td>
<td>IMPORTANT</td>
<td>IMPORTANT</td>
<td>NOT IN SCOPE</td>
</tr>
<tr>
<td>WASTE MANAGEMENT</td>
<td>(only if principal economic activity)</td>
<td>IMPORTANT</td>
<td>IMPORTANT</td>
<td>NOT IN SCOPE</td>
</tr>
<tr>
<td>CHEMICALS</td>
<td>Manufacture, production, distribution</td>
<td>IMPORTANT</td>
<td>IMPORTANT</td>
<td>NOT IN SCOPE</td>
</tr>
<tr>
<td>FOOD</td>
<td>Wholesale production and industrial production and processing</td>
<td>IMPORTANT</td>
<td>IMPORTANT</td>
<td>NOT IN SCOPE</td>
</tr>
<tr>
<td>MANUFACTURING</td>
<td>(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)</td>
<td>IMPORTANT</td>
<td>IMPORTANT</td>
<td>NOT IN SCOPE</td>
</tr>
<tr>
<td>DIGITAL PROVIDERS</td>
<td>online marketplaces, search engines, social networking platforms</td>
<td>IMPORTANT</td>
<td>IMPORTANT</td>
<td>NOT IN SCOPE</td>
</tr>
<tr>
<td>RESEARCH</td>
<td>Research organisations (excluding education institutions)</td>
<td>IMPORTANT</td>
<td>IMPORTANT</td>
<td>NOT IN SCOPE</td>
</tr>
</tbody>
</table>

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.
NIS 2
Sectors in scope

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

www.ncsc.gov.ie
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
NIS 2
Incident Notification

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

www.ncsc.gov.ie
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
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.
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

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

Authorities can take a risk based approach to prioritise supervisory tasks.
NIS 2
Enforcement and Penalties

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

www.ncsc.gov.ie
### Enforcement and Penalties

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

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

**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.
Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities.
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.
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
𝕏 https://twitter.com/ncsc_gov_ie

www.ncsc.gov.ie