# NIS2 FAQS -NTA WEBSITE

**1) What is NIS2 Regulations?**

The NIS2 Directive (Directive (EU) 2022/2555) is the European Union's cybersecurity legislation designed to achieve a high common level of security of network and information systems across the EU. It establishes cybersecurity risk management, governance, incident reporting, business continuity and supply chain security requirements for organisations operating in sectors that are important to society and the economy. The number of sectors of high criticality increases from 7 to 11 and the number of other critical sectors increases from 1 to 7.

**2) Who are the National Competent Authorities (NCAs) under NIS2?**

The designated National Competent Authorities in Ireland are:

- **National Cyber Security Centre (NCSC)**: Lead National Competent Authority and Single Point of Contact (SPOC) for NIS2.
- **Commission for Regulation of Utilities (CRU)**: Energy-related sectors, Drinking water and Wastewater
- **Commission for Communications Regulation (ComReg)**: Digital Infrastructure, ICT Service Management, Space, and Digital Providers
- **Central Bank of Ireland (CBI)**: Banking and Financial Market
- **Minister of Transport:** Maritime
- **National Transport Authority:** Road
- **Commission of Rail Regulation:** Rail
- **Irish Aviation Authority:** Aviation
- **Healthcare:** Department of Health

The NCSC for all other sectors set out in Schedule I and II

**3) Who will be the competent authority for the NIS2 road transport subsector in Ireland?**

Subject to enactment of the national transposing legislation, the published General Scheme of the National Cyber Security Bill provides for the National Transport Authority to act as the sectoral competent authority for the road transport subsector. It provides for the National Cyber Security Centre to perform the lead national and coordination functions specified in the legislation.

Until the legislation is enacted, the existing Irish NIS framework continues to apply to organisations already designated under that framework.

**4) What does the road transport subsector cover under NIS2?**

The road transport subsector includes road authorities responsible for traffic management control and operators of intelligent transport systems, as those terms are defined in the applicable EU legislation.

The scope does not automatically include every organisation that owns, operates, maintains or supplies road infrastructure or technology. An organisation must assess whether it is a type of entity covered by NIS2, whether it meets the applicable size criteria, and whether any size-independent inclusion criteria apply.

Public passenger transport operators are addressed separately and may fall within scope should they be identified as critical entities under the Critical Entities Resilience framework.

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4637829

https://ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf

**5) Which organisations may need to assess whether they are in scope?**

Organisations that may need to carry out a NIS2 scope assessment include:

- road authorities with responsibility for traffic management control;
- organisations that operate intelligent transport systems;
- public passenger transport operators identified as critical entities under the applicable critical-entities framework; and
- organisations separately covered by another NIS2 sector or subsector, such as certain managed service providers, cloud service providers or data centre service providers.

Supplying technology, maintenance or other services to a road-sector organisation does not, by itself, mean that a supplier is regulated as a road entity under NIS2. Suppliers may nevertheless have important contractual and supply-chain cybersecurity obligations.

NIS2 generally covers medium-sized and large entities of a type listed in Annex I or Annex II. Entity size is assessed using the EU SME definition, including the rules concerning partner and linked enterprises. Certain entities may also be brought within scope regardless of size, for example because they are the sole provider of an essential service or because disruption could have a significant impact on public safety, public security or public health.

**6) How will entities be classified "Essential" vs "Important"?**

NIS2 classifies in-scope entities by criticality and size:

- ❑ Essential entities (Annex I sectors of high criticality, typically large): subject to ex-ante (proactive) supervision.
- ❑ Important entities (Annex II or medium-sized in Annex I): subject to ex-post (reactive) supervision. Road transport is in Annex I, so large road-sector entities will generally be Essential; medium-sized entities will generally be Important.

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4637829

**7) What role is the NTA expected to perform?**

Subject to the final national legislation, the NTA is preparing to perform the supervision and enforcement functions assigned to the competent authority for the road transport subsector. These are expected to include:

- supporting the identification and registration of entities within the relevant subsector;
- supervising compliance with applicable cybersecurity risk-management and incident-reporting obligations;
- conducting or commissioning supervisory activities in accordance with the legislation;

- issuing guidance and engaging with the road transport sector; and
- coordinating with the NCSC and other competent authorities.

The NTA's final responsibilities and powers will be determined by the enacted legislation.

**8) What is the NTA doing to prepare for its role as NCA?**

Ireland is still finalising the National Cyber Security Bill. In the interim, sectoral NCAs are collaborating via the NCA Forum led by NCSC; the National Transport Authority is expected to coordinate similarly - aligning to draft Irish RMM guidance and to the ENISA technical implementation guidance for consistent supervision practices.

**9) Where can the legal instruments and official guidance be found?**

- ✓ NIS2 Directive (EU) 2022/2555 (scope, obligations, reporting, supervision/enforcement) and EU overview pages: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- ✓ Ireland's General Scheme of the National Cyber Security Bill (designation of competent authorities incl. NTA for road): https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/general-scheme-of-the-national-cyber-security-bill-2024/
- ✓ Commission Implementing Regulation (EU) 2024/2690 (technical/methodological requirements for certain sectors/subsectors and "significant incident" criteria - note its current applicability is limited to specific digital sectors): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402690
- ✓ NCSC Ireland: NIS2 site, FAQ, Quick Reference Guide, and draft RMM guidance; CyFun framework announcement. (see NCSC section further in this document)

**10) When and how do road-sector entities register?**

The NIS2 registration portal (and incident reporting portal) will become available only after the national legislation is enacted. Until then, entities should prepare by assessing scope and implementing cybersecurity risk-management measures.

**11) What are the incident reporting expectations?**

NIS2 establishes a staged reporting process for significant incidents, including an early warning within 24 hours, an incident notification within 72 hours and, generally, a final report within one month. The applicable Irish reporting arrangements, forms and portal will be confirmed when the national legislation and supporting procedures are in place.

Organisations already regulated under the existing NIS framework should continue to follow their current reporting obligations.

**12) What sanctions does NIS2 provide for?**

NIS2 requires Member States to provide for effective, proportionate and dissuasive enforcement measures. For infringements of the cybersecurity risk-management or reporting obligations, the Directive requires maximum administrative fine levels of at least:

- €10 million or 2% of total worldwide annual turnover, whichever is higher, for essential entities; and

- €7 million or 1.4% of total worldwide annual turnover, whichever is higher, for important entities.

The national legislation will determine how these sanctions and other enforcement measures apply in Ireland, including their application to public administration entities. NIS2 also places governance responsibilities on the management bodies of essential and important entities.

**13) How does NIS2 interact with the CER Directive (critical entities)?**

There is interplay between NIS2 and the CER Directive (EU) 2022/2557 in determining certain transport cases (e.g., public passenger transport special case). Irish guidance notes that coverage may depend on CER identification in some scenarios; detailed national transposition will clarify.

**14) Which Member State supervises an organisation operating in more than one EU country?**

As a general rule, an entity is subject to the jurisdiction of the Member State in which it is established. Special jurisdiction rules apply to certain categories of digital and ICT service provider. Organisations operating across several Member States should assess the applicable jurisdiction rules based on the type of service they provide and where they are established.

**15) How can a road entity check if it is in scope right now?**

Use the NCSC's resources:

- ✓ "Am I in Scope?" tool (indicative) and the NIS2 FAQ for Ireland.
- ✓ Review EU/Irish sector lists (Annex I & II) and size thresholds; consider size-independent criteria (sole provider, public safety/systemic risk).

**16) What's the current status of NIS2 transposition in Ireland?**

Ireland did not meet the NIS2 transposition deadline of 17 October 2024. On 8 July 2026, the European Commission announced that it had referred Ireland to the Court of Justice of the European Union for failing to notify full transposition of the Directive.

The National Cyber Security Bill remains the proposed vehicle for transposition. Until the new legislation is enacted, the existing NIS framework continues to apply to organisations already designated under it.

This page will be updated when the national legislation is enacted.

**17) What should road-sector organisations do now (practical steps)?**

- ✓ Determine scope & classification (Annex I transport/road; entity size/criticality; any size-independent conditions).
- ✓ Map services and dependencies (assets, systems, data flows, third parties- including ITS suppliers and maintenance providers).
- ✓ Align with Irish NCSC Risk Management Measures guidance and prepare evidence across governance, asset management, incident handling, supply chain security, business continuity, secure development/maintenance, and training; consider CyFun as a baseline maturity framework.
- ✓ Plan incident reporting (roles, 24/7 contact channel, detection thresholds, draft templates) pending national forms/portals.
- ✓ Engage leadership - NIS2 sets direct management board-level accountability.

IMPORTANT

This information is provided for general awareness and reflects the NIS2 Directive, published Irish policy material and the proposed approach to national transposition as at [date]. The National Cyber Security Bill has not yet been enacted. The final legal position will be determined by the enacted legislation. Organisations should obtain professional advice where necessary.

## NIS2 DIRECTIVE INFORMATION

Transposition of NIS1 Directive into Irish law :
https://www.irishstatutebook.ie/eli/2018/si/360/made/en/print

NIS2 Directive (Directive (EU) 2022/2555):
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

General Scheme for the National Cyber Security Bill 2024: The draft heads of bill to transpose NIS2 Directive into Irish law published by Government
https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/general-scheme-of-the-national-cyber-security-bill-2024/

Commission Implementing Regulation (EU) 2024/2690: Outlines risk management measures and criteria in relation to significant incidents for certain sectors and subsectors :

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402690

Commission Recommendation 2003/361/EC: Commission recommendation concerning the definition of enterprise size which inputs into whether an entity is in scope for NIS2:

https://eur-lex.europa.eu/eli/reco/2003/361/oj

Commission's user guide to the SME definition: provides general guidelines on definition of SME enterprise size which inputs into whether an entity is in scope for NIS2:

https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1

## NCSC

NCSC website for general information: https://www.ncsc.gov.ie/NCSC

NCSC NIS2 website: https://www.ncsc.gov.ie/nis2/FAQ/

Am I in Scope: NCSC tool which will help entities understand if they are in scope for NIS2:
https://www.ncsc.gov.ie/nis2/amiinscope/

NIS2 Quick Reference Guide: NCSC document providing high level information on NIS2:
https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf

NCSC FAQs on NIS2: https://www.ncsc.gov.ie/nis2/FAQ/

NIS2 Risk Management Measures Guidance: provides guidance on measures and granular actions under NIS2 for entities to improve their cybersecurity posture :
https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf

CyFun FAQ: NCSC FAQs on Cyber Fundamentals Framework:
https://www.ncsc.gov.ie/CyFun/CyFunFAQ/

## ENISA

ENISA NIS2 website: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2

ENISA 2024 Report on the State of the Cybersecurity in the Union: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

ENISA NIS2 Technical Implementation Guidance: offers practical advice to help entities implement the Commission Implementing Regulations (EU) 2024/2690: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf