FEDIL

Publikation

NIS 2.0 DIRECTIVE

Zusammenfassung / Inhalte

The NIS 2.0 directive on cybersecurity was adopted on December 14, 2022 and repeals the 2016 NIS directive. (Full text of the Directive HERE)

This directive aims to ensure a high common level of cybersecurity of networks and information systems across Europe, and to strengthen the resilience of the European Union's IT infrastructures against cyberattacks.

Compared with NIS 1, the NIS 2.0 directive includes a **wider variety of organizations** from different sectors.

For the first time, this directive takes into account the **security of the information and communication technology supply chain**.

In addition, the NIS 2.0 directive introduces more stringent supervisory measures for national authorities, as well as stricter requirements for enforcement.

SECTORS IN SCOPE

The sectors concerned fall into 2 categories, each covering many more areas than in the NIS 1:

- The **11 « Sectors of High Criticality »** are identified in Annex 1 : Energy – Transport – Banking – Financial market infrastructures – Health – Drinking water – Waste water – Digital Infrastructure – ICT service management (business-to-business) – Public administration – Space.
- The **7 « Other Critical Sectors »** are indentified in Annex 2 : Postal and courier services – Waste management – Manufacture, production and distribution of chemicals – Production, processing and distribution of food – Manufacturing – Digital providers – Research.

Check the list of sectors, sub-sectors and types of entities in Annex 1 and 2 **HERE** to confirm if your activity falls within the scope of the NIS 2.0 directive.

ENTITIES IN SCOPE

The NIS 2.0 directive introduces a proportionality mechanism that distinguishes two categories of regulated actors according to the level of criticality of the associated sector: **„Essential Entities"** (EE) and **„Important Entities"** (EI).

Company size and turnover are also parameters to be taken into account when distinguishing between categories of player. It consists in the application of a **size-cap rule** covering almost **all SMEs and large companies** and which operate within the sectors and provide the types of service or carry out the activities covered by the NIS 2.0 directive, falling within its scope.

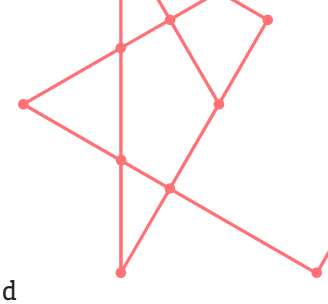
- Medium-sized: >= 50 employees or turnover of >= 10 million euros
- Large: >= 250 employees or turnover of >= 50 million euros

Small and micro enterprises fall outside the scope of NIS 2.0, unless the national authorities consider them essential if they fulfil specific criteria that indicate a key role for society, the economy or for particular sectors or types of service (check the exceptions explained in Article 2. (2) and Article 2. (4)).

ESSENTIAL ENTITIES

1) The following entities shall be considered to be **Essential Entities**:

a. entities of a type referred to in Annex I which exceed the ceilings for medium-sized enterprises provided for in Article 2(1) of the Annex to Recommendation 2003/361/EC*;
b. qualified trust service providers and top-level domain name registries as well as DNS service providers, **regardless of their size**;
c. providers of public electronic communications networks or of publicly available electronic communications services which qualify as medium-sized enterprises or exceed the ceiling for medium-sized entreprises under Article 2 of the Annex to Recommendation 2003/361/EC*;
d. public administration entities referred to in Article 2(2), point (f)(i);



- (f) the entity is a public administration entity:
  - (i) of central government as defined by a Member State in accordance with national law; or

e. any other entities of a type referred to in Annex I or II that are identified by a Member State as essential entities pursuant to Article 2(2), points (b) to (e);
   a. the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
   b. disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;
   c. disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
   d. the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

f. entities identified as critical entities under Directive (EU) 2022/2557, referred to in Article 2(3) of this Directive :
   (3) Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities;

g. if the Member State so provides, entities which that Member State identified before 16 January 2023 as operators of essential services in accordance with Directive (EU) 2016/1148 (NIS 1) or national law.

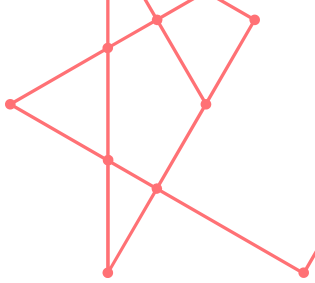
IMPORTANT ENTITIES

2) Entities of a type referred to in Annex 1 or 2 which do not qualify as essential entities pursuant to paragraph 1 of this Article shall be considered to be **Important Entities**. This includes entities identified by Member States as important entities pursuant to Article 2(2), points (b) to (e).

References

* NIS 2.0 directive: Article 2 – Scope

2. 2) Regardless of their size, this Directive also applies to entities of a type referred to in Annex I or II, where:
   a. services are provided by:
      i. providers of public electronic communications networks or of publicly available electronic communications services;
      ii. trust service providers;
      iii. top-level domain name registries and domain name system service providers;
   b. the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;
   c. disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;
   d. disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;
   e. the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for



other interdependent sectors in the Member State;
   f. the entity is a public administration entity:
      i. of central government as defined by a Member State in accordance with national law; or
      ii. at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.
3. 3) Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.
4. 4) Regardless of their size, this Directive applies to entities providing domain name registration services.

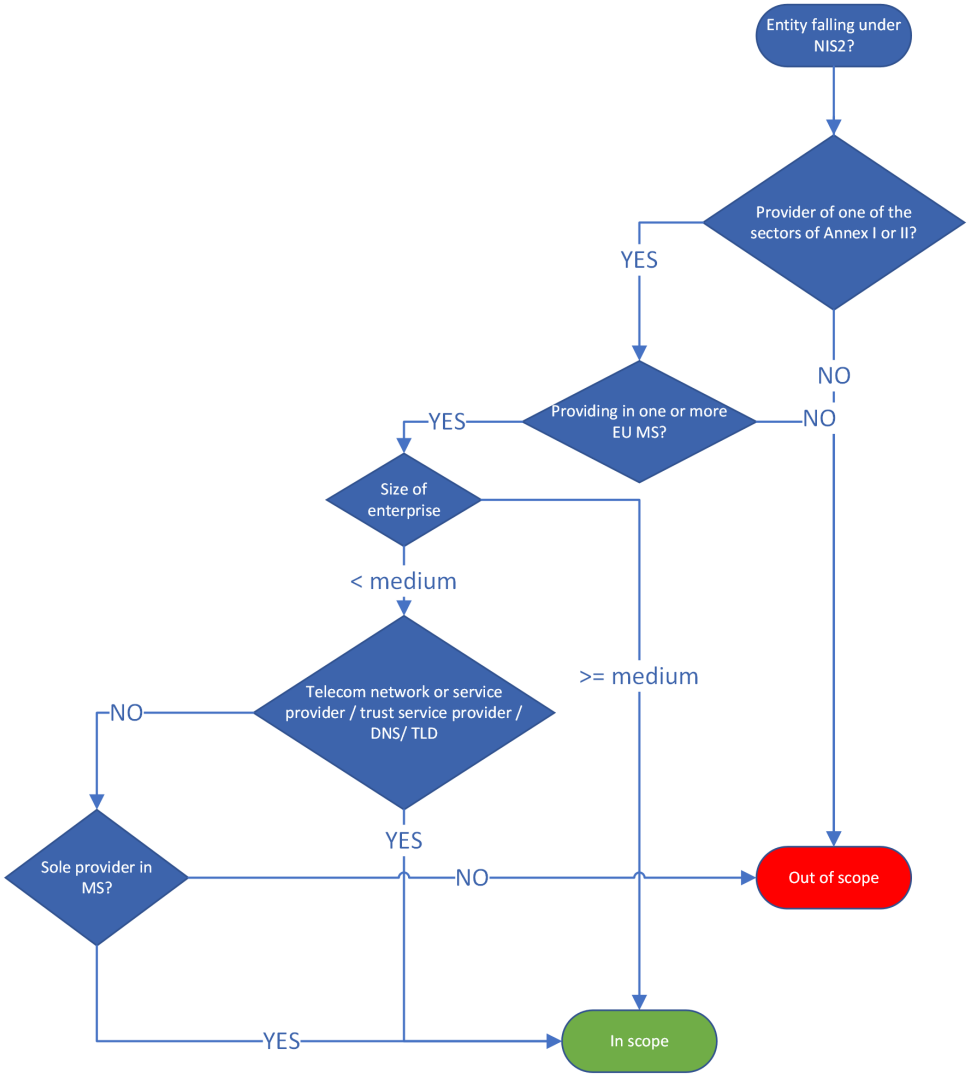
* Article 2 of Commission Recommendation 2003/361/EC
Staff headcount and financial ceilings determining enterprise categories

1. 1) The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.
2. 2) Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
3. 3) Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.

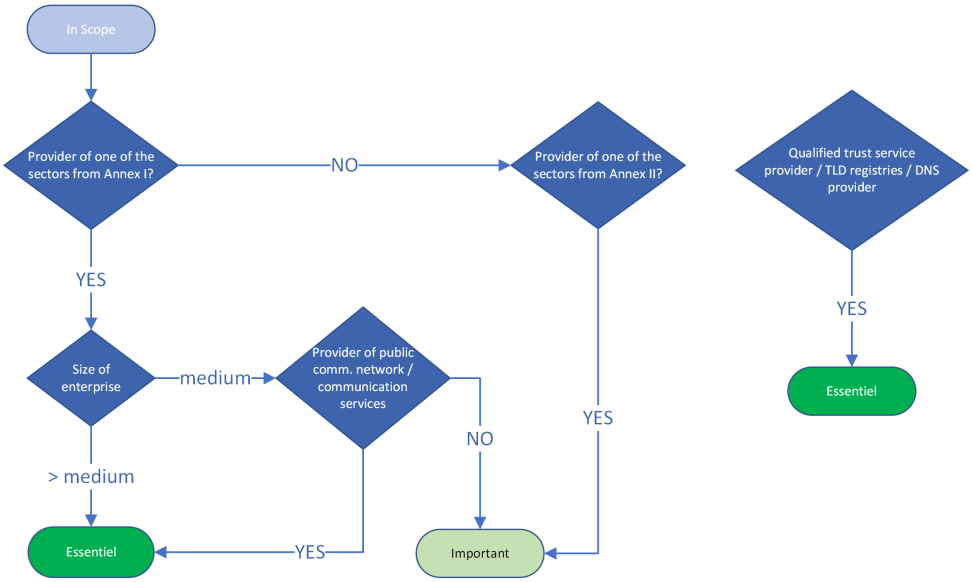
EEs and IEs face the same obligations, but those in the second category are subject to a lighter supervisory and enforcement regime.

FLOW CHARTS

SCOPE



ESSENTIAL – IMPORTANT ENTITIES



MEASURES TO IMPLEMENT

EEs and IEs will have to implement an efficient cybersecurity policy and take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other service.

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

a. policies on risk analysis and information system security;la gestion des incidents;
b. incident handling;
c. business continuity, such as backup management and disaster recovery, and crisis management;
d. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
e. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
g. basic cyber hygiene practices and cybersecurity training;
h. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
i. human resources security, access control policies and asset management;
j. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Taking into account the « **state-of-the-art** » and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred shall ensure a level of security of network and information systems appropriate to the risks posed.

When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

Entities may be required to carry out regular tests and technical audits, including penetration tests and vulnerability scans, to assess the effectiveness of the security measures deployed.

Entities will also need to focus on knowledge sharing. They will share information on cyber security risks and measures with each other and with the local government through communities and automatized tools. This will help to create a centralized European 'vulnerability register' of ICT products and services, for which every member state will have a dedicated point of contact.

INCIDENT NOTIFICATION

The directive introduces a 2-stage incident notification mechanism, so that

information can be gathered as quickly as possible to prevent the spread of similar attacks, and to enrich future resilience plans.

1. 1) An **early warning** of all significant incidents must be done **within 24 hours** ;
   Then,
2. 2) **Within 72 hours**, an **incident notification** which shall update the information shared in the early warning and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise.

A final report not later than **one month** after the submission of the incident notification shall be provided as a follow-up measure.

MANAGEMENT'S ACCOUNTABILITY

The NIS 2.0 directive introduces **greater responsibility for legal representatives and decision makers such as CEOs, board members, company directors (RCS registered persons)**. Indeed, members of the management bodies of EEs and IEs are required to **undergo training, approve the risk management measures undertaken, and oversee their implementation**. In the event of a breach of their obligations, they will be directly liable.

SANCTIONS IN CASE OF NON-COMPLIANCE

Entities that fail to comply with the regulations set forth by the national transposition of the NIS 2.0 directive, are subject to a number of possible sanctions, such as:

- Imposing of deadlines for compliance ;
- Withdrawal of certification ;
- Mandatory discontinuation ;
- Fines or administrative sanctions ;
- Administrative liability.

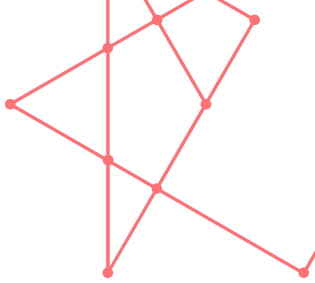
Administrative sanctions may add up to a maximum of :

- **Essential Entities: 10 million euros** or 2% of the company's total worldwide annual turnover in the preceeding financial year, whichever is higher.
- **Important Entities: 7 million euros** or 1,4% of the company's total worldwide annual turnover in the preceeding financial year, whichever is higher.

If you have any questions about the NIS 2.0 directive or wish to confirm/inform FEDIL that your organization falls within its scope, please contact celine.tarraube@fedil.lu.

CONFERENCE – ONE YEAR TO GO: HOW TO PREPARE FOR NIS 2.0 DIRECTIVE? | 17.10.2023

Céline Tarraube (FEDIL) – One year to go: How to prepare for NIS 2.0 Directive?
Laurent de la Vaissière (KPMG) – Compliance Odyssey
Sheila Becker (ILR) – Collaborative approach
Cécile Gellenoncourt (CSSF) – From NIS1 to NIS2



François Thill (MECO) – Increase cybersecurity maturity
Pascal Steichen (LHoC) – Securing Luxembourg's Digital Future