FEDIL

Publication

TEST LISTS

Résumé / Contenu

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 – 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 entity in Annex 1 and 2 **HERE** to confirm if your activity falls within the scope of the Directive.

ENTITIES IN SCOPE

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 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)

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

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. 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. 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.

MEASURES TO IMPLEMENT

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 audits and technical and, 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.

1. Item 1
2. Item 2
    - Item 2.1
    - Item 2.2
        1. Item 2.2.1
        2. Item 2.2.2
        3. Item 2.2.3
            - Item 2.2.3.1
            - Item 2.2.3.2
            - Item 2.2.3.3
                1. Item 2.2.3.3.1
                2. Item 2.2.3.3.2
                3. Item 2.2.3.3.3
                    - Item 2.2.3.3.3.1
                    - Item 2.2.3.3.3.2
    - Item 2.3
    - Item 2.4
        1. Item 2.4.1
        2. Item 2.4.2
        3. Item 2.4.3
        4. Item 2.4.4
            - Item 2.4.4.1
            - Item 2.4.4.2
            - Item 2.4.4.3
                1. Item 2.4.4.3.1
                2. Item 2.4.4.3.2
3. Item 3
4. Item 4
    1. Item 4.1
    2. Item 4.2
    3. Item 4.3
        - Item 4.3.1
        - Item 4.3.2
        - Item 4.3.3
            1. Item 4.3.3.1
            2. Item 4.3.3.2
            3. Item 4.3.3.3
                - Item 4.3.3.3.1
                - Item 4.3.3.3.2

UNION DES ENTREPRISES LUXEMBOURGEOISES