Version 2.0
02/2025

CENTRE FOR CYBERSECURITY BELGIUM

Frequently Asked Questions (FAQ) NIS2 in Belgium

The purpose of this document is to answer frequently asked questions about the NIS2 legal framework in Belgium. It supplements the information already available on the CCB website and on Safeonweb@Work.

Version 2.0 entails the following changes (new numbering due to insertions):

Added questions	Extended questions
1.2, 1.6, 1.8, 1.13, 1.15, 1.15.1, 1.15.2, 1.15.3, 1.15.4, 1.15.5, 1.16, 1.16.1, 1.16.2, 1.16.3, 1.16.4, 1.16.5, 1.16.6, 1.16.7, 1.20, 1.21.2, 1.21.3, 1.22, 1.22.1, 1.22.2, 1.22.3, 1.22.4, 1.22.5, 1.22.6, 1.22.7, 1.22.8, 1.22.9, 1.22.10, 1.22.11, 1.22.12 2.2, 2.3, 2.6, 2.7, 2.8, 2.9 3.3.2, 3.4, 3.7, 3.8, 3.9, 3.10, 3.11, 3.13.2, 3.13.3, 3.13.4, 3.13.5, 3.13.6, 3.13.7, 3.13.8, 3.13.9, 3.13.10 4.3, 4.5, 4.7, 4.10, 4.12, 4.16 5.2, 5.3	1.3, 1.5, 1.12, 1.14, 1.17, 1.19, 1.21.1 2.4, 2.5 3.2, 3.3, 3.3.1, 3.6, 3.14 4.2.1, 4.4, 4.6, 4.9, 4.11, 4.14 5.1

A correlation table is available at the end of the document.

Table of contents

Abbreviations & References

The following abbreviations and references are used in this document:

- BELAC: Belgian Accreditation Body
- CAB: Conformity Assessment Body
- CCB: Centre for Cybersecurity Belgium (national cybersecurity authority & national CSIRT)
- CSIRT: Computer Security Incident Response Team (in Belgium the national CSIRT is the CCB)
- CyFun®: Cyberfundamentals Framework (available on SafeonWeb@Work)
- DORA: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (available on Eur-Lex)
- GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (available on Eur-Lex)
- NCCN: National Crisis Centre
- NIS1 Law: Law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security (available on Justel)
- NIS1 Directive: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (available on Eur-Lex)
- NIS2 Directive : Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a common high level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (available on Eur-Lex)
- NIS2 Law: Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (available on Justel)
- NIS2 Royal decree: Royal decree of 9 June 2024 implementing the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (available on Justel)
- Recommendation (2003/361/EC): Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (available on Eur-Lex)

1. General - Scope of application

1.1. What are the objectives of the NIS2 law?

Directive 2022/2555 (known as "NIS2") and the Belgian NIS2 law transposing it, aim to strengthen cyber resilience by focusing on the following key objectives:

1) Cybersecurity protection for essential services provided in the European Union. Compared with the NIS1 Directive, the NIS2 Directive extends the number of essential services covered in various highly critical sectors (Annex I) or other critical sectors (Annex II). The scope of application is now determined mainly by the use of European definitions (such as "type of entity") and a "size-cap" criterion;
2) Reinforcement of the cybersecurity risk-management measures that entities must take, as well as notification of significant incidents (with two categories of essential or important entities);
3) Encourage the sharing of information on cybersecurity incidents and risks between the entities concerned and the national CSIRTs;
4) Strengthening supervision and sanctions;
5) Ensure European and national cooperation.

1.2. What has changed between the NIS1 law and NIS2 law?

The scope of NIS2 has been largely extended compared to NIS1, with an important change of paradigm. Instead of relying on a formal identification procedure, the NIS2 law now relies mainly on two criteria : the service provided (type of entity) by an organisation in specific sectors or subsectors and its size (equivalent to a large or medium enterprise). With certain exceptions, only organisations established in Belgium fall under its NIS2 law, either as “essential” or “important” entities. More information about the scope of NIS2 are available in section 1.3.

Most NIS1 entities (operators of essential service or digital service providers) are subject to the NIS2 law and have to register as a NIS2 entity on the CCB’s platform (https://atwork.safeonweb.be). Entities that have already registered themselves for the CCB’s Early Warning System (EWS) also have to register again. More information about registration is available in section 3.13.1.

The cybersecurity measures that NIS2 entities have to implement are similar to those under NIS1, but the NIS2 law now contains a minimum list of specific measures. Requirements range from supply chain management to vulnerability management and to MFA (Multi Factor Authentication), and are more explicit and detailed than before. More information about cybersecurity measures is available in section 3.2.

The incident notification procedure is now more detailed and extensive. Notification is mandatory for essential and important entities when a significant incident occurs, within certain deadlines (without undue delay and no later than 24 hours for the early warning, 72 hours for the notification and 1 month for the final report). Other incidents, cyberthreats and near-misses can also be notified voluntarily. The NIS1 incident reporting platform has been replaced by a new online form,

accessible by everyone without requiring a login (https://notif.safeonweb.be). More information about incident notification is available in section 3.3.

For entities falling into the banking and financial sectors of the annexes of the NIS2 law, the DORA Regulation (Digital Operational Resilience Act) is a *lex specialis*, meaning that it replaces certain NIS2 obligations, such as those related to cybersecurity measures and incident reporting. More information about DORA is available in section 1.17.

NIS2 emphasizes on the liability of management bodies of NIS2 entities regarding cybersecurity. More information about this liability is available in section 3.9.

The extension of the sectors in scope required a different approach for the supervision:

- Essential entities are subjected to a mandatory regular conformity assessment performed by a conformity assessment body (CAB), or alternatively an inspection by the CCB;
- Important entities may voluntary undergo the same regular conformity assessment and are in any case subject to ex-post controls;

More information about supervision is available in chapter 4.

The same new supervision approach also contains a more extensive regime of administrative sanctions, with various fines and measures available to the supervisory authority. The criminal sanctions from NIS1 have been removed. More information about sanctions is available in section 4.18.

As for the authorities involved in the supervision, the NIS1 sectoral authorities have all become NIS2 sectoral authorities, even though their role has been adapted. The CCB indeed now leads the supervision for all sectors. More information about competent authorities are available in section 4.1.

1.3. What is the scope of the NIS2 law?

Art. 3 to 7 NIS2 law

The NIS2 law applies to public or private entities which are, in principle, established in Belgium (there are a few exceptions to this rule) and which provide a service listed in annex I or II of the law within the European Union.

To be considered as an entity subject to the law, it is sufficient to carry out, regardless of its legal form, at least one of the activities listed in annexes I or II of the law within the European Union and to at least meet the threshold of a medium-sized enterprise within the meaning of European Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (the “size-cap”).

Essential entities are those organisations which provide a service listed in annex I and which meet the thresholds of a large enterprise within the meaning of Recommendation 2003/361/EC.

Important entities are organisations that provide a service:

- listed in annex I and meet the thresholds of a medium-sized enterprise within the meaning of Recommendation 2003/361/EC;
- listed in annex II and meet the thresholds of a medium-sized or large enterprise within the meaning of Recommendation 2003/361/EC;

Article 1 of the Annex of the Recommendation 2003/361/EC considers as an "enterprise" any entity engaged in an economic activity, irrespective of its legal form. This notion can include public administration or public entities when they provide critical services (like others private entities) mentioned in the annexes of the NIS2 directive.

The size-cap rule is not applicable to some types of entities such as public administrations, identified critical entities, trust service providers, top-level domain name registries and domain name system service providers.

It is important to emphasise that the **scope of the NIS2 law covers the whole entity** concerned and not just the activities listed in the annexes of the law.

Unless the definition of the type of entity (service) in the annex takes into account the ancillary or non-essential nature of the activity concerned, an entity falls into the scope of the law **even if the concerned service it provides is only an ancillary or non-essential part of all its activities.**

For more information, see the following sections.

1.4. What is an "entity" under NIS2?

The NIS2 law applies to organisations if they can be qualified as an "entity" in the meaning of the law.

Art. 8, 37° NIS2 law; Art. 6 (35) NIS2-Directive

An "entity" is defined in the NIS2 law as following: "*a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations*".

The NIS2 law applies to all entities individually, even if they are grouped together and held by the same holding company. The scope of application and the obligations of the NIS2 law must thus be analysed by each entity individually, based on its own provided services.

For the public administration sector, the NIS2 directive provides a specific notion of "public administration entity" which allows Member States to take into account each entity recognised as such in accordance with their national public law.

For example, it is possible to distinguish in the public administration sector several distinct NIS2 entities within a single legal person governed by public law - provided that a legally recognised distinction is made between the different public administrations concerned.

1.5. How do you calculate the size of an entity?

For the purposes of the scope of the NIS2 law, the size of the entity is calculated on the basis of the rules in the annex of Recommendation 2003/361/EC. The European Commission has published a detailed explanatory guide and provided a calculation tool.

Art. 3, §§ 1 and 2 NIS2 law & Recommendation 2003/361/CE

An organisation qualifies as a medium-sized enterprise when it:

- employs between 50 and 249 workers (employees, temporary or interim staff, owner-managers, partners, etc.) - workforce calculated in annual work units (AWU); or

- has an annual turnover exceeding 10 million € up to 50 million € and an annual balance sheet total exceeding 10 million € up to 43 million €.

For the application of these financial data thresholds, the organisation concerned has the choice of using either its annual turnover or its total annual balance sheet. **One of these two figures may exceed the threshold for a large enterprise**, without this having any impact on the classification of an organisation as a medium-sized enterprise.

An organisation qualifies as a large enterprise when it:

- employs 250 workers or more (employees, temporary or interim staff, owner-managers, partners, etc.) - workforce calculated in annual work units (AWU); or
- has an annual turnover exceeding 50 million € and an annual balance sheet total exceeding 43 million €.

It should be borne in mind that in situations involving "partner" or "linked" enterprises, a proportional consolidation of the data (workforce and financial) of the entity concerned and of these other entities must be carried out in order to calculate the size.

With certain exceptions, an enterprise is considered a "partner" when it holds between 25% and 50% of the capital or voting rights (whichever is greater) in the entity concerned (or vice versa). This type of relationship describes the situation of enterprises that establish certain financial partnerships with other enterprises, without the former exercising actual direct or indirect control over the latter.

With certain exceptions, an enterprise is considered to be "linked" when it holds more than 50% of the capital or voting rights (whichever is higher) in the entity concerned (or vice versa).

In the case of partner enterprises, the enterprise in question must add to its own data a proportion of the other enterprise's workforce and financial data in order to determine its size. This proportion will reflect the percentage of shares or voting rights held (whichever is greater). In the case of linked enterprises, the enterprise in question must add 100% of the data of the linked enterprise to its own.

For example, if an enterprise has a 30% shareholding in another enterprise, it adds to its own figures 30% of the partner enterprise's workforce, turnover and balance sheet total. If there are several partner companies, the same type of calculation must be made for each partner company located immediately upstream or downstream of the company in question.

Under the NIS2 law, however, a mechanism is provided for enabling the national cybersecurity authority (CCB), in the event of a disproportionate situation, to take account of the degree of independence enjoyed by an entity with regard to its partners and linked enterprises, in particular with regard to the networks and information systems it uses to provide its services and with regard to the services it provides. These elements will have to be demonstrated to the CCB, on a case-by-case basis, by the organisation wishing to benefit from it. The application of this mechanism may result in an organisation being reclassified as an important entity rather than an essential entity or being excluded from the scope of the law altogether.

According to article 4 of the annex of the Recommendation, the headcount and financial data to take into account relate to those from the latest approved accounting period, calculated on an annual basis, from the date of the closure of the accounts, VAT excluded. To change from one size qualification to another, the enterprise must exceed or fall below a threshold for at least two

consecutive years. An enterprise fluctuating between two thresholds might have to go back more than two years to determine its qualification.

See also section 1.21.3. and the detailed guide to size calculation for more information.

1.6. Why does what the CCB website and FAQ state about the size-cap seem to be different from what is written in the EU Recommendation 2003/361?

The text of Recommendation 2003/361 refers to 'and' when describing the thresholds of an SME. This is because the Recommendation describes the thresholds from the largest enterprise size to the smallest. On the website of the CCB however, and for the purpose of NIS2, these thresholds are described from the smallest to the largest enterprise, which results in a different description. As explained hereafter, the thresholds do remain the same:

- "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."

  ➔ Text says SME = < 250 FTE **and** < 50 mil. AT / < 43 mil. ABT
  ➔ So large enterprise = > 250 FTE **or** > 50 mil. AT (and/or) > 43 mil. ABT

- "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."

  ➔ Text says small enterprise = < 50 FTE **and** < 10 mil. AT / ABT
  ➔ So medium enterprise = > 50 FTE **or** > 10 mil. AT (and/or) > 10 mil. ABT, but not > 250 FTE **or** > 50 mil. AT (and/or) > 43 mil. ABT

This is a logical application of the thresholds for NIS2's purposes.

The European Commission's official 'SME Wizard' Tool, designed to help companies check whether they are an SME or not, confirms the results from the above interpretation.

Our NIS2 page on Safeonweb@Work thus correctly states (worded slightly differently in section 1.5 above):

> *"**Exceed** the size thresholds of a medium-sized enterprise set out in the Recommendation 2003/361/EC, i.e. have a workforce of at least 50 full-time workers or an annual turnover or balance sheet total exceeding 10 million euros;"*

This is also correctly reflected in our scoping tool.

A little further on the NIS2 page, it also states the following:

> *"Afterwards, the staff headcount must be combined with the financial amounts to receive the definitive categorisation: an enterprise may choose to meet either the turnover or the balance sheet total ceiling. **It may exceed one of the financial ceilings** without impact on its SME status. We thus **only look at the lowest of the two amounts**."*

This text is based on the European Commission's official guide on the application of Recommendation 2003/361/EC (p. 11).

An entity is therefore classified as a medium-sized enterprise in several possible situations, either on the basis of the number of full-time employees or on the basis of financial data, or both together. This corresponds to the logic of the word 'or'.

With regard to the qualification of an organisation as an essential or important entity under NIS2 law, it is irrelevant whether it is first determined whether the organisation provides a service listed in the annexes to the law, or whether size is determined first (or the size-cap does not apply). The end result will be the same.

1.7. What sectors and services are covered by the NIS2 law?

Annexes I and II of the NIS2 law

The entity concerned must provide at least one of the services listed in annexes I or II of the law (even if this service constitutes only an ancillary part of its activities - except where the definition itself uses the principal or incidental nature of the service provided as a criterion) from among the following sectors:

Highly critical sectors (annex I)	**Other critical sectors (annex II)**
○ Energy (electricity, district heating and cooling, oil, gas, hydrogen) ○ Transport (air, rail, water, road) ○ Banking sector ○ Financial market infrastructures ○ Public health ○ Drinking water ○ Waste water ○ Digital infrastructure ○ ICT service management ○ Public administration ○ Space	○ Postal and courier services ○ Waste management ○ Manufacture, production and distribution of chemicals ○ Food production, processing and distribution ○ Manufacture (medical devices and in vitro diagnostic medical devices; computer, electronic and optical products; electrical equipment; machinery and equipment n.e.c.; motor vehicles, trailers and semi-trailers; other transport equipment) ○ Digital providers ○ Research

Each service covered by the NIS2 law **is defined** in annexes I or II, with a reference to the definitions in the relevant European legal texts or in article 8 of the NIS2 law. These definitions must be consulted in order to understand the service concerned (entity type). To this end, the annexes are available on the website of the Belgian Official journal (after the text of the law).

See also section 1.21.4. for more details about how to determine which service(s) your organisation provides in the European Union and the NIS2 scope test tool.

See section 1.22 for more specific information on the sectors.

1.8. Does the service mentioned in the annexes have to be the entity's main activities?

The explanatory memorandum of the NIS2 law states the following about article 3 of the law:

Art. 3 NIS2 law

> *"To be considered as a public or private entity of a type referred to in Annex I or II of the law, it is sufficient to carry out, regardless of its legal form, at least one of the activities listed in Annexes I or II of the law,* ***even if this service only constitutes an ancillary part of its activities****, and to exceed the ceilings referred to in paragraph 1 or to meet one of the criteria referred to in paragraphs 3 and following (see below)."* (we highlighted)

Article 3 of the NIS2 law, which defines its scope, refers to the concepts of public or private entities of a type referred to in Annex I or II, and which constitute a medium-sized or large enterprise within the meaning of European recommendation 2003/361/EC.

In the same way as the Directive itself, this means in practice that the scope of the NIS2 Law depends directly on the definitions set out in its annexes I and II.

In general, the **ancillary or the non-essential nature of the activity for the concerned entity is not taken into account in the definitions** (and therefore does not influence the scope of application of the NIS2 law). However, there are few limited exceptions where the criterion of "principal economic activity" or "non-essential part of the general activity" is used in the definitions and is indeed relevant (such as in the waste management, drinking water or waste water sectors).

It is **only in those limited exceptions foreseen explicitly** in the definitions of the annexes that the **ancillary or non-essential nature of the activity should be taken into account**. An entity may thus fall into the scope of the law, **even if the concerned service it provides is only an ancillary or non-essential part of all its activities**, unless provided otherwise in the annexes**.**

There is therefore no contradiction between the explanatory memorandum and the provisions of the NIS2 law (and its annexes), and the service only has to be an entity's main activity if explicitly mentioned in the annexes.

1.9. Could the sectors covered by the NIS2 law be extended in the future?

The King may add sectors or subsectors to annexes I and II by decree deliberated in the Council of Ministers after consulting the concerned sectoral authorities and the national cybersecurity authority (CCB).

Art. 3, § 6 NIS2 law

In this way, when it becomes apparent in the future that a sector not yet covered by the scope should be included because of its importance for critical societal and/or economic activities, the annexes can be extended.

1.10. Is it possible for an entity to fall within several sectors?

Yes, it is possible for the same entity to fall within several sectors (depending on all of its activities). In this case, there are a number of considerations to take into account:

Art. 8, 34°; 25; 39, subpara. 2; and 44, §1, subpara. 2 NIS2 law

- More stringent obligations prevail over less stringent ones. Consequently, if the size criterion is met (large enterprise), an entity that provides services that fall under both annex I and annex II will, as a whole, be subject to the obligations related to an essential entity;
- The entity can potentially come under the supervision of the national cybersecurity authority (CCB) and several sector authorities. These authorities will collaborate with each other in the supervision process;
- A public administration entity whose principal activity is the performance of a service listed in another sector of the annexes of the law, is covered solely by that sector (and not simultaneously by that sector and the public administration sector).

1.11. What is the difference between "essential" and "important" entities?

Essential and important entities are distinguished mainly in terms of supervision and sanctions. Essential entities are monitored proactively "*ex ante*" and reactively "*ex post*". More specifically, essential entities are subject to regular conformity assessments.

Art. 39-42; 48, §§ 1 and 2; 58 and 59 NIS2 law

Important entities are subject to "*ex post*" supervision, i.e. on the basis of evidence, indications or information that an important entity is not complying with its obligations under the law.

For more information on supervision, see section 4.4.

For the rest, both types of entity are subject to the same obligations, for example with regard to incident reporting (section 3.3) or taking cybersecurity risk-management measures (section 3.2.).

1.12. How does the additional identification procedure work?

On its own initiative or on a proposal from the relevant sectoral authority (if there is one), the national cybersecurity authority (CCB) may identify, within an existing sector of the annexes of the NIS2 law, an entity as essential or important, regardless of its size, in the following cases:

Art. 11 NIS2 law

1. the entity is the sole provider in Belgium of a service which is essential for the maintenance of critical societal or economic activities, in one of the sectors or sub-sectors listed in annexes I and II to the law;
2. a disruption of the service provided by the entity could have a significant impact on public security, public safety or public health;
3. a disruption to the service provided by the entity could lead to significant systemic risk, particularly in sectors where such a disruption could have a cross-border impact;

4. the entity is critical because of its specific importance at national or regional level for the sector or type of service in question, or for other interdependent sectors, in Belgium.

A proposal for an identification decision is communicated to the concerned entity and to the competent sectoral authorities, which may issue an opinion within sixty days.

The CCB assesses and, if necessary, updates the identification of essential and important entities at least every two years, in accordance with the same procedures.

1.13. What happens when a NIS2 entity is acquired by another organisation ?

If a company or association acquires a NIS2 entity, the concerned NIS2 entity will still have to comply with the law, as long as the service(s) it provides and size-cap criteria remain. The NIS2 qualification of the concerned entity is not transferred to the acquiring organisation or mother organisation (if they remain two different legal entities). Of course, the acquiring organisation could itself also fall under law if it provides a NIS2 service within the EU itself and fulfils the size-cap criteria.

The qualification as an important NIS2 entity could change after the acquisition, as the entity will possibly become larger under the calculations of the size-cap. These can indeed be reviewed after a period of two years (section 1.5.). Depending on the service provided by the NIS2 entity (annexes), an increase in size could lead to a new qualification as essential instead of important.

In any case, the acquiring organisation might have to implement appropriate cybersecurity risk-management measures due to the obligation from the NIS2 entity to secure its supply chain or in case they share the same networks and information systems (section 3.14.).

1.14. What does “(main) establishment” mean? Does the law apply only to Belgian organisations or also to other entities?

The Belgian NIS2 law applies in principle to entities **established in Belgium** that provide their services or carry out their activities within the EU (establishment rule).

Art. 4 NIS2 law

The concept of "entity" is defined in article 8, 37° of the NIS2 law as: *"a natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations"*. See also section 1.4.

The concept of establishment consists of the actual pursuit of an activity by means of a permanent installation, irrespective of the legal form adopted, whether this is the registered office, a simple branch, a subsidiary, an establishment unit, a factory, a commercial office, etc.

The NIS2 law provides for three exceptions to the rule of establishment in Belgium:

1) when providers of public electronic communication networks and providers of publicly available electronic communications services provide their service in Belgium (service location rule);

2) when DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines or of social networking services platforms have their main establishment in Belgium(main establishment rule);
3) when public administration entities have been created by Belgium.

To determine the "main establishment" of an entity, the following establishments should be determined in a cascading order (if the first criterion cannot be determined or is outside of the EU, the second or third one is used):

1° where the decisions related to the cybersecurity risk-management measures are predominantly taken;
2° where the entity carries out its cybersecurity operations;
3° where the entity has the highest number of employees in the Union.

In case an entity is not established within the EU but provides a service subject to the main establishment jurisdiction rule, it must appoint a legal representative who is established in one of the Member State where it provides its services. If this representative is located in Belgium, the entity will be considered to have its main establishment in Belgium.

Under the main establishment jurisdiction regime, if an entity has several establishments in different EU Member States, it will only be subject to the NIS2 obligations in the Member State where it has its main establishment.

See the following sections for more complex scenarios.

1.15. Specific questions relating to jurisdiction and establishment (who does the law apply to?)

1.15.1. What if my organisation provides services that fall under the establishment and the main establishment jurisdiction rules ? How do you combine different jurisdiction rules?

Depending on the type of services provided, NIS2 entities may have to combine different jurisdiction rules (e.g. a telecom operator can provide public electronic communications networks falling under the service location rule, produce electricity falling under the establishment rule and a managed security service falling under the main establishment rule) and possibly be subject to several transposition legislations and competent supervisory authorities (depending on the service concerned and the location of its establishments).

The various competent national authorities will work together regarding inspections and the notification of significant incidents. However, this entails that the entity, in this case, will have to combine the rules of at least two different Member States by applying the most stringent rules of one to all its services. This ensures that the rules in multiple Member States are properly respected.

1.15.2. What if an entity has a daughter/parent company/branch in another EU Member State that also has to comply with NIS2?

This depends on the service provided by the concerned organisation in the other Member State. The daughter/parent company/branch must be qualified as an "entity" under the NIS2 law (see section 1.4).

The NIS2 law **applies to all organisations individually**, even if they are grouped together and/or held by the same holding company. The scope of application and the obligations of the NIS2 law must thus be analysed by each organisation individually, based on its own provided services. It is thus possible that a daughter company has to be NIS2 compliant, while a mother company does not.

The following points provide a more in-depth analysis of the different possibilities.

A. The service provided does not fall into one of the jurisdiction exceptions (section 1.14.)

The organisation in the other Member State will have to respect the NIS2 law of that Member State where it is established.

Example: The mother company is established in Belgium and the daughter company is established in France. They both provide services falling into the food sector (annex II of the NIS2 law). Their consolidated headcount (size-cap) is sufficient to be qualified as medium-sized enterprises. The mother company in Belgium will have to respect NIS2 in Belgium, and the daughter company will have to respect NIS2 in France.

B. The service provided falls into the service location exception (electronic communication)

The organisation in the other Member State will have to respect the NIS2 law of the Member State(s) where it provides its services.

Example: The mother company is established in Belgium and the daughter company is established in Luxemburg. The daughter company provides public electronic communication services in Belgium, Luxemburg, and Germany. Combined with the data of the mother company, it is a large enterprise. It thus has to respect the NIS2 transposition laws of Belgium, Luxemburg and Germany (as an essential entity). In practice, the different requirements will have to be combined, and the strictest rules will have to be respected to ensure compliance with all three legal frameworks.

C. The service provided falls into the main establishment exception

The organisation in the other Member State will have to respect the NIS2 law of the Member State where it has its main establishment (see section 1.14.).

Example: The mother company is established in Belgium. It predominantly takes the decisions relating to the cybersecurity risk-management measures for itself but also for its branch in the Netherlands. The mother company does not provide a NIS2 service and thus does not fall under NIS2 itself. The branch is established in the Netherlands, is a medium-sized enterprise and provides managed services there. Nevertheless, because its main establishment is in Belgium, the branch falls under NIS2 in Belgium (and must for example register only in Belgium).

1.15.3. What if within the same group there are NIS2 entities established in multiple EU Member States?

As for section 1.15.2., depending on the service(s) offered by the different organisations, they might be subject to several jurisdictions within the EU.

It is entirely possible that one company in a group has to comply with NIS2 in Belgium, while another company has to comply with NIS2 in Poland, for example. If the group has a holding company, the latter will also need to analyse whether it falls under NIS2 because of a service it provides (NIS2 applies to all organisations individually but size is calculated on group level with partners or linked enterprises).

1.15.4. A company active in one of the NIS2 sectors has to follow NIS2 in country A, but its parent company established in country B does not. How does that work?

The company n° 1 has to follow the obligations contained in the NIS2 law from country A. This includes registration, incident reporting, cybersecurity measures, etc. The parent company n° 2 in country B does not have to respect all these obligations as it does not fall under NIS2.

However, there are other ways in which the parent company could be impacted:

1. If the two companies share the same networks and IT systems, the application of NIS2 to company n° 1 will require the cybersecurity risk-management measures to be taken on the whole system(s) and network(s) in order to protect everything (all hazards approach of the cybersecurity risk-management measures of NIS2, see section 3.2.).
2. The obligation for company n° 1 under NIS2 to ensure the security of its supply chain could prompt it to impose the implementation of cybersecurity measures on its parent company n° 2 (see section 3.14.).

In case the entity established in country A is only a branch (same legal entity) of the company established in country B, it is the entire legal entity that is subject to the NIS2 obligations according to NIS2 in country A (regardless of where its network and information systems are physically located).

1.15.5. What if the(daughter/parent) organisation is established outside of the EU but provides services in the EU?

In principle, organisations established outside of the EU do not fall under NIS2 unless they provide a service in the EU that falls under one of the three exceptional rules on jurisdiction as explained in section 1.14.

For the service falling under the service-location jurisdiction rule (electronic communication), the NIS2 law of the Member State(s) where the organisation from outside of the EU provides its services applies.

If the organisation outside of the EU provides a service within the EU that falls under the main establishment exception, it must appoint a legal representative who is established in a Member State where it provides its services. If this representative is located in Belgium, the entity will be considered as having its main establishment in Belgium.

The law defines a legal representative as: *"a natural or legal person established in the Union explicitly designated to act on behalf of a DNS service provider, a TLD name registry, an entity providing domain name registration services, a cloud computing service provider, a data centre service provider, a content delivery network provider, a managed service provider, a managed security service provider, or a provider of an online marketplace, of an online search engine or of a social networking services platform that is not established in the Union, which may be addressed by a competent authority or a CSIRT in the place of the entity itself with regard to the obligations of that entity under the present law"*.

In order to determine whether an entity is offering services within the Union, it should be ascertained whether the entity is planning to offer services to persons in one or more Member States. The mere accessibility in the Union of the entity's or an intermediary's website or of an email address or other contact details, or the use of a language generally used in the third country where the entity is established, should be considered to be insufficient to ascertain such an intention. However, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering services in that language, or the mentioning of customers or users who are in the Union, could make it apparent that the entity is planning to offer services within the Union.

The representative should act on behalf of the entity and it should be possible for the competent authorities or the CSIRTs to address the representative. The representative should be explicitly designated by a written mandate of the entity to act on the latter's behalf with regard to the latter's obligations laid down in the law, including incident reporting.

On how to register an organisation established outside of Belgium, see section 3.13.7.

1.16. Specific questions relating to groups of organisations or companies

1.16.1. How to assess the scope of NIS2 in relation to a group of organisations or companies?

Within a group of organisations or companies, as explained in the previous sections, every legal entity / organisation has to analyse itself and individually whether it falls into the scope of application of NIS2 based its activities and provided services. The sharing of data, networks or information systems within the group has no impact on the scope of application. Every organisation is advised to individually proceed through the explanations contained in section 1.21.

It should be noted that within a group of organisations or companies, the amount of full time equivalents and the financial data will have to be consolidated based on the different rules of the Recommendation 2003/361/CE. For more information see section 1.5

1.16.2. What impact does a NIS2 entity have on other organisations or companies within the same group?

See the explanations from section 1.15.4.

1.16.3. What if another organisation or company from the same group uses the same IT networks and/or systems as a NIS2 entity?

If the two organisations share the same networks and IT systems, the inclusion of one entity within the scope of NIS2 will require the cybersecurity risk-management measures to be taken on the whole shared system(s) and network(s) in order to protect everything (according to the "all hazards approach" of the cybersecurity risk-management measures of NIS2, see section 3.2.).

1.16.4. What if there are both essential entities and important entities within the same group of organisations or companies?

The NIS2 law applies per legal entity. The entities that do not fall under NIS2 but are part of the same group will not be directly impacted by NIS2 beyond what is outlined in section 1.15.4. Whether entities within the same group are qualified as essential or important will not change the situation.

1.16.5. What if an organisation or company enters into contract with a NIS2 service provider and allows this contract/service to be used by other organisations ?

For example, a company X enters into contract with a digital service provider – company Y (such as a data centre provider) – and then allows this contract/service to be used by a partner company Z. In such a situation, the NIS2 services remains provided by company Y and not by company X (as long as company X does not play a role in the provision of the NIS2 service for company Z).

1.16.6. What about holding companies that have (almost) no personnel, no turnover, just a positive balance sheet?

If a holding company does not provide a NIS2 service, it will not fall under NIS2. However, its headcount and financial data will be taken into account for the size-cap assessment of any linked or partners enterprises providing a NIS2 service.

Apart from these elements, the considerations from section 1.15.4. also apply.

1.16.7. What if one organisation provides IT services to other organisations within the same group of organisations or companies?

Within a group of organisations or companies, every separate legal entity has to analyse for itself and individually whether it falls into the scope of application of NIS2, based on its own activities and provided services (headcount and financial data will however in principle be consolidated with linked or partners enterprises (see section 1.5)).

When one legal entity provides a NIS2 service (e.g. as a managed service provider or as a cloud-computing service provider) to another separate legal entity, it can fall under NIS2 (depending on its size), **even if the activity is only offered to a limited number of organisations or companies within the same group**.

However, the situation can be seen differently if two or several organisations are actually sharing data, networks or systems between themselves within a group (and share together the relevant costs) and there is not one specific organisation providing managed services to the others.

See also section 1.22.6.2. on managed service providers.

1.17. How do the DORA Regulation and the NIS2 Directive interact?

Art. 6 NIS2 law
Art. 2 & 47 DORA

The NIS2 Directive and its transposition law are aimed at transversal cybersecurity measures in the EU. The aim is to improve the overall cybersecurity in the EU and, in particular, to ensure a high level of cybersecurity for certain entities that are critical to societal and economic activities.

The DORA (Digital Operational Resilience Act) Regulation specifically targets operators in the financial sector. It aims to strengthen the operational resilience of information systems in the financial sector and to coordinate existing regulations in this area.

DORA applies to the financial institutions listed in article 2 of the regulation. These are:

- credit institutions;
- payment institutions;
- account information service providers;
- electronic money institutions;
- investment firms;
- crypto-asset service providers;
- central securities depositories;
- central counterparties;
- trading venues;
- trade repositories;
- managers of alternative investment funds;
- management companies;
- data reporting service providers;
- insurance and reinsurance undertakings;
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;
- institutions for occupational retirement provision;
- credit rating agencies;
- administrators of critical benchmarks;
- crowdfunding service providers;
- securitisation repositories;
- ICT third-party service providers.

The requirements of NIS2 and DORA overlap for entities operating in the banking and financial sectors. The NIS2 Directive therefore set out a *lex specialis* rule: when equivalent EU sectoral requirements in terms of cybersecurity and notification of significant incidents exist, they override the general/cross-sectoral requirements from NIS2.

However, ICT third-party service providers covered by DORA are not concerned by the *lex specialis* rule and can be subject to DORA and NIS2 obligations.

It's important to note that NIS2 entities in the banking and financial sectors established in Belgium must still register like the other NIS2 entities. Significant incidents notified by DORA entities via their own notification mechanism will be forwarded by the competent authorities (National Bank of Belgium and FSMA) to the CCB.

1.18. Do critical infrastructures (or critical entities identified under the CER Directive) fall into the scope of the NIS2 law?

Art. 9, 5° and 25, §2 NIS2 law

Yes, the operator of one or more critical infrastructure(s) identified under the law of 1er July 2011 on the security and protection of critical infrastructures (or as critical entities within the meaning of Directive 2022/2557 - CER Directive) is considered to be an essential entity within the meaning of the NIS2 Law.

The NIS2 authorities and the competent authorities under the law of 1er July 2011 (and the future CER law which will transpose the CER Directive) work together to supervise these entities.

More information on critical infrastructures can be found on the National Crisis Centre website.

1.19. Can NACE codes be used to determine whether an entity falls under the NIS2 law?

Annexes I and II of the NIS2 law

Some of the services listed in annexes I and II refer to NACE codes. Entities established in Belgium that provide services falling under these NACE codes should therefore carefully consider if the NIS2 law applies to them.

For all entities outside of those cases provided for in the annexes of the NIS2 law, NACE codes are **not a sufficient base** for determining whether an entity falls under the NIS2 law. Some NACE codes may be used preliminarily by entities, but further verification of their exact service provided is required to determine whether or not they fall within the often more restrictive scope of the NIS2 law. The indication of a certain NACE code on the Crossroad Bank of Enterprises (CBE) has no effect on the scope of application for these types of entities.

1.20. Are conformity assessment bodies in the scope of the law?

The services normally provided by conformity assessment bodies (CABs) are not as such included in the list of entities from annexes I and II of the NIS2 law. This entails that CABs which limit their activities to the assessment of conformity are not within the scope of the NIS2 law.

However, CABs which additional provide services that are described in annex I or II of the NIS2 law may fall within the scope of the law if their if their also fulfil the size criterion, even if these services are just ancillary/accessory to their main activities.

1.21. What is the method for determining whether an organisation falls within the scope of the NIS2 law?

The method described below sets out in detail the various stages of reasoning relating to the scope of the NIS2 law. However, it does not claim to be exhaustive or the only method that can be used.

This section covers the following items:

1. Before examining the NIS2 law itself:
    a. Does my organisation operate a critical infrastructure within the meaning of the law of 1 July 2011 on the security and protection of critical infrastructures (or the future CER law)?
    b. Is my organisation subject to DORA?
2. What is the size of my organisation?
3. What service(s) does my organisation provide in the European Union?
4. Where in Europe is my organisation based?
5. Could my organisation be identified afterwards or is it in the supply chain of a NIS2 entity?

See also our NIS2 scope test tool.

1.21.1. Before examining the NIS2 law itself

Before entering into the actual analysis, it is first necessary to look at two possibilities which have a major impact on how the scope of the NIS2 law works for the organisations concerned.

1.21.1.1. Does my organisation operate a critical infrastructure within the meaning of the law of 1er July 2011 on the security and protection of critical infrastructures (or the future CER law)?

Article 3, §4 of the NIS2 Law specifies that the law automatically applies to entities identified as operators of a critical infrastructure within the meaning of the Law of 1er July 2011 on the security and protection of critical infrastructures (and in the future to critical entities within the meaning of the CER Directive), regardless of their size.

Operators of critical infrastructure therefore do not need to analyse whether or not their organisation falls within the scope of the NIS2 Directive: they are falling under the NIS2 law and are automatically qualified as essential entities.

1.21.1.2. Is my organisation subject to DORA ?

Entities established in Belgium and subject to the DORA Regulation are excluded from the main NIS2 law requirements.

See section 1.17.

1.21.2. Is my organisation an “entity” (group of companies)?

For the law to be applicable, an organisation must be qualified as an “entity” according to article 8, 37° of the NIS2 law: “a natural or legal person created and recognised as such under the

national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations".

This elements is particularly important for larger organisations or groups of companies, where establishments in other Member States, such as branches, may not be able to act under their own name or exercise rights and be subject to obligations. In such a situation, the NIS2 law would apply to the company which has the legal personality of the branch.

1.21.3. What is the size of my organisation?

To fall into the scope of the NIS2 law, an entity must be of a certain size. To calculate this size, the NIS2 law refers to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. This Recommendation defines the thresholds above which an enterprise (any entity engaged in an economic activity, irrespective of its legal form) can be considered to be a small, medium-sized or large enterprise. With a few exceptions, only medium-sized and large enterprises fall within the scope of the NIS2 law.

Two conditions must be met to establish the size: workforce (measured in annual work units (AWUs)[1]) and financial amounts (annual turnover and/or annual balance sheet total).

The number of employees must be combined with the financial amounts to obtain the size of the enterprise: an enterprise may choose to comply with either the turnover ceiling or the balance sheet total ceiling. It **can exceed one of the financial ceilings without this affecting its SME status**. In principle, therefore, we **only consider the lower of the two** amounts.

Example 1: an enterprise with 35 AWUs (small) has an annual turnover of 1,000,000€ (small) and an annual balance sheet total of 50,000,000€ (large). For the financial amounts, it chooses to take into account only the smallest: its turnover. It is therefore a small or micro enterprise.

Example 2: an enterprise with 80 AWUs (medium) has an annual turnover of 1,000,000€ (small) and an annual balance sheet total of 70,000,000€ (large). For the financial amounts, she chooses to take into account only the smallest: her turnover. Since the turnover is small but the workforce is medium-sized, it is a medium-sized enterprise.

You may find a visual summary of the possible enterprise sizes on our website.

If we combine the different possible sizes with the criterion of the service provided, we obtain the following scope:

- A medium-sized enterprise with a workforce between 50 and 249 AWUs or annual turnover / annual balance sheet total exceeding 10 million €:
  - ➔ Falls within the scope of application as an "important entity" if it provides a service listed in annex II of the law.
  - ➔ **In principle,** falls within the scope of application as an "important entity" if it provides a service listed in annex I of the law.
- A large enterprise has a workforce of at least 250 AWUs or an annual turnover exceeding 50 million € and an annual balance sheet total exceeding 43 million €:

[1] Annual work units (AWU) correspond to the number of persons who worked full-time within the enterprise in question or on its behalf during the entire reference year under consideration. The work of persons who have not worked the full year, the work of those who have worked part-time, regardless of duration, and the work of seasonal workers are counted as fractions of AWU.

- ➔ Falls within the scope of application as an "important entity" if it provides an essential service listed in annex II of the law.
- ➔ **In principle,** falls within the scope of application as an "essential entity" if it provides a service listed in annex I of the law.

In particular, the Recommendation provides that in the case of entities grouped together as "partner " or "linked" enterprises, depending on the criteria defined, the data (number of full-time workers & financial amounts) of the other entities forming part of the group of entities are taken into account to calculate the size (see also section 1.5.).

For more information on the application of the Recommendation, we advise you to consult the Commission's User's Guide to the definition of SMEs. It contains all the criteria and visual examples to help you apply the Recommendation. The Commission has also set up a tool to test the size of your organisation.

However, there are a few **exceptions**. The following types of entity fall into the scope of the NIS2 law, regardless of their size:

- qualified trust service providers (essential);
- non-qualified trusted service providers (important for micro, small and medium-sized enterprises and essential for large enterprises);
- DNS service providers (essential);
- TLD name registries (essential);
- domain name registration services (only for the registration obligation);
- providers of public electronic communications networks (essential);
- providers of publicly available electronic communications services (essential);
- entities identified as operators of critical infrastructure under the law of 1er July 2011 on the security and protection of critical infrastructures (essential);
- public administration entities dependent on the federal State (essential).

The following section explains how to find the definitions of the services provided by these types of entity.

1.21.4. What service(s) does my organisation provide in the European Union?

Once the size of an entity is known, it is then necessary to carry out a detailed analysis of all the services it provides to third parties, by sector or sub-sector. It is important to map out each service, even if it is only an ancillary activity of the entity (unless the definition of the service takes into account whether it is the main or ancillary service).

Annexes I and II (or the definitions) of the NIS2 law detail the services concerned ("type of entity"), often with a reference to the corresponding European legislation or to the definitions set out in article 8 of the law.

The various sectors and sub-sectors are as follows:

Highly critical sectors (Annex I)	Other critical sectors (Annex II)
1. Energy a. Electricity b. District heating and cooling c. Oil d. Gas e. Hydrogen 2. Transport a. Air b. Rail c. Water d. Road 3. Banking 4. Financial market infrastructures 5. Public Health 6. Drinking water 7. Waste water 8. Digital infrastructure 9. ICT service management (business-to-business) 10. Public administration 11. Space	1. Postal and courier services 2. Waste management 3. Manufacture, production and distribution of chemicals 4. Food production, processing and distribution 5. Manufacture a. Manufacture of medical devices and *in vitro* diagnostic medical devices b. Manufacture of computer, electronic and optical products c. Manufacture of electrical equipment d. Manufacture of machinery and equipment n.e.c. e. Manufacture of motor vehicles, trailers and semi-trailers f. Manufacture of other transport equipment 6. Digital providers 7. Research

One must then make the link between the services provided and the aforementioned definitions. The condition relating to the service provided is thus met if there is a match between the two. It is quite possible for an organisation to provide several of the listed services in different sectors (see section 1.10.).

In conclusion, "important" entities and "essential" entities are the following (with the exception of the types of entities listed at the end of the section 1.21.3 above):

	Medium-sized enterprise	Large enterprise
Annex I services	Important	Essential
Annex II services	Important	Important

1.21.5. The establishment

In principle, the Belgian NIS2 law applies to entities **established in Belgium that provide their services or carry out their activities within the EU**.

The concept of establishment simply implies the actual pursuit of an activity by means of a permanent installation, irrespective of the legal form adopted.

However, depending on the type of entity concerned, there are certain exceptions to the Belgian establishment rule. The rules governing the territorial scope/jurisdiction of the Belgian NIS2 law are explained in section 1.14.

1.21.6. Additional identification and supply chain

Notwithstanding the aforementioned rules, the CCB may, if necessary, identify certain entities established in Belgium and active in the sectors listed in the annexes to the NIS2 law. This additional identification is carried out in consultation with the organisation concerned - see section 1.12.

Regardless of the scope of the NIS2 law, it should be borne in mind that a large number of organisations will be indirectly impacted by these new legal requirements if they are in the supply chain of one or more NIS2 entities. The latter are obliged to guarantee the security of their own supply chain and can therefore impose contractual obligations on their direct suppliers or service providers. For further explanation, see section 3.14.

1.22. Specific questions relating to certain types of entities and sectors

1.22.1. Annex I – 1. Energy – (a) Electricity

1.22.1.1. Do organisations producing electricity mainly for their own consumption (including solar panels, etc.) fall into the scope of the law?

Annex I NIS2 law & Directive (EU) 2019/944

Pursuant to Article 3, read in conjunction with Annex I, point (1)(a) dash 4, of the NIS2 Law, "[p]roducers as defined in Article 2, point (38), of Directive (EU) 2019/944" are in scope where they qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises.

Article 2, point (38), of Directive (EU) 2019/944 defines **'producer'** as "a natural or legal person who generates electricity", while **'generation'** is defined as "the production of electricity" according to Article 2, point (37), of Directive (EU) 2019/944.

Pursuant to these definitions, entities operating solar panels or wind turbines connected to the electrical grid, even if they mainly consume the self-generated electricity themselves, qualify as producers pursuant to Article 2, point (38), of Directive (EU) 2019/944, and consequently fall into the scope of application of NIS2 if they are at least a medium-sized enterprise.

However, it has been agreed at EU level that these aforementioned "producers" are not the intended highly critical entities targeted in the electricity sub-sector of the NIS2 directive. Therefore, a less stricter supervision approach can be applied to them.

In Belgium, entities that fall under the definition of a service in the electricity sub-sector **just** because they mainly produce electricity for their **own consumption**, retain their NIS2 qualification (essential or important), but are subject to a less stringent supervision. In practice, they still have to register, report significant incidents, and apply cybersecurity measures, but the use of a **lower assurance level of the CyberFundamentals (CyFun®) Framework** (e.g. Basic) to comply with their obligations will be considered as proportionate. This solution takes into account the rather limited societal and economic impact of their electricity production.

1.22.1.2. What falls under "operators of recharging points"?

Annex I, sub-sector electricity of the NIS2 law mentions "operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider". In the absence of additional definitions, the words must be understood in their usual meaning.

The definition entails the following conditions:

1) An operator of a recharging point
2) Responsible for the management and operation of said recharging point
3) Recharging is provided to end users (including in the name and on behalf of a mobility service provider)

For example, if a supermarket places recharging points on its parking, it can fall under NIS2 if it is responsible for the management and operation of the recharging point. This management and operation is often contractually delegated to a third-party organisation, even if the recharging points are labelled with the name of the supermarket. An organisation must thus concretely check whether it manages and operates a recharging point itself, or whether this service is left to a third-party organisation.

1.22.2. Annex I – 1. Energy – (c) Oil

1.22.2.1. What is covered by "operators of oil transmission pipelines"?

The NIS2 law and its annex do not provide a definition of "operators of oil transmission pipelines". The words must thus be understood in the usual meaning.

1.22.3. Annex I – 2. Transport

The sector transport includes several subsectors and types of entities:

a) Air:
    a. Air carriers
    b. Airport managing bodies
    c. Traffic management control operators providing air traffic control
b) Rail:
    a. Infrastructure managers
    b. Railway undertakings
c) Water:
    a. Inland, sea and coastal passenger and freight water transport companies
    b. Managing bodies of ports
    c. Operators of vessel traffic services
d) Road:
    a. Road authorities
    b. Operators of intelligent transport systems

•

1.22.4. Annex I – 5. Health

The sector health includes several types of entities:

- Healthcare providers
- EU reference laboratories
- Entities carrying out research and development activities of medicinal products
- Entities manufacturing basic pharmaceutical products and pharmaceutical preparations
- Entities manufacturing medical devices considered to be critical during a public health emergency

1.22.4.1. What organisations fall under the definition of a healthcare provider (hospitals, retirement homes, residential care, etc.)?

Healthcare providers in annex I, 5. Health, refer to healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council and are defined as: "any natural or legal person or any other entity legally providing healthcare on the territory of a Member State."

To determine if an organisations falls under the definition of healthcare provider, it should be verified if "healthcare" is provided by these entities:

1) Healthcare is defined in that directive as "health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices." This could for example be the use of syringes, injections, etc.).
2) The directive also defines "health professionals" as "a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment"

Every concerned organisation should thus for itself ascertain whether the activities carried out by the entity constitute health services/healthcare provided by a health professional or whether these entities merely provide care.

Under healthcare/health services fall for example: elderly care, psychiatric care, hospitals, revalidation centres, retirement homes, residential care, home nursing activities, centre for ambulatory rehabilitation, doctors, nurses, … Entities who provide care to people with disabilities and ordinary/specialised education can also fall hereunder, if activities related to healthcare are also provided within these entities.

Entities who generally do not provide health services are for example: home care (only domestic work is provided), childcare, …

It is important that every organisation analyses its own activities in practice to verify if they provide any health services. As mentioned before, all activities of an entity need to be taken into account to determine if an entity is a NIS2 entity. Even ancillary activities can lead to an entity falling under NIS2, not only their main activity. It is also important to note that an entity carrying out a NIS2 activity and fulfilling the size criterion will be subject to the NIS2 law as a whole (for all its networks and information systems).

1.22.4.2. What is the difference between "care" and "healthcare"?

Healthcare means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices.

Care is broader and can for example also be childcare, home care activities, etc.

1.22.4.3. Do retirement homes have to follow the same obligations as other healthcare providers?

Retirement homes fall under the definition of a healthcare provider (see section 1.22.4.1). They are therefore, if they meet the size criteria and are established in Belgium, either an essential or an important entity under the NIS2 law.

However, it has been agreed at EU level that these aforementioned "healthcare providers" are not the intended highly critical entities targeted in the healthcare sector of the NIS2 directive. Therefore, a less stricter supervision approach can be applied to them.

In Belgium, entities that fall under the definition of a healthcare provider **just** because they have a **retirement home**, retain their NIS2 qualification (essential or important), but are subject to a less stringent supervision. In practice, they still have to register, report significant incidents, and apply cybersecurity measures, but the use of a **lower assurance level of the CyberFundamentals (CyFun®) Framework** (e.g. Basic) to comply with their obligations will be considered as proportionate. This solution takes into account the rather limited societal and economic impact of their health services.

1.22.4.4. What if my organisation does not employ its own healthcare professionals?

Under NIS2, an organisation must provide a NIS2-service itself in order to fall within its scope of application. This entails that organisations which do not employ their own healthcare professionals, but call upon third parties to provide the healthcare service, would not fall into the scope of application as a healthcare provider.

1.22.4.5. Do entities manufacturing medical devices fall under the NIS2 law?

Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list), within the meaning of Article 22 of Regulation (EU) 2022/123, fall under annex I, sector 5. Health of the NIS2 law.

This regulation refers to a list, to be drawn up by the Executive Steering Group on Shortages and Safety of Medicinal Products in case of an emergency. It refers to categories of medical devices considered critical in the context of the public health emergency. Currently, no such list is available yet.

Entities manufacturing medical devices might also fall under Annex II, sector 5., subsector a) Manufacture of medical devices and in vitro diagnostic medical devices. For more information on this subsector, see section 1.22.11).

In addition, most entities manufacturing medical devices will fall into the supply chain of NIS2 entities (e.g. healthcare providers from annex I, sector 5). Entities covered by the NIS2 law must

take appropriate and proportionate measures to secure their network and information systems. One of those measures is supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. For more information regarding supply chain obligations, see section 3.14.

1.22.4.6. Do pharmacies fall under NIS2?

Pharmacies can potentially fall into multiple sectors of the law, most predominantly the health sector.

First, considering the definition of a healthcare provider, as explained in section 1.22.4.1, pharmacists in Belgium can administer injections and vaccines in certain situations. These acts can be considered health services, bringing the pharmacies in question within the scope of NIS2. Everything here therefore depends on whether the pharmacist provides healthcare services or not.

Second, pharmacies could theoretically be "Entities carrying out research and development activities of medicinal products" if they research and develop their own pharmaceutical products (see section 1.22.4.7, point A.). These R&D activities are however mostly reserved to companies specialised in pharmaceutical research.

Third, pharmacies could also be "Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2" (see section 1.22.4.7, point B.), if they have the necessary NACE code.

Fourth, pharmacies could fall into the annex II, sector 3. of manufacturing, production or distribution of chemicals through the production of articles or the distribution of substance or mixtures. For more information, see section 1.22.9.

Lastly, pharmacies could theoretically fall into Annex II, sector 5. Manufacturing if they produce medical equipment. For more information, see section 1.22.11.1.

As a pharmacy, these five different possibilities must be analysed to determine whether or not they fall under NIS2. Be aware that a pharmacy must, for these five possibilities, at least be a medium-sized enterprise (see section 1.5)

1.22.4.7. Do other health-related companies or those in the pharmaceutical supply chain fall under NIS2?

A. Entities carrying out research and development activities of medicinal products

Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC fall under annex I, sector health. These are entities carrying out research and development activities of:

> *"a) Any substance or combination of substances presented as having properties for treating or preventing disease in human beings; or*
>
> *b) Any substance or combination of substances which may be used in or administered to human beings either with a view to restoring, correcting or modifying physiological functions by exerting a pharmacological, immunological or metabolic action, or to making a medical diagnosis"*

It is important to note that research organizations can also fall within annex II, sector 7. Research. For more information, see section 1.22.12.

B. Entities manufacturing basic pharmaceutical products and pharmaceutical preparations

Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 fall under annex I, sector health. These entities have following NACE codes:

- 21.10 Manufacture of basic pharmaceutical products
- 21.20 Manufacture of pharmaceutical preparations

The NACE code of a Belgian organisation can for example be checked on the website of the Crossroad Bank of Enterprises.

C. Entities manufacturing, producing or distributing chemicals

These entities fall into the chemicals sector from annex II. More information can be found in section 1.22.9.

D. Pharmaceutical wholesalers (sale of pharmaceutical products)

The sale of pharmaceutical products, to costumers or to businesses, is not explicitly targeted in the annexes of the NIS2 law. However, they could fall under the distribution of chemicals if the criteria and definitions are met, as explained in section 1.22.9.2.

E. Courier services for medicines

Courier services for medicines do not fall under annex I, sector 5. Health. In certain cases, however they may fall under the sector 1. Postal and courier services in Annex II.

For more information see section 1.22.8.

F. Social security funds

Social security funds are not explicitly targeted in the annexes of the NIS2 law. If these institutions are private, and they solely provide this service, then they are not included in the scope of application of NIS2.

However, public social security funds could fall into the Public administration sector from annex I if the different criteria are established. For more information, see section 2.1.

G. Providers of health-related software

As with other providers of other software, the definitions from cloud-computing service providers and managed services providers have to be analysed. For more information, see respectively sections 1.22.6.1 and 1.22.7. Next to that, providers of health-related software can also fall under supply chain obligations (for more information, see section 3.14.).

H. Health data (eHealth) networks

Providers of health data networks (such as CoZo, Réseau de Santé Wallon or Réseau de Santé Bruxellois), do not fall into the definitions from the Health sector in annex I.

However, theses types of entities could fall into the definitions in the digital infrastructure sectors, for example as data centre service providers, cloud-computing service providers, or managed service providers. For this, they must be at least a medium-sized enterprise. These types of entities must therefore verify if their activities correspond to the definitions from this sector. For more information, see sections 1.22.6 and 1.22.7 below.

Whether they might also fall into the Public administration sector depends on their legal nature. Most importantly, they must be public legal entities. For more information, see section 2.1.

1.22.5. Annex I – 6. Drinking water

1.22.5.1. What organisations qualify as "suppliers and distributors of water intended for human consumption"?

The words "water intended for human consumption" are defined in article 2, (1) of directive (EU) 2020/2184. They cover:

"(a) all water, either in its original state or after treatment, intended for drinking, cooking, food preparation or other domestic purposes in both public and private premises, regardless of its origin and whether it is supplied from a distribution network, supplied from a tanker or put into bottles or containers, including spring waters;
(b) all water used in any food business for the manufacture, processing, preservation or marketing of products or substances intended for human consumption;"

The annex of the NIS2 law adds that it excludes distributors for which distribution of water for human consumption is a non-essential part of their general activity of distributing other commodities and goods. The word "essential" could be interpreted as following: distribution of water would be "essential" if the distributor could not effectively continue its operations without distributing water intended for human consumption.

Examples of organisations included in the definition are thus companies selling (bottled) water, which would be unable to effectively continue their operation if the sale of such water would stop. See also section 1.22.10 on the production and distribution of food.

1.22.6. Annex I – 8. Digital infrastructure

1.22.6.1. What exactly is a cloud-computing service provider?

Art. 8 NIS2 law; Recital 33 NIS2 directive; NIS2 Impact Assessment

Article 8, 29° of the NIS2-law defines a cloud computing service provider as "a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations."

Recital 33 of the NIS2 directive clarifies this further: "*Cloud computing services should cover digital services that enable on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations. Computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications, and services.*

- *The term 'broad remote access' is used to describe that the cloud capabilities are provided over the network and accessed through mechanisms promoting use of heterogeneous thin or thick client platforms, including mobile phones, tablets, laptops and workstations.*
- *The term 'scalable' refers to computing resources that are flexibly allocated by the cloud service provider, irrespective of the geographical location of the resources, in order to handle fluctuations in demand.*
- *The term 'elastic pool' is used to describe computing resources that are provided and released according to demand in order to rapidly increase and decrease resources available depending on workload.*
- *The term 'shareable' is used to describe computing resources that are provided to multiple users who share a common access to the service, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.*
- *The term 'distributed' is used to describe computing resources that are located on different networked computers or devices and which communicate and coordinate among themselves by message passing.*

The service models of cloud computing include, inter alia, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Network as a Service (NaaS). The deployment models of cloud computing should include private, community, public and hybrid cloud. The cloud computing service and deployment models have the same meaning as the terms of service and deployment models defined under ISO/IEC 17788:2014 standard. The capability of the cloud computing user to unilaterally self-provision computing capabilities, such as server time or network storage, without any human interaction by the cloud computing service provider could be described as on-demand administration."

In the 2020 impact assessment of the NIS2 directive[2], the European Commission gave examples of enterprises qualifying as cloud computing service providers. Providers of SaaS, IaaS, and PaaS were explicitly mentioned:

- SaaS: instant computing infrastructure, provisioned and managed over the internet Examples: Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
- IaaS: cloud computing model that provides virtualized computing resources over the internet. Examples: DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)
- PaaS: cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its own infrastructure. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift.

The elements from the list above are examples, thus neither exhaustive nor limited in any way.

[2] Commission staff working document. Impact assessment report accompanying the document "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", SWD(2020) 345 final, 16 December 2020, part 2/3, online under https://ec.europa.eu/newsroom/dae/redirection/document/72178, page 45.

Cloud-computing service providers are thus defined in a broad way and include providers of SaaS, IaaS and PaaS.

1.22.6.2. What exactly is a data centre service provider?

A data centre service provider is defined in article 8, 30° of the NIS2 law, as a provider of "a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control".

Recital 35 of the NIS2 directive additionally states: *"Services offered by data centre service providers may not always be provided in the form of a cloud computing service. Accordingly, data centres may not always constitute a part of cloud computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should therefore cover providers of data centre services that are not cloud computing services. [...]*
The term 'data centre service' should not apply to in-house corporate data centres owned and operated by the entity concerned, for its own purposes.".

The exception mentioned at the end of the recital does not apply if within a group of companies, one of the companies inside said group provides data centre services to another.

1.22.7. Annex I – 9. ICT service management (B2B): What exactly is a managed service provider (helpdesk, B2B, etc.)?

Article 8, 38° of the NIS2 law defines a managed service provider as: "an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely".

It is important to note that two terms of this definition are also defined by the NIS2 law or other legal instruments:

- "ICT product" means an element or a group of elements of a network or information system (Regulation (EU) 2019/881, article 2, (12));
- "Network and information systems" means:
    a) an electronic communications network as defined in Article 2, point (1), of Directive (EU) 2018/1972;
    b) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or
    c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance.

The definition of a managed service provider is relatively large and entails 3 different conditions:

1) Either installation, management, operation or maintenance;
2) Of either ICT products, networks, infrastructure, applications or any other network and information systems;
3) Via assistance or active administration (on premise or remotely).

These 3 conditions are all required cumulatively to fall into the definition. The activities/tasks listed in the definition are not mutually exclusive. Several of them can be performed by the same entity. There are no other conditions to consider when checking whether an organisation is a managed service provider. For example, the name 'managed service provider' does not have to be used explicitly in a contract.

Examples of a managed service provider include:

- a helpdesk providing operational support to the users of a network or application via remote assistance;
- a software developer providing remote assistance in the installation and/or maintenance of its applications;
- a maintenance service for a customer's networks and other activities carried out on the customer's premises.

Next to the definition, the term "business-to-business" in Annex I of the NIS2 law should be understood as referring to all relationships between service providers and other organisations/professionals (companies, public authorities, craftsmen, professions, associations, entities within the same group, etc.), as opposed to services provided to the general public/individuals ('business-to-customers'). The fact that an entity is not making a profit or commercial use does not appear to be a criterion for excluding an entity from this sector.

The interpretation of the concepts of "assistance" and "active administration" are also important for the definition of a managed service provider. As it is usual in legal interpretation of European texts, if there is no definition in the concerned legal instrument, the terms must be understood in their usual meaning.

The interpretation for these two concepts could therefore be as follows:

- For "assistance", the term could cover the action of providing support. In the context of an MSP, this could include helping customers when their encounter problems or when they need guidance. The term would therefore be more reactive in nature. It could also include troubleshooting, best practices, helping with setup and configuration, etc.

- For "active administration", the concept appears to be intrinsically more proactive. In the context of an MSP, "administration" in particular seems to include the management and overseeing of a customer's systems, applications, networks, … It could also include system monitoring, regular maintenance and updates, as well as generally ensuring the proper functioning of the concerned networks and information systems, without the customer necessarily asking for it.

"Remotely" simply means that it is not done on the premise of the customer (it could thus be from an organisation's offices).

1.22.8. Annex II – 1. Postal and courier services: Do courier services and/or the distribution of medicine fall into this sector?

This sector covers postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services. This directive contains multiple definitions:

- Postal service providers: "undertaking[s] that provides one or more postal services"

- Postal services: “services involving the clearance, sorting, transport and distribution of postal items”.

To find out whether this also covers courier services, we also have to look at the law of 26 January 2018 relating to postal services (Postal Law). The latter contains the following definitions:

- Postal item “an item addressed in the definitive form to which it is to be sent by the postal service provider and weighing no more than 31.5 kg”
- Postal parcel or parcel: “a postal item containing goods, with or without commercial value, other than an item of correspondence, weighing up to 31.5 kg;”

The delivery of a medicinal product by a courier falls within the scope of the Postal Law (and thus also under NIS2) if it meets the legal criteria, which often proves to be the case with regard to the criteria defining the notion of parcel: weight less than 31.5 kg, product not excluded from postal services by Article 24, § 1, 6° of the Royal Decree of 14 March 2022 on postal services (it is not a narcotic or psychotropic drug, such as flunitrazepam, and it is not a counterfeit product, etc.), the medicine must be packaged, and the packaging must bear the recipient's address (or a code to identify the place of distribution).

The delivery of loose, non-individualised goods does not fall under the definition of a postal parcel and those who make such deliveries are therefore not postal service providers falling into this sector of the NIS2 law.

1.22.9. Annex II – 3. Manufacture, production and distribution of chemicals

This sector covers “Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council [(REACH)] and undertakings carrying out the production of articles, as defined in Article 3, point (3), of that Regulation, from substances or mixtures”.

1.22.9.1. What is meant by “substances” and “mixtures”?

Art. 3, points (1) & (2) REACH Regulation

A **substance** is defined as “*a chemical element and its compounds in the natural state or obtained by any manufacturing process, including any additive necessary to preserve its stability and any impurity deriving from the process used, but excluding any solvent which may be separated without affecting the stability of the substance or changing its composition*.”

A **mixture** is defined as “*a mixture or solution composed of two or more substances*”.

By referring to undertakings carrying out the manufacture of **substances** and the distribution of **substances** or **mixtures** in the sector “manufacture, production and distribution of chemicals”, the NIS2 law seems to refer to all chemical substances, regardless of whether they are potentially hazardous industrial chemicals or used in day-to-day products.

1.22.9.2. What types of entities would fall in scope of NIS2 as undertakings carrying out the manufacture of substances and the distribution of substances or mixtures?

A manufacturer under REACH means "*any natural or legal person established within the Community who manufactures a substance within the Community*". Substances and mixtures are to be understood as explained in section 1.22.9.1.

The NIS2 Impact Assessment Report provides qualitative aspects supporting the inclusion in the scope of the NIS framework, thereby referring to hazardous chemicals. Despite being absent in the legal text, the reference to hazardous chemicals in the impact assessment report seems to indicate that the intention of the legislators was not to include companies that manufacture or distribute any type of chemical element.

It is also necessary to consider the registration obligation set out by the REACH Regulation as the registration obligation serves as a key instrument to ensure the purpose of the REACH Regulation. As elaborated by Recitals (17)-(19) of the REACH Regulation, all available and relevant information on substances on their own, in preparations and in articles should be collected to assist in identifying hazardous properties, and recommendations about risk management measures should systematically be conveyed through supply chains, as reasonably necessary, to prevent adverse effects on human health and the environment. Responsibility for the management of the risks of substances should lie with the natural or legal persons that manufacture, import, place on the market or use these substances. Therefore, the registration provisions should require manufacturers and importers to generate data on the substances they manufacture or import, to use these data to assess the risks related to these substances and to develop and recommend appropriate risk management measures. To ensure that they actually meet these obligations, as well as for transparency reasons, registration should require them to submit a dossier containing all this information to the European Chemicals Agency. Registered substances should be allowed to circulate on the internal market.

The scope of this definition thus primarily concerns entities that are subject to the obligation of registration under the REACH regulation.

While other organisations that are not subject to the obligation of registration could also be qualified as undertakings carrying out the **manufacture of substances** and **the distribution of substances or mixtures** as referred to in Article 3, points (9) and (14) REACH, it has been agreed at EU level that these aforementioned undertakings are not the intended critical entities targeted in the chemical sector of the NIS2 directive. Therefore, a less stricter supervision approach can be applied to them.

In Belgium, entities that fall under the definition of a manufacturer but are not required to register under the REACH regulation, remain NIS2 entities (essential or important), but are subject to a less stringent supervision. In practice, they still have to register, report significant incidents, and apply cybersecurity measures, but the use of a **lower assurance level of the CyberFundamentals (CyFun®) Framework** (e.g. Basic) to comply with their obligations will be considered as proportionate. This solution takes into account the rather limited societal and economic impact of their services.

1.22.9.3. Would a retailer be covered under the distribution of substances or mixtures?

Under Annex II, point (3) of the NIS2 law, the definition for the term distribution of chemicals refers to Article 3, point (14) of Regulation (EC) 1907/2006 (REACH Regulation).

As per that Regulation, a distributor "*means any natural or legal person established within the Community, including a retailer, who only stores and places on the market a substance, on its own or in a mixture, for third parties*". Point (12) of Article 3 REACH Regulation defines the notion of "placing on the market" as "*supplying or making available, whether in return for payment or free of charge, to a third party*", and specifies that "import shall be deemed to be placing on the market". The definition encompasses making available a product, whether or not it is the first time that the product is introduced into the market.

Therefore, a retailer of chemical substances or mixtures falls within this definition of distributor (provided that the remaining elements of applicability are fulfilled).

1.22.9.4. What types of entities would fall in scope of NIS2 as undertakings carrying out the production of articles from substances or mixtures?

Undertakings carrying out the production of articles from substances or mixtures, as defined in Article 3, point (3), of Regulation (EC) No 1907/2006 (REACH Regulation) are in scope of the NIS2 law, where they qualify as medium-sized enterprises or exceed the ceilings for medium-sized enterprises.

Article 3, point (4), of the REACH Regulation defines the term **"producer of an article"** as "*any natural or legal person who makes or assembles an article within the Community*". Hence, an entity is a producer of an article if it produces articles within the EU, regardless of how the article is produced and whether it is placed on the market.

For the definition of articles, the NIS2 law refers to Article 3, point (3), of the REACH Regulation. According to Article 3, point (3), of the REACH Regulation, **article** "*means an object which during production is given a special shape, surface or design which determines its function to a greater degree than does its chemical composition*". Examples of articles are clothing, flooring, furniture, jewellery, newspapers and plastic packaging.

However, when construing to what extent **producers of articles** are in scope of the NIS2 law, it is necessary to take into account that the first column of Annex II, point (3), of the NIS2 law defines the sector as "[m]anufacture, production and distribution of chemicals", and thereby sets a limit to the scope of the third column of Annex II, point (3) insofar as chemicals should be the subject of the manufacturing, production and distribution activity of the entities referred to in the third column of Annex II, point (3).

In addition, the NIS2 law defines a separate sector for manufacturing in Annex II, point (5), where it limits the scope to manufactures of medical devices, in vitro diagnostic medical devices, computer products, electronic products, optical products, electrical equipment, machinery and equipment n.e.c. motor vehicles, trailers, semi-trailers and other transport equipment. Since the definition of articles under the REACH Regulation is very broad, the specification in scope of the sector manufacturing as per Annex II, point (5), would be rendered meaningless if any undertaking carrying out the production of articles as defined in Article 3, point (3), of the REACH Regulation were considered to be in scope of Annex II, point (3) of the NIS2 law.

Therefore, the types of entities referred to in the third column of Annex II, point (3), which are operating in this sector as undertakings carrying out the production of articles, as defined in Article 3, point (3), of the REACH Regulation, from substances or mixtures, should not cover entities that are also in scope of the sector 'manufacturing' pursuant to Annex II, point (5).

The scope of this definition thus primarily concerns entities that are subject to the obligation of registration and notification of substances in articles under the REACH regulation.

Regarding other entities that are not subject to the obligation of registration and notification of substances in articles which could also be qualified as undertakings carrying out the production of articles from substances or mixtures, in light of the above-mentioned considerations, it has been agreed at EU level that these aforementioned undertakings are not the intended critical entities targeted in the chemical sector of the NIS2 directive. Therefore, a less stricter supervision approach can be applied to them

In Belgium, entities that fall under the definition of an undertaking carrying out the production of articles from substances or mixtures but are not required to register under the REACH regulation, remain NIS2 entities (essential or important), but are subject to a less stringent supervision. In practice, they still have to register, report significant incidents, and apply cybersecurity measures, but the use of a **lower assurance level of the CyberFundamentals (CyFun®) Framework** (e.g. Basic) to comply with their obligations will be considered as proportionate. This solution takes into account the rather limited societal and economic impact of their services.

1.22.10. Annex II – 4. Production, processing and distribution of food

This sector covers food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council which are engaged in wholesale distribution and industrial production and processing. A food business is defined as "*any undertaking, whether for profit or not and whether public or private, carrying out any of the activities related to any stage of production, processing and distribution of food*".

Annex II of the NIS2 law adds that it only covers food businesses that are "are engaged in wholesale distribution and industrial production and processing". The emphasis here lies on wholesale distribution, which implies a B2B factor (in opposition to B2C). This emphasis is meant to keep retail out of scope. Similarly, 'industrial production and processing' is meant to limit production and processing to large-scale food production and processing.

It is sufficient that the food business carries out one of the following activities to fall under this sector: wholesale, industrial production or industrial processing of food. These elements are not cumulative, but alternative conditions.

As explained in section 1.8, it is sufficient that one of the three activities is simply an accessory activity of an organisation.

1.22.10.1. Do supermarkets fall under the sector Food at Annex II, sector 4 of NIS2?

As mentioned in section 1.22.10, the sector production, processing and distribution of food is focused on wholesale distribution, industrial production or industrial processing of food. Supermarkets are retail. In general they do not fall under Annex II, sector 4.

However when a supermarket chain produces certain food products on a large scale (e.g. under its proper label), the entity producing those goods will fall under industrial production and therefor fall under this sector. The fact that the entity produces these food products with the sole purpose of supplying its own supermarkets, does not make a difference for the qualification under this sector. The other entities within the supermarket group will fall in the supply chain of that entity. For more information regarding supply chain, see section 3.14.

1.22.10.2. Do restaurants fall under Annex II, sector 4 of NIS2?

As mentioned in section 1.22.10, the sector production, processing and distribution of food is focused on wholesale distribution, industrial production or industrial processing of food. Restaurants in principle do not fall into these three possibilities and thus not within annex II, sector 4 of the NIS2 law.

However when a restaurant chain produces certain food products on a large scale (e.g. under its proper label), the entity producing those goods will fall under industrial production and therefor fall under this sector. The fact that the entity produces these food products with the sole purpose of supplying its own restaurants, does not make a difference for the qualification under this sector. The other entities within the restaurantgroup will fall in the supply chain of that entity. For more information regarding supply chain, see section 3.14.

1.22.11. Annex II – 5. Manufacturing

1.22.11.1. What does "manufacture of medical devices and in vitro diagnostic medical devices" mean?

Entities manufacturing medical devices as defined in article 2, point (1), of Regulation (EU) 2017/745 and entities manufacturing in vitro diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of the NIS2 law fall within the this subsector of Annex II 5. Manufacturing.

A medical device is defined as: *"any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:*

- *diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,*
- *investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,*
- *providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,*
- *and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.*

The following products shall also be deemed to be medical devices:

- *devices for the control or support of conception;*

- *products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point."*

An invitro medical device is defined as: *Any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system, whether used alone or in combination, intended by the manufacturer to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information on one or more of the following:*

a) concerning a physiological or pathological process or state;
b) concerning congenital physical or mental impairments;
c) concerning the predisposition to a medical condition or a disease;
d) to determine the safety and compatibility with potential recipients;
e) to predict treatment response or reactions;
f) to define or monitoring therapeutic measures.

Specimen receptacles shall also be deemed to be in vitro diagnostic medical devices;"

Next to this entities manufacturing medical devices considered to be critical during a public health emergency, can also fall under Annex I, 5. Health. For more information, see section 1.22.4.5.

In addition to the situation explained above, most entities manufacturing medical devices will fall into the supply chain of NIS2 entities (e.g. healthcare providers from annex I, sector 5). Entities covered by the NIS2 law must take appropriate and proportionate measures to secure their network and information systems. One of those measures is supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. For more information regarding supply chain obligations, see section 3.14)

1.22.12. Annex II – 7. Research

Research organisations fall under Annex II, 7. Research and are defined as "an entity which has as its primary goal to conduct applied research or experimental development with a view to exploiting the results of that research for commercial purposes, but which does not include educational institutions".

1.22.12.1. Do research organisations also cover sponsors?

Research organisations fall under Annex II, 7. Research and are defined as indicated above.

The NIS2-directive provides some context to this definition in its recital 36:

> *Research activities play a key role in the development of new products and processes. Many of those activities are carried out by entities that share, disseminate or exploit the results of their research for commercial purposes. Those entities can therefore be important players in value chains, which makes the security of their network and information systems an integral part of the overall cybersecurity of the internal market. Research organisations should be understood to include entities which focus the essential part of their activities on the conduct of applied research or experimental development, within the meaning of the Organisation for Economic Cooperation and Development's Frascati Manual 2015: Guidelines for Collecting and Reporting Data on*

> *Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing or development of a product or process, the provision of a service, or the marketing thereof.*

Following the Frascati Manual (2015), applied research is original investigation undertaken in order to acquire new knowledge, and Experimental development is systematic work, drawing on knowledge gained from research and practical experience and producing additional knowledge, which is directed to producing new products or processes or to improving existing products or processes.

The commercial purpose is broadly defined as encompassing *the manufacturing or development of a product or process, the provision of a service, or the marketing thereof*. If the goal of the research activities is to produce a new product, then there is a commercial purpose to the research.

The services provided by sponsors do not include applied research or experimental development activities, but only the funding of research activities by another organisation. Thus, these organisations, which do not provide the actual NIS2 service, do not fall within the scope of the NIS2 Law.

1.22.12.2. Are educational institutions "research organisations"?

As indicated in the definition mentioned in section 1.22.12, educational institutions are explicitly excluded. However, the latter could still fall under NIS2 if they are part of the public sector. More information can be found in section 2.7.

2. Public sector

2.1. How does the law apply to the public sector?

Art. 8, 34° and annex I, sector 10 (Public administration) NIS2 law

Art. 8, 34° of the law defines an "entity of the public administration" as an administrative authority referred to in article 14, § 1, subpara. 1, of the coordinated laws on the Council of State that meets the following criteria:

a) it is not of an industrial or commercial nature;
b) it does not carry out as its principal activity an activity listed in the type of entity column of another sector or sub-sector of one of the annexes of the law;
c) it is not a legal entity under private law.

For the definition of a public administration entity, article 6, 35) of the NIS2 Directive specifies that the concept must be recognised as such in accordance with national law, excluding the judiciary, parliaments, and central banks. It has therefore been decided to refer to existing concepts in Belgian law which cover the entities concerned so as not to multiply the application of different concepts.

In this case, the definition is based on the concept of administrative authority referred to in article 14, § 1, subpara. 1, of the coordinated laws of 12 January 1973 on the Council of State (see section 2.2), to which are added the criteria of not having an industrial or commercial nature, of not carrying out on a principal basis an activity falling within one of the other sectors or sub-sectors listed in the annexes to the law and of not being a legal person governed by private law.

This definition must be combined with the standard entity categories listed in annex I, sector 10 (Public administration):

- Public administration entities depending on the federal state;
- Public administration entities depending on federated entities, identified in accordance with article 11, § 2 of the law;
- Emergency zones within the meaning of article 14 of the law of 15 May 2007 relating to civil security or the Firefighting and emergency medical assistance service of the Brussels Capital Region created by the ordinance of 19 July 1990 creating a firefighting and emergency medical assistance service of the Brussels Capital Region.

The concept of dependency (which "depend on") is inspired by article 5 of the Law of 30 July 2018 on the protection of individuals with regard to the processing of personal data. In particular, it covers entities that are part of a level of power because they were created by these public authorities, their activity is financed mainly by these public authorities, their management is subject to control by these public authorities, or more than half of the members of their administrative, management or supervisory body are appointed by these authorities.

See also the following sections of this chapter for more details.

2.2. What is an “administrative authority”?

According to the case law from the Council of State, a public legal entity automatically qualify as an administrative authority in the meaning of article 14, § 1 of the coordinated laws of 12 January 1973 on the Council of State y, if it exercises powers under the executive branch.

To analyse whether a private legal entity can be qualified as an administrative authority, the following criteria are applied :

1) created or approved by the federal, federated, provincial or municipal authorities;
2) entrusted with a public service;
3) not part of the judiciary or the legislature;
4) operation determined and controlled by the public authorities ;
5) may take decisions that are binding on third parties.

These five criteria must be cumulatively met for a private legal entity to be qualified as an administrative authority.

2.3. What about organisations from the public sector active in another NIS2 sector (such as a public hospital, an intermunicipal organisation or a public retirement home)?

As the definition in art. 8, 34° indicates (see section 2.1), a public entity that primarily provides a service listed in another sector or sub-sector of one of the annexes to the law **is subject to the rules of that sector and not the public administration sector.**

This includes for example:

- an intermunicipal organisation providing gas and/or electricity;
- an intermunicipal organisation providing drinking water;
- an intermunicipal waste disposal organisation;
- a public hospital;
- a public retirement home;
- a public ICT service organisation;
- a public postal service;
- a public airport;
- etc.

If these examples are part of a local public administration (same legal entity), then the whole organisation will fall within the scope of the law in the (those) concerned sector(s) only. Local public administrations do indeed not fall into the public administration sector in annex I of the NIS2 law. See section 2.4 below for more information about local public administrations.

If a public administration depending on the federal State or on the federated entities also provides (not as its principal activity) a service covered by another NIS2 sector (same legal entity), it will fall into both sectors and have to apply the most stringent obligations from both (and thus also register in both). When public administrations depending on the federated entities fall into multiple sectors, they do not have to wait until they are identified to apply the obligations stemming from the NIS2 law and to register.

2.4. Are local public administrations within the scope of the law?

Art. 8, 34°; annex I, sector 10 (Public administration) NIS2 law

Local public administrations (municipalities, provinces, inter-municipalities, public social welfare centre (CPAS/OCMW), municipal companies, etc.) are **not automatically subject to the requirements of the NIS2 law.** They are indeed not explicitly listed in the annexes of the NIS2 law in the public sector.

Even though local public administrations such as those listed above comply with the definition enshrined in article 8, 34° (see section 2.1), they are neither dependent on the federal State, nor on the federated entities.

In accordance with the principle of local self-government enshrined in article 162 of the Constitution, local administrations must not be considered, despite the exercise of supervisory control or their financing, as public administrations depending on the federated entities or the federal State within the meaning of annex I of the NIS2 law.

However, these local entities are in scope of the NIS2 law when they provide a service listed in annex I or II of the law and at least qualify as a medium-sized enterprise. Their qualification as an essential or important entity under the law then depends on the service provided and their size (see also section 1.5).

Local public administrations may also be identified by means of article 11, § 1 (designation by the national cybersecurity authority - CCB), subject to compliance with the consultation procedures provided for in article 11, § 3. The initiative for such identification could be taken at the request of the national cybersecurity authority, the entity concerned, or a Region.

2.5. Are regional or community public administrations subject to the obligations of the NIS2 law?

Art. 11, §2-3 and annex I, sector 10 (Public administration) NIS2 law

Regional and community public administrations are part of the public administration sector covered by the NIS2 law, explicitly mentioned as "Public administration entities depending on federated entities". This notably includes federated public administrations, but also various public entities created, financed or otherwise managed by the federated level, under the condition that they comply with the definition from article 8, 34° of the NIS2 law (see section 2.1)

However, a **formal identification procedure** must first be carried out by the national cybersecurity authority (CCB). This involves recognizing, on the basis of a risk analysis, the entities that provide services whose disruption could have a significant impact on critical societal or economic activities.

In accordance with article 11, § 2 and 3 of the NIS2 law, this identification is carried out in consultation with the public entities concerned and the governments of the federated entities. At the end of this procedure, the Regional or Community public administration may be designated as an essential entity or an important entity.

If a public administration entity depending on a federated entity is also active in another sector of the NIS2 law, the identification process described above is not necessary for NIS2 law to apply (see also section 2.3).

See section 2.8 for information on registration.

2.6. What personnel has to be taken into account to calculate the size of my (local) public administration entity?

As long as it is not formally identified as a NIS2 entity and depending on the services delivered, a federated public administration or a local public administration might have to calculate it size.

Public entities must take into account all the personnel working **within the legal entity** of said public entity. According to User guide on the SME definition from the European Commission, *"[t]he staff headcount criterion covers full-time, part-time, temporary and seasonal staff and includes the following:*

- *employees;*
- *persons working for the enterprise who have been seconded to it and are considered to be employees under national law (this can also include temporary or so-called interim employees*;
- *owner-managers;*
- *partners engaged in a regular activity in the enterprise and deriving financial advantages from the enterprise."*

This does not include:

- *"apprentices or students who are engaged in vocational training and have apprenticeship or vocational training contracts;*
- *employees on maternity or parental leave."*

The basic headcount required for the calculation of the size-cap (see section 1.5) is expressed in AWUs (Annual Work Units). Anyone who worked full time within an enterprise, or on its behalf, during the entire reference year, counts as one unit. Part-time staff, seasonal workers and those who did not work the full year are treated as fractions of one unit.

In this context, a person who has worked on a fixed-term contract or on an assignment for only part of the year should be counted as a fraction of a unit based on the number of days worked over the previous year (divided by the working days over the year).

Personnel made available by a Public social welfare centre (CPAS/OCMW) to work in an organisation under article 60, §7 of the organic law from 8 July 1976 on public social welfare centres are included in the headcount calculation as interim employees.

It is important to note that the provisions on consolidation of data from partner and linked enterprises from Recommendation 2003/361/CE do not apply for public administrations. This entails that only the data from the administration itself must be taken into account. If, for example, a municipality providing drinking water services also has a school, it must only take the data from the school into account if said school is part of the same legal entity as the municipality.

2.7. Do public educational establishments, schools or universities fall into the scope of the law?

On the one hand, the education sector is not featured explicitly in annexes I and II of the NIS2 law. Private educational establishments are thus not in scope of the NIS2 law.

Annexes I and II & art. 8, 34° NIS2 law

On the other hand, **public** educational establishments, such as public universities or public high schools, **could** be included in the definition of a "public administration entity". To do so, they must:

- meet the size criterion (see section 1.5);
- be established in Belgium (see section 1.14);
- meet the definition of a public administration entity in article 8 of the NIS2 law (see sections 2.1 and 2.2);
- be dependent on the federal state or the federated entities (see section 2.1).
- if dependent on the federated entities: be identified in accordance with art. 11, § 2 (see section 2.5).

Furthermore, an educational establishment could also qualify as a "healthcare provider" (see section 1.22.4.1) within the meaning of annex I of the NIS2 law if, for example, it runs a university hospital which is part of the same legal entity (if it isn't, only the hospital will be in scope if the size-cap is reached).

2.8. When and how should public sector entities register?

Depending on which entities from the public sector are concerned, different regimes apply:

- For public entities depending on the federal state, the normal registration deadline (until the 18th of March 2025) applies since the law entered into force.
- For public entities depending on federated entities, the registration deadline is equal to 5 months after the concerned entity has been formally identified by the CCB (notification letter).
- For emergency zones, the normal registration deadline (until the 18th March 2025) applies since the law entered into force.

It is important to note that these deadlines only apply if the concerned organisation solely falls into the public administration sector. If it also falls into another sector, stricter deadlines might apply.

Registration takes place on our Safeonweb@Work platform (see section 3.13.1)

2.9. Do sanctions apply to public administration sector entities? What if the organisation also belongs to another sector?

According to article 62 of the NIS2 law, all administrative measures indicated in section 4.18.1 can be taken in response to a breach of the law by public administration sector entities. However,

these entities may not be subject to the administrative fines indicated in section 4.17 and some specific administrative measures

These statements are also true if a public administration entity belong to the public administration sector and to another NIS2 sector at the same time (the most favourable regime takes precedence over the other).

However, a public entity which mainly carries out an activity listed in the type of entity column of another sector or sub-sector can be subject to administrative fines and specific administrative measures (because they do not fall under the definition of an entity of the public administration).

3. Obligations

3.1. What are the legal obligations for the entities concerned?

The NIS2 law imposes a number of obligations on essential and important entities:

- the adoption of appropriate cybersecurity measures;
- timely notification of significant incidents;
- registration with the competent authorities (CCB's platform for most entities);
- training of members of management bodies (section 3.11);
- regular conformity assessments (mandatory for essential entities and voluntary for important entities);
- information sharing and collaboration with the relevant authorities.

These various obligations are explained in the following sections.

3.2. What are the obligations in terms of cybersecurity measures?

Art. 30, 31 and 42 NIS2 law

Essential and important entities must take appropriate and proportionate (technical, operational, and organisational) measures to manage the risks threatening the security of the networks and information systems that these entities use in the course of their activities or the provision of their services, and to eliminate or reduce the consequences that incidents have on the recipients of their services and on other services.

It is important to emphasise that, unlike the NIS1 law, the **scope of the NIS2 law covers the whole entity concerned** and not just the activities listed in the annexes of the law.

To facilitate the practical implementation of these cybersecurity measures, the CCB has already developed and made available free of charge a reference framework for entities concerned: the "Cyberfundamentals Framework" (CyFun®) with different levels and an analysis tool to determine the most appropriate level to follow. The law and its implementing decree will offer essential and important entities that decide to use the CyFun® framework or the international standard ISO/IEC 27001 (with the scope in line with NIS2 - i.e. all networks and information systems), a **presumption of conformity** with regard to security measures.

The minimum measures contained in the law are based on an "all-hazards approach" that aims to protect network and information systems and the physical environment of those systems from incidents, and include at least the following:

1. policies on risk analysis and information systems security;
2. incident management;
3. business continuity, such as backup management and disaster recovery, and crisis management;
4. supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
5. security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

6. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
7. basic cyber hygiene practices and cybersecurity training;
8. policies and procedures regarding the use of cryptography and, where appropriate, encryption;
9. human resources security, access control policies and asset management;
10. 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;
11. A coordinated vulnerability disclosure policy.

The measures to be adopted by essential and important entities must be **appropriate and proportionate**. On this point, it is important to specify that to avoid a dispositioned financial and administrative burden for essential and important entities, cybersecurity risk-management measures should be **proportionate to the risks** to which the concerned network and information system are exposed. In this respect, entities shall in particular take into account **the state of the art** of such measures as well as, where applicable, relevant European or international **standards**, and the **cost of implementing** such measures.

It should be noted that some NIS2 entities have to follow the Commission implementing regulation 2024/2690 of 17 October 2024 detailing the technical and methodological requirements of cybersecurity risk-management measures (see section 5.1).

3.3. What are the obligations in terms of incident reporting?

More information about incident reporting can be found on our website and in our incident notification guide.

3.3.1. General rules

Art. 8, 5° and 57°; 34 and 35 NIS2 law

The law defines an incident as *"an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems"*.

In the event of a **significant incident**, the entity must notify the national CSIRT (CCB) and, in certain cases, the recipients of their services.

See our incident notification guide for more details about “significant” incidents.

Notification takes place in several stages (see section 3.3.4): first an early warning within 24 hours of the incident being discovered, then a formal incident notification within 72 hours of the incident being discovered, and finally a final report no later than 1 month after the incident notification. In the meantime, the national CSIRT may request interim reports.

The CCB developed a comprehensive guide to when and how an incident should be notified. The currently latest version of the guide is available on our website or via this direct link: https://ccb.belgium.be/sites/default/files/nis2/NIS2 Notification guide 10-2024 v1.2 - EN.pdf.

NIS2 incidents may be reported to the CCB via its platform: http://notif.safeonweb.be/.

More information are also available here: https://ccb.belgium.be/en/cert/report-incident.

3.3.2. When is an incident “significant”?

The NIS2 law contains the obligation for all entities within its scope to notify the CCB about any incident that can be considered as a "significant" incident. Such an incident is defined in the law as follows:

“*Any incident that has a significant impact on the provision of any service listed in the sectors or sub-sectors in Annexes I and II of the law and which:*

1° *has caused or is likely to cause severe operational disruption to any of the services provided in the sectors or sub-sectors listed in Annex I and II or financial loss to the entity concerned; or*
2° *has affected or is capable of affecting other natural or legal persons by causing considerable material, personal or non-material damage*.”

Firstly, the incident must have an impact on the provision of one of the services provided in the sectors or sub-sectors listed in annexes I and II to the law, i.e. it must **affect the networks and information systems that support the provision of one or more of these services** (e.g. electricity distribution).

The mandatory notifications therefore only concern the information systems and networks on which the entity concerned depends to provide the service(s) listed in the annexes to the law. An incident affecting an isolated information system unrelated to the provision of the aforementioned services therefore does not have to be notified.

Secondly, the impact must be significant, i.e. cause or be likely to cause at least one of the following three situations:

- **serious operational disruption** of one of the services provided (in the sectors or sub-sectors listed in annexes I and II of the NIS2 law);
- **financial loss for the entity concerned**;
- **considerable material, physical or moral damage to other natural or legal persons**.

Further information about incident notification is available in our **NIS2 Incident Notification Guide**[3].

NIS2 incidents can be reported via our incident notification webform: **https://notif.safeonweb.be**.

3.3.3. Recipients of a mandatory notification of a significant incident

In principle, each NIS2 entity must notify an incident to the CCB only. The CCB will forward notifications to any sectoral authorities and to the Crisis Centre (for essential entities).

Art. 34, §1 NIS2 law

However, there is an exception to this rule for entities falling into the scope of the DORA Regulation in the banking and financial sectors. Entities in these two sectors notify their incident,

[3] https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20EN.pdf
See also the Commission implementing act (section 5.1)

as appropriate, to the National Bank of Belgium (NBB) or the Financial Services and Markets Authority (FSMA), which automatically forward the incident notification to the CCB.

Where appropriate, the entity shall notify the recipients of its service of significant incidents which could adversely affect the services provided by the entity. It also notifies recipients who are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat of any corrections and measures that they can apply in response. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

Art. 34, §2 NIS2 law

3.3.4. Incident notification procedure

Notification of significant incidents takes place in several stages:

Art. 35 NIS2 law

1. without undue delay and at the latest within **24 hours** of becoming aware of the significant incident, the entity shall transmit an early warning;
2. without undue delay and at the latest within **72 hours** (24 hours for trusted service providers) of becoming aware of the significant incident, the entity communicates an incident notification;
3. **at the request of** the national CSIRT or, where appropriate, the sectoral authority concerned, the entity shall submit an interim report;
4. no later than **one month** after the incident notification referred to in 2., the entity sends a final report;
5. if the final report cannot be sent because the incident is still in progress, the entity sends a progress report and then, in the month following the final handling of the incident, the final report.

In practice, an incident notification can be made via our platform: http://notif.safeonweb.be/.

3.3.5. Information to be sent when an incident is notified

The various notification stages involve different types of information to be transmitted:

Art. 35 NIS2 law

- The early warning indicates whether it is suspected that the significant incident may have been caused by illicit or malicious acts or whether it may have a cross-border impact. This early warning includes only the information necessary to bring the incident to the attention of the CSIRT, and enables the entity concerned to request assistance, if necessary.
  Such an alert should not divert the reporting entity's resources from incident management activities that should have priority, to avoid incident reporting obligations diverting resources from the management of significant incidents or otherwise compromising the entity's efforts in this regard.
- The purpose of incident notification within 72 hours is to update the information communicated as part of the early warning. It also provides an initial assessment of the incident, including its severity and impact, as well as indicators of compromise, where available.
  As with early warning, incident reporting should not divert the entity's resources, to avoid incident reporting obligations diverting resources from the management of significant incidents or otherwise compromising the entity's efforts in this regard.

- The interim report contains relevant updates on the situation.
- The final report should include a detailed description of the incident, including its severity and impact; the type of threat or root cause that is likely to have triggered the incident; the mitigation measures applied and in progress; and where relevant, the cross-border impact of the incident.
- The progress report contains as much as possible the information that should be in the final report and that is in the entity's possession at the time the progress report is submitted.

3.3.6. Confidentiality rules that apply to information transmitted during an incident

Art. 26, §3-4 NIS2 law

The NIS2 entity and its subcontractors restrict access to information relating to incidents, within the meaning of the NIS2 law, on a need-to-know basis and to those who have access to it in order to carry out their functions or duties in relation to this law.

This rule also applies to the CCB (national CSIRT), the NCCN and the sectoral authority.

Information provided to the CCB, the NCCN and the sectoral authority by a NIS2 entity may be exchanged with authorities in other EU Member States and with other Belgian authorities where this is necessary for the application of legal provisions.

However, this transmission of information is limited to what is relevant and proportionate to the purpose of this exchange, in compliance with EU Regulation 2016/679 (GDPR), the confidentiality of the information concerned, security and the commercial interests of the NIS2 entities.

3.4. Where can I report a NIS2 incident?

All NIS2 incidents can be reported via our online notification form: http://notif.safeonweb.be/.

More information about incident reporting can be found on our website.

See also our incident notification guide for more details about “significant” incidents.

3.5. What happens if an incident occurs that also involves personal data?

As is already the case, incident notifications under the law will not replace any notifications in the event of a personal data breach, for example to the Data Protection Authority (DPA). Two separate notifications will still be required.

However, the law provides for closer collaboration between the national cybersecurity authority and the data protection authorities. This collaboration could lead to the development of common tools.

The competent data protection authority can be notified via their website.

3.6. Is it possible to voluntarily report incidents or cyber-threats?

Yes, the national CSIRT (CCB) can also receive, on a voluntary basis, notifications of incidents, cyber threats or near misses from entities subject or not subject to the NIS2 law.

Art. 38 NIS2 law

A cyber-threat means "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons".

A near miss means "an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialize".

These voluntary notifications are processed in the same way as mandatory notifications, but mandatory notifications may nevertheless be given priority.

A voluntary notification does not have the direct effect of leading to an inspection of the entity that issued the notification or of imposing additional obligations on it to which it would not have been subject had it not issued the notification.

See the procedure explained in section 3.3.

3.7. What if my supplier or a company in my group has an incident? Who has to report? What if it happens in multiple Member States?

Every organisation falling under NIS2 that is affected by a significant incident has to report it separately to the competent NIS2 authorities in the EU. All other organisations may also voluntarily notify their incidents to the CCB via the platform mentioned in section 3.3.1.

If the incident affecting the supplier or another company of the group also becomes a significant incident for the concerned NIS2 entity, then the latter has to report it. NIS2 entities and their suppliers or partner companies should communicate together and mutually inform themselves about cybersecurity incidents affecting the provision of their services.

If the significant incidents affects multiple companies (or one company) established in multiple different Member States, then the incident will have to be reported according to the rules on jurisdiction as explained in section 1.14. It is possible that the incident has to be reported in multiple Member States in certain exceptional cases (for example one company with one legal entity established in multiple Member States and not only under the main establishment exception). In practice, an incident often affects only one Member State and thus the entity will have to report it only in one Member State.

3.8. What is covered by the two liability regimes from the law (art. 31 & 61) ?

See also sections 3.9 and 3.10 below.

Article 31, § 1 of the NIS2 law provides that management bodies are liable for breaches of Article 30 (cybersecurity measures) by their entities. According to the theory of the organ, the liability of the legal person is in principle engaged through the action of its organs, as provided for in article 2:49 of the Companies and Associations Code.

However, the theory of cumulative liability is applicable to civil liability, in particular under the conditions and within the limits established by articles 2:56 to 2:58 of the Companies and Associations Code, so that the civil liability of members of the supervisory bodies (of members of the administrative bodies at the very least) may be incurred on the twofold condition that the fault is of an extra-contractual nature and manifestly exceeds the margin within which normally prudent and diligent directors would be placed in the same circumstances.

In addition, article 61, subsection 1 of the NIS2 law establishes specific liability for any natural person responsible for an essential or important entity or acting as the legal representative of an essential or important entity on the basis of the power to represent it, to take decisions on its behalf or to exercise its control, by virtue of their power to ensure that the entity complies with this law. Such persons are liable for breaches of their duty to ensure compliance with the NIS2 law.

From the point of view of administrative measures, the NIS2 law allows, in the event of repeated breaches, the temporary prohibition of any natural person exercising managerial responsibilities at the level of managing director or legal representative in the essential entity concerned from exercising managerial responsibilities in that entity, until such time as the essential entity concerned has taken the necessary measures to remedy the shortcomings or to comply with the requirements of the competent authority at the origin of the application of these enforcement measures (Article 60, subsection 1, 2°, and subsection 2, NIS2 Law; see also section 4.18.2).

Finally, it can be noted that the NIS2 law does not prevent the application of any criminal liability. The criminal liability of legal persons does not exclude that of natural persons who are perpetrators of the same acts or who have participated in them.

With the exception of the provision relating to administrative measures, which applies only to essential entities, the elements set out above are applicable to both essential and important entities.

3.9. What are management's obligations and responsibilities?

Art. 31 & 61 NIS2 law

The management bodies of NIS2 entities must approve cybersecurity risk-management measures and oversee their implementation. If the entity breaches its obligations with regard to risk-management measures, the management body is liable.

Members of management bodies are obliged to undergo training to ensure that their knowledge and skills are sufficient to identify risks and assess risk-management measures in terms of cybersecurity and their impact on the services provided by the entity concerned.

The natural persons responsible and/or legal representatives of an entity must have the power to ensure that the entity complies with the law. They are liable for their failure to do so.

The aim of this accountability is to transform cybersecurity into a subject that really matters to the entities concerned.

These rules on liability are without prejudice to the rules on liability applicable to public institutions, as well as to the liability of civil servants and elected or appointed officials.

It should be noted that natural persons exercising managerial functions at the level of managing director or legal representative in a NIS2 entity may be temporarily barred from exercising managerial responsibilities in this entity, in the event of breaches of the requirements of the NIS2 law.

3.10. What is a "management body"?

The concept of "management body" is not defined in the directive.

The explanatory memorandum of the NIS2 Law defines "member of a management body" as follows:

Any natural or legal person who :

(i) exercises a function within or in relation to an entity which authorises him or her (a) to administer and represent the entity in question or (b) to take decisions in the name and on behalf of the entity which are legally binding on it or to participate, within a body of that entity, in the taking of such decisions, or

(ii) has control over the entity, meaning the power, in law or in fact, to exercise decisive influence over the appointment of the majority of the entity's directors or managers or over the direction of the entity's management.

Where the entity in question is a company governed by Belgian law, this control is determined in accordance with articles 1:14 to 1:18 of the Companies and Associations Code.

Where the person whose role is being examined is a legal person, the concept of "member of a management body" is examined recursively and covers both the legal person in question and any member of a management body of that legal person.

3.11. What should be the content of the training for management?

The purpose of training members of the management body is to enable them to properly perform the duties assigned to them under the law, i.e. to approve risk-management measures relating to cybersecurity and to supervise the implementation of these measures. There is no indication of the exact training requirements. Its content and duration are therefore left to the discretion of the entities.

Our CyberFundamentals Framework contains information on the training process, in particular in terms of content and target audience. In the Important level, for example, the section on training can be found from page 28 onwards (CyFun® 2023).

As a supervisory authority, the CCB cannot offer trainings for NIS2 entities, nor can we recommend specific training programs.

3.12. What are the legal conditions for using the protective framework when researching and reporting vulnerabilities (ethical hacking)?

The NIS2 law incorporates the provisions of the NIS1 law, which provides a protective framework for "ethical hackers" or "digital whistleblowers".

Art. 22 and 23 NIS2 law

To benefit from this framework, the person must:

- Act without fraudulent or malicious intent;
- Send a simplified notification within 24 hours after the discovery of the vulnerability to both the national CSIRT and the responsible organisation;
- Send a full notification within 72 hours after the discovery to the same recipients;
- Act only within the limits of what is necessary and proportionate to verify the existence of a vulnerability and to report it;
- Refrain from making public a vulnerability without the agreement of the national CSIRT.

In addition, to be able to search for vulnerabilities in the networks and information systems of certain authorities such as intelligence services, defence, judicial authorities, etc., ethical hackers must first conclude an agreement with these entities.

The CCB website provides general information on ethical hacking, in particular with a page dedicated to the reporting procedure.

3.13. What are the obligations in terms of registration?

3.13.1. How do NIS2 entities register?

Essential and important entities will have to register on the CCB portal, Safeonweb@Work.

Art. 13 NIS2 law

The deadline for registration depends on the type of entity. In principle, essential and important entities, as well as domain name registration service providers, have **5 months** to register after the law comes into force, i.e. by **18th March 2025**. When registering, they must provide the following information:

1. their name and CBE registration number or equivalent registration in the European Union;
2. their current address and contact details, including e-mail address, IP ranges and telephone number;
3. where applicable, the relevant sector and sub-sector referred to in annex I or II of the law;
4. where applicable, a list of the Member States in which they provide services falling within the scope of the law.

There is an exception for entities that have already communicated this information to a NIS2 sectoral authority because of a legal obligation. In this case, the information simply needs to be

completed with this authority. If the information changes, the changed information must be communicated within two weeks.

A slightly adapted regime exists for the following types of entity:

Art. 14 NIS2 law

- DNS service providers;
- TLD name registries;
- Entities providing domain name registration services;
- Cloud computing service providers;
- Data centre service providers;
- Content delivery network providers;
- Managed service providers;
- Managed security service providers;
- Online marketplace providers;
- Online search engine providers; and
- Social networking service platform providers.

They must register within **2 months** of the law coming into force, i.e. by **18th December 2024**, and provide the following information:

1. Their name;
2. Their sector, sub-sector and type of entity, as listed in Annex I or II, as applicable;
3. The address of their principal place of business and of their other legal establishments in the Union or, if they are not established in the Union, of their representative;
4. Their current contact details, including e-mail addresses and telephone numbers, and, where applicable, those of their representative;
5. The Member States in which they provide their services falling within the scope of the law;
6. Their IP ranges.

Here again, every entity is required to inform the CCB immediately of any changes to their information.

In practice, some of this information is obtained directly from the Crossroads Bank for Enterprises (CBE) during the registration process.

3.13.2. How can I register my organisation?

All practical details relating to the registration procedure are explained in our NIS2 registration guide available online.

In short: the legal representatives of an organisation mentioned in the Crossroad Bank of Enterprises (CBE) (search for your organisation here) can connect themselves to the My eGov Role Management Platform to provide the necessary authorisations to any suited Belgian citizen to register an organisation on our Safeonweb@Work platform. All information are available in the guide.

3.13.3. How do I know if my organisation is already registered?

The person indicated in section 3.13.2 must connect itself to the platform to verify.

3.13.4. Which entities have to register in a group of companies? Can only the holding register?

Within a group of companies, all organisations/separate legal entities (even potentially the holding – depending on the services provided) falling under NIS2 **have to register individually**. The holding cannot register in place of the companies in its group.

3.13.5. What if my organisation has departments or sub-entities that are different types of entities?

If these departments or sub-entities are all part of the same legal entity, then said legal entity must register as all the different types of entities it qualifies as.

If the different sub-entities are separate legal entities that all qualify as an "entity" under NIS2 (see section 1.4), then they all have to register separately.

3.13.6. Do organisations in the supply chain of NIS2 entities have to register?

Only organisations falling into the scope of application of NIS2 have to register. It is possible that organisations in the supply chain of NIS2 entities are not NIS2 entities themselves and thus do not have to register.

Fore more information about supply chain, see section 3.14.

3.13.7. How can an organisation established outside of Belgium register? How can a legal representative register an organisation?

There are two exceptional situations where organisations outside of Belgium would have to register:

1) They provide electronic communication services or networks in Belgium (see section 1.14);
2) They fall under the main establishment jurisdiction regime (see section 1.14), are established outside of the EU, provide services in Belgium, chose Belgium as their place of registration in the EU, and designate a legal representative there.

In these two situations, if organisation are unable to register via the Safeonweb@Work website, they should contact the CCB via info@ccb.belgium.be.

3.13.8. Do I have to register again if my organisation already fell under NIS1?

Yes, the organisation has to register again.

3.13.9. How can I prove that my organisation is registered?

NIS2 organisations can ask the CCB via info@ccb.belgium.be to provide them a document as proof of their registration.

This manual process will soon be replaced by a downloadable document on the platform.

3.13.10. What will the CCB do with organisations that don't register?

The CCB will, based on the information at its disposal as a federal government authority, proactively attempt to search and reach out to entities that did not register. It is important to note that entities who did not register could be seen as having breached the NIS2 law and potentially expose themselves to appropriate administrative measures and fines.

3.14. Supply chain: How can an entity manage the relations with its supplies and direct service providers ?

Art. 30, §3, 4° NIS2 law

As part of the minimum list of cybersecurity risk-management measures, entities covered by the NIS2 law must take appropriate and proportionate measures to secure their network and information systems.

One of these measures is the security of the entity's supply chain. This includes the security aspects of the relationship between each entity and its **direct suppliers or service providers**.

The impact of this obligation can be felt from two perspectives: Not only does it imply that NIS2 entities must impose cybersecurity risk-management measures on the organisations in their supply chain(s) (such as suppliers and subcontractors) and oversee them, it also implies that entities not within the scope of application of NIS2 will also be required to take appropriate and proportionate cybersecurity risk-management measures.

The NIS2 law does not state how NIS2 entities should handle the direct supply chain obligation. In particular, it leaves it up to the entities themselves to verify if the organisations in their supply chain respect their obligations. The CCB recommends all NIS2 entities to contractually impose a label or certification on the organisations in their supply chain, such as those included in the CyberFundamentals (CyFun®) Framework, in order to facilitate the demonstration of compliance with the supply chain obligation.

For ongoing contracts with suppliers and service providers, it is the responsibility of the entity to assess the currently applying provisions and make sure they comply with the obligations. Existing contracts may have to be revised. The NIS2 entity should put sufficient contractual safeguards in place in case the organisation in its supply chain does not comply with its obligations. See the timeline in section 4.14 for when the contracts should be adapted.

To chose the proper CyFun® level to impose on suppliers and service providers, the NIS2 will have to make a risk assessment and impose the most appropriate level based on its result. The CyFun® Risk Assessment tool could be used for that purpose.

For all entities not within the scope of application of the NIS2 law, the CCB recommends that they also take appropriate and proportionate cybersecurity risk-management measures to prepare themselves for the eventuality that they constitute part of the supply chain of a NIS2 entity. Here again, they can have recourse to the CyFun® Framework to identify and implement the concrete measures they could be required to take.

Neither a certain ownership by the NIS2 entity of an organisation in its supply chain, nor the latter's size have no impact on the scope of this obligation. It may only possibly have an impact on the NIS2 entities supply chain risk assessment.

For handling of incidents from suppliers, see section 3.7. See also section 3.9 on the responsibility of management bodies for cybersecurity risk-management measures.

3.15. What confidentiality obligations have to be respected ?

Art. 26 NIS2 law

The competent authorities, essential and important entities as well as their subcontractors shall restrict access to information under the NIS2 law to persons on a need-to-know basis and to those who have access to it in order to carry out their functions or duties in connection with the execution of the law.

Information provided to the competent authorities by essential or important entities may nevertheless be exchanged with authorities in the European Union, with Belgian authorities or with foreign authorities, where this is necessary for the application of legal provisions.

The information exchanged is limited to what is relevant and is proportionate for the purpose of the exchange, in particular in compliance with Regulation (EU) 2016/679 (GDPR). This exchange of information preserves the confidentiality of the information concerned and protects the security and commercial interests of essential or important entities.

Art. 27 NIS2 law

However, the law allows for the voluntary exchange of relevant cybersecurity information, in particular information relating to cyberthreats, avoided incidents, vulnerabilities, etc. This exchange takes place under certain conditions within the framework of information exchange communities, implemented by means of information sharing agreements.

4. Control / Supervision

4.1. Who will be the competent authorities?

Art. 15, 16 ff. NIS2 law and art. 3 NIS2 royal decree

4.1.1. The Centre for Cybersecurity Belgium (CCB)

The national cybersecurity authority (CCB) is responsible for coordinating and monitoring the law. To this end, the law combines the existing tasks of the CCB with the additions provided for by the NIS2 Directive, in particular regarding the supervision of entities. The CCB is responsible for supervising essential and important entities (with the help of the sector authorities) and is the central contact point for implementing NIS2.

The national Computer Security Incident Response Team (national CSIRT) is also part of the national cybersecurity authority. NIS2 entities are required to report significant incidents to this CSIRT.

4.1.2. Sectoral authorities

The following sectoral authorities have been designated:

1. **for the energy sector**: the Federal Minister responsible for Energy or, by delegation, a senior member of staff from his administration (where appropriate, the Minister may appoint a different delegate for each sub-sector);
2. **for the transport sector:**
    a. With regard to the transport sector, with the exception of water transport: the Federal Minister responsible for Transport, or by delegation, a senior member of staff from his administration (where appropriate, the Minister may designate a different delegate for each sub-sector);
    b. With regard to water transport: the Federal Minister responsible for Maritime Mobility, or by delegation, a senior member of staff of his administration (where appropriate, the Minister may designate a different delegate for each sub-sector);
3. **for the health sector**:
    a. For entities carrying out research and development activities in the field of medicines; entities manufacturing basic pharmaceutical products and pharmaceutical preparations; and entities manufacturing medical devices considered critical in the event of a public health emergency: the Federal Agency for Medicines and Health Products (FAMHP);
    b. the Federal Minister responsible for Public Health or, by delegation, a senior member of staff from his administration;
4. **for the digital infrastructure sector:** Belgian Institute for Post and Telecommunications (BIPT);
5. **Regarding trust service providers**: the Federal Minister for Economic Affairs or, by delegation, a senior member of staff from his administration;
6. **for the digital providers sector**: the Federal Minister for Economic Affairs or, by delegation, a senior member of staff from his administration;

7. **for the space and research sectors**: the Federal Minister for Science Policy or, by delegation, a senior member of staff from his administration;
8. **for drinking water**: the National security committee for the supply and distribution of drinking water;
9. **for the banking sector**: the National Bank of Belgium (NBB);
10. **for the financial market infrastructure sector**: the Financial Services and Markets Authority (FSMA);

The sector authorities have a number of powers. For more information, see section 4.8.

Entities covered by a sectoral authority can turn to it for information, assistance, etc.

4.1.3. The National Crisis Centre (NCCN)

The National Crisis Centre is also involved in the implementation of the NIS2 Law, in particular regarding incident notification, cyber-crisis management and physical security measures implemented by operators of critical infrastructures and critical entities (subject to the CER Directive).

4.2. Which reference frameworks can be used by NIS2 entities to demonstrate their compliance?

Essential entities subject to the regular conformity assessment obligation may choose to use one of the two reference frameworks mentioned in the NIS2 royal decree.

Art. 5, §1 NIS2 royal decree

The use of these frameworks for control is explained in the next section (4.4.).

4.2.1. The CyberFundamentals (CyFun®) Framework

The CyberFundamentals (CyFun®) Framework[4] is a set of concrete measures to:

- protect data;
- significantly reduce the risk of the most common cyber-attacks;
- increase an organisation's cyber resilience.

To respond to the severity of the threat to which an organisation is exposed, in addition to the starting level Small, 3 assurance levels are provided: Basic, Important and Essential. The framework has been validated using CERT attack profiles (obtained following successful attacks). The conclusion is that:

- measures in assurance level Basic can mitigate 82% of the attacks;
- measures in assurance level Important can mitigate 94 % of the attacks;
- measures in assurance level Essential can mitigate 100% of the attacks.

A tool allows to select the most appropriate level to apply.

[4] https://cyfun.be

In addition, the CyFun® Framework:

- is **based on recognised norms**: CyFun® selects relevant controls based on common standards such as NIST CSF, ISO/IEC 27001, CIS controls and IEC 62443;
- **corresponds to the measures needed** to prevent the main attacks identified by the CCB;
- can **be used by yourself**: each control is accompanied by guidance to help implementation. CyFun®'s self-assessment tool helps you to have oversight of your implementation;
- can **validate your implementation**: you can validate your implementation by requesting an assessment of an accredited and authorised conformity assessment body (CAB). This attestation demonstrates your implementation to your customers and your authorities (i.e. to comply with NIS2).

In the context of NIS2, the CyFun® Framework is a particularly useful tool, not only for essential entities subject to a regular conformity assessment, but also for important entities. It is freely available and offers straight-forward solutions for risk-assessment, self-assessment and for concretely putting in place the minimum cybersecurity risk-management measures required by the NIS2 law. In addition, a validated or certified implementation of the CyFun® framework awards concerned entities with a presumption of conformity in the context of the supervision under NIS2.

The CCB highly recommends all NIS2 entities to use the CyFun® Framework, which is available publicly and free of charge on our Safeonweb@Work website.

4.2.2. ISO/IEC 27001

The European norm ISO/IEC 27001 is an internationally recognised technical norm that sets out the general and structured approach to be adopted for the management of the security of any information system. It is therefore a base norm setting out the general principles for implementing security measures in information systems and is applicable to all sectors.

The most recent version dates from 2022, but it is mentioned in the royal decree without any date indication, so that the most recent version can always be applied.

More information can be found on the official website.

4.3. Where can I find more information about CyFun®?

All information, documents, guidance, etc. are centralised on https://cyfun.be.

CyFun® also has its own FAQ available at: https://atwork.safeonweb.be/cyberfundamentals-frequently-asked-questions-faq.

4.4. How will the concerned entities be audited? Does the CCB do CyFun certifications?

When we talk about control/supervision in the context of the law, we need to distinguish between two categories of entities: essential entities and important entities.

Art. 39 ff. NIS2 law

Art. 6-13 NIS2 royal decree

It is mandatory for essential entities to undergo regular conformity assessment. This assessment is carried out on the basis of a choice made by the entity between three options:

- Either a CyberFundamentals (CyFun®) certification granted by a conformity assessment body (CAB) authorised by the CCB (after accreditation by BELAC);
- or an ISO/IEC 27001 certification, issued by a CAB accredited by an accreditation body that has signed the mutual recognition agreement (MLA) governing the ISO/IEC 27001 standard within the framework of the European co-operation for Accreditation (EA) or the International Accreditation Forum (IAF), and authorised by the CCB;
- or an inspection by the CCB's inspection service (or by a sectoral inspection service).

The inspection service may also control essential entities at any time (in the absence of an incident - *ex ante* - and after an incident or with sufficient evidence of non-compliance with the law - *ex post*).

For important entities, supervision is only carried out "*ex post*" by the inspection department, i.e. after an incident or in the light of evidence, indications, or information that an important entity is not complying with its obligations (art. 48, §2 of the NIS2 law). In principle, therefore, they are not subject to regular conformity assessment. However, these entities may voluntarily submit to the same regime as essential entities.

For details about the inspection carried out by the inspection service, see section 4.15.

The CCB does not do regular conformity assessments of NIS2 entities which may lead to a presumption of conformity, and therefore also does not give out CyFun® certifications. Only CABs may do so.

4.5. Does an organisation have to get a CyFun® certification or verification if it wants to use ISO/IEC 27001?

No, a CyFun® certification or verification is not a necessary intermediate step in order to receive an ISO/IEC 27001 certification.

However, it is possible to obtain a CyFun label by using an existing ISO/IEC 27001 certification with the correct scope and Statement of Applicability. For this, the necessary documents have to be uploaded via the "Labels" tab on your registered organisation's dashboard on Safeonweb@Work.

4.6. What is a conformity assessment body (CAB)?

A Conformity Assessment Body (CAB) is a body responsible for checking and certifying compliance with the requirements set out in the CyFun® reference framework or the ISO/IEC 27001 norm (applied under the NIS2 law) by NIS2 entities subject to regular conformity assessment (mandatory for essential entities, voluntary for important entities).

For CyFun®, it is accredited by the Belgian accreditation authority (BELAC) and authorised by the CCB. For ISO/IEC 27001, it is accredited by an accreditation body that has signed the Mutual Recognition Agreement (MLA) governing the ISO/IEC 27001 standard within the framework of the European co-operation for Accreditation (EA) or the International Accreditation Forum (IAF) and

authorised by the CCB. More information can be found in the CAB authorisation conditions on our website.

4.7. Where can I find more information for CABs?

All information in relation to accreditation in Belgium is available on the official website of BELAC: https://economie.fgov.be/en/themes/quality-and-safety/accreditation.

Additional information for CABs under CyFun® are available here on our website: https://atwork.safeonweb.be/conformity-assessment-bodies-cab.

4.8. What are the missions of the sectoral authorities?

The sectoral authorities also play a role under the NIS2 law, due to their specific knowledge and expertise in each of the sectors concerned. Where appropriate, they may be involved in the following tasks:

Art. 11, 13, 24, 25, 33, 34, 39, 44, 51 and 52 NIS2 law

- Additional identification (consultation and proposition);
- Registration of entities;
- Organisation of sectoral exercises;
- Analysing and managing the consequences of an incident for a sector;
- Participation in some of the work of the NIS Cooperation Group;
- Raising awareness of entities in their sectors;
- Cooperation at national level;
- Additional cybersecurity risk-management measures;
- Notification of incidents (transmission of notifications of significant incidents from the national CSIRT to the sectoral authorities, consultation in various situations on this subject);
- Supervision and inspection (joint or delegated);
- Administrative fines.

4.9. How can an entity prove that it is in compliance with its obligations? What is a presumption of conformity?

As part of the regular conformity assessment - which is mandatory for essential entities - it will be possible for the entity to obtain a certification or a label, making it possible to presume, until proven otherwise, that the entity is in compliance with its cybersecurity obligations.

Art. 42 NIS2 law

Art. 5, §1 NIS2 royal decree

This certification will be based on the two frameworks mentioned in the royal decree: the CyberFundamentals or the international norm ISO/IEC 27001 (with the appropriate scope and statement of applicability). See also section 4.2.

It is important to note that the **scope** of a certification must be **identical to the scope of the NIS2 law**, meaning that it has to include the networks and information systems of an organisation as a

whole, otherwise the certification will not allow an organisation to benefit from a presumption of conformity.

Of course, an entity may also use another reference framework or technical norm to implement its legal cybersecurity requirements. In this case, it will not benefit from the presumption of conformity and will have to demonstrate to the inspection service that it is applying all the required measures, based on a mapping table with one of the two aforementioned standards.

4.10. Can you limit to scope of a certification or verification to only the NIS2-related services and activities?

As noted in section 4.9, the scope of a certification or verification may not be smaller than the scope of the NIS2 law, which covers the whole organisation.

4.11. Can an entity use a CyFun® level of assurance that is lower than the level assigned to its entity category? Does that change its NIS2 qualification?

Art. 7 NIS2 royal decree

The royal decree allows an entity to use a lower CyFun® level (for example, the use of the Important assurance level for an essential entity) provided that it can justify this objectively on the basis of its risk analysis. This choice remains the sole responsibility of the entity concerned and **has no impact on its legal qualification as an essential or important entity**. It should be emphasised that this choice may be called into question at any time by the inspection service as part of its control missions.

The CCB offers a risk assessment tool available on Safeonweb@Work so that an entity can make an informed choice about the CyFun® assurance level it requires.

4.12. Do organisations need the agreement from the CCB to use a lower level of CyFun®?

No, NIS2 entities do not have to ask the CCB to confirm their analysis to use a lower level of CyFun®. As indicated in section 4.11, every NIS2 entity is itself responsible for that choice. The justification for said choice must only be internally documented.

During an inspection, the relevant inspection service may control the choice made by the entity.

4.13. Can an entity that was an Operator of Essential Services (OSE) under NIS1 keep its ISO27001 certification?

Art. 8, 12 and 14-15 NIS2 royal decree

If an entity that was an operator of essential services (OSE) under NIS1 has an ISO/IEC 27001 certification, it will be able to use its certification as part of the NIS2 regular conformity assessment. If necessary, the

scope of the certification should be extended to ensure that it covers all the networks and information systems of the entity concerned.

Certification must be carried out by a conformity assessment body accredited by BELAC in Belgium (or by another accredited national European body if this certification comes from another Member State) and authorised by the CCB.

4.14. [Timeline] When will the entities concerned have to apply the obligations of the law?

Most obligations contained in the NIS2 legal framework are applicable from the 18th of October 2024. However, for some of them the law or the royal decree give entities an additional deadline before they must be applied.

Art. 13 & 75 NIS2 law
Art. 22-23 NIS2 royal decree

Starting from 18th October 2024, notably the following obligations apply:

- Taking the minimum cybersecurity risk-management measures;
- Notifying all significant incidents;
- Subjecting to the supervision of and co-operate with competent authorities;
- For management bodies: approve cybersecurity risk-management measures, oversee implementation of measures, be liable for violations by the entity, and follow cybersecurity training.

Concerning the registration of entities at the CCB via Safeonweb@Work, the law provides the following deadlines:

- Entities providing services falling into the digital sectors of the annexes (list in Art. 14, §1 of the law) have 2 months from the 18th of October 2024 of register (**until 18th December 2024 at the latest**);
- All other entities have 5 months from the 18th of October 2024 to register (**until 18th March 2024 at the latest**).

The supervision/regular conformity assessment of essential entities also takes a gradual approach:

- For the CyberFundamentals (CyFun®) Framework:
  - Entities who, based on their risk-assessment, determine that they must comply with the **assurance level (AL) Basic**, have a deadline of 18 months (**until 18th April 2026 at the latest**) during which they must acquire a verification by an accredited and authorised conformity assessment body (CAB);
  - Entities who, based on their risk-assessment, determine that they must comply with **AL Important**, have a deadline of 18 months (**until 18th April 2026 at the latest**) during which the must either obtain a Basic or an Important verification by an accredited and authorised CAB.
    If necessary, they may obtain an initial verification at level Basic and a verification at level Important after a further period of 12 months (**until 18th April 2027 at the latest**);
  - Entities who, based on their risk-assessment, determine that they must comply with **AL Essential**, have a deadline of 18 months (**until 18th April 2026 at the**

latest) during with the must either obtain a Basic or an Important verification by an accredited and authorised CAB.
They have an additional deadline of 12 months (**until 18th April 2027 at the latest**) during which they must acquire an Essential certification by an accredited and authorised CAB.

- Entities who chose to be ISO/IEC 27001 certified must transmit their scope & statement of applicability by **18th April 2026 at the latest** to the CCB and acquire a certification by an accredited and authorised CAB by **18th April 2027 at the latest**.
- Entities who chose to be directly inspected by the CCB:
  - **By 18th April 2026 at the latest**: Transmit their self-assessment of CyFun® AL Basic or Important, or transmit their ISO/IEC 27001 information security policy, scope and statement of applicability to the CCB;
  - **By 18th April 2027 at the latest**: Report on progress towards compliance.

Important entities are not subject to mandatory regular conformity assessments (because of ex-post supervision only). In respect of the appropriate and proportionate nature of cybersecurity measures, the inspection service will supervise important entities for a similar 18 month period after the law enters into force (to enable them to fully achieve the required level).

If, for example, a significant cyberincident occurs at the beginning of 2025, the concerned entity will have to take the necessary measures to manage it and notify the CCB, possibly under the supervision of the competent inspection services. We therefore encourage all NIS2 entities not to wait until the registration deadline and their first conformity assessments to implement the required measures.

4.15. How are inspections carried out?

Art. 44 ff. NIS2 law

The inspection service of the national cybersecurity authority is responsible for carrying out inspections to check that essential and important entities comply with cybersecurity risk-management measures and incident reporting rules.

Inspections relating to essential entities may be both *ex ante* (proactive) and *ex post* (reactive). They are carried out by the inspection service of the national cybersecurity authority or by the designated sectoral inspection service (specific/complementary sectoral measures). These inspections may, at the request of the sectoral authority, be carried out jointly by the aforementioned authorities.

Essential entities are also required to undergo regular conformity assessments. Important entities may also voluntarily undergo a conformity assessment based on ISO/IEC 27001 or the CyberFundamentals (see section 4.4.).

Ex-post inspections of important entities are carried out on the basis of indicators, such as the occurrence of an incident or objective evidence of possible shortcomings. Once again, this inspection may be carried out by the CCB inspection service, by the designated sectoral inspection service, or by both. The aim of joint controls or delegated controls to sectoral inspection services is to simplify and rationalise government resources.

The inspectors will be able to carry out on-site visits, record their findings and draw up reports. On the basis of these findings, a procedure may be launched to enjoin the entity to put an end to

a violation and, if necessary, to take appropriate administrative measures, ranging from a warning to an administrative fine.

4.16. What if my organisation cannot prove that they are compliant after 18 months?

During their controls, the inspection service will put a lot of emphasis on the evolution of an organisation over time towards its goal. It is thus of high importance that proof of practical progress towards compliance can be put forward.

The primary goal of the CCB is to reach a high level of cybersecurity across the country, in close collaboration with all the concerned entities. There are, nevertheless, situations in which sanctions may be necessary. To this end, the law (Title 4, Chapter 2) provides for a specific procedure that sets out the interaction between the CCB and the concerned entity. This procedure notably includes an obligation for the CCB (or a sectoral authority) to inform the entity about its intention to impose a sanction. It goes without saying that this draft sanction decision must be accompanied by a sufficient motivation. The entity then has the possibility to defend itself.

Should a sanction still be deemed necessary, the CCB must take into account a certain minimum number of elements to determine an appropriate and proportionate sanction; for example, the category of the entity, prior infractions, the gravity of the infraction, its length, damages, negligence, etc.

In any case, upon non-compliance the competent inspection service can take appropriate measures and/or fines to ensure that the organisation becomes compliant with the law. Depending on the effect of these measures and/or fines on the behaviour of the organisation, further measures and/or fines could be taken until compliance has been achieved.

Further information about measures and fines are available in sections 4.17 and 4.18.

4.17. Are administrative measures and fines proportionate? How high are the fines?

Art. 59 NIS2 law

The purpose of administrative measures and fines is to strengthen the level of cybersecurity of essential and important entities. Subject to compliance with the procedures laid down by law (including the hearing of the entity concerned, see art. 51-57), an administrative measure or fine may be imposed, in a proportionate manner, taking into account the seriousness of the breaches, the attitude of the entity and any repeat offences.

The following administrative fines may be imposed:

1. 500€ to 125.000€ for non-compliance with the information obligations from art. 12 (identification process);
2. 500€ to 200.000€ for an entity that has sanctioned one of its employees or subcontractors for performing the obligations of the law in good faith and within the scope of their duties;
3. 500€ to 200.000€ for non-compliance with supervision obligations;

4. From 500€ to 7.000.000€ or 1.4% of the total worldwide annual turnover for the previous financial year of the company to which the important entity belongs (whichever is higher), for the important entity that does not comply with the obligations relating to cybersecurity risk-management measures and/or incident reporting;
5. From 500€ to 10.000.000€ or 2% of the total worldwide annual turnover for the previous financial year of the company to which the essential entity belongs (whichever is higher), for the essential entity that does not comply with the obligations relating to cybersecurity risk-management measures and/or incident reporting.

The administrative fine is doubled in the event of a repeat offence for the same acts within a period of three years.

A combination of breaches may give rise to a single administrative fine, proportionate to the seriousness of all the breaches.

4.18. What other administrative measures can be taken?

4.18.1. Basic measures

The following administrative measures may be imposed on essential and important entities:

Art. 58 NIS2 law

1. issue warnings about breaches of the law by the entities concerned;
2. adopt binding instructions or an injunction requiring the entities concerned to remedy the shortcomings observed or the breaches of the law;
3. order the entities concerned to put an end to behaviour that violates the law and to not repeat it;
4. order the entities concerned to ensure the compliance of their cybersecurity risk-management measures or to comply with the incident reporting obligations set out, in a specific manner and within a specific timeframe;
5. order the entities concerned to inform the natural or legal persons to whom they provide services or carry out activities likely to be affected by a significant cyber threat, of the nature of the threat, as well as of any preventive or remedial measures that these natural or legal persons may take in response to this threat;
6. order the entities concerned to implement the recommendations made following a security audit within a reasonable period of time;
7. order the entities concerned to make public aspects of breaches of the law in a specific manner;

Where the entity concerned is an essential entity:

- the CCB may appoint, for a specified period, a control officer with clearly defined tasks to supervise compliance by the entities concerned with cybersecurity risk-management and incident reporting measures;
- the binding instructions referred to in point 2 also concern the measures necessary to prevent or remedy an incident, as well as the deadlines for implementing these measures and reporting on their implementation.

4.18.2. Additional measures

If the measures requested are not taken within the allowed deadline, the following administrative measures may be imposed on essential entities:

Art. 60 NIS2 law

1. temporarily suspend a certification or authorisation concerning all or part of the relevant services provided or relevant activities carried out by the entity concerned;
2. temporarily prohibit any natural person exercising managerial responsibilities at the level of managing director or legal representative in the entity concerned from exercising managerial responsibilities in that entity.

The temporary suspensions or prohibitions referred to in point 1 shall only be applied until the entity concerned has taken the necessary measures to remedy the deficiencies or to comply with the requirements of the competent authority which initiated the enforcement measures.

5. Other

5.1. Does the NIS2 directive give a mandate to the European Commission for an implementing act? Where can I find the act?

Art. 21, § 5 & 23, § 11 NIS2 directive

An Implementing Regulation has been adopted by the European Commission. It is called Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

This implementing regulation is available on Eur-Lex.

Indeed the NIS2 directive gives the power to the European Commission to adopt some implementing regulation in specific cases.

Article 21, § 5, (1) of the Directive concerns the **technical and methodological requirements relating to risk management measures** for DNS service providers, top-level domain name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking services platforms, and trust service providers.

Article 23, § 11 of the Directive deals with the **concept of a significant incident** for DNS service providers, top-level domain name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, online search engines and social networking services platforms.

The NIS2 Directive also envisages the (optional) possibility of other implementing regulations:

- an implementing regulation laying down technical and methodological requirements and sector-specific requirements for other types of essential and important entities (Art. 21, § 5, para. 2) ;
- an implementing regulation specifying in greater detail the type of information, format and procedure for notifications and communications relating to incident notifications (art. 23, § 11, para. 1) ;
- an implementing regulation detailing the concept of a significant incident for other types of essential and important entities (art. 23, § 11, para. 2, in fine);

However, there are currently no projects for those implementing regulations.

5.2. Is there a specific person within an organisation that is in charge of implementing the cybersecurity measures?

The NIS2 law does not require to appoint a specific person (like a DPO in the context of the GDPR) within the organisation in charge of implementing the NIS2 requirements.

5.3. Is there a public list of all important and essential entities?

The NIS2 directive requires Member States to set up a list of all important and essential entities to communicate statistical information about this list (number of entities by sector or sub-sector) to the NIS Cooperation Group and the European Commission.

Art. 3, § 3 - 6 NIS2 directive

However, this list is not publicly available.

6. Correlation table

FAQ version 1.0	FAQ version 2.0
1.1	1.1
	1.2
1.2	1.3
	1.4
1.3	1.5
	1.6
1.4	1.7
	1.8
1.5	1.9
1.6	1.10
1.7	1.11
1.8	1.12
	1.13
1.9	1.14
	1.15
	1.15.1
	1.15.2
	1.15.3
	1.15.4
	1.15.5
	1.16
	1.16.1
	1.16.2
	1.16.3
	1.16.4
	1.16.5
	1.16.6
	1.16.7
1.10	1.17
1.11	1.18
1.12	2.7
1.13	1.19
	1.20
1.14	1.21
1.14.1	1.21.1
	1.21.2
1.14.2	1.21.3
1.14.3	1.21.4
1.14.4	1.21.5
1.14.5	1.21.6
	1.22

	1.22.1
	1.22.2
	1.22.3
	1.22.4
	1.22.5
	1.22.6
	1.22.7
	1.22.8
	1.22.9
	1.22.10
	1.22.11
	1.22.12
2.1	2.1
	2.2
	2.2
2.2	2.4
2.3	2.5
	2.6
	2.7
	2.8
	2.9
3.1	3.1
3.2	3.2
3.3	3.3
3.3.1	3.3.1
	3.3.2
3.3.2	3.3.3
3.3.3	3.3.4
3.3.4	3.3.5
3.3.5	3.3.6
	3.4
3.4	3.5
3.5	3.6
	3.7
	3.8
	3.11
3.6	3.12
3.7	3.13
	3.13.1
	3.13.2
	3.13.3
	3.13.4
	3.13.5
	3.13.6
	3.13.7

	3.13.8
	3.13.9
	3.13.10
3.8	3.14
3.9	3.15
4.1	4.1
4.1.1	4.1.1
4.1.2	4.1.2
4.1.3	4.1.3
4.2	4.2
4.2.1	4.2.1
4.2.2	4.2.2
	4.3
4.3	4.4
	4.5
4.4	4.6
	4.7
4.5	4.8
4.6	4.9
	4.10
4.7	4.11
	4.12
4.8	4.13
4.9	4.14
4.10	4.15
	4.16
4.11	4.17
4.12	4.18
4.12.1	4.18.1
4.12.2	4.18.2
4.13	3.9
4.14	3.10
5.1	5.1
	5.2
	5.3