Version 1.0
07/2024

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.

Table of contents

Abbreviations & References

The following abbreviations and references are used in this document:

- BELAC: *Belgische Accreditatie-instelling* (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 SafonwebAtWork
- 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 9th 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 is the scope of the law NIS2?

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.

Art. 3 to 7 NIS2 law

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 be at least considered as 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.

Essential entities are those organisations which provide a service listed in annex I and which meet the definition 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 definition of a "medium-sized enterprise" within the meaning of Recommendation 2003/361/EC;
- listed in annex II and meet the definition of a medium-sized or large enterprise within the meaning of Recommendation 2003/361/EC;

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

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

For more information, see the following sections.

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

Art. 3, §§ 1 and 2 NIS2 law

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.

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

- employs between 50 and 249 people (employees, temporary or interim staff, owner-managers, partners, etc.) - workforce calculated in annual work units (AWU);
- has an annual turnover exceeding 10 million € up to 50 million € or 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 people or more (employees, temporary or interim staff, owner-managers, partners, etc.) - workforce calculated in annual work unit (AWU);
- 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.

See also section 1.14.2. and the detailed guide to size calculation for more information.

1.4. What sectors and services are covered by the 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:

Annexes I and II of the NIS2 law

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. To this end, the annexes are available on the website of the Belgian Official journal (after the text of the law).

See also section 1.14.3. for more details and the NIS2 scope test tool.

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

Art. 3, § 6 NIS2 law

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).

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.

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

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

Yes, it is possible for an entity to fall within several sectors. In this case, there are a number of considerations to take into account:

- 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, qualify as an essential entity;
- The entity will 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 a sector (other than the public administration sector) of the annexes of the law, is covered solely by that sector (and not simultaneously by that sector and the public administration sector).

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

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

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.

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 4.3.

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.).

1.8. How does the additional identification procedure work?

Art. 11 NIS2 law

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

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 particular 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 draft identification decision is communicated to the entity concerned and then to any federated entities concerned, as well as to the sectoral authorities, which issue an unpublished opinion within sixty days.

In the event of an unfavourable opinion from a sectoral authority and if the CCB wishes to maintain its draft decision, the draft decision, together with the opinion, is submitted to the Strategic Committee for Intelligence and Security (created by the royal decree of 22nd December 2020), which issues a binding opinion. On the basis of this opinion, the CCB will decide whether or not to proceed with the identification.

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.

1.9. What is the territorial scope of the law? What about entities operating in several countries (multinationals, etc.)?

Art. 4 NIS2 law

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

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"*.

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 or a subsidiary with legal personality.

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

1) Belgian law applies to providers of public electronic communications networks and providers of publicly available electronic communications services when they provide their service in Belgium;

2) The Belgian NIS2 law applies to 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, if they have their main establishment in Belgium or their legal representative for the EU in Belgium*;
3) The Belgian NIS2 law applies to public administration entities, which have been established by Belgium.

The concept of "main establishment" refers to the establishment where the decisions related to the cybersecurity risk-management measures are predominantly taken. If this cannot be determined or if such decisions are not taken in the Union, the main establishment shall be the establishment where the entity carries out cybersecurity operations. If this place can again not be determined, then the main establishment is where the entity has the highest number of employees in the Union.

(*) If an entity referred to in point 2) is not established in the EU but provides its services there, 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.

If an entity has several establishments in different EU Member States, it will be subject to the transposition laws in each of the Member States concerned. The various competent national authorities will work together regarding inspections and the notification of significant incidents.

1.10. 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 scope of NIS2 and DORA overlap for certain entities operating in the banking and financial sector. The NIS2 Directive therefore provides for a *lex specialis* rule: where equivalent sectoral requirements in terms of cybersecurity and notification of significant incidents exist at European level, the specific legal framework (in this case the DORA Regulation) applies rather than the general legal framework (in this case the NIS2 Directive).

However, entities in the banking and financial sector that fall within the scope of both the DORA Regulation and the NIS2 Directive must register in the same way as other NIS2 entities.

Finally, significant incidents notified by DORA entities will be forwarded to the NIS2 authorities.

1.11. 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 CER Directive) work together to supervise these entities.

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

1.12. Does an educational establishment fall into the scope of the law?

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

The education sector is not featured explicitly in annexes I and II of the NIS2 law.

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

- meet the size criterion (see section 1.3.);
- be established in Belgium (see section 1.9.);

- meet the definition of a public administration entity in article 8;
- Dependent on the federal state or federated entities

Furthermore, an educational establishment could also qualify as a "healthcare provider" within the meaning of annex I of the NIS2 law (for example, a university hospital).

1.13. Can NACE codes be used to determine whether an entity falls under the 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 whether the NIS2 law would not apply to them.

Annexes I and II of the NIS2 law

For all entities that do not fall into the above category, NACE codes are not a valid basis for determining whether an entity falls into the scope of the NIS2 law. Some NACE codes may be used preliminarily by entities, but further verification of their exact economic activity is required to determine whether or not they fall within the often more restrictive scope of the NIS2 law.

1.14. 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?
    b. Is my organisation an operator of essential services or a digital service provider (NIS1 law)?
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.

1.14.1. 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.

A. 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?

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 automatically qualified as essential entities.

B. Is my organisation an Operator of Essential Services (OSE) or a Digital Service Provider (DSP)?

Entities identified as operators of essential services or which were digital service providers under the law of 7th April 2019 establishing a framework for the security of networks and information systems of general interest for public security (NIS1 law) will be subject to the provisions of the NIS2 law. The scope of the NIS2 Directive is based on the sectors covered by the NIS1 Directive.

In the absence of formal identification by the CCB, OSEs must satisfy the size criterion (see next point). DSPs, on the other hand, were already required to be at least medium-sized under Recommendation 2003/361/EC.

1.14.2. 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 a company 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

[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.

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 €:
  - ➔ 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 1.3.).

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.

1.14.3. 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 1.6.).

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 1.14.2 above):

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

1.14.4. 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, whether this is the registered office, a simple branch or a subsidiary with legal personality.

However, depending on the type of entity concerned, there are certain exceptions to the Belgian establishment rule. The rules governing the territorial scope of the Belgian NIS2 law are explained in section 1.9.

1.14.5. 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 1.8.

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 cantherefore impose contractual obligations on their direct suppliers or service providers. For further explanation, see section 3.8.

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, 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.

As the definition in art. 8, 34° indicates, a public entity that primarily provides a service listed in another sector or sub-sector of one of the annexes to the law (for example, an intermunicipal company active in the energy or drinking water sector, a public hospital, a public body providing ICT services, etc.) is subject to the rules of that sector and not the public administration sector.

2.2. Are local public administrations subject to the obligations 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. 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 subject to the provisions of the NIS2 law when they provide a service listed in annex I or II of the law and are larger than a small enterprise.

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.

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

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

Regional and Community public administrations are among the public administrations covered by the NIS2 law. However, a formal identification procedure must first be carried out by the national cybersecurity authority (CCB). This involves assessing, 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.

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;
- training of management bodies (section 4.13.);
- 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.

It should be noted that the CCB's CyFun® framework is aligned with the work of the NIS Cooperation Group on this subject.

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.

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

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.

Notification takes place in several stages (see section 3.3.3): 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.

A significant incident is defined as: "*any incident has a significant impact on the provision of services in the sectors or subsectors listed in the annexes of the NIS2 law, and which:*

1. *has caused or is likely to cause serious disruption to the operation of any of the services in the sectors or subsectors listed in Annexes I and II or financial loss to the concerned entity; or*
2. *has caused, or is likely to cause, significant material, personal or non-material damage to other natural or legal persons*".

In practice, the CCB will provide recommendations on when notification is required and on the procedure to follow.

3.3.2. 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, 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 cyberthreat of any corrections and measures that they can apply in response.

Art. 34, §2 NIS2 law

3.3.3. 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, notification will take place via the procedure established on the CCB website.

3.3.4. 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.

3.3.5. 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. 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 DPA can be notified via their website.

3.5. Is it possible to voluntarily report incidents or cyberthreats?

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

Art. 38 NIS2 law

See the procedure explained in section 3.3.

3.6. 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.

3.7. 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.

3.8. How can an entity manage the relations with its supplies and direct service providers (supply chain)?

Entities covered by the NIS2 law must take appropriate and proportionate measures to secure their network and information systems.

Art. 30, §3, 4° NIS2 law

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.

Although the requirements of the NIS2 law apply only to NIS2 entities, they must nevertheless ensure that their suppliers and direct service providers implement similar measures. To ensure compliance with its legal obligations, an NIS2 entity may contractually require its suppliers or service providers to have one of the certifications recognised under the NIS2 law: CyFun® or ISO 27001.

3.9. How confidential is the exchanged information?

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.

Art. 26 NIS2 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.

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.

Art. 27 NIS2 law

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 4.5.

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 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 (4.3.).

4.2.1. The CyberFundamentals (CyFun®) Framework

The CyberFundamentals framework, developed by the CCB, is based on several commonly used cybersecurity frameworks or standards, including NIST CSF, ISO 27001 / ISO 27002, CIS Controls and IEC 62443.

It comprises the starting level Small and several assurance levels: Basic, Important and Essential (to provide the best possible response to the risks to which an organisation may be exposed). A tool allows to select the most appropriate level to apply.

The framework 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.

4.3. How will the concerned entities be audited?

Art. 39 ff. NIS2 law
Art. 6-13 NIS2 royal decree

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.

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) approved 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 27001 standard within the framework of the European co-operation for Accreditation (EA) or the International Accreditation Forum (IAF), and approved 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 4.10.

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

CABs play an important role in our economy in ensuring that companies meet the regulatory requirements imposed on them.

4.5. 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.

4.6. How can an entity prove that it is in compliance with its obligations?

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 standards mentioned in the royal decree: the CyberFundamentals or the international norm ISO 27001 (with the appropriate scope and statement of applicability). See section 4.2.

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.

4.7. Can an entity use a CyFun® level of assurance that is lower than the level assigned to its entity category?

Yes, 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

Art. 7 NIS2 royal decree

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.

4.8. 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 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 approved by the CCB.

4.9. When will the entities concerned have to apply the obligations of the law?

Art. 13 & 75 NIS2 law

Art. 22-23 NIS2 royal decree

The NIS2 law and royal decree will enter into force on 18th October 2024. As a result, and barring exceptions, **all the obligations** of the law and the royal decree **will apply** to essential and important entities (cybersecurity measures, incident reporting, etc.) **from that date**.

By way of derogation, the obligation to register will be phased in over time. The timeframe depends on the type of entity (see section 3.7.):

- In principle, entities have **5 months** to register after the law comes into force.
- For entities in certain information and communication technology sectors (cloud service providers, DNS service providers, data centres, etc.), the deadline for registration is **2 months** after the law comes into force.

By way of derogation, the regular conformity assessment of essential entities will also follow a gradual and differentiated implementation depending on the reference system chosen:

- **18 months after the law comes into force**, i.e. before 18th April 2026:
  - Those who determine that they must comply with the CyFun® Basic or Important assurance levels must have a verification carried out by an accredited CAB approved for CyFun®. Those who determine that they must comply with the CyFun® Essential assurance level must also have such a Basic or Important verification carried out;
  - Those who have opted for ISO 27701 certification must send the scope and statement of applicability to the CCB;

    - Those who have opted for inspection by the CCB must submit the CyFun® self-assessment or the information security policy, scope and ISO 27001 statement of applicability to the CCB.
- **30 months after the law comes into force**, i.e. before 18th April 2027:
    - Those who determine that they must comply with the CyFun® Essential assurance level must, in addition to the Basic or Important verification mentioned above, acquire a certification from an accredited and approved CAB for CyFun®;
    - Those who have chosen an ISO 27701 certification must obtain the certification from an accredited CAB approved for ISO 27001;
    - Those who have opted for inspection by the CCB must submit a progress report on 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.

4.10. 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 27001 or the CyberFundamentals (see section 4.3.).

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.

4.11. 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.

4.12. What other administrative measures can be taken?

4.12.1. Basic measures

Art. 58 NIS2 law

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

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.

4.12.2. 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.

4.13. What are management's obligations and responsibilities?

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.

Art. 31 & 61 NIS2 law

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.

4.14. What is a "management body"?

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

From the point of view of European law, the Court of Justice has recalled on several occasions: firstly, that if a word or concept is not defined in the legal instrument, its usual meaning must be retained; and secondly, unless otherwise indicated, that every concept in European law should have the same definition. Such a definition can be found in Directive 2013/36, in article 3 (7): "*an institution's body or bodies, which are appointed in accordance with national law, which are empowered to set the institution's strategy, objectives and overall direction, and which oversee and monitor management decision-making, and include the persons who effectively direct the business of the institution."*

The explanatory memorandum to the NIS2 Directive 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.

5. Other

5.1. Does the European Commission still need to adopt implementing acts?

Yes. An implementing act, which must be adopted by the European Commission by 17 October 2024 at the latest, covers a limited number of entities subject to the Directive for which certain arrangements are provided for at European level in a harmonised manner.

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.

These provisions also state that the Commission should follow, as far as possible, relevant European and international standards and technical specifications. The Commission must also exchange advice and cooperate with the Cooperation Group and ENISA on these draft implementing acts.

In practical terms, the future implementing act should relate exclusively to the following elements (the Commission has indicated its desire, if possible, to adopt both types of clarification in a single act):

- details of the technical and methodological requirements relating to risk management measures for these specific entities;
- details of the notion of significant incident for these specific entities, excluding trust service providers.

ENISA and the workstreams of the NIS Cooperation Group are currently working to provide advice to the Commission in preparation for the Comitology procedure.

On the basis of these exchanges, the Commission will formulate a proposal for an implementing act, which will then be shared and discussed within the NIS2 Committee (once it has been formally constituted). The Committee will have to follow the comitology rules set out in Regulation (EU) No 182/2011.