



CENTRE FOR
CYBERSECURITY
BELGIUM



● THE NIS2 DIRECTIVE IN BELGIUM

Introduction

The law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security (the « NIS2 law »), transposes EU directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 (the « NIS2 directive »).

In order to address the expanding cyber-threat landscape and the emergence of new challenges, the European Union has adopted new legislation on measures to ensure a common high level of cybersecurity across the Union (Directive 2022/2555 of 14 December 2022 – the so-called "NIS2 directive"), which replaces the "NIS1 directive" (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of network and information system security in the Union).

The NIS2 Directive introduces major changes compared to the NIS1 Directive: expansion of the sectors and entities concerned, new selection and registration methods, more cybersecurity requirements, new deadlines for reporting incidents and strengthened supervision mechanisms.

The directive also aims to strengthen the national cybersecurity strategy and national policies. The latter include the national cybersecurity crisis-management frameworks and processes, the tasks of the competent authorities and national as well as international cooperation.

As the national cybersecurity authority, the Centre for Cybersecurity Belgium (CCB) has a key role in coordinating and implementing this directive. The CCB assumes the tasks of competent authority for all sectors (in collaboration with the potential sectoral authorities). It also plays the role of national CSIRT, single national point of contact and representative within the NIS Cooperation Group, the CSIRT network and EU-CyCLONe.

Essential and important entities have to take appropriate and proportional measures to manage their cyber-risks. These include all organisational, but also technical, and operational measures with two objectives: prevent cyber-incidents and minimise the impact of successful incidents on the provision of their services.

To support organisations, the CCB developed clear guidance with the creation of the CyberFundamentals (CyFun®) framework. To this end, entities will benefit from a presumption of conformity if they obtain a CyFun® or ISO/IEC 27001 certification/label.

NIS2 entities shall notify their significant incidents to the national CSIRT. This allows to mitigate the potential spread of an incident and enables affected entities to request assistance. By receiving this information, the CCB can manage crisis situations in the best possible way and share relevant technical information with other entities.

Finally, the CCB also plays a role in supervising the concerned entities with its inspection service (in collaboration with the potential sectoral authorities). The primary purpose of the supervision is to strengthen entities' cyber-resilience, but it also allows sanctions to be imposed on entities that do not take the required measures.

The purpose of the present document is to provide general information on the scope and content of the transposition of the NIS2 directive¹ in Belgium.

¹ NIS2 Law: <https://www.ejustice.just.fgov.be/eli/loi/2024/04/26/2024202344/justel>

Royal Decree: <https://www.ejustice.just.fgov.be/eli/arrete/2024/06/09/2024005260/justel>

Table of contents

- Summary: NIS2 in 7 steps 4
- I. Why NIS2? And for Whom? 5
- II. Scope of application 6
 - A. The size (“size-cap”)..... 6
 - B. The service provided 8
 - C. Establishment..... 9
 - D. Identification and supply chain 9
 - E. Interplay between NIS2 and DORA 9
- III. Obligations 11
 - A. Registration 11
 - B. Cybersecurity risk-management measures 11
 - C. Supply chain security..... 12
 - D. Incident notification (see guide)..... 13
 - E. Obligations for management 15
- IV. Supervision..... 17
 - A. General regime..... 17
 - B. The CyberFundamentals (CyFun®) 18
- V. Sanctions 20
- VI. Timeline..... 21

Summary: NIS2 in 7 steps

It appears as if your organisation is concerned by NIS2, but you are unsure where to begin? The CCB has outlined the following recommendations to help you meet the requirements of the Belgian NIS2 legislation in just 7 steps.

1. Am I affected by NIS2?

- a. In scope: NIS2 entities: Use our scope test tool² to determine whether or not your organisation falls within the scope of the Belgian NIS2 law;
- b. In the supply chain: : The CCB recommends NIS2 entities to identify the organisations who are vital to their cybersecurity, and invite them to implement at least the CyberFundamentals Framework assurance level Basic.

2. Register your NIS2 entity

All NIS2 entities are required by law to register on Safeonweb@Work³:

- Entities in the digital sectors of the law must register before 18th December 2024 at the latest;
- All other NIS2 entities must register before 18th March 2025 at the latest.

3. Prepare your organisation to report and treat significant incidents as from 18/10/2024

Starting from the 18th October 2024, all NIS2 entities are required to notify the CCB about significant incidents (see guide).

Significant incidents can be notified to the CCB via its incident notification platform : <https://notif.safeonweb.be> (or by phone to +32 (0)2 501 05 60, but **only for emergencies for NIS2 entities or if the platform is unavailable**).

Incident notification is just one element of an incident response plan. If your organisation does not yet have an incident response plan, it might be useful to start from our policy template.

4. Determine your CyberFundamentals (CyFun®) level

If you're choosing our CyFun® Framework, our CyFun® selection tool allows you to determine the appropriate assurance level (Basic, Important or Essential) for your organisation.

5. Plan cybersecurity training

Board-level decisions on cybersecurity strategies and measures require basic knowledge of risk management and cybersecurity. The CCB recommends to plan management training before April 2025. In addition to management training, employee training should always be part of your cybersecurity measures.

6. Implement the security measures

NIS2 entities can use the CyFun® framework in 3 steps to comply with NIS2:

- 1) Perform a gap analysis using the CyFun® self-assessment tool;
- 2) Implement the required measures. Your implementation plan should gradually implement cybersecurity measures taking into account the review deadlines as indicated in step 7 below;
- 3) Update your self-assessment and gather required evidence to confirm implementation.

7. Have your cybersecurity reviewed

Essential entities must have their implementation regularly assessed and reviewed by a third party. This can be done through a CyFun® certification granted by an accredited and authorised conformity assessment body (CAB). Essential entities must obtain the Basic or Important assurance level before 18th April 2026, the final level needs to be certified before 18th April 2027.

² <https://atwork.safeonweb.be/nis2>

³ <https://atwork.safeonweb.be/register-my-organisation>

Important entities may subject themselves to the same regular conformity assessment under CyFun®, which gives them a presumption of conformity.

Please be aware that having the appropriate CyFun® label or certificate might be very important for the boards and management to be able to demonstrate compliance in case of an incident.


I. Why NIS2? And for Whom?

Networks and information systems have become a central part of our daily lives as a result of the digital transformation and interconnection of society; many critical societal and economic activities now depend on their smooth operation.

This development has led to an ever-expanding landscape of cyber-threats and cyber-incidents. These represent real threats to security for the general public, businesses and public authorities. These days, a cyber-incident is likely to cause serious operational disruption in critical sectors, affecting individuals or companies and causing considerable material, physical or moral damage.

All citizens, businesses and public authorities must therefore be aware of the importance of protecting themselves preventively against cyber-threats and cyber-incidents.

The following infographic provides an introductory overview of the NIS2 law:



NIS 2: FOR WHOM ? WHY ?

WHAT?
The directive n°2022/2555 ("NIS 2") is a revision of the directive n°2016/1148 ("NIS 1") (Network and Information Security). It is an EU legislation on the subject of cybersecurity.

WHICH OBLIGATIONS?


1. Register at the CCB (Safeonweb@work)
2. Take appropriate cybersecurity management measures.
3. Notify the CCB about significant cybersecurity incidents.
4. Carry out regular conformity assessments, verified by a conformity assessment body (essential entities).




WHY?
NIS 2 aims to establish a high and common level of cybersecurity in the EU by setting requirements regarding cybersecurity risk management measures and reporting obligations for organisations operating in different critical sectors.

FOR WHOM?
The (essential and important) entities which are established in Belgium and provide services in the sectors mentioned in annexes I and II.


Annex I: sectors of high criticality



Energy



Transport


DORA



Financial market institutions



Banking



Health



Drinking water


Waste water


Digital infrastructure



ICT service management


Public administration



Space

Annex II: other critical sectors



Postal and courier services



Manufacture, production and distribution of chemicals


Waste management


Manufacturing


Digital providers


Research


Production, processing and distribution of food

II. Scope of application

To be covered by the Belgian NIS2 law, an organisation must (with some exceptions) in principle:

1. Provide in the European Union a service listed in annexes I and II of the NIS2 law;
2. 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; and
3. Be established in Belgium.

A. THE SIZE (“SIZE-CAP”)

The size of an entity is calculated on the basis of Annex I of Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (the "Recommendation").

The size of an organisation is established using two criteria: staff headcount/workforce (measured in full-time equivalents (FTE)⁴) and financial amounts (annual turnover and/or annual balance sheet total). With some exceptions⁵, an organisation must be considered as at least a medium-sized enterprise within the meaning of the Recommendation in order for the NIS2 law to apply. A medium-sized enterprise has a workforce of at least 50 FTE or an annual turnover and/or annual balance sheet total exceeding 10 million euros.

How exactly these two criteria are established can be found in the annex of the Recommendation itself or in the Commission’s “User guide to the SME definition”⁶. However, it is important to mention that an enterprise may choose to meet either the turnover or the balance sheet total ceiling. It may indeed exceed one of the financial ceilings without impact on its SME status. Thus, we only look at the lowest of the two amounts.

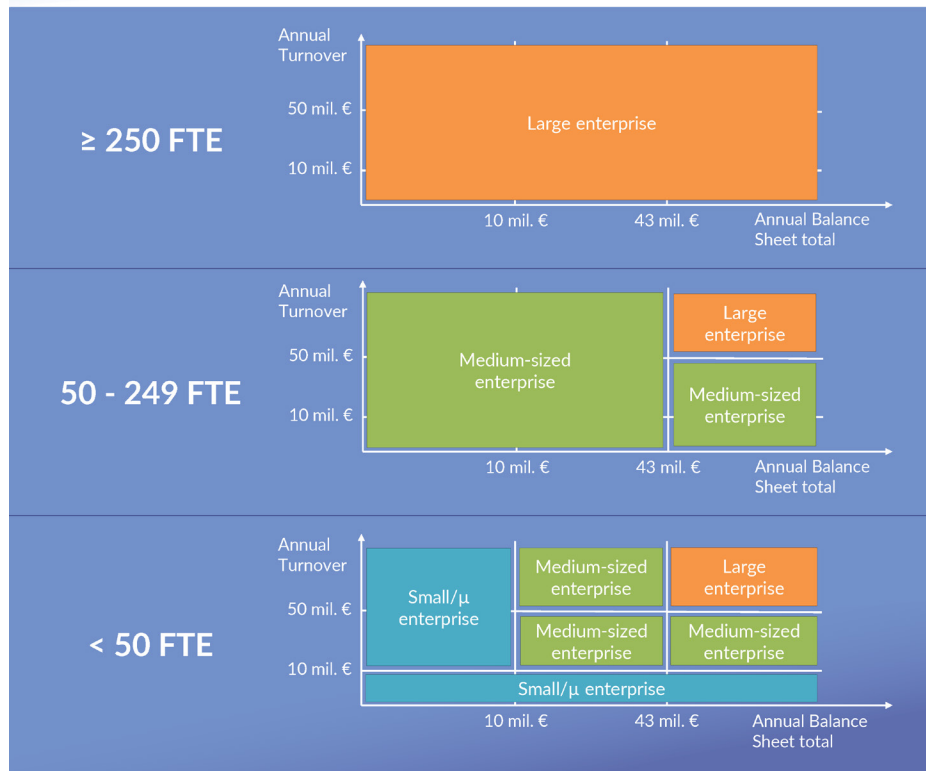
The diagram on the following page provides a visual representation of the different enterprise sizes.

⁴ Full-time equivalents (FTE) (called “annual work units (AWU)” in the Recommendation) are 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. The Recommendation and the guide further detail which staff members have to be counted.

⁵ See p. 7-8.

⁶ <https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1>

Enterprise sizes under Recommendation 2003/361/EC



The Recommendation also specifically stipulates that the calculation of the size of an organisation which is part of a group (“partner” or “linked” enterprises) implies a consolidation of the data of the different components of this group. For more information we invite you to consult the previously mentioned Commission’s User guide or its online “SME Wizard” tool⁷.

However, there are two important specificities regarding the application of the Recommendation in the context of the NIS2 law:

- 1) The consolidation of data from the various components within a group may be waived, in certain circumstances, where the network and information systems of the organisation concerned are independent of those of linked or partner enterprises;
- 2) The number of workers and the financial figures of a public body that controls a concerned organisation should not be taken into account when determining the size of the latter.

If we combine the different possible sizes with the service criterion, we get the following scope of application (with some exceptions⁸):

	Medium-sized enterprise	Large enterprise
Services from Annex I	Important NIS2 entity	Essential NIS2 entity
Services from Annex II	Important NIS2 entity	Important NIS2 entity

⁷ <https://ec.europa.eu/growth/tools-databases/SME-Wizard/>

⁸ See list below the table.

There are nevertheless a number of exceptions to the size-cap. Certain types of entities fall within the scope of application of the NIS2 law, regardless of their size:

- Qualified trust service providers (Essential);
- Non-qualified trust service providers (Important if micro, small or medium enterprise and Essential if large enterprise);
- 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 1st July 2011 on the security and protection of critical infrastructure (Essential);
- Public administration entities depending on the federal state (Essential).

Independently of these rules, the national cybersecurity authority (the CCB) is also able to identify specific entities as "essential" or "important", for example where they are the sole provider of a service or where the disruption of the service provided could have a significant impact on public security, public safety, or public health.

B. THE SERVICE PROVIDED

The service condition requires an organisation to fully analyse every single one of its services provided to third parties, by sector and sub-sector. This is important given that even the most ancillary service provided may make an organisation as a whole fall within the scope of the NIS2 law, except when stated otherwise in the definition of said service. All services falling under the NIS2 law are detailed in Annexes I and II (or in the definitions⁹) of the law and grouped together by sectors:

Highly critical sectors (Annex I)	Other critical sectors (Annex II)
<ol style="list-style-type: none"> 1. Energy <ol style="list-style-type: none"> a. Electricity b. District heating and cooling c. Oil d. Gas e. Hydrogen 2. Transport <ol style="list-style-type: none"> a. Air b. Rail c. Water d. Road 3. Banking 4. Financial market infrastructure 5. Health 6. Drinking water 7. Waste water 8. Digital infrastructure 9. ICT service management (B2B) 10. Public administration 11. Space 	<ol style="list-style-type: none"> 1. Postal and courier services 2. Waste management 3. Manufacture, production and distribution of chemicals 4. Production, processing and distribution of food 5. Manufacturing <ol style="list-style-type: none"> 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

It is of very high importance to **consult the definitions of these services** to verify whether or not they correspond to the actual service provided by an organisation.

For a better overview of the scope of the law, we invite you to consult our visual summary of the scope on pages 23 and 24.

⁹ See article 8 of the NIS2 law.

C. ESTABLISHMENT

In principle, the Belgian NIS2 law only 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, there are three exceptions to the rule of establishment in Belgium:

- 1) The Belgian NIS2 law applies to providers of public electronic communications networks or providers of publicly available electronic communications services, which provide their services 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 market-places, online search engines or 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.

Apart from the exceptions, 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.

D. IDENTIFICATION AND SUPPLY CHAIN

It is possible that after a thorough analysis of the scope of application of the NIS2 law, certain organisations realise that they do not, in fact, fall under said law. All non-NIS2 organisations should be aware that the NIS2 law can still affect them in two ways.

First, the national cybersecurity authority (the CCB) can identify certain organisations, regardless of their size, as essential or important entities under the NIS2 law in four circumstances relating to the critical character of the organisation. This process unfolds in concertation with the concerned entity and other authorities, and is set out in article 11 of the NIS2 law.

Second, an organisation may fall into the direct supply chain of a NIS2 entity and be faced with the obligation to implement cybersecurity risk-management measures because, for example, of a contractual requirement from the NIS2 entity. In this context, the CCB advises all organisations that may find themselves in the supply chain of a NIS2 entity to at least comply with the measures set out in the CyberFundamentals (CyFun®) Framework level Basic¹⁰.

E. INTERPLAY BETWEEN NIS2 AND DORA

The NIS2 law foresees that titles 3 to 5 of the law (cybersecurity risk-management measures, supervision and sanctions, specific provisions for the public administration sectors) **do not apply to entities in the banking and financial market sectors that fall within the scope of application of DORA**. The latter is the abbreviation for EU Regulation 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, which sets out requirements for the security of network and information systems of the financial entities within its scope.

This comes from the NIS2 directive, namely from the exclusion of sector-specific Union legal acts (so-called *lex specialis*), where such acts require NIS2 entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in NIS2.

In practice, all NIS2 entities covered by DORA can limit themselves to following DORA with respect to the obligations contained in titles 3 to 5 of the NIS2 law. This includes the cybersecurity risk-management measures, mandatory and voluntary notification of incidents, supervision, administrative measures, and fines. However, all other

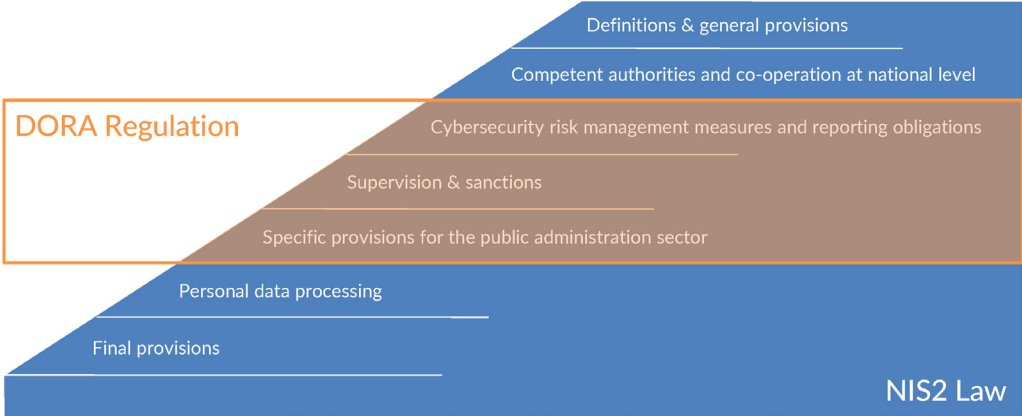
¹⁰ <https://cyfun.be>

provisions from the NIS2 law, such as those relating to registration and the competence of the CCB, still apply to these entities.



INTERPLAY NIS2 – DORA (LEX SPECIALIS)

NIS2 Entities from banking and financial sectors falling also under the Digital Operation Resilience Act (DORA) do not have to apply titles 3-5 of the NIS2 law



III. Obligations

A. REGISTRATION

NIS2 entities falling within the scope of the Belgian NIS2 law must register their organisation at the CCB. In practice, this registration is made by means of an online form to be completed on [Safeonweb@Work](https://atwork.safeonweb.be/register-my-organisation)¹¹.

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** from the entry into force of the law to register, meaning by **18th March 2025** at the latest¹².

There is a slightly adapted regime for the following types of entities from the digital sectors:

- 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.

These entities must register with different information within **2 months** of the law entering into force, i.e. by **18th December 2024** at the latest¹³.

Every entity is required to inform the CCB immediately (at the latest after 2 weeks) of any changes to their relevant information.

B. CYBERSECURITY RISK-MANAGEMENT MEASURES

The cybersecurity risk-management measures are technical, operational or organisational measures that allow the concerned entity to manage the risks relating to the security of their network and information systems, and to prevent or minimise the impact of cyberincidents. The measure shall be adopted by taking into account the “state-of-the-art”, existing norms, and their costs.

For each entity, cybersecurity risk-management measures must be appropriate and proportionate to the risks faced, the degree of the entity’s exposure to risks, its size, the likelihood of incidents and their severity.

The NIS2 law lists 11 minimum measures that entities must implement¹⁴. An overview is available in the diagram on the following page.

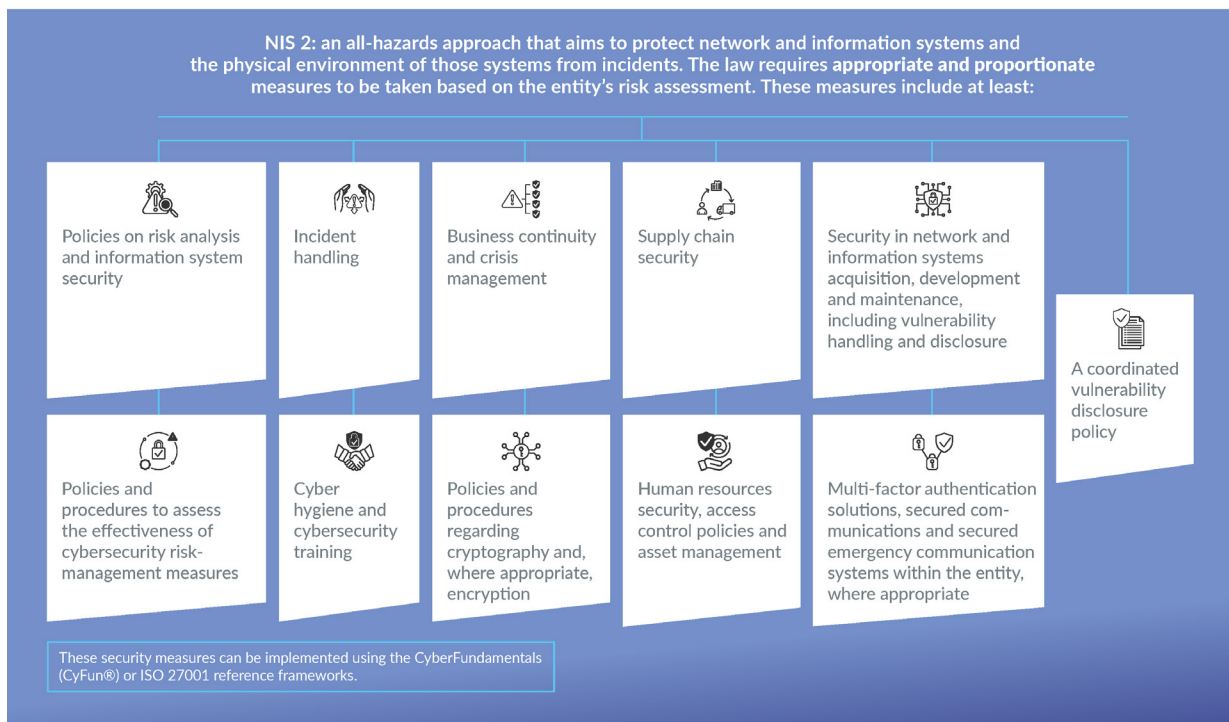
¹¹ <https://atwork.safeonweb.be/register-my-organisation>

¹² The information to be provided under the default registration deadline can be found in article 13, §1 of the NIS2 law.

¹³ The information to be provided under the adapted regime can be found in article 14, §1 of the NIS2 law.

¹⁴ See also the Commission implementing act: <https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks>

THE CYBERSECURITY MEASURES TO BE IMPLEMENTED



The CCB has created a free and public framework called the “CyberFundamentals” (CyFun®) which covers each of these points and with which NIS2 entities can comply with the obligation of taking appropriate and proportionate cybersecurity risk-management measures¹⁵.

C. SUPPLY CHAIN SECURITY

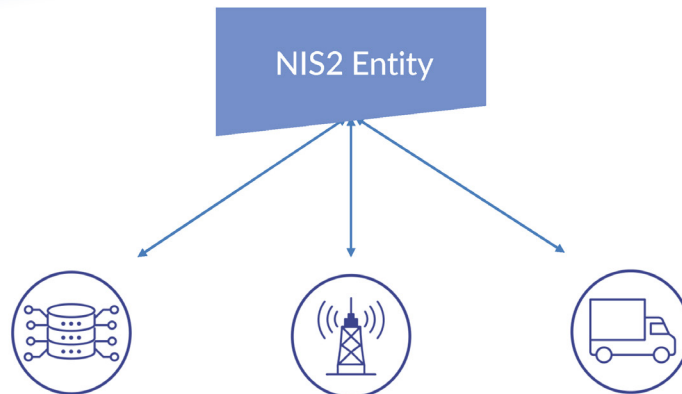
The NIS2 law requires all entities within its scope of application to take appropriate and proportionate cybersecurity risk-management measures. One of these specific measures is “**supply chain security**, including security-related aspects concerning the relationships between each entity and its direct 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 the 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 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.

¹⁵ For more information, see Chapter IV, Section B.



To mitigate the supply chain risk, NIS2 entities should define appropriate security measures for their suppliers based on a risk analysis. Both suppliers of products and suppliers of services are concerned.

These requirements are typically included in the contractual agreement with the supplier.

A way to do so, is by requesting the appropriate CyFun® label from a supplier



D. INCIDENT NOTIFICATION (SEE GUIDE)

The NIS2 law also 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:

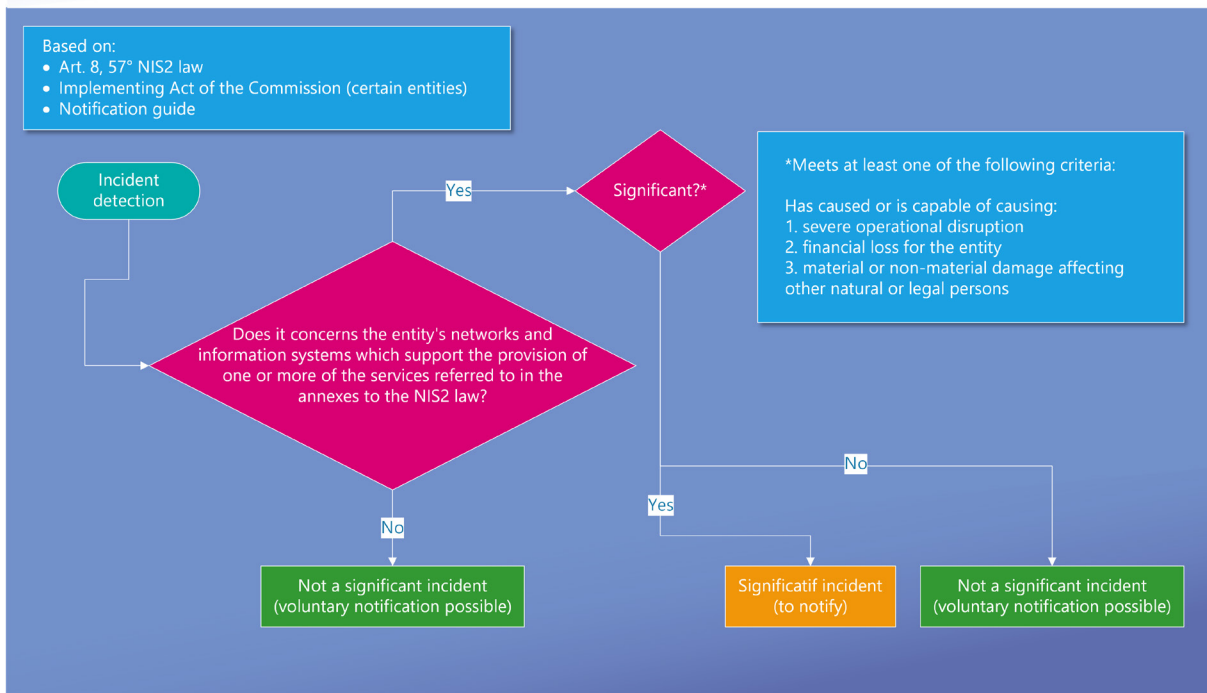
- 1° has caused or is likely to cause severe operational disruption to any of the services provided in the sectors or sub-sectors listed in Annex I and II or financial loss to the entity concerned; or
- 2° has affected or is capable of affecting other natural or legal persons by causing considerable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

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.**



As soon as a NIS2 entity encounters such an incident, it must notify the CCB. This notification takes place in several stages (see also the visual below):

- 1) **without undue delay and in any event within 24 hours** of becoming aware of the significant incident, the entity submits an early warning;
- 2) **without undue delay and in any event within 72 hours (24h for trust service providers) of becoming aware of the significant incident**, the entity submits an incident notification;
- 3) upon the request of the national CSIRT or, where applicable, the competent sectoral authority, the entity submits an intermediate report;
- 4) **not later than one month after the submission of the incident notification under point 2**, the entity submits a final report;
- 5) in the event of an ongoing incident at the time of the submission of the final report, the entity concerned submits a progress report and then, one month after the incident is finished, a final report.

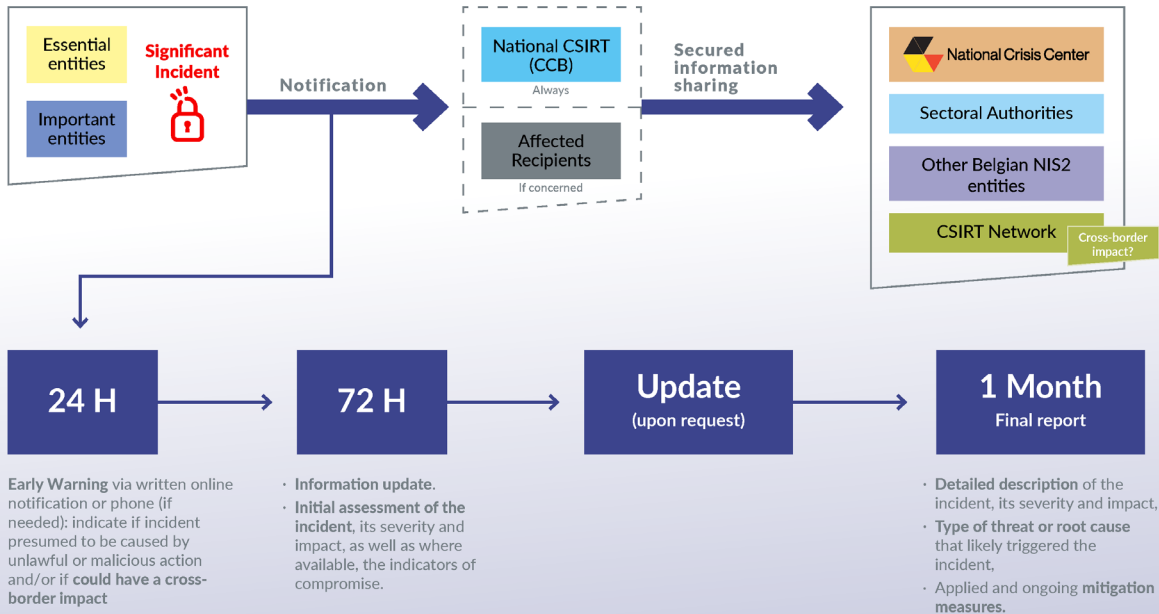
Depending on the extent of the incident, the entity must also inform the recipients of its service of the existence of the incident and of the measures and corrections that the recipients can take to respond to it. The CCB may share the information received by the entity with other authorities within the limits of what is necessary.

Further information about incident notification is available in our **NIS2 Incident Notification Guide**¹⁶.

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

¹⁶ <https://ccb.belgium.be/en/cert/report-incident>

See also the Commission implementing act: <https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks>



E. OBLIGATIONS FOR MANAGEMENT

The NIS2 law foresees several specific elements applicable to management bodies of NIS2 entities:

- 1) Management bodies have to approve cybersecurity risk-management measures and supervise their execution;
- 2) Members of management bodies have to follow training to ensure that their knowledge and skills are sufficient to identify risks and assess cybersecurity risk-management measures and their impact on the services provided by the entity;
- 3) Management bodies are liable for decisions taken in relation to cybersecurity risk-management measures, including incident management;

The objective of these measures is to ensure that cybersecurity becomes a subject of importance for management.

The explanatory memorandum of the NIS2 law explains that "member of a management body" means:

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.

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.



ACCOUNTABILITY OF MANAGEMENT BODIES

Under NIS2, management bodies:

Are liable for infringements by their entity

Oversee the implementation of cybersecurity risk-management measures



Follow training & encourage their employees to follow similar training

Approve cybersecurity risk-management measures

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

IV. Supervision

A. GENERAL REGIME

When it comes to supervision, the law makes a difference between important and essential entities:

- Important entities are supervised in an “*ex-post*” manner, meaning that an inspection will only take place after an incident has happened or when the supervisory authority has enough elements at its disposal to suspect that an important entity has violated the law;
- Essential entities can be supervised in an “*ex-post*” but also in an “*ex-ante*” manner, meaning that they must, at any moment be able to prove that they are respecting the law. To this effect, the law subjects essential entities to a mandatory regular conformity assessment.

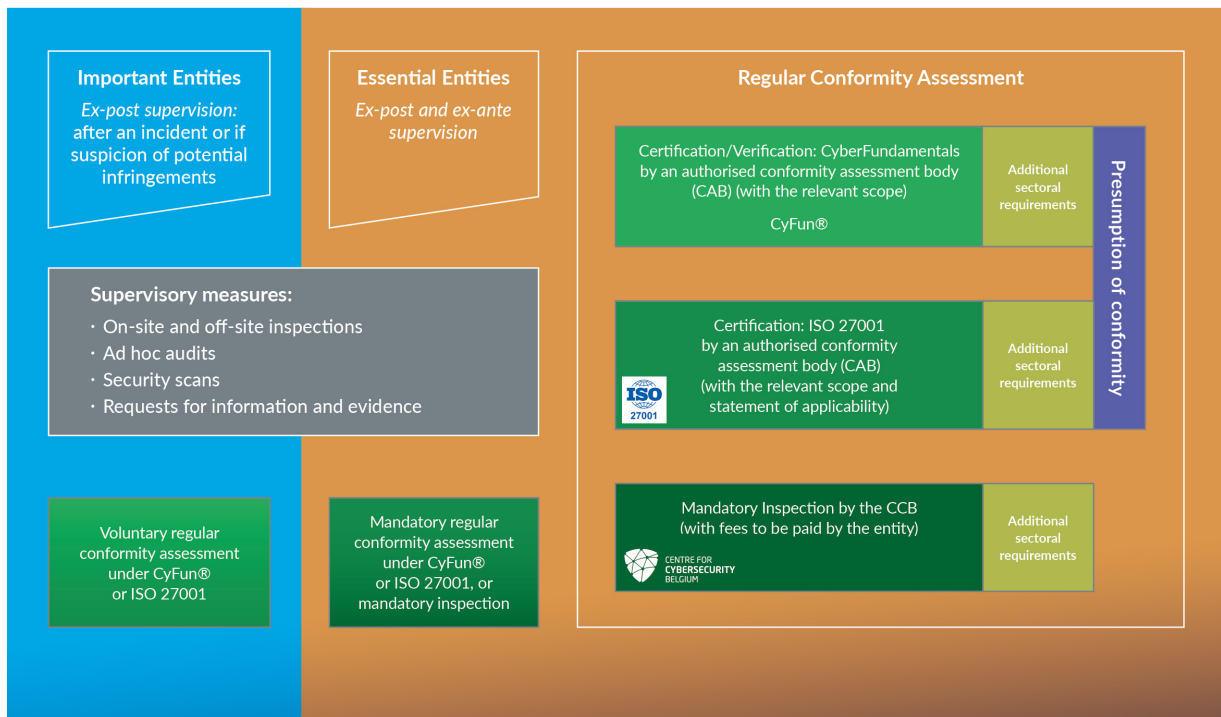
Such a mandatory regular conformity assessment can be accomplished in three different ways:

- 1) A certification (level essential) or verification (level important or basic) of the entity under the **CyberFundamentals (CyFun®) Framework** by a conformity assessment body (CAB) accredited by BELAC and authorised by the CCB, with the relevant scope of application;
- 2) A certification of the entity under the **ISO/IEC 27001 norm** granted by an accredited CAB with the relevant scope of application and statement of applicability. For ISO/IEC 27001, the CAB must be accredited by an accreditation body that has signed the Multi-Lateral Agreement (MLA) under which ISO 27001 falls in the framework of the European co-operation for Accreditation (EA) or the International Accreditation Forum (IAF), and it must be moreover authorised by the CCB;
- 3) An **inspection** by the inspection service of the CCB (a fee is asked for this service).

For all these three possibilities, a sectoral authority may add additional requirements to be respected by the entities within its sector. Moreover, entities choosing to perform their regular conformity assessment through CyFun® or ISO 27001 may benefit from a presumption of conformity.

During its supervision, the inspection service may use on-site inspections, off-site supervision, ad hoc audits, but also security scans and general requests for information and evidence. All NIS2 entities must at all times comply with the requests made by the inspection service. If they do not comply, they risk administrative measures and fines.

Important entities may also voluntarily subject themselves to a regular conformity assessment. In this case, they can only choose between CyFun® and ISO 27001.



B. THE CYBERFUNDAMENTALS (CYFUN®)

The CyberFundamentals (CyFun®) Framework¹⁷ 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.


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 approved conformity assessment body. 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

¹⁷ <https://cyfun.be>





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.

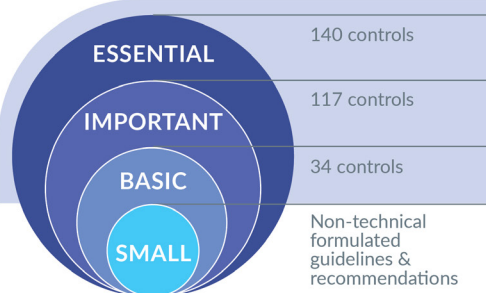


THE CYBERFUNDAMENTALS CyFun® FRAMEWORK

CYBERFUNDAMENTALS (CyFun®) FRAMEWORK

Based on various frameworks and standards



ESSENTIAL → 140 controls

IMPORTANT → 117 controls

BASIC → 34 controls

SMALL

Non-technical formulated guidelines & recommendations

ESSENTIAL → 100% Attacks countered ✓✓


IMPORTANT → 94% Attacks countered ✓✓✓

BASIC → 82% Attacks countered ✓✓✓


Figures result from validation of the framework using CERT attack profiles (obtained from successful attacks)

→ Can be used for conformity assessment according to the NIS2-law

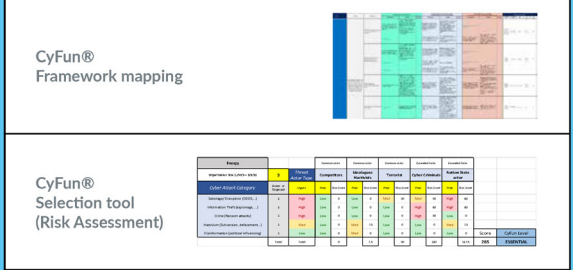
→ Implementation verified/certified by an accredited and authorised conformity assessment body = Presumption of conformity



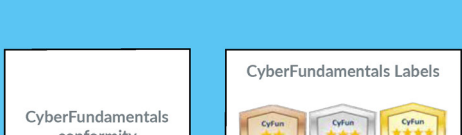
THE CYBERFUNDAMENTALS ECOSYSTEM



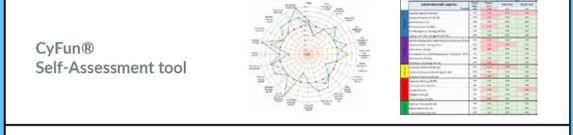
CyFun® Framework mapping



CyFun® Selection tool (Risk Assessment)




CyFun® Self-Assessment tool



CyFun® BASIC Policy templates

CyberFundamentals conformity assessment bodies (CABs)

CyberFundamentals Labels



CyberFundamentals Toolbox is publicly available → www.cyfun.be

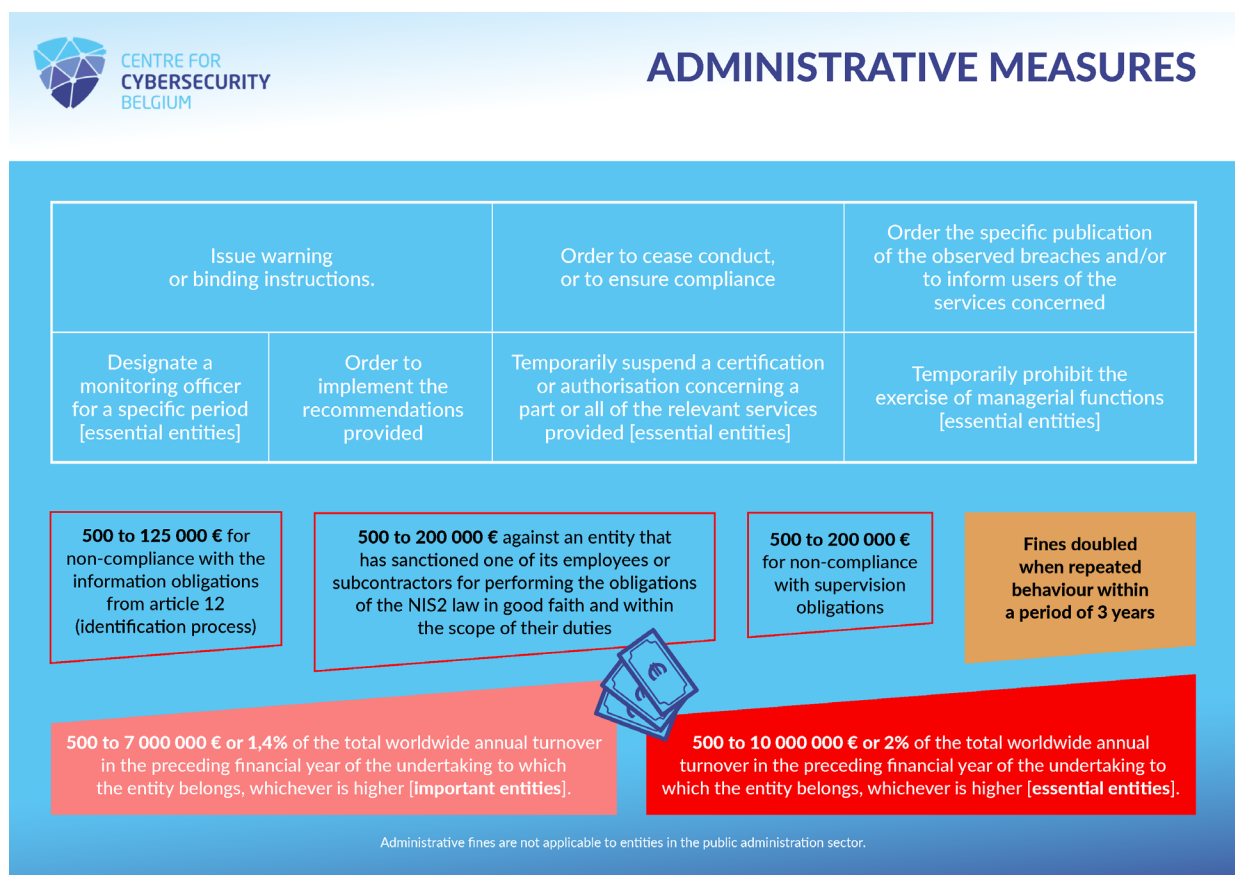
V. Sanctions

NIS2 entities which do not respect their obligations can be subjected to a series of administrative measures and fines.

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.

The list of possible administrative measures and fines can be found in the infographic below:



VI. Timeline

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.

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.

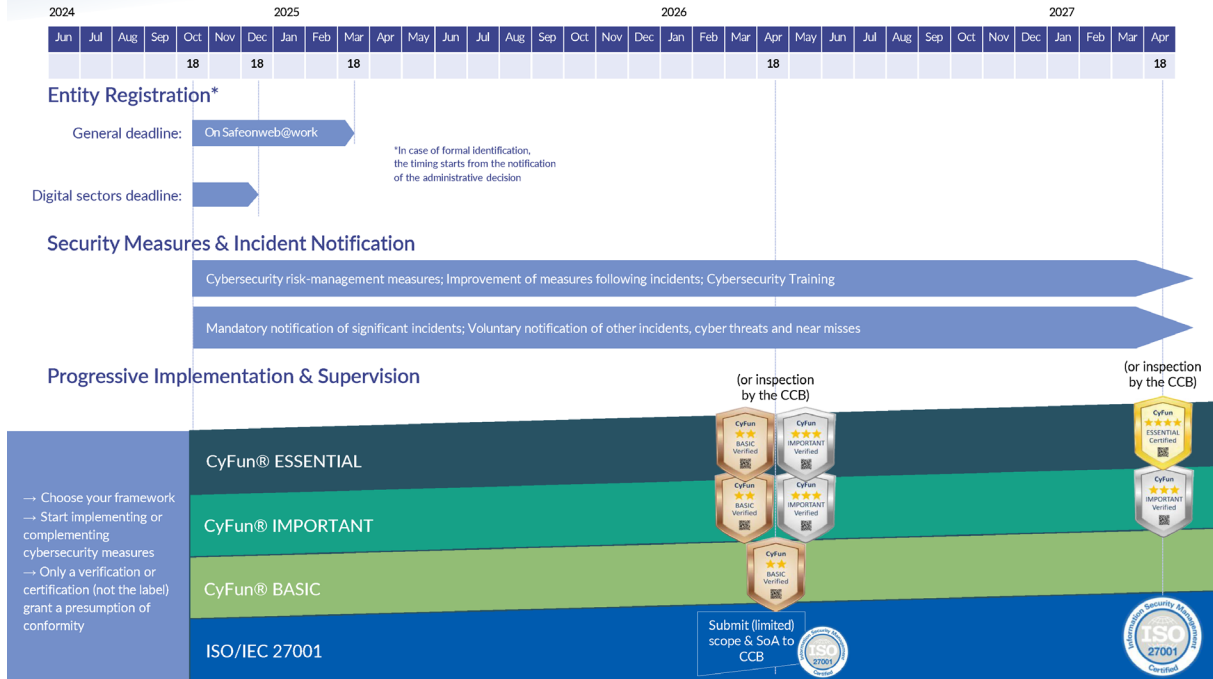
Concerning the registration of entities at the CCB via Safeonweb@Work, the law provides the following deadlines:

- 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 to 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**).

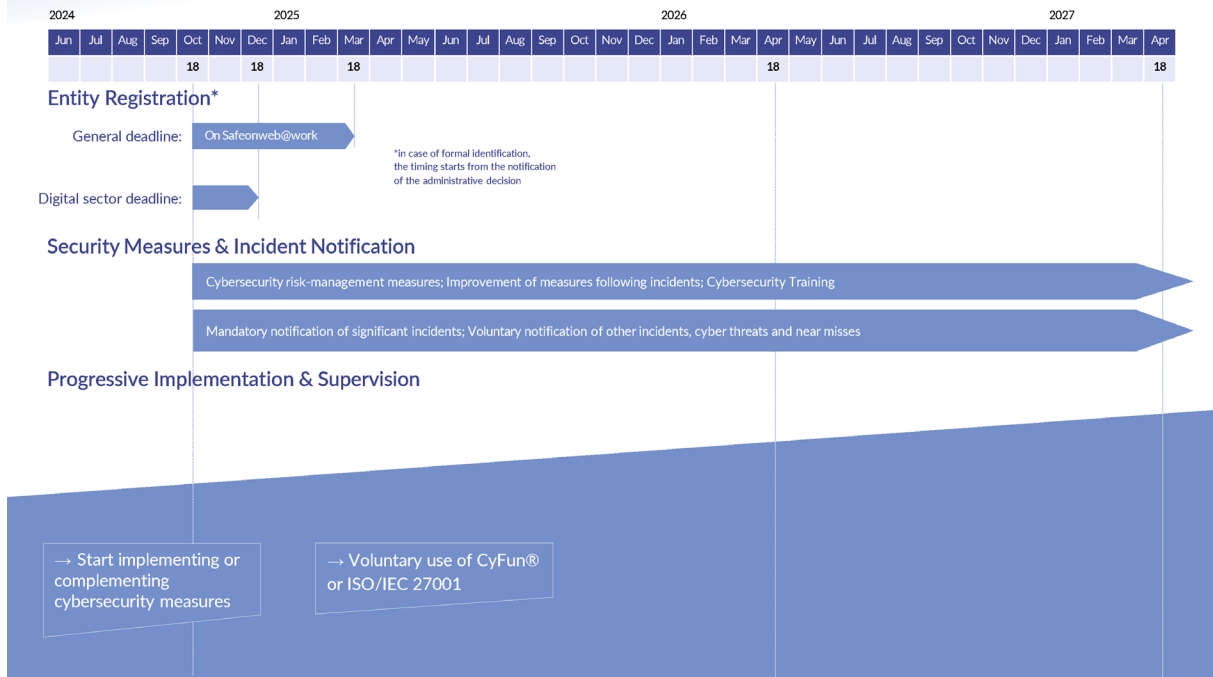
The supervision/regular conformity assessment of essential entities also takes a gradual approach:

- 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 they 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 which they 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 27001 information security policy, scope and statement of applicability to the CCB;
 - **By 18th April 2027 at the latest**: Report on progress towards compliance.

IMPLEMENTATION TIMELINE ESSENTIAL ENTITIES



IMPLEMENTATION TIMELINE IMPORTANT ENTITIES



ANNEX I: SECTORS OF HIGH CRITICALITY

SECTOR	SUB-SECTOR and/or ENTITY TYPE	LARGE ENTERPRISES Staff: > 250 FTEs; or > € 50m annual turnover and or > € 43m annual balance sheet total	MEDIUM ENTERPRISES Staff: > 50 FTEs; or > € 10m annual turnover and or > € 5m annual balance sheet total	SMALL & MICRO ENTERPRISES
1. Energy	Electricity	Electricity undertakings; Distribution system operators; Transmission system operators; Producers; Nominated electricity market operators; Market participants; Operators of a recharging point		
	District heating & cooling	Operators of district heating or district cooling		
	Oil	Operators of oil transmission pipelines; Operators of oil production, refining and treatment facilities, storage and transmission; Central stockholding entities		
	Gas	Supply undertakings; Distribution system operators; Transmission system operators; Storage system operators; LNG system operators; Natural gas undertakings; Operators of natural gas refining and treatment facilities		
	Hydrogen	Operators of hydrogen production, storage and transmission		
2. Transport	Air	Air carriers used for commercial purposes; Airport managing bodies, airports, and entities operating ancillary installations contained within airports; Traffic management control operators providing air traffic control (ATC) services		
	Rail	Infrastructure managers; Railway undertakings		
	Water	Inland, sea and coastal passenger and freight water transport companies; Managing bodies of ports and entities operating works and equipment contained within ports; Operators of vessel traffic services (VTS)		
3. Banking	Road	Road authorities responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity; Operators of Intelligent Transport Systems	Essential	Only if identified*
	Credit institutions [DORA Lex specialis]			
4. Financial Market Infrastructure	Operators of trading venues; Central counterparties [DORA Lex specialis]			
5. Health	Healthcare providers; EU reference laboratories; research and development activities of medicinal products; manufacturing of basic pharmaceutical products and pharmaceutical preparations; manufacturing of medical devices considered to be critical during public health emergency			
6. Drinking Water	Suppliers and distributors of water intended for human consumption, <u>only</u> if essential part of their general activity			
7. Waste Water	Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water, <u>only</u> if essential part of their general activity			
8. Digital Infrastructure	Qualified trust service providers			
	DNS service providers [excluding root name servers]			
	TLD name registries			
	Providers of public electronic communication networks or electronic communication services available to the public		Essential	Essential
	Non-qualified trust service providers			Important*
	Internet Exchange Point providers			
	Cloud computing service providers		Essential	Important*
	Data centre service providers			
	Content delivery network providers			
	Managed (Security) Service Providers			
9. ICT-service management	Public administrations depending on the federal State		Essential	
	Public administrations depending on the federated entities (only after identification following a risk-based assessment of the criticality of the services provided)			
	Emergency zones (including the Firefighting and emergency medical assistance service of the Brussels Capital Region)		Important*	
10. Public Administration (excluding judiciary, banks; national security, public security, defence or law enforcement)	Operators of ground-based infrastructure that support the provision of space-based services, excluding providers of public electronic communications networks		Essential	Only if identified*
11. Space				

(*) The CCB may, where appropriate, depending on the criticality of the services provided and the risks incurred, identify certain important entities as essential or identify other categories of entity types as important or essential within a sector.

The definitions of these entity types can be found in annexes I and II in Article 8 of the NIS2 law.

ANNEX II: OTHER CRITICAL SECTORS

SECTOR	SUB-SECTOR and/or ENTITY TYPE	LARGE ENTERPRISES staff headcount of at least 250 FTEs, or > € 50m annual turnover and € 43m annual balance sheet total	MEDIUM ENTERPRISES staff headcount of at least 50 FTEs, or > € 10m annual turnover / annual balance sheet total	SMALL & MICRO ENTERPRISES
1. Postal and courier services	Postal service providers, including providers of courier services	Important*		Only if identified*
	2. Waste Management			
3. Chemicals	Manufacture of substances and distribution of substances or mixtures; Production of articles from substances or mixtures			
4. Food	Wholesale distribution and industrial production and processing			
5. Manufacturing	(In vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery and equipment n.e.c.; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)			
	6. Digital providers			
7. Research	Research organisations, excluding education institutions			

(*) The CCB may, where appropriate, depending on the criticality of the services provided and the risks incurred, identify certain important entities as essential or identify other categories of entity types as important or essential within a sector.

Note: Entities providing domain name registration services also fall under NIS2, but they only have to register on Safeonweb@Work as well as create and maintain an accurate and complete database of domain name registration data.

THE NIS2 DIRECTIVE IN BELGIUM

This document was written by the Centre for Cybersecurity Belgium (CCB). This federal administration was created by the Royal Decree of 10 October 2014 and is under the authority of the Prime Minister.

All texts, layout, designs, and other elements of any kind contained in this document are subject to copyright laws. Extracts from this document may only be reproduced for non-commercial purposes and if the source is mentioned.

The CCB disclaims any liability in connection with the content of this document.

The information provided:

- is purely general in nature and does not aim to cover all specific situations;
- is not necessarily complete, accurate or up to date in all respects.

Responsible publisher:

Centre for Cybersecurity Belgium

M. De Bruycker, Managing Director

Wetstraat 18

1000 Brussels

Legal deposit:

D/2024/14828/009

