How to comply with the Belgian NIS2 law ?

Patrick Soenen, Partner, Qualified Audit Academy

NIS2 Directive

On the 16 January 2023, the EU Parliament and Council adopted the ***2022/2555 Directive***[1] on measures for a high common level of cybersecurity across the Union. On 26 April 2024, the Directive was transposed in ***Belgian Law***[2] and will enter into force on 18 October 2024.

This new Directive aims to extend the scope of obligations on entities required to take measures to increase their cybersecurity capabilities. The Directive also aims to harmonise the EU approach to incident notifications, security requirements, supervisory measures and information sharing.

NIS2 in brief

The NIS2 Directive aims to strengthen cyber resilience at European level by focusing on the following key objectives:

- Expansion of the number of critical services and entities falling within the scope of the directive through the use of definitions and a size cap criterion;
- Reinforcement of the cybersecurity risk management measures that entities must take and the notification of significant incidents;
- Encourage the sharing of information on cyber security incidents and risks between entities and the national CSIRT (Computer Security Incident Response Team), i.e. www.cert.be in Belgium;
- Strengthening compliance monitoring and sanctions;
- Ensure European and national cooperation.

Scope of application

An organisation must be

- Provide a service in a sector that is either “essential” or “important”;

[1] Link: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[2] Link NL: https://www.ejustice.just.fgov.be/cgi/article.pl?language=nl&sum_date=2024-05-17&lg_txt=n&pd_search=2024-05-17&s_editie=1&numac_search=2024202344&caller=sum&2024202344=4&view_numac=2024202344fx2024202344n
Link FR: https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2024-05-17&lg_txt=f&pd_search=2024-05-17&s_editie=1&numac_search=2024202344&caller=sum&2024202344=4&view_numac=2024202344nx2024202344f

- Reach the size thresholds of a medium-sized enterprise
- Be established in Belgium

The scope covers the whole of the entity i.e., all the networks and information systems of the entity concerned, and not only the NIS listed activities.

Sectors

The entity concerned must provide at least one of the listed services:

- Essential entities (in green additional sectors/subsectors)

Sector	Subsectors NIS I	NIS II additional subsectors
Energy	Electricity / Oil / Gas	District heating & cooling / Hydrogen
Transport	Air / Rail / Water / Road	
Banking Financial market structures		
Health		
Drinking water		
Digital infrastructure	*e.g. Internet, networking, cloud, hosting....*	
Waste water		
ICT service mgt	*Managed services e.g. SOC...*	
Public admin	*Local public administrations are normally excluded*	
Space		

DORA

New sectors

- Important entities

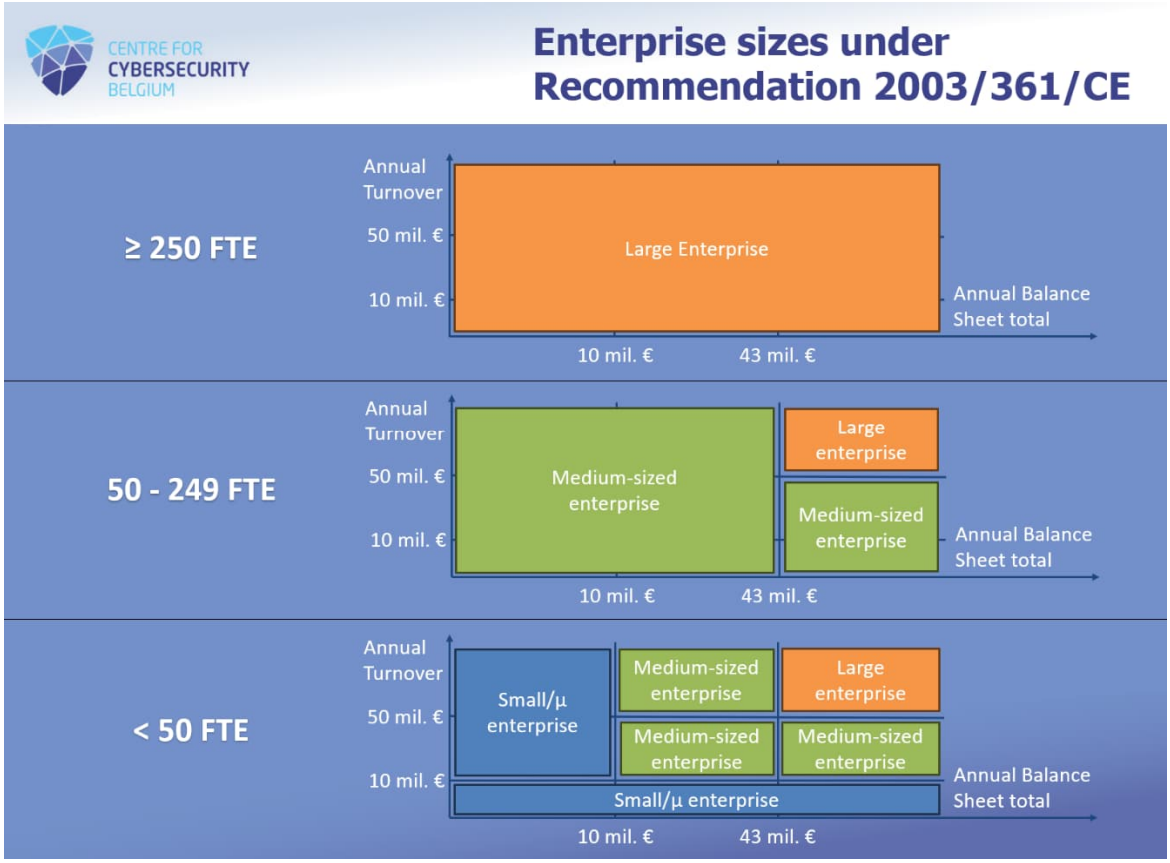
Sector	NIS II subsectors
Postal and courier services	
Waste management	
Chemicals	*Manufacturing, transformation, distribution*
Food	*Manufacturing, transformation, distribution*
Manufacturing	Medical devices / electronic products / electrical equipment / machinery & equipment / automotive / transport equipment
Digital providers	*Online marketplaces, search engines, social media...*
Research	

Size

The size of an organisation, i.e. being at least a medium sized enterprise, is established when one of the two criteria below is reached:

- staff headcount, i.e. at least 50 FTE;
- financial amounts, i.e. an annual turnover of at least 10 million € and a balance sheet of at least 10 million € (combination of both).

The CCB chart below presents graphically the above criteria, where large and medium-sized organisations are in scope.



Source **:** [3]

However, certain types of entities fall within the scope of the NIS2 law, regardless of their size (cf. https://atwork.safeonweb.be/nis2)

Applicable standards

The certification will be based on the 2 standards mentioned in the royal decree: the CyberFundamentals (CyFun®) or the international norm ISO 27001.

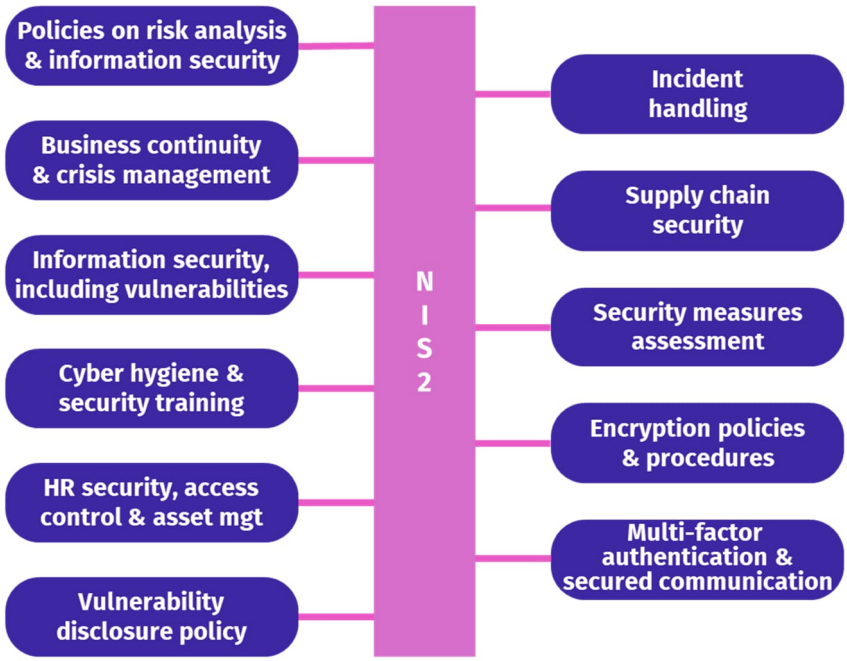
An entity may also use another reference framework e.g. NIST to implement its legal cybersecurity requirements. In this case, it will not benefit from the presumption of conformity and will have to demonstrate to the inspection service that it is applying all the required measures, based on a mapping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

Obligation in terms of security measures

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 to eliminate or reduce the consequences that incidents have on the recipients of their services.

[3] Link: https://atwork.safeonweb.be/nis2

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:



Source :[4]

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 security measures should be proportionate to the risks to which the concerned network and information system are exposed.

The CCB made available free of charge the "***Cyberfundamentals Framework" (CyFun®)***[5] with different levels and an analysis tool to determine the most appropriate security level to follow by the concerned entities.

[4] Link: https://www.linkedin.com/posts/centre-for-cybersecurity-belgium_cybersecurity-nis2law-belgium-activity-7217523356298833920-Y4XK?utm_source=share&utm_medium=member_desktop
[5] Link: CyberFundamentals Framework | CCB Safeonweb

Incident reporting obligations

An incident is 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".

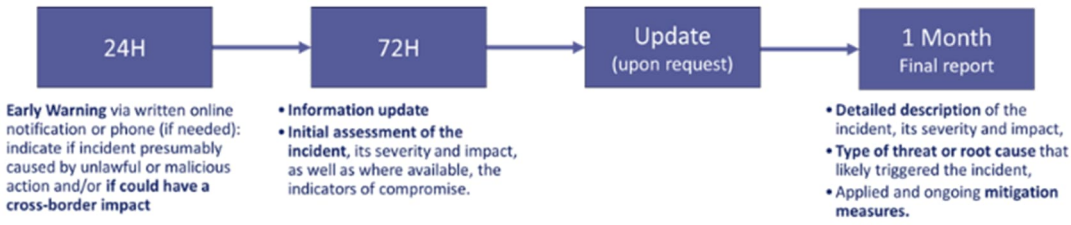
A significant incident is defined as: "any incident has a significant impact on the provision of services which:

1. has caused or is likely to cause serious disruption to the operation of any of the services 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 the event of a significant incident, the entity must notify the national CSIRT, i.e. CCB (except for DORA entities who notify the NBB and the FSMA) and, in certain cases, the recipients of their services. When personal data is involved, the Data Protection Authority should also be notified.

The notification takes place in 3 stages:

1. An early warning within 24 hours of the incident being discovered;
2. A formal incident notification within 72 hours of the incident being discovered; and
3. A final report no later than 1 month after the incident notification.



Source: [6]

Supervision

Essential entities are monitored proactively "ex ante" and reactively "ex post". More specifically, essential entities are subject to regular conformity assessments. 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 CCB inspection service may also control essential entities at any time.

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

[6] Link: https://ccb.belgium.be/sites/default/files/NIS2%20FAQ%20Website%20v1.0%20EN.pdf

When do the NIS2 obligations become applicable?

The NIS2 law and royal decree will enter into force on 18th October 2024. All the obligations will apply to essential and important entities from that date.

After the law comes into force, entities have 5 months i.e. 18 Marc 2025, to register on the CCB portal, Safeonweb@Work. (Information and communication technology entities need to register within 2 months).

The regular conformity assessment of essential entities follows a gradual implementation depending on the reference system chosen.

- 18 months after the law comes into force i.e. 18 April 2026, a verification carried out by an accredited CAB approved for CyFun® or the scope and the statement of applicability to be transmitted to the CCB for ISO 27001.
- 30 months after the law comes into force, i.e. 18 April 2027, a CyFun® or ISO 27001 certification or in case of inspection by the CCB, the transmission of a progress report.

Important entities are not subject to mandatory regular conformity assessments. The CCB inspection service will supervise the important entities.

The management's obligations and responsibilities

The management bodies of NIS2 entities must

- approve cybersecurity risk-management measures and oversee their implementation.
- 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.

If the entity breaches its obligations with regard to risk-management measures, the legal representatives of an entity are liable for their failure to ensure NIS2 compliance.

Sanctions

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. Various administrative measures may be imposed such as warnings, implementation of recommendations, suspension of activities, obligation to inform the service recipients or prohibiting a person to exercise managerial responsibilities. Fines can amount up to 2% of the total annual worldwide turnover.