GET READY FOR THE NIS2 DIRECTIVE

APPROACH CYBER HELPS YOU NAVIGATE THE NEW LEGISLATION AIMED AT STRENGTHENING CYBER SECURITY IN EUROPE, AND TAKE THE RIGHT STEPS TO COMPLY QUICKLY.

Start on time

With the adoption of the NIS2 (Network and Information Systems Directive), the European Union (EU) is strengthening its cyber security requirements for a wide range of businesses and organisations.
The directive was transposed into Belgian law by the federal parliament on 19 April 2024. Many sectors are affected, and NIS2 requires them to take enhanced cyber security measures, report incidents, and be supervised by the national cyber security authority.

The entities concerned have until 18 October 2024 to comply with the Belgian NIS2 law. This means that they should already have taken all the required measures.

Are you affected by NIS2?

The scope of the NIS2 Directive is considerably broader than its predecessor, NIS1, to include a greater number of companies and organisations in many sectors. The NIS2 directive is aimed at organisations of a certain size that provide services in critical sectors. Entities in these sectors are considered vital for maintaining critical societal or economic functions in Belgium. Size cap and the service provided are therefore the two main criteria for determining whether the NIS2 directive applies to an organisation.

The sectors concerned are as follows:

- **Highly critical sectors:** such as energy, transport, banking and financial market infrastructures (also subject to DORA), health, drinking water, wastewater, digital infrastructures, ICT service management, public administration (central and regional) and space.

- **Other critical sectors:** such as postal and shipping services, waste management, chemicals and food, manufacturing, digital suppliers and research.

With certain exceptions, an organisation must be considered at least as a medium-sized enterprise in order to be covered by the NIS2 directive. A medium-sized enterprise has at least 50 full-time employees and/or an annual turnover (or annual balance sheet total) of more than €10 million.

The NIS2 Directive also draws a distinction between "essential" and "important" entities. This distinction is made on the basis of the size of the entity and the service provided.

The difference between essential and important entities lies mainly in the control and sanction mechanisms. Essential entities will be monitored more regularly and more strictly than important ones.

And what about companies that aren't covered?

NIS2 does not explicitly specify the obligations for companies that do not fall within this scope.

However, even if a company does not fall within the scope of NIS2, it may nevertheless be indirectly affected as a supplier, or choose to follow certain recommended practices to improve its cyber security.

The NIS2 directive is aimed at organisations of a certain size that provide services in critical sectors, the so-called "essential" and "important" entities.

A supervisory and control body, the CCB

Each EU Member State must designate one or more competent authorities to oversee the application of the directive, ensure the implementation of appropriate security measures, and manage cyber security incidents and crises. In Belgium, the competent authority is the Centre for Cybersecurity Belgium (CCB). The entities concerned are required to register with the CCB via the Safeonweb@work portal. Barring exceptions, this obligation can be fulfilled until 18 March 2025.

Concerned Belgian organisations must register themselves with the Centre for Cybersecurity Belgium (CCB) before 18 March 2025.

What are your obligations?

The entities concerned must take appropriate and proportionate measures to manage the risks that threaten the security of their networks and information systems, and to eliminate or reduce the consequences that incidents have on the recipients of their services and on other services.

The entities concerned will also have to notify, without undue delay, the national CSIRT of significant cyber incidents (in Belgium, cert.be). Finally, essential entities are required to carry out regular compliance assessments, verified by a compliance monitoring body.

Contact us for more information about appropriate and proportionate measures.

The CCB has the power to adopt measures to encourage entities to take appropriate action. To this end, it may, for example, require regular external audits, carry out inspections or request the production of certain documents.

In particular, the CCB may issue warnings or binding instructions to remedy any shortcomings observed or to inform their customers.

NIS2 requires you to strengthen your cyber security risk management measures, and to report incidents to the CCB within set deadlines.

What are the penalties for non-compliance?

The NIS2 directive not only strengthens cyber security requirements and your obligations, it also provides stricter penalties to ensure compliance.

For example, breaches of risk management measures or incident notification could be punished by dissuasive administrative fines.

In this case, the fine is of the GDPR type. For essential entities, these fines can reach €10 million or 2% of annual worldwide turnover. For important entities, the fine is €7 million or 1.4% of annual worldwide turnover. And in the event of a repeat offence for the same acts within a period of three years, the amount of the administrative fine is doubled. It should be noted that these fines do not apply to public authorities, unlike the other administrative penalties, which do apply.

Penalties are severe and dissuasive to ensure compliance. In some cases, they are comparable to those of the GDPR.

Top management is now directly concerned

NIS2 makes the management of each entity more accountable, so that cyber security becomes a real topic of discussion right up to board level. To raise awareness, the individuals who represent these entities may be held liable for failure to comply with the directive's obligations.

The penalties are severe, ranging from a personal fine for the CEO and directors to a temporary ban on holding a management position.

It is therefore essential that the Board of Directors can easily grasp the challenges of Information Security and assess the relevance of the measures taken to strengthen this security.

Top management is held directly responsible for NIS2 compliance. In the event of non-compliance, sanctions and personal fines are provided for.

What measures need to be put in place?

Firstly, in terms of governance, top management will have to approve cyber security risk management measures, oversee their implementation and may be held responsible for any failings.

To ensure that they understand the measures they are approving, members of management will have to undergo cyber security training and provide similar training to their staff on a regular basis.

Security measures must be appropriate and proportionate, based on a risk analysis. Of course, all basic cyber hygiene practices must be put in place. But these measures are not enough.

NIS2 requires a global and comprehensive approach, a management and continuous improvement system, including a set of technical security measures (such as encryption, cryptography, multi-factor authentication, etc) and non-technical measures (such as policies and procedures, organisation, business continuity plan, backup management, crisis management, security management of suppliers and service providers, physical and perimeter security, human resources security, etc). Additional measures have also been added in the Belgian NIS2 law.

The measures to be put in place are both technical and non-technical. In addition to these measures, a genuine risk management and continuous improvement system is required.

You're not on your own! Approach Cyber is at your side

NIS2 compliance is one of the major compliance issues in 2024, and an effective response requires thorough preparation and expertise. Here's how we can help you prepare for and ensure compliance with NIS2:

1. Risk assessment and gap analysis

- We carry out a gap analysis to compare your current practices with the requirements of NIS2, based on the reference frameworks cited by the CCB (such as CyberFundamentals or "CyFun", and ISO27001).
- We carry out a comprehensive risk assessment to identify potential vulnerabilities and threats in your networks and information systems.

2. Implementation of security measures

- We implement the appropriate technical and organisational measures to manage the risks identified, in accordance with the CCB's recommendations.
- We ensure that all security measures are regularly updated and tested to meet new threats and NIS2 requirements.

3. Establishment of incident response protocols

- We develop detailed protocols for detecting, notifying, reporting and responding to cyber security incidents, in line with the requirements of the CCB and the GDPR when personal data is involved.
- We train your staff to recognise and respond effectively to security incidents, including personal data leaks.

4. Awareness-raising and training

- We train management and your employees in good cyber security practices and the procedures to follow in the event of an incident.
- We raise awareness throughout your organisation of the importance of NIS2 compliance.

5. Documentation and regulatory compliance

- We document all policies, including the information security policy, the coordinated vulnerability policy, essential NIS2 prerequisites, and the security procedures and measures in place.
- We maintain up-to-date documentation so that we can demonstrate your compliance to the authorities if necessary.

6. Monitoring, maintenance and certification

- We provide regular monitoring and continuous updating of your security measures to ensure lasting compliance, in particular by drawing up dashboards for management and the board of directors.
- For essential entities, we can help you prepare for and pass CyFun or ISO27001 audits, inspections and certifications within the legal deadlines (18 April 2027).

Real expertise in the field is crucial to ensuring compliance, responding effectively to incidents and protecting your critical infrastructures.

Contact us for more information on the key steps to NIS2 compliance and find out how we put them into practice. Based on the frameworks cited by the CCB and our successful experience working with many organisations, we are ready to support you at every stage of your compliance journey.

Approach Cyber supports you at every stage of your compliance journey. Based on the frameworks cited by the CCB and our successful experience with numerous organisations.

What are the benefits of the NIS2 directive for your organisation?

Beyond compliance, NIS2 offers an opportunity to differentiate yourself in the marketplace, or to set a good example if you are a public authority. Companies that demonstrate a proactive commitment to cyber security can not only minimise the risk of operational disruption, but also boost the confidence of their customers and partners.

NIS2 enables companies to differentiate themselves in the market and strengthen the confidence of customers and partners by demonstrating a proactive commitment to cyber security.

Testimonial from our CEO

"*This is one of the hot compliance topics of the year, alongside the AI Act. Rather than seeing NIS2 as a second GDPR, with its regulatory pressures and penalties, let's see it as an opportunity to strengthen your company's cyber serenity in a threatening digital landscape,*" **David Vanderoost, CEO of Approach Cyber.**

Why choose Approach Cyber as your compliance partner?

We are committed to providing you with the resources, tools and expertise you need to effectively navigate this complex regulatory landscape. By working with us, you can be confident that your organisation is well prepared to meet the challenges of NIS2 and to protect your digital assets from potential threats.

Approach Cyber is your partner of choice for this process:

- **A solid, recognised partner:** Established for over 20 years, with numerous references and ISO 27001/27701 certifications, Approach Cyber is a benchmark service provider in Belgium.
- **Can help you benefit from regional subsidies:** If your company is an SME, you can benefit from substantial financial assistance from your region. Approach Cyber is a service provider recognised/labelled by the authorities in the country's three regions.
- **Full sectoral cooperation:** We actively participate in initiatives to share information and experience on NIS2, and in sectoral groups to help businesses (e.g. Agoria, UWE/AKT, CyberWal, Cyber Security Coalition, SecAppDev, ISACA, FSMA, etc).
- **A multidisciplinary team of over 100 people:** We offer technical, strategic and legal expertise to guide you through the complex requirements of NIS2.
- **Customised, business-focused solutions:** We develop solutions tailored to your specific needs, and to the size of your organisation. We address cyber security challenges and needs at every level, right up to the boardroom.
- **A global, integrated approach:** We offer a complete range of cyber security services (360°) with an all-in-one approach. Our strong technology partnerships enable us to deliver advanced, integrated solutions that simplify the management of your security. This frees you up to focus on your core operations without the complexity of coordinating multiple service providers.

Contact us

Contact us to find out more about the NIS2 directive and how we can help you comply.

info@approach-cyber.com
+32 10 83 22 11
+32 3 366 21 76