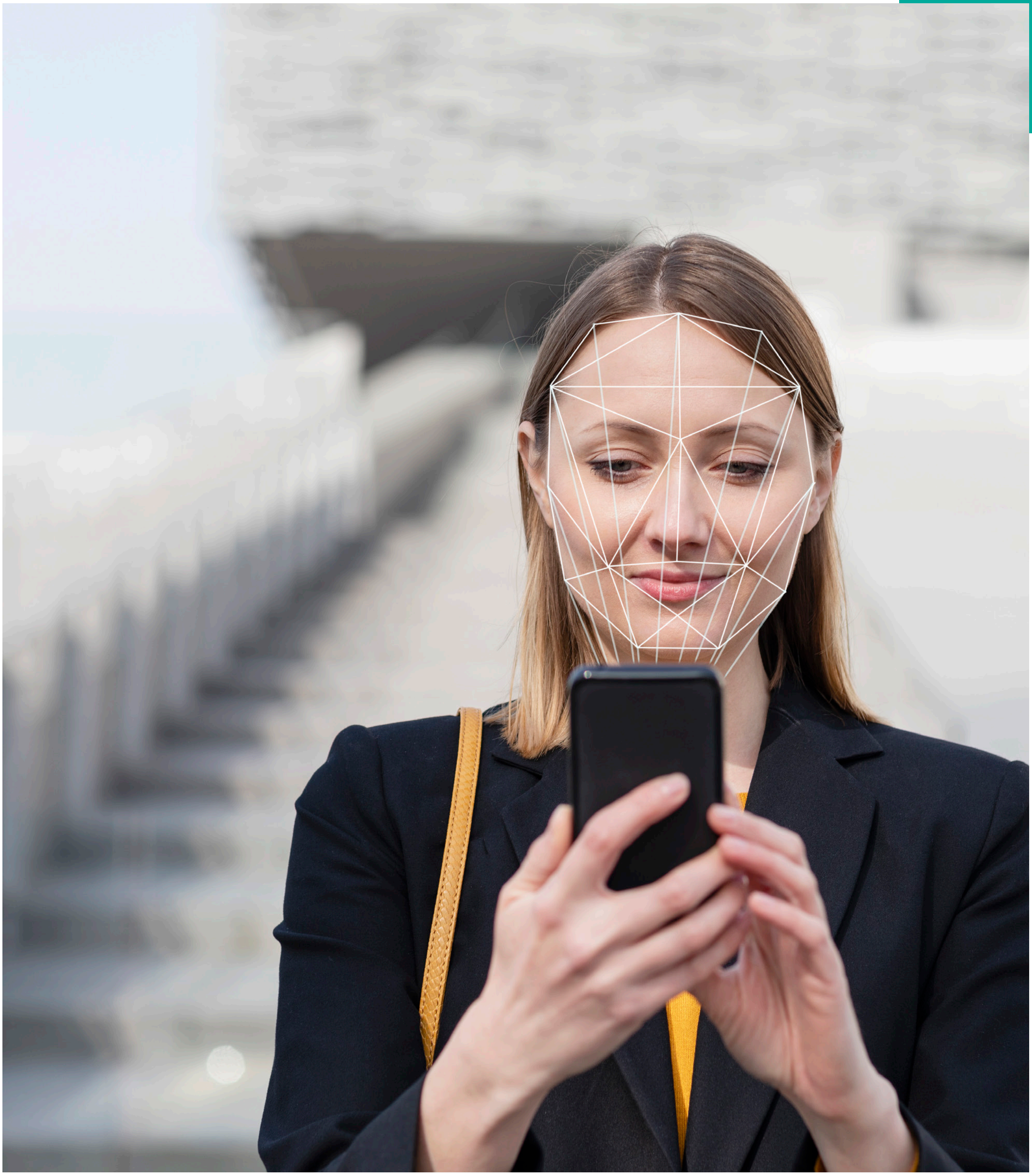


NIS2: cybersecurity lever and accelerator

Cybersecurity versus Compliance

Belgian CIOs are all too aware of the importance of cybersecurity. But what about compliance? Do those CIOs also consider it important to comply with the imposed regulations around cybersecurity to the best of their ability?

The answer to that question is found in local market research by **Beltug**, Belgium's e largest association for CIOs and IT decision-makers, with 2200 members.

Cybersecurity remains "top of mind"

Cybersecurity has ranked remarkably high for some time in Beltug's **annual priority survey**. While you could hardly ignore the breakthrough of artificial intelligence (AI) in 2023, cybersecurity was once again at the very top of the Belgian CIO's priority lists.

In 2023, no fewer than four of the top ten priorities were linked to cybersecurity: from developing an IT security strategy and architecture to promoting security and privacy awareness among IT users and planning for cyber incident response, including setting up a dedicated Computer Security Incident Response Team (CSIRT). In fact, in total, security topics occupied nearly half of the top 40 CIO priorities in 2023.

That Belgian CIOs are serious about their focus on cybersecurity is also evident in Beltug's **biennial user survey**, where investments in cybersecurity remain clearly up to standard. For example, at the beginning of 2023, only 3.5 percent of companies expected that investment to decrease in that year, and a quarter expected them to remain stable, while nearly seven in ten respondents (68%) saw their investments in cybersecurity increasing.

> Today, no IT decision-maker really questions the point of investing in cybersecurity.
>
> **Levi Nietvelt,**
> *Beltug*

Compliance not explicitly mentioned

If we look at Belgian CIOs' attention to compliance, a very different picture emerges. Unless you want to include terms such as governance (of data, IT, AI, etc.) or ESG (sustainability reporting) under the same name, the word compliance hardly appears in the Belgian CIO's list of priorities.

Nevertheless, compliance is already a major challenge today, especially in the area of cybersecurity and data privacy, and it is likely that this challenge will only increase in the coming years. New laws and regulations, especially from the European Union, are following in rapid succession, which doesn't make it easy to keep up, especially since the regulations for one country don't always apply in another.

> Since compliance is barely mentioned in CIOs' priorities, could it be 'unimportant'?
>
> **Levi Nietvelt,**
> *Beltug*

NIS2 compliance: playtime is over

Governments, with the EU leading the way, are imposing increasingly high cybersecurity requirements on companies. A striking example is NIS2, the successor of the 2016 **Network and Information Security (NIS)** Directive. The original version is sometimes referred to as the very first cybersecurity law. The ultimate goal of both European directives—the old and the improved version—is to better protect companies, better manage risks and prevent incidents or at least minimize their consequences to the extent possible.

NIS2 is part of a growing wave of EU cybersecurity requirements, from the 2014 eIDAS Regulation to the 2023 GPSR Directive. Within this ever-expanding EU legislation, NIS2 stands apart by its **far-reaching scope** and deep **impact on the entire organization**, not just on a part of it or a single service, product or technology.

For starters, NIS2 covers as many as **18 sectors**—11 more than the first version—and applies to **more than 180,000 companies within the European Union**. According to an initial estimate by the Center for Cybersecurity Belgium (CCB), some 2400 Belgian companies would be covered by the new European directive. Inetum estimates approximately 3000 companies, but whatever the final figure, NIS2 is considered to be **the most comprehensive EU cybersecurity legislation to date**.

> NIS2 is an important law in any case, whether you fall under it or not.
>
> **Levi Nietvelt,**
> *Beltug*

The supply chain places (added) pressure

The scope of NIS2 not only extends beyond the original directive, but its impact on the companies it covers is significantly greater. The EU's **requirements** on those companies—including **reporting**, for example—are noticeably heavier and more stringent than before.

The same applies to the **penalties** that the companies in question may incur if they fail to comply. In addition to **administrative fines**, appointment of a supervisor and suspension of certifications or authorizations, failure to comply with the directive may henceforth carry **legal consequences for senior** management. For example, even the CEO of the company can now be temporarily banned from holding an executive function.

The new NIS2 directive also places a strong emphasis on ensuring **business continuity**. This security requirement also extends to the entire supply chain. As a result of this heightened focus on **securing the supply chain**, in many cases it is advisable to comply with the NIS directive, even if it does not apply directly to your business. After all, by imposing the same compliance throughout their supply chain, companies can avoid data breaches or block hackers who might otherwise still cause cyber problems through their suppliers.

> To put it bluntly: playtime is over. Europe wants all companies to achieve a minimum level of cybersecurity. The NIS2 directive is a lever to accelerate that security bottom line.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

Time is also running out!

The proposal for the new European Cybersecurity Directive NIS2 was submitted by the European Commission in December 2020. After a quick negotiation process, the final text was adopted by the Council and the European Parliament two years later, published on December 27, 2022, to **officially** enter into force in **January 2023**.

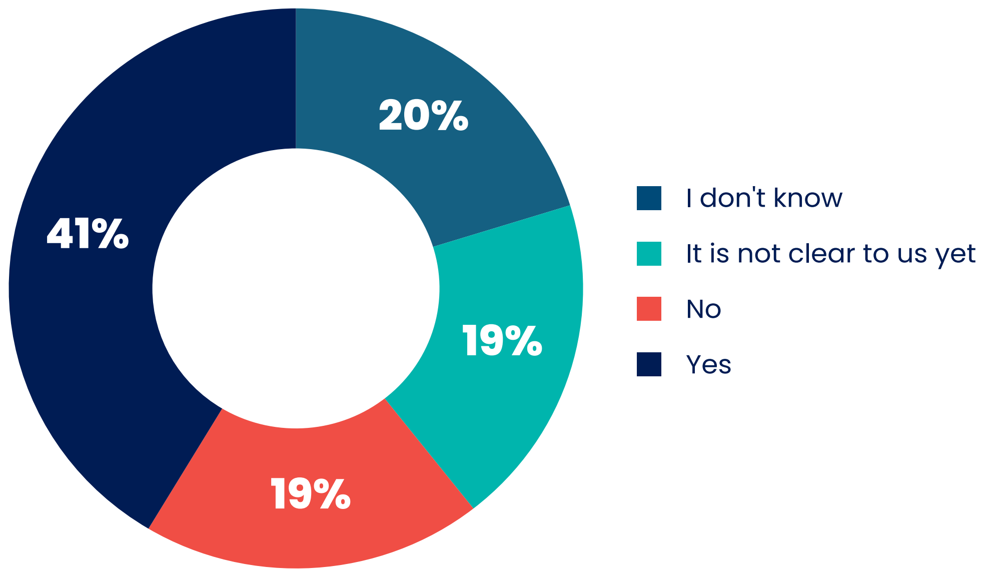
Belgium, like all other EU Member States, then had 21 months until October 2024 to implement the NIS2 directive into national law. On **November 10, 2023** the Federal Council of Ministers already ensured **that it was transposed into Belgian law.** The law is expected to be approved in parliament in April.

As of **October 2024**, it is expected that NIS2 will replace the existing NIS directive in Belgium as well. From that moment on, all companies and organizations involved must comply with these new regulations. In the event of a cyber incident, your company could be held responsible, and sanctions could be imposed.

> October 2024 is approaching quickly. So, I strongly encourage everyone not to wait until the new law comes into effect, and to start the process of meeting all obligations as soon as possible.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

To comply, or not to comply, that is the question

Does your organisation need to comply with the NIS2 directive?
All marks (n=303)



Does the NIS2 directive apply to your organization? Four out of ten Belgian companies (39%) still had to answer this question from Beltug's annual priority survey in 2023. Half of these companies simply had no idea, while for the other half it was still not entirely clear whether or not they were covered by the Directive.

The following criteria will help determine that for you:

Criterion 1: sector

The NIS2 directive applies to all sectors already covered by the first NIS directive, as well as to a number of new sectors, bringing the total to **18 sectors**. As a result, the number of organizations covered is increasing.

The NIS2 directive distinguishes between **critical** and **highly critical** sectors:

Critical Sectors

- Waste management
- Chemicals
- Digital providers
- Food
- Research
- Postal and courier services
- Manufacturing companies (manufacturing)

Highly critical sectors

- Wastewater
- Banking
- Managers of ICT services
- Digital infrastructure
- Drinking Water
- Energy
- Healthcare
- Financial market infrastructure
- Government
- Space
- Transportation

Criterion 2: scope and criticality

A key difference from the first NIS directive is that organizations are automatically covered by the NIS2 directive if they operate in any of the above sectors and can be characterized as **"essential"** or **"significant" entities**. That qualification depends on factors such as the **industry**, as well as the **size**, in terms of turnover and number of employees, and the organization's **criticality.**

In **critical industries**, for example, no one type of business is essential, but all are **important**. With the exception of companies with fewer than 50 full-time employees and a turnover of less than €10 million, NIS2 simply does not apply to them.

This is also the case for companies in **highly critical sectors**. Here you will find a number of essential companies, in addition to important ones. Virtually all companies that employ more than 250 full-time employees are essential, regardless of the turnover they generate, as well as a number of companies that generate more than €50 million in turnover, regardless of their number of employees. For these essential companies, the **Directive is more stringent** because it is generally assumed that the failure of their services has a much more **disruptive impact** on the economy and society than the failure of major companies.

> If you employ fewer than 50 people, you are not covered by NIS2. But be careful, because if you supply critical services or products to companies covered by NIS2, you will have to demonstrate to them that you operate safely, through an official audit if necessary. After all, they are responsible for their supply chain risk.
>
> **Arnaud Martin,**
> *Agoria*

Becoming NIS2 compliant: what does it mean for you?

Does your company fall under the NIS2 directive based on the criteria above? If so, there are basically two main requirements for you.

First, you need to **take a number of measures to adequately manage and mitigate your cybersecurity risks.** They may be both technical and operational as well as organizational measures. Most importantly, they must be appropriate and proportional. Specifically, they are measures in these ten areas:

1. Risk analysis and management
2. Security policy and asset management
3. Incident handling (prevention, detection and response to incidents)
4. Business continuity and crisis management
5. Supply chain security (taking supplier vulnerabilities into account)
6. Vulnerability management and handling
7. Regular assessments
8. Use of encryption where necessary
9. Basic hygiene and cybersecurity training
10. Use of multifactor authentication (MFA) or continuous authentication

Second, you must also meet a number of obligations for **reporting incidents.** For example, from now on, you must report significant incidents to the Computer Security Incident Response Team (CSIRT) or the relevant competent authority without delay—**within 24 hours**, to be precise. After a maximum of **three days (72 hours)**, a more detailed progress report must follow. At the latest **one month** after reporting, you must be able to submit the final report on the incident, including the actions taken, which may or may not have been ongoing.

> "You need to know: what risk am I running today? And how can I reduce that risk to an acceptable level?
>
> **Koen Tamsyn,**
> *Solution Manager Cybersecurity, Inetum* "

If you need help, Inetum is happy to assist!

Do you lack the necessary people or resources in-house to ensure smooth NIS2 compliance? Are you increasingly dreading the additional burden that such a major operation entails?

At Inetum, we not only understand the importance and necessity of complying with regulatory frameworks such as NIS2, we also have the **experts** and **solutions** to successfully assist you on your path to compliance—with both advice and action.

Ad hoc advice/consultancy

You can call on our team of cybersecurity specialists to analyze and assess your current security posture. Based on that **preliminary assessment,** they can then develop a customized **security** plan to meet your specific needs.

Finally, to help you meet the minimum measures required by NIS2, we also offer a wide range of tools and guidance, such as **risk assessments**, **security procedures** and **incident response plans**.

> We've been doing assessments of how far along a company is in terms of cybersecurity for quite a while now. We've recently updated this service and completely adapted it to the NIS2 measures.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

Cybersecurity Roadmap

With our Cybersecurity Roadmap, we chart your cybersecurity **maturity** in three steps and analyze any **weaknesses** in light of your NIS2 implementation. Based on that snapshot, we also eventually formulate concrete **optimizing proposals**.

Our cybersecurity Roadmap consists of a technology section in the form of a **data scan** and a non-technology section where you answer a **questionnaire** as part of a **workshop**.

During the assessment, we go through these **three steps** together:

Step 1: Preparing for your assessment

We host a kick-off meeting with a cybersecurity specialist to get to know each other better, discuss your assessment **objectives** and share **system requirements**. This lets us optimally prepare your IT environment for the actual assessment.

Step 2: Your IT assets: data collection and analysis

We install a tool in your IT environment that connects to all kinds of **platforms** both **locally** (Active Directory, SharePoint, email DNS, endpoints and servers) and in the **cloud** (Azure, Microsoft 365, etc.). This means that one of our cybersecurity specialists carries out the necessary scans and tests to collect all relevant data. We also conduct an **interview** with your CIO or CISO using a set questionnaire, including discussion of your organization's cybersecurity posture.

Step 3: Presentation of your final report

During a presentation, we will share our findings, conclusions and recommendations with you. We will then provide you with that **management presentation** as well, along with the comprehensive **final report**.

CISO as a service

However, cybersecurity is not a static thing, but a **cyclical process**. You could call it an eternal "work-in-progress" of continuing to align your cybersecurity goals with your overall business objectives and risk management strategies, on the one hand, and staying compliant with regulations on the other. NIS2 is not only **about technology solutions**, but also around **policies & procedures**.

There is a whole list of must-haves if you want to pass an NIS2 audit, e.g., policies for information security, access control, incident response, cryptography, vendor management, data classification and handling.

Is a full-time CISO still too much for you? Then we would like to introduce our CISO as a Service to you: a security expert who will take on the role of CISO part-time with you.

Together, we'll make it work!

Does your company fall under the NIS2 guideline or are you a key supplier to a company covered by NIS2? If so, we recommend that you start working on a cybersecurity assessment now and work with us to create a Cybersecurity Roadmap. This will give you enough time to take the necessary measures to (continue to) operate securely, in compliance with the new NIS directive. In addition, this well-thought-out, phased approach allows you to spread not only the work but the costs as well.

CONTACT US

Inetum
A. Vaucampslaan 42
1654 Huizingen, Belgium
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world