Deloitte.

Navigating NIS2 Compliance

July 2024 - A current view on local NIS2 legislations for organizations with cross-border European operations

Executive Summary

The Network and Information Security 2 (NIS 2) Directive establishes more rigorous cybersecurity requirements for organisations in EU Member States, with an anticipated transposition deadline of October 2024. This whitepaper provides an analysis until June 2024 of the current regulatory landscape, touching upon key aspects such as sector definition, identification of entities, registration requirements, and security measures, as well as management accountability and government oversight.

Across the EU, Member States display varied transpositions of the NIS2 Directive until July 2024, with the following notable highlights:

- Croatia, Czech Republic and Poland, have expanded upon the Directive's sector scope, recognizing **additional critical entities and sectors.**
- Belgium on the other hand has adhered to the Directive's scope classifications, but defines a **custom cyber security controls framework to which entities can certify next to ISO 27001.** Belgium also requires a **coordinated vulnerability disclosure policy** for each entity.
- Italy will require organizations to be compliant by **september 2026** (transition period) and requires the adaption of a **National Cyber Security Framework (based on NIST CSF)** which defines cyber security controls for highly critical, critical and standard services.
- Ireland, and Poland's approach to security controls aligns with international standards **ISO/IEC 27001, NIST CSF** or ISO/IEC 22301, as benchmarks for compliance.
- Austria requires entities to demonstrate the effectiveness of these risk measures through a **self-declaration process**.
- Croatia has not setup a registration platform, but the relevant governing body will request information from entities for categorization. **Croatian entities will thus not have to register themselves** and the initiative will be with the Croatian government

The Directive's emphasis on management accountability is clear, with executive boards and managing directors mandated to ensure compliance with risk management measures. While Austria, Italy and Poland provide detailed definitions and responsibilities for management bodies, Belgium, Croatia, Hungary, and Germany do not further specify the concepts.

Government oversight and audit mechanisms vary, with Austria proposing dual audit approaches and Germany draft law establishing a 3 yearly verification process. Croatia and Poland propose an audit frequency of at least every two years.

In essence, the transpositions studied showcase important specifics which can have significant impact for organisations operating in these countries. For these organisations, it means **closely following up on the transpositions and trying to define a common ground to reach a workable level of compliance**. Having a strategic cybersecurity control framework to navigate this evolving regulatory landscape will be important moving forward.

Introduction

The adoption of the Network and Information Security 2 (NIS 2) Directive by EU Member States, aimed for October 2024, marks an important milestone in the European Union's cybersecurity landscape. Building upon its predecessor, **NIS2 introduces stricter requirements and broadens its reach.** This legislative move aims mainly to strengthen national and cross-border cybersecurity resilience.

In this whitepaper, we will cover the fragmented EU NIS2 regulatory landscape, providing a comprehensive overview of its current state in the beginning of July 2024. Please note that the NIS2 landscape is rapidly evolving. This whitepaper reflects the current state of knowledge and regulations as of its publication date. Readers are encouraged to stay informed about new developments and evolving laws in this area.

We already know that Member States have clearly outlined different requirements and timelines and with still so many unknowns, organizations may question whether it is even possible to start on a NIS2 implementation. However even with those differences and uncertainties, waiting would be the lesser option. **Organisations can already start now** with common requirements outlined by the directive and should not lose any time (after all, hackers are also not waiting).

The different stages of NIS2 adoption and implementation across the EU

The implementation of the NIS2 Directive is currently making its way across the European Union. With all Member States at varying stages of adoption and readiness, the new regulatory landscape can quickly become overwhelming, especially for organizations that operate cross-border. But what does this mean concretely?

Most countries are currently still waiting for guidance from their National cybersecurity authorities, who are playing a crucial role in overseeing the transposition process of the Directive. However, their approaches vary strongly across Member States. This results in **notable differences in adoption and readiness timelines**, with some countries being well ahead in their implementation efforts and others still waiting to see which way the cat jumps. These differences are clearly highlighting the need and importance of collaboration and knowledge sharing across the EU, to be able to ensure a high level of cyber security. In the following part, we will examinate the current landscape more closely.

The following **final laws were analysed: Belgium, Croatia, and Hungary**. Please note that for these laws typically final pieces of legislative text are missing to fully transpose the directive. The following **draft laws were analysed: Austria, Poland, Czech Republic, Finland, Germany, Italy, and Luxembourg,** along with expectations in **Ireland**.

A comparison of the transposition of the NIS2 Directive will be made on the following aspects:

- Essential and important entities
- Sector definition
- Registration processes
- Security controls requirements
- Board level/management accountability
- Government oversight and audit

For other countries Deloitte has insights, but draft laws are not publicly available. For example in Italy, the agency responsible for the transposition and the oversight of the Directive has provided indictions on how they want to transpose the Directive. In this whitepaper we limited ourselves mainly to public draft or final laws.

Essential and important entities

The NIS2 Directive has identified the sectors that are in scope, which has expanded significantly compared to its predecessor:

This classification between essential and important determines the application of different requirements regarding supervision and sanctions. While some Member States align closely with the European Commission's enterprise size criteria for classifying essential and important entities, others take a more tailored approach. For instance, the Polish (Draft) law also **elevates several sectors from 'important' to 'essential'**, such as the production and distribution of chemicals, food, medical devices, and various manufacturing industries.

NIS 1 vs NIS2

Essential sectors

- 🟦 Energy
- 🟦 Transport (air, rail, water, road)
- 🟦 Banking
- 🟦 Financial market infrastructure
- 🟦 Health
- 🟦 Digital infrastructure
- 🟦 Drinking water
- 🟩 Waste water
- 🟩 Public administrator
- 🟩 Space
- 🟩 ICT service management (B2B)

Important sectors

- 🟩 Postal and courier services
- 🟩 Waste management
- 🟩 Food
- 🟩 Chemicals (manufacturing, production, distribution)
- 🟩 Manufacturing
- 🟩 Digital providers
- 🟩 Research

🟦 Sectors defined by NIS1

🟩 New sectors added by NIS2

Most other countries such as Belgium (Final), Germany (Draft), Czech Republic (Draft), Croatia (Final), Luxembourg (Draft), Italy (Draft) and Austria (Draft) are essentialy takenover the classification in essential and important entities as specified by the NIS2 directive.

Sector definition

When we look at how different countries are expanding the scope of sectors required by the NIS2 directive, we see a variety of approaches. At least Belgium, Luxembourg, Italy Germany, Finland, Ireland and Austria have chosen to stay within the scope outlined by the Directive itself, without adding new sectors.

Croatia, Czech Republic and Poland identify **additional sectors** that are classified as essential:

- Croatia's (final) law includes entities crucial in the electronic invoicing space. As well as entities that play a pivotal role in managing, developing, or maintaining the information infrastructure of the government. Moreover, Croatia has recognized the education system as a critical sector, extending this to both private and public educational entities. In comparison,
- Poland, in its draft law, has opted as well for an expansive adaptation by incorporating additional subsectors within the energy and transport sectors. This includes entities involved in the extraction of energy resources and managed cybersecurity service providers with clients in the energy sector. Service providers to airlines and other aircraft users are considered critical as well.
- The Czech Republic includes the Defense Sector to its list of essential sectors.
- Italy has defined that universities are also in scope as research organisations.

Sector-wise, an interesting overlap with NIS2 in the regulatory landscape is the Digital Operational Resilience Act (**DORA**). In several Member States, like Belgium (Final), Germany (Draft Law) and Finland (Draft Law), financial entities need to adhere only to DORA, which will supersede NIS2 compliance requirements in these countries. In other countries, like Croatia, the law does not reference to DORA, making both NIS2 and DORA applicable to organisations from the banking and financial market infrastructure sector. In Ireland the Central Bank of Ireland will act as the competent authority for NIS2.

Registration processes

When looking at registration requirements, we see the differences increasing. In the case of Croatia, there currently isn't a dedicated registration platform. Instead, the governing body tasked with implementing the law will actively reach out to entities in scope, requesting the necessary information for categorization and for maintaining an up-to-date list of entities. These entities must respond with the required information within a 45-day timeframe.

Looking at other countries, we see Austria's review draft stipulates a three-month deadline for registration, while Belgium's final law allows for a five-month period. For Italy entities need to register themselves between January 1st and February 28th as from 2025.

Most countries have or are creating an online portal by which countries can register themselves. Examples are Belgium, Luxembourg, Italy, Austria, Hungary and the Czech Republic. They require entities to submit information, but the specific details are not always known yet. In most cases contact details need to be shared, and in Austria's case even IP addresses. The Czech Republic expands the scope of the portal not only registration functionalities but also real-time threat intelligence sharing and other NIS2-relevant services. Finland, through its draft legislation, also mandates registration, but the specifics are unclear, as is the case for Germany.

While registration platforms and timelines are being defined in some Member States, **there is less uniformity regarding FAQs or guidance on NIS2 implementation**.

- **Hungary:** Engaged in extensive outreach through public consultations and media to disseminate information.;
- **Finland:** Provided draft recommendations for local authorities;
- **Czech Republic:** The Czech cyber authority operates a website entirely dedicated to NIS2 implementation;
- **Germany:** Designated the BSI[1] as the central reporting office without stipulating a registration timeline;
- **Poland:** Acknowledges the need for registration in its draft law, but also has yet to detail the timeline.
- **Belgium:** Engaged in extensive outreach through

[1] Bundesamt für Sicherheit in der Informationstechnik

public consultations and public-private working groups and conferences. On the website of the CCB[2] template security policies are shared, as well as tools to facilitate risk assessments per sector and current state assessments of the security controls.

Security controls requirements

When looking to the approach to defining and implementing security measures, different approaches are becoming clear. Some countries like Finland (Draft), Czech Republic and Germany (Draft) however still need to further clarify the specific security requirements.

When evaluating what is currently known for the other countries, some initial conclusions can be drawn:

- The CCB in Belgium, has made the security controls requirements very concrete and has established their **Cyberfundamentals Framework**, mainly based on the **NIST Cybersecurity Framework**, providing a structured baseline of controls for organizations to follow.
- Similarly Italy leverages their **National Cyber security Framework from 2016** based on NIST CSF which is regularly updated.
- Belgium also expands the 10 cybersecurity risk-management measures from article 21 with a new one, namely a coordinated vulnerability disclosure policy.
- Hungary (Final Law) reference a detailed framework and list of controls based on **NIST 800-53**.
- Poland (Draft) has chosen to align with recognized international standards, such as **ISO/IEC 27001 and ISO/IEC 22301**, as benchmarks for compliance.
- Ireland's National Cyber Security Centre (NSCS) aims to leverage NIST CSF 2.0 and is also looking at ISO 27001 certification,
- Austria (Draft) puts the focus on risk management and requires entities to demonstrate the effectiveness of these risk measures through a **self-declaration process.**
- Croatia (Final Law) and Luxembough (draft) do not further define specific security controls requirements.

Board level/ management accountability

NIS2 explicitly mandates bodies of essential and important entities to supervise and ensure compliance with risk management measures. This is complemented by a requirement for targeted cybersecurity training for these management bodies, emphasizing the importance of informed leadership in mitigating cyber risks. However the concept of management bodies as specified in the NIS2 Directive is not well defined.

Austria's current draft law **further specifies these management bodies** as executive boards and managing directors of essential and important entities. Meanwhile, Poland's draft law provides a comprehensive definition of a Management Body, inclusive of a broad spectrum of leadership roles, and stipulates explicit responsibilities for cybersecurity oversight, though without additional sanctions beyond those in the directive. Belgium's and Croatia's final NIS2 laws and Hungary's and Germany's draft, on the other hand, are less prescriptive and do not provide a further clarification of management bodies.

Government oversight and audit

Lastly, Member States are tailoring their oversight and audit mechanisms to align with the NIS2 Directive.

Austria's review draft proposes a dual approach: essential entities are subject to **both regular and targeted safety inspections**, while important entities face supervisory measures on a reasonable suspicion basis. Essential entities are required to demonstrate the implementation of risk management measures every three years through an independent audit, marking a shift from the NIS Directive audits.

Similarly, Germany has established a **3-yearly verification process** for operators of critical systems, with random checks for essential entities and occasional audits for important entities. Poland and Croatia simplify the audit frequency to at least once every two years for all entities under its jurisdiction.

Belgium has opted for a **3-yearly cerfication with yearly surveillance audits** for essential entities. Important entities can voluntarely choose for a verified self-assessment. Ireland is simarly looking at a **voluntary certification scheme** to showcase compliance.

Luxembourg, Italy and Finland have yet to define the precise audit frequency but have established the principle of periodic and risk-based audits. Finnish competent authorities retain the right to conduct audits, utilizing parties with the requisite expertise.

[2] Centre for Cyber Security Belgium

In summary: NIS2 transposition requirements and timelines require attention moving forward

Initial analysis of the transposed draft and final laws of the NIS2 Directive across the EU presents a **complex set of nuances to the original Directive**. Member States will continue with the deadline of October 17th in mind.

It is important for organizations to remain vigilant and aware of changes to critical sectors, specifics on management responsibilities, registration protocols and timelines, as well as audit frequencies. The emphasis on management accountability, the adaptation to various national risk management frameworks, and the necessity for timely compliance with registration and audit processes show the importance of a strategic, informed approach to cybersecurity governance.

Collaboration and knowledge exchange will be key to navigating this dynamic environment.

With so many unknowns, is it even possible to start on the implementation of NIS2?

NIS2 compliance, especially for organizations with cross-border operations, might seem very overwhelming at first. That's why focusing on the key areas as outlined in the NIS2 Directive is essential to start preparing on:

- Risk management (a risk-based approach to cybersecurity);
- Management/ board level accountability and specific training and awareness plans;
- Supply chain and third party risk management;
- Incident reporting obligations to (national) authorities;
- Business continuity and the ability to recover from cyber attacks.

The value of public-private partnerships and cross-organization information sharing cannot be overstated. Alliances should help to facilitate the exchange of threat intelligence and collaborative response strategies, significantly enhancing an organization's capacity to identify and respond to specific sectoral cyber threats. The adaptability of an organization's cybersecurity control framework is equally crucial, allowing for the incorporation of new control requirements as legislation gets more clear.

If you have **already implemented ISO 27001** and have a well-functioning ISMS, you are significantly closer to achieving NIS2 compliance. However an analysis should be well made towards the Directive and transpositions when they are available. Large organizations may opt for a centralized approach, or leave the implementation up to local subsidiaries, while maintaining strong reporting lines and situational awareness.

As organizations work towards NIS2 compliance, it is essential to view the directive not as a regulatory hurdle but as an opportunity to elevate their organization's cybersecurity maturity. The distinction between a compliance-driven and a security-driven approach will be a clear indicator of an organization's cybersecurity maturity. By implementing a structured, informed, and collaborative approach to cybersecurity, leaders will not only ensure compliance with the NIS2 Directive but will also contribute to a more secure and resilient digital infrastructure within the EU, which is of course the ultimate goal of the Directive.

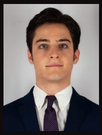
In the coming months, **Deloitte will keep following up** on the transposition of the NIS2 directive in order to provide further guidance. Reach out in case you want to get further updates.

Contacts

Contributors:

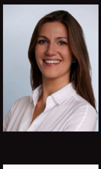
Evert Koks
Director
ekoks@deloitte.com
+32 476659927

Julie Colle
Senior Consultant
jcolle@deloitte.com
+ 32 478608496

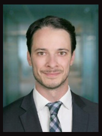


Davide Lo Prete
Senior Consultant
dloprete@deloitte.it
+ 39 3385300577

Subject matter experts:



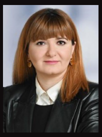
Julia Kitzmüller
Manager
jkitzmueller@deloitte.at
+ 43 1537003779



Balazs Agardy
Senior Manager
bagardy@deloittece.com
+ 36 302392475

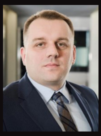
Ratko Drca
Director
rdrca@deloittece.com
+ 38 5916786091

Tapio Rihimaki
Manager
tapio.riihimaki@deloitte.fi
+ 35 8406787470



Tamara Okropiridze
Manager
tokropiridze@deloitte.de
+49 69756957215

Viktor Paggio
Senior Manager
vpaggio@deloittece.com
+42 0725009732



Pawel Klosek
Senior Manager
pklosek@deloittece.com
+48 664199134

Francesco Binaschi
Senior Manager
fbinaschi@deloitte.it
+39 3475399463

Nastassia Salash
Senior Consultant
nsalash@deloitte.lu
+352 621568298

Malik Vaibhav
Partner
vaimalik@deloitte.ie
+353 871504992

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax and legal, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 312,000 professionals, all committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu

Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.