Navigating NIS2 Compliance

March 2026 - 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 a long passed transposition deadline of October 2024.

This whitepaper provides an analysis as of March 2026 of the current regulatory landscape of countries that have transposed NIS2, 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 and the EEA, countries display varied transpositions of the NIS2 Directive, with the following notable highlights:

- **Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Finland, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Malta, Liechtenstein, Portugal, Romania, Slovakia, Slovenia and Sweden have transposed NIS2.**
- **Registration deadlines already passed for a significant number of countries** that have transposed NIS2. Organisations that did not register yet, should do so as soon as possible.
- **Security measures of the transpositions can be categorized in three main approaches:** either a maturity based national cybersecurity control frameworks, a compliance based control framework or more principle based approach. Most countries define their list of required security controls.
- Countries such as Croatia, Hungary, Italy and Slovakia extend beyond the sectors mentioned in the Directive and **add sectors such as education, defence or culture.**
- **Most countries align with the reporting schedule of the Directive**, however Cyprus imposes a 6-hour early warning for significant incidents instead of the standard 24 hours. Lithuania requires an 'automated' incident reporting.

The Directive's emphasis on management accountability is clear, with executive boards and managing directors mandated to ensure compliance with risk management measures.

Government oversight and audit mechanisms vary. In most countries essential entities require audits by a government accredited auditor. Frequency varies between yearly and every 5 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**. The remaining NIS2 laws are expected throughout 2026. Having a strategic cybersecurity control framework to navigate this evolving regulatory landscape will be important moving forward.

The European commision proposed in November 2025 and January 2026 amendments that aim to streamline NIS2. The aim is to clarify sectors in scope, harmonize requirements, align incident reporting and introduce ways to demonstrate compliance with EU based certification (under the revised Cybersecurity Act (CSA2).

It is important to note that next to the EU and the EEA, the United Kingdom and Switzerland are also working on legislation that is heavily inspired by NIS2.

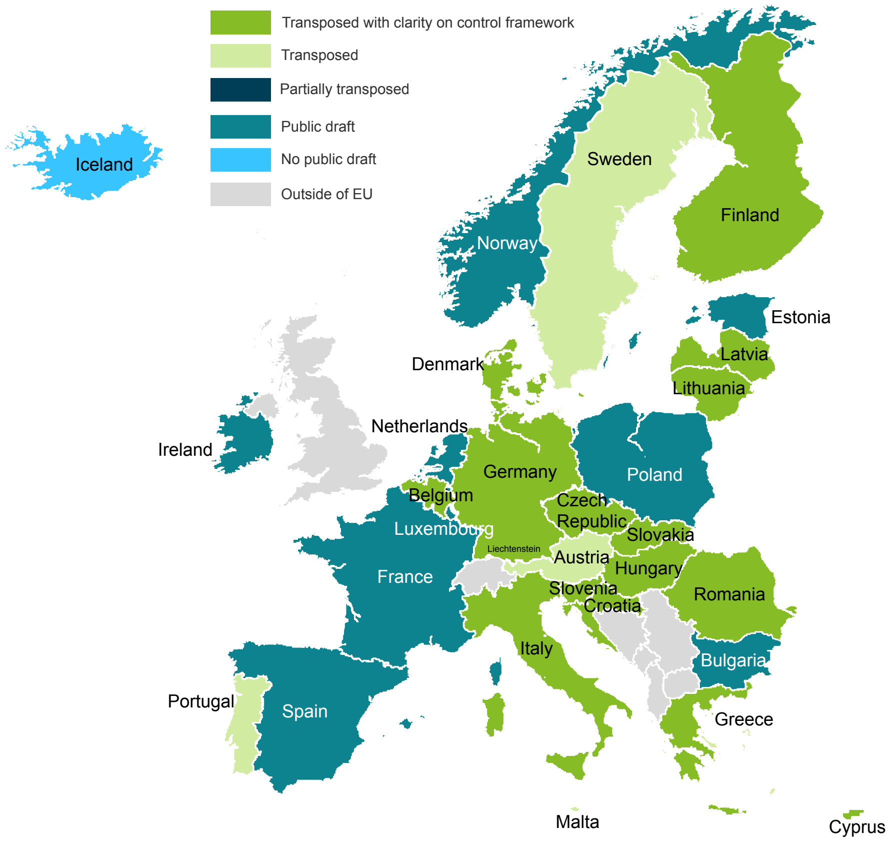
Introduction

The adoption of the Network and Information Security 2 (NIS 2) Directive by EU Member States, 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 everything you need to know about EU NIS2 regulatory landscape as of January 2026, providing a comprehensive overview of its current state focusing on final NIS2 transpositions. Please note that the NIS2 landscape is rapidly evolving on that more laws are expected throughout 2026. 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 some Member States have clearly outlined different requirements and timelines, but with still so many unknowns, organizations may question how to best approach the implementation of NIS2. However even with those differences and uncertainties, waiting would be the least recommended option. **In countries the NIS2 Directive hasn't been transposed in, organisations can already start with common requirements (such as ISO 27001 or NIST CSF)** outlined by the directive and should not lose any time (after all, hackers are also not waiting).

Deloitte's view on the state of NIS2 transpositions in March 2026



The different stages of NIS2 adoption and implementation across the EU

As we are long past the transposition deadline of October 2024, the majority of European union member states have transposed the NIS2 Directive into local law. With all Member States at varying stages of adoption and local transpositions, the new regulatory landscape can quickly become overwhelming, especially for organisations that operate cross-border.

As of March 2026, **18 EU member states have adopted a transposed NIS2 law** in their country, where **notable differences exist in adoption and readiness timelines**. Most remaining countries are expected in 2026. We examine the available final laws in detail. Draft laws were not analysed, but will be included once they become final.

Members of the European Economic Area (EEA) which are not member states also need to transpose the NIS2 Directive. This is the case for Liechtenstein, Iceland and Norway. The NIS2 Directive was planned to be added in the second half of 2025 to the EEA agreement, however this has not happened yet. Also no deadline to transpose NIS2 is set afterwards for the EEA countries. Liechtenstein however has already transposed its local legislation. The United Kingdom and Switzerland are also working on similar legislations to NIS2, but have not finalised them.

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**
- **Reporting requirements**
- **Fines**

The following **final laws were analysed: Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Finland, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Malta, Liechtenstein, Portugal, Romania, Slovakia, Slovenia and Sweden. Liechtenstein** (as part of the EEA) also already transposed NIS2 and was looked into. When additional **decrees, amendments or acts** were issued, these were also analysed.

Essential and important entities

The NIS2 Directive has identified the sectors that are in scope, which has expanded significantly compared to its predecessor NIS1, as visualised below it now includes two classification levels, Essential and Important.

This classification determines the application of different requirements regarding supervision and sanctions. While some Member States align closely with the European Commission's size criteria for classifying essential and important entities, others take a more tailored approach.

NIS2 Sectors

Essential

- 🟦 Energy
- 🟦 Transport (air, rail, water, road)
- 🟦 Banking
- 🟦 Financial market infrastructure
- 🟦 Health
- 🟦 Digital infrastructure
- 🟦 Drinking water
- 🟩 Waste water
- 🟩 Public administration
- 🟩 Space
- 🟩 ICT Service Management (B2B).

Important

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

🟦 Sectors defined by NIS1

🟩 New sectors added by NIS2

For instance, the Lithuanian law specifically lists ICT hosting providers as important instead of essential. Germany distinguishes between very important and important entities, with special requirements for critical facilities.

Most other countries such as Austria, Belgium, Cyprus, the Czech Republic, Slovakia, Slovenia, Sweden, Malta, Finland, Denmark, Greece, Italy and Latvia have essentialy taken over 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, Cyprus, Denmark, Finland, Greece, Lithuania, Malta, Romania, Slovenia and Liechtenstein have chosen to stay within the scope outlined by the Directive itself, without adding new sectors.

Other countries go further. Either by adding additional sectors or clarifying sector boundaries:

- Austria limits the public sector to federal and state institutions, while municipalities and municipal associations are excluded.
- Croatia's 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.
- Czech Republic include the Education sector next to Research and also adds the Defense industry.
- Germany regulates the federal public sector with individual regulations on the regional level, excluding municipalities.
- Hungary includes the National Bank and defensive forces as essential sectors. Companies performing activities related to defense interests are included as well as companies that manufacture cement, lime, and gypsum.

- Italy also includes local public transport providers. Furthermore, the research sector is clarified by including educational institutions undertaking research activities. Also entities carrying out activities of cultural interest are included.
- Latvia's law adds companies that manage and maintain physical road infrastructure. Entities that offer educational information systems are also seen as important.
- Portugal adds higher education institutions.
- Slovakia includes entities that provide meteorological services.
- Sweden explicitely brings regions, municipalities and municipal associations in scope and also added certain private education providers in scope

Sector-wise, we note an interesting overlap with NIS2 in the regulatory landscape with the Digital Operational Resilience Act (**DORA**). In several Member States, like Belgium and Finland, financial entities need to adhere only to DORA, which will supersede NIS2 compliance requirements. 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. Austria explicitely keeps ICT third party providers in scope even where DORA applies.

Important to note is that for certain digital service providers (characterised by the cross-border nature of their services) such as managed (security) service providers, an exclusive jurisdiction is determined by the location of their so-called "main establishment" within the European Union. This means that these organisations will need to comply only to the NIS2 law applicable for this location.

Registration processes

When looking at registration requirements, we see the differences increasing on one hand regarding **registration modalities** and on the other hand regarding **registration deadlines**.

In a number of countries, registration is not primarily driven by self-registration, but by identification and outreach by the competent authority. In the case of Croatia, 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 organisations in scope.

Similarly, in Cyprus and Lithuania, entities will be identified by the relevant national authority.

Most countries however rely on clear self-registration, often via an online portal. A number of countries have email based submissions. In Greece registration is done by email until the designated platform becomes available. In Latvia a signed form is used (rather than fully web-based)

For the following countries the **registration period has passed**:

- For Hungary, the deadline was October 2024.
- In Romania, the original deadline was December 2024.
- Greek entitities had a two month registration window which ended on January 2025.
- Belgium's law allowed for a five-month period to register by February 2025.
- In Liechtenstein entities had to register by February 2025.
- The Italian deadline to register has passed (February 2025), with an annual registration/update cycle from January 1st till February 28th each year.
- In Lithuania, the deadline for identification has already passed (April 2025).
- Latvia's deadline was April 2025
- For Finland, entities needed to register with the relevant competent authority by May 2025.
- In Denmark the deadline was October 2025

For a number of other countries, the **registration period is still active or due to open**:

- For Austria the deadline to register is January 2027.
- In Germany entities need to register within 3 months, after transposition, resulting in the deadline being March 2026.
- Portugal put the deadline on June 2026.
- In Sweden the portal is scheduled to launch when the law comes into force on January 15th.
- Malta does not have specific deadlines for registration.
- Sweden mentions to register as soon as possible.

Most countries have or are creating an online portal by which companies can register themselves. Examples are Austria, Belgium, Germany, Italy, Hungary, Slovakia, Czech Republic and Lithuania. They require entities to submit information. In most cases contact details need to be shared, along with technical information such as IP addresses.

Lithuania expands the scope of the portal not only registration functionalities but also real-time to threat intelligence sharing and other NIS2-relevant services.

Some countries operate with distributed or sectoral registration rather than a single central point. Finland is an example where registration is done with the relevant sectoral authority.

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

- Belgium is engaged through public consultations, public-private working groups and conferences. On the website of the CCB[1] template security policies are shared, as well as tools to facilitate risk assessments per sector and current state assessments of the security controls.
- Cyprus: made various security policies and and plans available on the government website.
- Hungary is engaged in extensive outreach through public consultations and media to disseminate information.
- Italy: has issued an extensive list of FAQS.

Timelines

In order to give entities in scope time to adhere to the stricter requirements, countries define timelines by which the entities need to be compliant. These timelines often reflect a phased approach, prioritizing initial registration and identification, followed by the implementation of security measures and finally audit and verification processes.

Some countries do not define timelines, such as for Cyprus and Malta, assuming compliance from the date the transposition enters into force. Some countries only define timelines for registration (like Germany, Denmark and Liechtenstein). Most countries however define overall deadlines, or tie the timelines to the initial registration.

[1] Centre for Cyber Security Belgium

Notable compliance and implementation timelines are the following:

- **Austria**: requires a self-declaration in 12 months after registration.
- **Croatia**: stipulates that competent authorities must complete the identification of entities in scope. Once entitities receive the notification they have one year to implement the cybersecurity measures.
- **Belgium**: requires important entities to become compliant with all relevant controls by April 2026 and essential entitities by April 2027. For essential entities this means certification against the Belgian control framework (cyberfundamentals) or ISO 27001 certification for the complete legal entity in scope.
- **Croatia**: stipulates that competent authorities must complete the identification of entities in scope. Once entitities receive the notification they have one year to implement the cybersecurity measures.
- **Czech Republic**: organisations have 1 year to implement the required security measures and to have incident reporting processes in place. For measures not in place each organisation needs to document its own implementation deadlines.
- **Finland**: entities must have established a risk management procedure by July 2025.
- **Greece**: mentions that by February 27th 2025 the cyber risk measures to be taken, should have been approved by management and the implementation should have started to be monitored.
- **Hungary**: requires organisations to conduct a cybersecurity audit by June 2026. Contracts with auditors should have been completed by August 2025 already. By June 2025, entities must have submitted their information security policy and a security classification of existing electronic information systems.
- **Italy**: requires organisations to be compliant by October 2026 (transition period). The obligation to notify significant incidents must be met within 9 months.
- **Latvia**: entities needed to submit their firstcompliance self-assessment report by October 2025. Incident reporting is active since July 2025.
- **Lithuania**: foresees 12 months for implementing the cybersecurity requirements like automatic incident reporting, and 24 months for certain technical requirements.
- **Portugal**: the law enters into force 120 days after publication, resulting in the law becoming active in April 2026. Risk management and reporting obligation go into effect 24 months thereafter.
- **Romania**: outlines a multi-step process after initial notification:
  1) after 60 days a risk assessment needs to be performed, followed by
  2) an initial self-assessment after 60 days and
  3) essential entities need to submit a remediation plan after 90 days.
- **Slovakia**: allows for 12 months to implement security measures after registration. First audits for essential entities are due within 2 year of registration, while important entities have 5 years to perform the first audit.
- **Slovenia**: allows for 12 months to implement measures after registration.

The variance in timelines underscores the importance for organisations operating cross-border to closely monitor deadlines applicable in each country.

Cyber Security requirements

When looking at how security measures are defined and implemented per country, differences in approaches become clear. While the NIS2 directive outlines a minimum set of 10 risk and cybersecurity measures, the specificity and prescriptiveness of national transpositions vary considerably.

Overall the security measures of the transpositions can be categorized in three approaches: either a maturity level-based (CMMI) national cybersecurity control framework, a compliance based control framework or more principle based approach.

The countries that have established a maturity level based national cybersecurity control frameworks are:

- **Belgium:** has established their maturity based cyberfundamentals framework, mainly based on the NIST CSF v2, providing a structured baseline of controls for organisations to follow. Maturity level 3 is required for important entities and 3,5 for essential entities. The initial 2023 version of the framework was updated to a new version in 2025 version aligning the framework with NIST CSF 2.0. As an alternative, Belgium also accepts an ISO 27001 certification.
- **Romania** also adopted the Cyberfundamentals Framework, and Ireland is planning to also do so in their upcoming transposition.

- **Cyprus:** defines around 70 controls split accross Prevent, Protect, Detect and Repond pillars. The controls are maturity based with level 3 being the minimum compliance level for both important and essential entities.

On the other hand, countries that have established a compliance based approach, in which controls are considered in place or not (binary yes/no), are:

- **Italy:** leverages their Framework Nazionale per la Cybersecurity e la Data Protection edition 2025 which further specifies the NIST CSF 2.0 requirements with specific controls for essential and important entities
- **Croatia:** defines 13 control areas with specific sub-measures. Additional guidance is foreseen for IT and OT environments. Three levels of measures are foreseen (basic, medium and advanced) which entities must implement based on a national risk assessment framework.
- **Hungary:** requires organisations to classify their information systems into basic, significant and high security classes. Depending on the security class, a detailed framework and list of controls based on NIST 800-53 needs to be implemented. Deviations are allowed if justified by a risk assessment and approved.
- **Latvia:** defines 50 to 70 mininum security measures, spread accross 3 system classes to differentiate requirements.
- **Lithuania:** clarifies the security measures of the NIS2 Directive by defining 76 requirements appicable to both essential and important entities.
- **Liechtenstein:** specifies between 30 and 40 measures to further clarify the NIS2 Directive measures.
- **Slovakia**: defines a framework of 151 controls.
- **Slovenia**: specifies 17 mandatory measures and mandates an ISMS and BCMS with specific documentation requirements.
- **Czech Republic**: defines a framework with 91 controls.
- **Greece**: defines 25 control objectives linked to a more detailed self-assessment.

The last category of countries take a more **principles/ risk based approach**. These are:

- **Finland:** takes a more principles-based approach and adopts a risk-based approach rather than prescribing mandatory controls. The legislation sets a minimum level for risk management obligations, including establishing and maintaining a risk management policy and defining risk management principles. The Finnish agency Traficom provides recommendations rather than formal requirements and advises that other local NIS2 supervisory authorities also adopt them.
- **Germany:** requires organisations to take a state of the art (Stand der Technik) approach. For the federal government the BSI IT-grundschutz is specified, but no control framework is mandated for the private sector.

Some countries have not yet clarified the specific security controls needed, such as Austria, Denmark, Portugal and Malta. In Sweden this is planned for April 2026.

Specific requirements

Beyond the adoption of control frameworks, several countries have incorporated **additional specific obligations often linked to documentation, reporting or specific security practices**:

- **Greece:** mentions a cybersecurity policy for which a template will be provided. This policy for each entity will need to be approved by the government and shared afterwards on a yearly basis.
- **Germany** requires **attack detection systems** for critical facilities (a type of essential entity).
- **Belgium:** expands the 10 cybersecurity risk-management measures from Article 21 with a new measure, namely a coordinated vulnerability disclosure policy.
- **Lithuania:** expands on the aspects required by the directive with a mandatory policy for granting and managing access rights of users, administrators, suppliers and their subcontractors.
- **Malta:** adds logging and traceability of network and information systems as specific requirements.
- **Hungary:** requires the payment of an annual cybersecurity monitoring fee to the government.
- **Latvia:** requires a documented 'cyber risk management and ICT business continuity plan'
- **Romania:** requires participation in simulations or exercises coordinated by the national cybersecurity agency.

These changes indicate that next to implementing a national control framework, specific requirements still need to be analysed to ensure full compliance.

Appointment of specific formal roles

Next to requiring specific cybersecurity measures, a number of countries require the formal appointment of specific roles within entities in scope:

- **Czech Republic:** mandates the appointment of specific roles (e.g. Cybersecurity Manager, Cybersecurity Auditor, Cybersecurity Architect) and requires a cybersecurity management committee for higher-obligation entities.
- **Germany:** requires only for federal entities the appointment of an Information Security Officer and at least one deputy.
- **Portugal:** requires the appointment of a cybersecurity officer
- **Lithuania:** mandates the appointment of a cybersecurity manager and security officer, with experience and qualification requirements (at least two years of experience). Additionally these roles can not perform IT/network administration functions to ensure seggregation of duties.
- **Latvia:** requires the formal appointment of a cyber security manager. This individual must attend annual cybersecurity trainings organised by the government.
- **Cyprus:** requires the appointment of a person responsible for network and information security.
- **Hungary:** requires the appointment of a security officer who requires a clean criminal record and possesses the necessary qualifications and experience.
- **Greece:** requires the appointment of a competent executive as an Information and Communication Systems Security Officer (YASPE). This role must have appropriate qualifications, expertise and a level of autonomy in decision making. Its duties are incompatible with those of a Data Protection Officer (DPO).
- **Slovakia:** requires the appointment of a cybersecurity manager with specific operational and reporting requirements, including performing self-assessments.
- **Malta:** requires the appointment of a security liaison officer who must possess necessary expertise and be formally responsible for business continuity, risk assessments, and security plans.
- **Romania:** requires the appointment of a person with managerial authority, reporting directly to the CEO, and who operates independently from IT and OT. This person must obtain an accredited cybersecurity course within 12 months of designation.
- **Croatia:** defines that entities requiring "medium" or "advanced" levels of cybersecurity risk, must formally appoint a person who is operationally reponsible for cybersecurity at the entity level.
- **Belgium:** requires as part of its control framework a formally appointed communications officer.

Other countries such as Austria, Denmark, Finland, Sweden, Slovenia, Italy and Liechtenstein, do not require the appointment of specific named roles beyond requiring a general contact person.

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 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. Most countries closely reflect the directive on this topic and do not provide a further clarification of management bodies, nor define a frequency by which the training needs to be organised.

However certain countries are more descriptive on defining board and management bodies:

- **Italy:** defines management bodies as Board of Directors. The accountability is extended to also include approvals of cyber security plans (e.g. business continuity or vulnerabity management)
- **Finland:** requires that management bodies require sufficient expertise in cybersecurity risk management.
- **Romania:** mandates that management bodies undergo an accredited professional training recognized by the national authority (DNSC).
- **Lithuania:** requires training for management every two years, which must include the head of the entity. This training needs to be conducted in line with requirements of the national cybersecurity centre.
- **Hungary:** further clarifies management bodies as the head of the organisation as well as the person responsible for information security.

- **Germany:** explicitly excludes the management of public administration institutions in their definition of management bodies and exempts them from NIS2 management duties.
- **Croatia:** wants continuous engagement of management and requires that the training for management bodies includes cyber threats, cybersecurity best practices and the importance of proactive risk management.

Cybersecurity training for employees

Beyond the accountability and training requirements for management bodies, the NIS2 Directive includes cybersecurity and awareness programs for employees as the minimum security measures.

While the Directive does not prescribe a frequency, certain countries have introduced specific cadences. **Lithuania, Latvia and Greece require a cybersecurity training for employees at least once a year.**

Government oversight and audit

One important aspect is the degree of oversight that different countries require. **Most countries implement regular, proactive government accredited audits**, for entities classified as essential, with reports and remediation plans submitted swiftly thereafter to the government.

- **Belgium:** has opted for a 3-yearly certification scheme with yearly surveillance audits for essential entities. Important entities can voluntarely choose for a verified self-assessment. Auditors must be accredited by the Belgian Cybersecurity centre (CCB).
- **Czech Republic:** requires essential entities to conduct a formal cybersecurity audit at least once every two years, with the full scope covered at least once every five years. Important entities are subject to a yearly self-assessment.
- **Germany:** requires operators of critical facilities (a type of essential entity) to provide a proof of compliance every 3 years. For other essential entities the authority can order proofs/audits but there is no defined frequency.
- **Croatia:** requires entities to undergo a security audit at least every two years by government accredited parties. This is complemented by a periodic expert supervision by the government every 3 to 5 years.
- **Hungary:** specifies cybersecurity audits every two years, with the first audit being due two years after registration. In addition, these audits should also include vulnerability assessments, penetration testing and source code reviews for higher risk systems. Auditors need to be accredited by the local government body (SZTFH).
- **Romania:** requires an initial audit after one year, followed by audits every two years. Auditors must be certified by the government (DNSC), and there's an auditor rotation requirement after 3 years.
- **Slovakia:** requires essential entities to undergo the first audit within two years, with subsequent frequency set by the national authority.
- **Slovenia:** requires essential entities to perform a compliance assessment at least once every two years performed by certified auditors.
- **Austria:** only requires "proof by independent audit" on request. The proof must be an audit or risk analysis not older than two years. Audits must be performed by government accredited auditors. Essential entities have proactive oversight, but frequency has not yet been defined.
- **Portugal:** Essential entities have proactive oversight, but frequency has not yet been defined.

For some countries the frequency is defined and for others it is not yet defined. This is the case for example for Denmark, Italy, Malta, Liechtenstein and Greece.

For important entities most countries do not require mandatory audits. However, some countries do require them:

- **Czech Republic:** Important entities are subject to a yearly self-assessment.
- **Slovakia:** requires periodic self-assessment of important entities, but requires an audit every 5 years.
- **Lithuania:** requires all cybersecurity entities (both essential and important) to conduct a cybersecurity audit at least once every three years by government accredited auditors.
- **Romania:** audits for important entities are set in a risk-based manner.
- **Slovenia:** Important entities must perform a self-assessment at least every two years.
- **Cyprus:** takes a different approach and a risk-based annual audit program is defined by the government that specifies which entities are to be audited.
- **Latvia** and **Finland:** do not require regular audits,

neither for essential nor important entities.

Reporting requirements

Most countries stick to the multi-stage reporting timelines from the Directive. Only Cyprus deviates by requiring that the early warning notification is done after 6 hours. Lithuania on the other hand requires an 'automated' incident registration. Some countries also add specific national nuances, for example the Czech Republic includes an "intentional causation cannot be excluded" trigger and requires certain entities to define an "acceptable level of harm". Germany adds extra reporting requirements for operators of critical facilities.

Reporting mechanisms also vary. Most countries have set up an online portal to register incidents. However, Greece requires incident registration by e-mail. The Portuguese transposition also requires the issuance of technical instructions on incident taxonomies and thresholds which have not yet been released.

Regarding the **definition of a 'significant' incident**, Croatia, Lithuania, Hungary, Slovakia and Liechtenstein provide additional criteria in the law to determine what is significant (e.g. monetary thresholds or qualitative thresholds). Other countries such as Belgium provide further guidelines. The European agency Enisa also provides more details in its guidelines. In its NIS2 implementing act, the EU also defines what significant incident means for selected sectors.

Fines

The NIS2 Directive establishes significant administrative fines for non-compliance, up to 10 million euro or 2% of the global turnover and personal liability for management bodies. Most countries closely follow these fines in their transposition.

Croatia however also add **direct fines for responsible individuals in management**. Portugal and Slovenia also include direct fines for responsible individuals in management. Denmark also states that for essential entities **management can be sent temporarily relieved from their duties**.

Some countries also add fine for admistrative aspects, such as registration. Romania, Slovakia and Austria also includes a lower tier for administrative breaches (such as failing to register, to update data, or obstructing an inspection). The majority however does not identify a fine structure for these more administrative aspects.

Moving forward, as fines are imposed, it will become clearer how significant they will be.

NIS2 Directive is evolving

The European commision proposed in November 2025 and January 2026 amendments that aim to streamline NIS2. The aim is to clarify sectors in scope, harmonize requirements, align incident reporting and introduce ways to demonstrate compliance with EU based certification (under the revised Cybersecurity Act (CSA2).

While not final yet, these proposed amendments show how NIS2 might evolve. Key highlights are:

- Currently organisations of more than 250 employees are considered large organisation and categorised as essential. The proposition is to consider large organisation as of 750 employees and between 250 and 750 mid-sized and only important.
- Specific clarification per industry are proposed, like a minimum threshold of 1 MW for energy producers. For the chemical sector distribution is proposed to be removed while manufacturing and production remain.
- EU cyber security certifications that demonstrate compliance with NIS2 requirements. National authorities may not subject organisations to additional security audits for these aspects.
- Proposed streamlined reporting where now organisations need to submit incidents to all counties with an active NIS2 law.

In summary: NIS2 transposition requirements and timelines require attention

The analysis of the transposed final laws of the NIS2 Directive across the EU shows a **complex set of nuances to the original Directive**. Now that the deadline of October 17th 2024 has long passed, along with initial registration requirements for some countries, other countries still have not transposed the Directive with expectations going towards the end of 2026 or later.

As most organisations have already started working on compliance towards NIS2, this fragmented landscape will pose challenges. This is especially the case for multinationals with activities in countries for which NIS2 is not fully transposed for all countries it is active in. For those who assumed that the impact of NIS2 would be clear by the transposition deadline, we will have to remain patient for at least a couple more years.

A lesson from performing this analysis is that companies should follow up on draft laws and monitor when they are finalized. We noted significant changes to the texts during the legislative process. Focus should be on finalised laws or overall preparatory efforts that focus on increasing the overall cybersecurity maturity. With the proposed amandments to NIS2, the EU underscores this current complexity.

It is important however for organizations to remain vigilant and aware of specifics in transpositions on management responsibilities, registration protocols and timelines, as well as audit frequencies as they arise. Organisations should identify how their current cybersecurity implementation compares to more strict cybersecurity requirements in certain countries.

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

With 18 countires having transposed NIS2, how to best organise the implementation?

NIS2 compliance, especially for organizations with cross-border operations, might seem very overwhelming at first. For countries with a finalised local law, the requirements are tangible, but for other countries the unknowns remain. That's why leveraging existing control frameworks (such as ISO 27001/2 and NIST CSF) and focusing on the key areas as outlined in the NIS2 Directive is essential to start measuring compliance 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.**

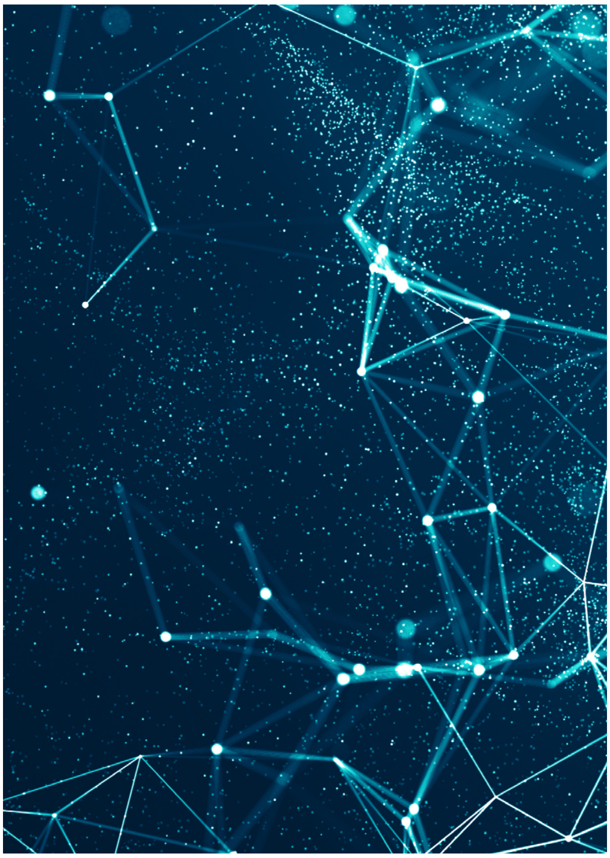
If a country has already transposed, use that as reference frame and build on that. These aspects should form the basis of the cyber roadmap both in the short term and long term.

The adaptability of an organization's cybersecurity control framework is equally crucial, allowing for the incorporation of new control requirements or mappings towards them 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 made towards the Directive and transpositions when they are available. Large organizations may opt for either 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. Choices also need to be taken with this in mind. 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 and proposed EU amandments, in order to provide further guidance. Reach out in case you want to get further updates.



Overview of legislation per EU country

Country	Status NIS2 law	Expected entry into force	Link to local NIS2 legislation	Link to local NIS2 underlaying regulation / recommendation or control list	Link to registration website
Austria	Final		Link	Not yet available	For now, there is no registration website.
Belgium	Final		Moniteur belge (fgov.be)	Link	Register my organisation | CCB Safeonweb
Bulgaria	Draft	2026	Not yet available	Link	Not yet available.
Cyprus	Final		Link	Link	Not yet available.
Croatia	Final		Link	Annex 2 of the regulation	Not applicable.
Czech Republic	Final		Link	Link Link	Portál NÚKIB (gov.cz)
Denmark	Final		Link	Link	The link has not yet been determined, but it is anticipated that registration will be conducted through this government portal: https://businessindenmark.virk.dk/
Estonia	Draft		Link	Not yet available	Not yet available
Finland	Final		Link	Link	Registration with relevant sectoral authority.
France	Not transposed	2026	Not yet available (no offical document).	Not yet available.	Link
Germany	Final		Link	Link	Link
Greece	Final		Link	Not yet available.	By email to register.ncsa@cyber.gov.gr
Hungary	Final		Link	Link	Link
Ireland	Draft	2026	Link	Potentially the CyFun framework	Not yet available.
Italy	Final		Link	Link	Link
Latvia	Final		Nacionālās kiberdrošības likums	Not yet available.	Not yet available.
Lithuania	Final		XIV-2902 Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas (e-tar.lt)	Link	Link
Luxenbourg	Draft	H1 2026	292642.pdf (chd.lu)	Not yet available	Link
Malta	Final		Link	Not yet available.	Not yet available.
Netherlands	Draft	H1 2026	Link	Link	Link
Norway	Draft	H2 2026	Not yet available	Not yet available.	Not yet available.
Poland	Draft	H1 2026	Link	Not yet available.	Not yet available
Portugal	Final		Not yet available	Not yet available.	Not yet available.
Romania	Final		Link	CyFun framework	Not yet available.
Slovakia	Final		Link	Not yet available.	Link
Slovenia	Final		Link	Not yet available.	Not yet available.
Spain	Draft	H1 2026	Not yet available	Not yet available.	Not yet available.
Sweden	Final		Link	Link Control list foreseen for april 2026	Link
Iceland	No draft	H2 2027	Not yet available	Not yet available	Not yet available
Liechtenstein	Final		Link	Link	Not yet available

Contacts

Contributors:

Evert Koks
Director
ekoks@deloitte.com
+32 476659927

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

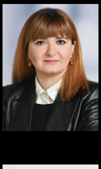
Subject matter experts:

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 Riihimäki
Senior Manager
tapio.riihimaki@deloitte.fi
+ 358 406787470



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

Remco van Mosel
Partner
rvanmosel@deloitte.nl
+31 882861570

Lorenzo Russo
Partner
lorusso@deloitte.it
+39 3401766111

Malik Vaibhav
Partner
vaimalik@deloitte.ie
+35 314173440

Albin Finne
Director
alfine@deloitte.se
+46 700802163

Maxime Verac
Partner
mverac@deloitte.lu
+35 2661451546

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.