WHITE PAPER

Omada

Charting the Path to NIS2 Compliance

Contents

Charting the path to NIS2 compliance

Identity is the new perimeter and identity goverance is essential to ensure NIS2 compliance

The European Union (EU) recognizes that information systems and networks, such as the public internet, have become essential to the fabric of our interconnected society. However, cyber threats—whether originating from nation states, organized crime syndicates, hacktivist groups, cybercriminals, or even disgruntled employees—pose significant risks to the security, privacy, and well-being of citizens as well as the stability of the European economy.

The saying "Identity is the new perimeter" has been widely embraced by security experts and practitioners, signifying a major shift in cybersecurity strategies. In the past, organizations heavily depended on network perimeters—firewalls, secure gateways, and other boundary defenses—to safeguard their digital assets. However, with the shift to cloud computing, remote workforces and the use of mobile devices, these traditional boundaries have become less effective. As a result, the focus has moved toward identity as a crucial aspect of security.

The need for cyber regulation within the EU was clear when ENISA (The European Agency for Cybersecurity) surveyed organizations across five EU member states (France, Germany, Italy, Spain and Poland) and 60% reported major information security incidents. 43% of organizations surveyed experienced information security incidents with financial impacts of up to € 500.000 [1].

In response, the NIS2 directive is an enhanced cybersecurity framework enacted by the European Union (EU) on January 16, 2023, with a deadline for member states to transpose and implement it by 17 October 2024. This means that by this date, all EU member states must have enacted national legislation that aligns with the requirements set out in NIS2.

As European nations work to transpose this directive into national law, the resulting preparation for NIS2 compliance is driving a surge in cybersecurity spending. This paper evaluates how Identity Management solutions assist organizations with NIS2 compliance and enhance their overall cybersecurity posture.

Which industry sectors and companies does NIS2 relate to?

NIS2 covers all entities with at least 50 employees and an annual turnover of 10 million EUR or more, focusing on those that provide essential or important services to the European economy and society. This includes companies, suppliers, and even organizations based outside the EU, as long as they deliver services within the EU.

The directive aims to fortify the security and resilience of critical infrastructure to secure the European economy, significantly expanding its scope from the first iteration of NIS to include not only healthcare, finance, energy, cloud computing, social networks, and digital services but also a broader range of sectors. NIS2 encompasses both "essential" and "important" entities across various sectors such as **transport (air, rail, water, and road), banking, financial market infrastructures, drinking water supply and distribution, wastewater management, digital infrastructure (including cloud services and data centers), public administration, space, postal and courier services, waste management, food production, manufacturing (including medical devices and electronics), and research.**

This expansion underscores the directive's goal to enhance cybersecurity across a wider spectrum of critical services and infrastructures within the EU, ensuring a more resilient and secure European economy and society.

[1] https://www.enisa.europa.eu/publications/nis-investments/

This directive imposes a legal requirement on businesses operating within the EU or providing services to EU markets, especially those involved in critical infrastructure.

NIS2 also increases **personal accountability** for company executives and introduces severe **penalties for non-compliance**, such as fines of up to **€10 million** or **2%** of global turnover.

State of the Union

The transposition of the NIS2 Directive into national law poses significant challenges for EU member states. Harmonizing the directive's stringent cybersecurity requirements with diverse national legal frameworks has proven complex. Many countries face legislative delays due to the intricacies of aligning existing laws with NIS2 mandates, resource constraints, and the necessity for thorough stakeholder consultations. Additionally, expanding the directive's scope to include a wider range of sectors and entities requires substantial efforts in raising awareness and providing support to organizations unaccustomed to such regulatory obligations. Ensuring consistent implementation across the EU is critical to prevent regulatory disparities that could affect cross-border operations and the collective cybersecurity posture.

To better understand the varied progress [2] among EU member states, the transposition process can be categorized into four distinct stages:

Stage 4 - Transposed

Countries at this stage have successfully transposed the NIS2 Directive into their national legislation, meeting the EU requirements ahead of the enforcement deadline. National laws and regulations are in place, and organizations within these countries are now legally obligated to comply with the new cybersecurity measures and standards. **Countries in Stage 4 include Belgium, Hungary, Croatia, and Latvia.**

Stage 3 - Drafts Submitted

Member states in this stage have developed and submitted draft legislation to transpose the NIS2 Directive. These drafts are undergoing review, feedback, and approval within their legislative bodies. While final approval is pending, organizations should begin preparing for compliance based on available draft information. **Countries in Stage 3 include Austria, Cyprus, Czech Republic, Finland, Germany, Greece, Italy, Lithuania, Luxembourg, Netherlands, Poland, Slovakia, Slovenia, and Sweden.**

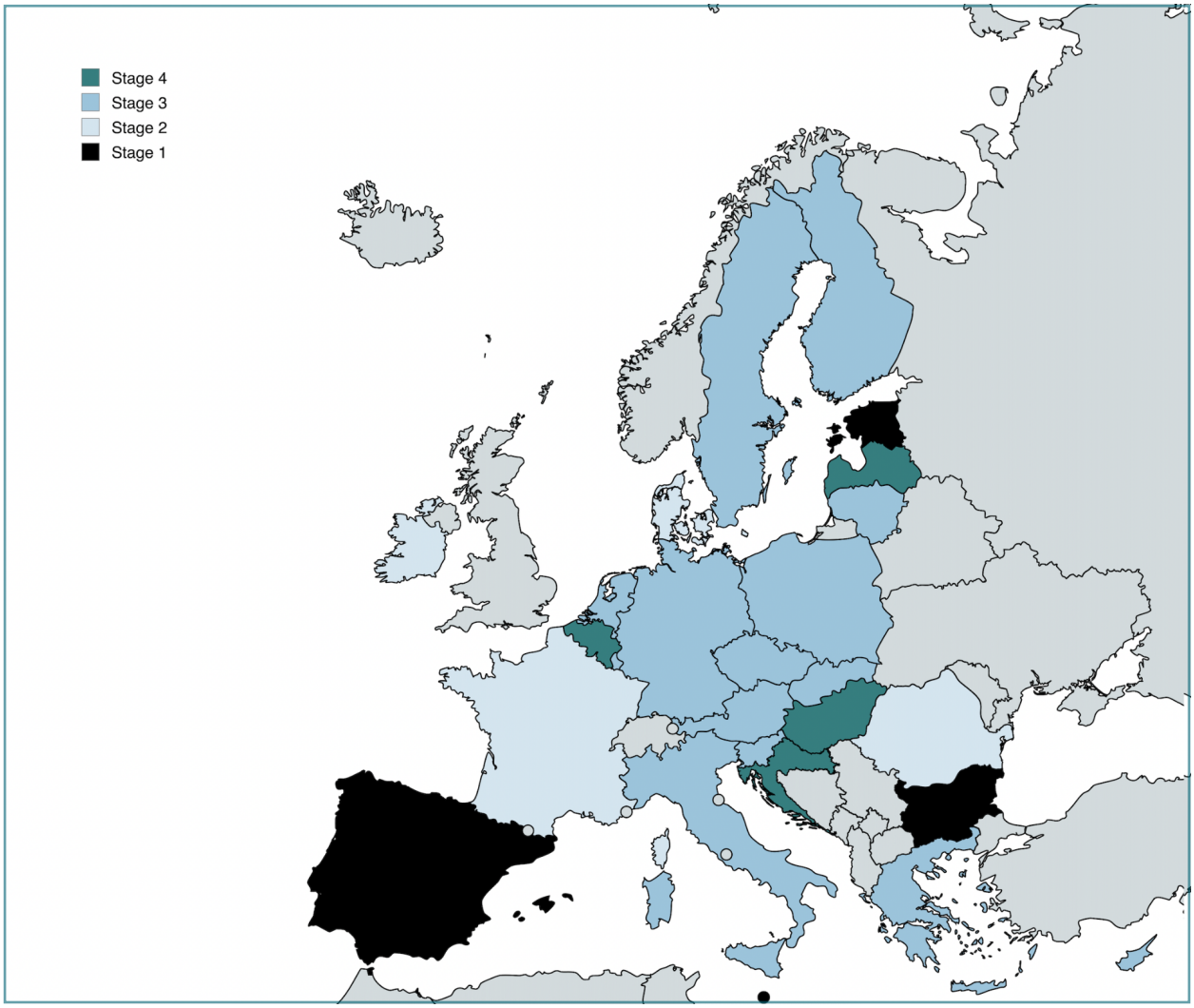
Stage 2 - Initial Progress

Countries at this stage have initiated the transposition process but are still in the early phases. They have started developing drafts or proposals but face delays and have not yet produced comprehensive legislative drafts. Organizations may have limited information on forthcoming obligations, making preparation challenging. **Countries in Stage 2 include Denmark, France, Ireland, and Romania.**

Stage 1 - Minimal Progress

Member states in this stage have made little to no progress in transposing the NIS2 Directive into national law. Public information on their efforts is scarce or non-existent. Organizations in these countries lack guidance on future regulatory requirements, leading to uncertainty. **Countries in Stage 1 include Bulgaria, Estonia, Malta, Portugal, and Spain.**

[2] As of October 1st, 2024



In preparation for NIS2 Compliance

For companies either in the process of aligning with NIS2 requirements or planning to embark on this compliance journey, understanding the directive's implications is essential. NIS2 introduces stricter cybersecurity obligations, expands the scope of regulated entities, and imposes more severe penalties for non-compliance. Navigating the complexities of this new regulatory landscape requires proactive engagement, comprehensive risk assessment, and strategic planning. By preparing diligently for NIS2 compliance, companies not only mitigate legal and financial risks but also enhance their resilience against cyber threats, safeguard critical operations, and build greater trust with customers and partners in an increasingly secure digital ecosystem. Although it is highly encouraged for companies to consult official sources and national authorities for the most current information and guidance on NIS2 compliance, here are a number of key measures recommended for companies to undertake:

- **Risk Assessment and Gap Analysis:** Identify gaps between existing cybersecurity measures and NIS2 requirements, focusing on access management, data protection, and supply chain security. This whitepaper provides a distilled and summarized checklist of NIS2 obligations as specified in the directive (https://www.nis-2-directive.com/) in Appendix A.

- **Implement Cybersecurity Controls:** A foundational key to achieve regulatory compliance, maintain a solid cyber hygiene and mitigate the risks from threat actors, is to adopt and implement a cybersecurity framework. There are several such frameworks that all provide similar goals, e.g. ISO 27000-standards

family, NIST CSF or CIS-18, to mention a few prominent ones. By adopting a security framework, key measures to strengthen defenses will be safeguarded by the controls in the framework of choice.

- **Training and Awareness:** Regular training on cybersecurity, emerging threats, and access management is crucial for employees and leadership.
- **Update Incident Response Plans:** NIS2 mandates comprehensive incident response and recovery plans, requiring organizations to notify relevant authorities of incidents within 24 to 72 hours.
- **Engage Third-Party Audits:** Regular audits focusing on internal systems and third-party vendors are essential for maintaining compliance.
- **Strengthen Supply Chain Security:** Third-party providers must also comply with NIS2, and organizations should implement robust security requirements across their supply chains. This activity needs to take into account the obligations to notify authorities within the specified deadlines.
- **Prioritize Identity Access Management (IAM):** With identity security being recognized as the frontline defense and primary entry point to any network or system, strengthening identity security is crucial for companies aiming to reduce their attack surface, comply with regulations such as NIS2, and support best practice initiatives like Zero Trust Architectures (ZTA). NIS2's Article 21.2(j) specifically stipulates *"the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications, and secured emergency communication systems within the entity, where appropriate."* Therefore, implementing IAM solutions that incorporate multi-factor authentication (MFA) and continuous authentication not only aligns with regulatory requirements but also enhances the overall security posture of the organization. Consider IAM as encompassing many disciplines and managing various types of identities, including suppliers, contractors, non-human entities, workloads, workforce, and consumer identities across a range of business processes such as authentication, authorization, and governance, risk, and compliance (GRC).

The **NIS2 Directive** demands that organizations manage cybersecurity risks comprehensively. This includes managing and continuously monitoring access and entitlements, as identity has repeatedly proven to be the most prominent attack vector.

Implementing an **Identity Governance and Administration (IGA)** solution plays a vital role in meeting these regulatory requirements as they apply both internally, to the organization's workforce, and externally, to the supply chain.

How Identity Governance aligns with NIS2

IGA solutions are a compelling option for organizations striving to meet the stringent requirements of the NIS2 Directive and enhance their cybersecurity posture. The directive underscores the imperative for essential and important service providers to establish robust cybersecurity measures and maintain proper cyber hygiene.

By aligning with NIS2 compliance mandates and industry-specific standards—like those in healthcare and other essential and important services sectors, IGA plays a pivotal role in enforcing access control policies, managing identity privileges, and enhancing cybersecurity risk management. These are all fundamental aspects of NIS2 compliance. IGA not only helps organizations achieve compliance but also strengthens their overall cybersecurity framework, ensuring both internal security measures and external partnerships adhere to the highest standards.

Cybersecurity Risk Management Measures

NIS2 emphasizes a holistic approach to risk management, addressing both technical vulnerabilities and human factors. IGA systems enhance risk management by enabling systemic controls over access, privileges, and identity behaviors, ensuring that only authorized individuals can access sensitive systems and data. This mitigation strategy addresses insider threats and human errors, which are significant contributors to security incidents.

How IGA Helps: IGA streamlines access governance, enforces consistent security policies, and monitors user activities in real-time. This proactive approach allows organizations to identify and address potential threats before they escalate, strengthening overall resilience to cyberattacks.

Enforcing the Least Privilege Security Principle

A fundamental cybersecurity measure aligned with NIS2 is the enforcement of the least privilege principle, which restricts user access to only what is necessary for their roles.

IGA's Role: By managing user identities and controlling access rights based on job responsibilities, IGA ensures that sensitive systems and data are accessible only to authorized users. This minimizes the attack surface by preventing privilege escalation and unauthorized access, thereby reducing the risk of internal threats and accidental breaches.

Regular Access Reviews: IGA solutions facilitate regular automated access reviews and certifications, as implicitly promoted under Article 21.2(i) of NIS2. Organizations can maintain continuous compliance by periodically evaluating who has access to data and systems, ensuring that access rights are appropriately adjusted as necessary.

Access Control Policies

Under NIS2, effective management of access control policies is crucial to ensure that users have appropriate access levels to critical infrastructure and services, extending to both human resources security and access to sensitive information systems.

How IGA Helps: IGA facilitates role-based access control (RBAC), ensuring that employees and third parties have access only to the resources needed for their job functions. By automating access management, IGA minimizes manual errors and prevents unauthorized access, ensuring compliance with NIS2's access control provisions.

Vulnerability and Threat Management

Protecting stored, transmitted, and processed data is a core requirement of NIS2, which includes shielding information systems from vulnerabilities and proactively managing threats.

How IGA Helps: IGA systems assist in managing user privileges and monitoring activities across networks to swiftly detect anomalies or unauthorized access. This capability supports the organization's ability to maintain data integrity and quickly respond to potential threats.

External Compliance and Supply Chain Security

NIS2 places significant emphasis on the cybersecurity practices of suppliers and service providers, requiring organizations to ensure that third parties meet equivalent security standards.

How IGA helps: IGA manages third-party access by enforcing strict policies that control and monitor the access rights of external partners. This mitigates risks posed by the supply chain by ensuring that suppliers have appropriate, limited access to systems and are regularly audited for compliance.

How Access Management helps: Access Management solutions support secure identity sharing between organizations and their external partners through federated identity management. This ensures controlled and temporary access to systems, aligning with NIS2's demands for robust third-party security protocols.

Managing Incident Response and Accountability

The NIS2 Directive mandates robust incident response plans and timely notification of significant cybersecurity incidents, emphasizing swift action and clear visibility into user activity.

How IGA Helps: In the event of a breach, IGA's detailed audit trails enable fast identification of compromised accounts or unauthorized access. IGA enhances incident detection and response by providing granular tracking of user access and activities across the network. Including the business origin of assigned user access, when was the access assigned and what business justification was provided for the access.

IGA solutions store relationships including identities, accounts and user access permissions within a centralized repository. Providing responders with the capability to query the relationships to discover associated application accounts and to take action such as quickly disabling access across the affected users estate.

Post-incident IGA solutions can be used to report on how and why an account was entitled with a particular permission that could have been used in a breach. IGA solutions audit the changes made to the account permissions and also the origin of the changes, whether authorized or not. This directly supports NIS2's incident reporting obligations (Article 23) by providing critical data on who accessed what and when, facilitating faster and more accurate reporting to authorities.

Compliance with ISO Standards and Security Frameworks

NIS2 compliance is closely tied to global security frameworks like ISO/IEC 27001, which emphasizes identity governance (e.g., A.9.2.1 - User Registration and A.9.4.1 - Information Access Restriction).

How IGA Helps: IGA helps organizations maintain continuous compliance with these standards by automating key tasks such as access control, user lifecycle management, and regular compliance reporting. Automated processes like user provisioning, de-provisioning, and access reviews ensure consistent enforcement of access policies, reducing human error—a significant factor in many security breaches.

Identity and Access Management

Adopting cyber hygiene practices, including robust identity and access management protocols, is a key aspect of NIS2. These practices ensure that only authorized personnel can access critical systems and that this access is regularly reviewed.
Also critical is implementing phishing-resistant multi-factor authentication (MFA), which adds an additional layer of protection against increasingly sophisticated cyber threats, such as credential phishing attacks. Phishing-resistant MFA methods, like hardware tokens or passwordless authentication, ensure that even if user credentials are compromised, attackers cannot easily gain unauthorized access.

How IGA Helps: Modern IGA solutions complement the need for MFA in a number of ways:

- End users accessing services - integration with modern identity providers that mandate MFA controls to access web resources such as IGA self-service capabilities.
- Identity Security Posture Management - reporting on identities that have poor security hygiene such as not having MFA enabled.
- Enforcing good security hygiene by the implementation of automated controls enforced by IGA such as lifecycle management workflows that ensure not only user access rights are controlled with a least privilege strategy but also that key security needs such as MFA are also enabled.

Early Warning and Reporting

NIS2 requires organizations to provide early warnings about significant incidents and ensure prompt response without undue delay.

How IGA Helps: IGA tools offer real-time tracking of user access and behavior, ensuring that incidents related to identity or access violations are flagged early. This capability enables organizations to quickly comply with early warning obligations under NIS2.

Glossary

CSIRT - Computer Security Incident Response Team

A team responsible for receiving, analyzing, and responding to cybersecurity incidents within an organization or country. CSIRTs aim to mitigate damage and restore normal operations quickly after a security breach.

DSP - Digital Service Provider

DSPs are organizations that offer digital services, such as online marketplaces, search engines, or cloud computing services.

Similar to OES, DSPs are required under NIS and NIS2 to ensure the security of their services, manage risks, and report incidents. The scope of DSPs has been expanded in NIS2 to address the growing importance of digital services in critical infrastructures.

EEA - European Economic Area

A region comprising the European Union (EU) member states and three of the European Free Trade Association (EFTA) states—Iceland, Liechtenstein, and Norway. The EEA allows for the free movement of persons, goods, services, and capital within the internal market of the EU.

ENISA - European Union Agency for Cybersecurity

ENISA plays a critical role in improving cybersecurity across the EU. It supports EU member states, EU institutions, and businesses in responding to cyber threats and incidents, providing guidance and cybersecurity recommendations. ENISA acts as the European Commission's arm for implementing the EU's cybersecurity strategy. It develops frameworks, conducts research, and provides best practices for improving resilience across networks and information systems in the EU.

EU - European Union

A political and economic union of 27 European countries that are located primarily in Europe. The EU operates through a system of supranational institutions and intergovernmental-negotiated decisions by the member states.

GDPR - General Data Protection Regulation

A regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It addresses the transfer of personal data outside the EU and EEA areas and sets guidelines for data handling.

GRC - Governance, Risk, and Compliance

An integrated approach that organizations use to align IT with business objectives while managing risk and meeting regulatory compliance requirements.

IAM - Identity Access Management

A framework of policies and technologies that ensures the right individuals have access to the appropriate resources within an organization. IAM manages identities and their access privileges.

ICT - Information and Communication Technologies

An umbrella term that includes all technologies for the manipulation and communication of information. It encompasses everything from computers and networks to telecommunication systems.

IGA - Identity Governance and Administration

Identity Governance and Administration (IGA) solutions enable organizations to manage digital identities, access rights, and provide compliance across complex IT environments. IGA platforms help automate the identity lifecycle, ensuring that users have the appropriate access to systems and data while minimizing security risks. The market is driven by the need for regulatory compliance, particularly in regulated sectors like finance, alongside growing concerns about data breaches and insider threats. IGA solutions offer key features such as identity provisioning, role-based access control (RBAC), audit and reporting capabilities, and access certification

ISO - International Organization for Standardization

An international standard-setting body composed of representatives from various national standards organizations. ISO develops and publishes worldwide technical, industrial, and commercial standards.

MFA - Multi-Factor Authentication

A security system that requires more than one method of authentication from independent categories of credentials to verify a user's identity. Common factors include something you know (password), something you have (token), and something you are (biometrics).

NCA - National Competent Authority

The NCA is designated by each EU member state to oversee and ensure compliance with the NIS and NIS2 directives within their jurisdiction.

NCAs enforce the cybersecurity requirements set forth by NIS and NIS2. They have the authority to investigate, issue penalties, and provide guidance to organizations subject to these regulations.

NIS - Network and Information Security

Refers to the protection of networks and information systems from activities that compromise their availability, authenticity, integrity, and confidentiality.

NIS2 - Network and Information Security Directive 2

An EU directive aimed at enhancing cybersecurity across member states. NIS2 expands the scope of cybersecurity obligations to more sectors and introduces stricter security requirements and incident reporting obligations.

NIST CSF - National Institute of Standards and Technology Cybersecurity Framework

A set of industry standards and best practices developed by NIST to help organizations manage cybersecurity risks. It provides guidelines and a methodology to assess and improve cybersecurity practices.

OES - Operators of Essential Services

OES refers to organizations that provide services critical to the economy, society, and the functioning of the state (e.g., energy, transport, healthcare, and financial services). These services, if disrupted, could have serious consequences for public safety and security.

Under NIS and NIS2, OES must comply with cybersecurity standards, report incidents, and implement risk management measures to ensure the resilience of their services.

RBAC - Role-Based Access Control

A method of regulating access to computer or network resources based on the roles of individual users within an organization. Users are assigned roles, and each role has specific permissions.

ZTA - Zero Trust Architecture

A security model that operates on the principle of "never trust, always verify." It requires continuous verification of user identities and access privileges, regardless of whether they are inside or outside the organization's network.

Appendix A - NIS2 Compliance Checklist

Link to the articles in the final text of the NIS 2 Directive

General Obligations

[ ] Read and understand the national cybersecurity strategy. (Art. 7.1, 7.2)

[ ] Familiarize with ENISA's best practices and guidance. (Art. 29.5)

[ ] Establish contact and cooperate with the national competent authority and CSIRTs. (Art. 8.3, 10.1, 10.4, 11.3)

[ ] Ensure that the management body follows the required cybersecurity training. (Art. 20.2)

Information Sharing and Reporting Obligations

[ ] Be ready to exchange relevant cybersecurity information with trusted communities (cyber threats, vulnerabilities, indicators of compromise, etc.). (Art. 29.1)

[ ] Sign information-sharing agreements with trusted communities. (Art. 29.2)

[ ] Notify the competent authorities about participation in information-sharing arrangements. (Art. 29.4)

[ ] Prepare to notify competent authorities or CSIRT of cybersecurity incidents (within 24 to 72 hours). (Art. 23.1, 23.2)

[ ] Submit a final incident report within 1 month after an incident. (Art. 23.4)

Cybersecurity Risk Management Measures

[ ] Develop and maintain policies on risk analysis and information system security. (Art. 21.2 a)

[ ] Establish and enforce incident handling procedures. (Art. 21.2 b)

[ ] Implement business continuity measures, including backup management, disaster recovery, and crisis management. (Art. 21.2 c)

[ ] Ensure supply chain security, including assessing the security of direct suppliers and service providers. (Art. 21.2 d, 21.3)

[ ] Secure network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure. (Art. 21.2 e)

[ ] Assess and review the effectiveness of cybersecurity risk-management measures. (Art. 21.2 f)

[ ] Promote basic cybersecurity hygiene practices and training within the organization. (Art. 21.2 g)

[ ] Implement policies for using cryptography and encryption where necessary. (Art. 21.2 h)

[ ] Ensure human resources security, implement access control policies, and manage assets appropriately. (Art. 21.2 i)

[ ] Use multi-factor authentication or continuous authentication solutions for secure communication (voice, video, text). (Art. 21.2 j)

[ ] Take appropriate corrective measures without delay if non-compliance is identified. (Art. 21.4)

Other Measures

Consider using ICT products, services, and processes certified under European cybersecurity certification schemes. (Art. 24.1)

[ ] Be ready for proactive non-intrusive scanning of publicly accessible network and information systems by CSIRT. (Art. 11.3)

[ ] Be prepared for inspections, off-site supervision, audits, and security scans by competent authorities. (Art. 32.2)

[ ] Be ready to provide information at the request of the competent authorities. (Art. 32.2)

[ ] Submit information to ENISA if applicable, including details such as the entity's name, sector, type of entity, address, and IP ranges. (Art. 27.1)

Appendix B - Transposition Status Country by Country

Stage 4: Transposition of NIS2 into National Law

These countries have made the most progress, having national regulations compliant with EU requirements.

Belgium

Belgium has proactively implemented the NIS2 Directive ahead of its October 2024 enforcement date by enacting the Belgian NIS2 Act and a Royal Decree. The framework expands the scope to include both "essential" and "important" entities across sectors such as energy, transport, banking, health, digital infrastructure, manufacturing, and research. Entities are required to register with the national cybersecurity authority, implement comprehensive risk management measures—including supply chain security—and adhere to strict incident reporting obligations. Enforcement involves both the Belgian Centre for Cybersecurity and designated sectoral authorities, with potential fines up to €10 million or 2% of annual global turnover, and introduces personal liability for management bodies.

Croatia

Croatia's Cybersecurity Act (Zakon o kibernetičkoj sigurnosti NN 14/2024) came into effect on February 15, 2024, effectively transposing the NIS2 Directive into national law ahead of the EU deadline.

Hungary

Hungary has successfully transposed the NIS2 Directive into national law. The NIS2 law commenced on May 23, 2023, following a consultation phase in February. Specific security measures were drafted and reviewed in early 2024, with the remaining parts of the implementation set to become effective by October 2024.

Latvia

On June 20, 2024, the Latvian Saeima adopted the National Cyber Security Law to strengthen the country's cybersecurity framework. The law is set to enter into force on September 1, 2024, pending final approvals.

Stage 3: Draft Submitted, Awaiting Feedback or Approval

These countries are in the process of transposing the directive and have submitted drafts of new legislation or proposed changes to existing laws.

Austria

On June 19, 2024, Austria announced the implementation of the directive through the enactment of the Information System Security Act 2024 (NISG 2024) and amendments to the Telecommunications and Health Telematics Acts.

Cyprus

Cyprus incorporated the directive into the text of Law 89(I)/2020, which has been open for public consultation since August 21, 2023.

Czech Republic

The Czech Republic submitted the bill to the government's Legislative Council at the end of 2023. The new Act on Cyber Security is expected to come into force in the second half of 2024.

Finland

Finland aims to adhere strictly to the EU's deadline. A first bill was shared for public consultation in November 2023, and on May 23, 2024, the government submitted a proposal to Parliament for national implementation. The new cybersecurity requirements will take effect from October 18, 2024, affecting critical sectors such as energy, healthcare, and digital services.

Germany

Germany is making progress with the NIS2UmsuCG (NIS2 Implementation and Cybersecurity Strengthening Act). A fourth draft bill was published on June 26, 2024, introducing key updates and clarifications. The Federal Ministry of the Interior is expediting the process, with cabinet discussions scheduled for July 24, 2024. Whether the act will meet the October 17, 2024 deadline remains uncertain.

Greece

Greece published a draft law titled "National Cybersecurity Authority and Other Provisions" for public consultation on January 3, 2024.

Italy

On June 10, 2024, the Italian Council of Ministers approved a draft legislative decree to comply with the directive. The proposal must undergo further stages, including parliamentary discussions and approvals.

Lithuania

Lithuania presented a draft amendment to cybersecurity law n°XII-1428 in April 2024, with public consultation until May 7, 2024. The Ministry of National Defence aims to complete the transposition by the EU deadline.

Luxembourg

On March 13, 2024, Luxembourg submitted a draft law (n°8364) to Parliament, currently under committee discussion.

Netherlands

The Netherlands is implementing the NIS2 Directive through a new Cybersecurity Act (Cyberbeveiligingswet), replacing the existing Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). The bill was shared for public consultation from May 21, 2024, to July 1, 2024. Due to legislative complexities and stakeholder consultations, it remains uncertain if the Netherlands will meet the October 17, 2024 deadline, with the Act now expected to come into effect in the second or third quarter of 2025.

Poland

Poland's Ministry of Digital Affairs published a draft amendment to the National Cybersecurity System Act (NCSSA) on April 24, 2024. Public consultations occurred until May 24, 2024.

Slovakia

On May 31, 2024, Slovakia's National Security Authority published draft legislation amending Act No. 69/2018 Coll. on cybersecurity, anticipated to come into effect on January 1, 2025.

Slovenia

Slovenia's draft law, known as the Act on Information Security (ZInfV-1), was published and underwent public consultation until March 18, 2024.

Sweden

Sweden is integrating the NIS2 Directive through a new Cybersecurity Act, set to replace the existing law. An interim report titled "New Rules on Cybersecurity" (SOU 2024:18) was published on March 5, 2024. The new Act is expected to be enforced by January 1, 2025.

Stage 2: Initial Stages of Development and Some Progress Made

These countries have made some progress and are actively developing initial drafts.

Denmark

Denmark initially aimed for early adoption but announced a delay on February 5, 2024. The proposed legislation has been postponed to the parliamentary session in October 2024, making it likely that Denmark will miss the October 17, 2024 implementation deadline.

France

France is working on structuring its initial draft, led by the National Cybersecurity Agency (ANSSI). However, it has yet to propose regulatory amendments covering all aspects of the NIS2 framework. The CSNP has provided recommendations, emphasizing communication, support, and phased enforcement until December 31, 2027.

Ireland

Ireland planned to introduce a bill by the end of 2023 but has delayed it until late summer 2024. The aim is still to meet the EU transposition deadline.

Romania

Romania's National Cyber Security Directorate initiated a public consultation on certain aspects until May 10, 2024. A comprehensive draft has not yet been published.

Stage 1: Limited Information Available or Minimal Progress Made

These countries have provided little public information or have made minimal progress.

Bulgaria

Bulgaria has not published a draft bill. The Ministry of Electronic Governance is responsible for the transposition process.

Estonia

Estonia's Ministry of Economic Affairs and Communications is reportedly drafting legislation, but limited information is available.

Malta

Malta has not commenced the parliamentary legislative process. The Critical Information Infrastructure Protection Unit (CIIP Unit) is anticipated to oversee the directive's implementation.

Portugal

Portugal is in the early stages of developing compliance measures. A draft bill has not been published.

Spain

Spain has not started the legislative process, with no significant updates or public consultations.

European countries outside of the European Union

Norway

While not a member of the European Union, is part of the European Economic Area (EEA) and typically aligns its legislation with EU directives to maintain access to the single market. The Norwegian government is actively working on transposing the NIS2 Directive into national law. The directive was adopted by the EU on December 14, 2022, and is set to replace the original NIS Directive (NIS1). Member states, including EEA countries like Norway, are required to implement necessary national legal changes by October 17, 2024, with the laws coming into effect the following day.

The Norwegian Ministry of Justice and Public Security is responsible for the implementation of NIS2. The process involves significant legal changes, which require approval by the Norwegian Parliament (Stortinget). The implementation is being followed up in the EFTA's working group for electronic communication, audiovisual services, and information society services (ECASIS).

United Kingdom

Although the United Kingdom is no longer a member of the European Union and is not directly impacted by the NIS2 Directive, it is indirectly affected due to close economic ties with EU member states and the necessity to maintain robust cybersecurity standards. In July 2024, the newly elected UK government introduced the Cyber Security and Resilience Bill, aimed at strengthening the nation's digital defenses. Announced in the King's Speech on July 17, this bill builds upon the foundations laid by the EU's original Network and Information Systems (NIS)Directive and is seen as the UK's response to NIS2.