CYRIS360

BARE CYBERSECURITY

NIS2 TRANSPOSITION PROGRESS ACROSS EUROPEAN COUNTRIES:

A MATURITY-BASED ASSESSMENT

TABLE OF CONTENTS

INTRODUCTION

The NIS2 Directive, which came into effect on October 17, 2024, represents a significant regulatory shift aimed at strengthening cybersecurity resilience across the European Union (EU). Expanding upon its predecessor (NIS1), NIS2 introduces stricter security obligations, enhances incident reporting requirements, increases oversight from national cybersecurity authorities, and broadens the sectors covered under its scope.

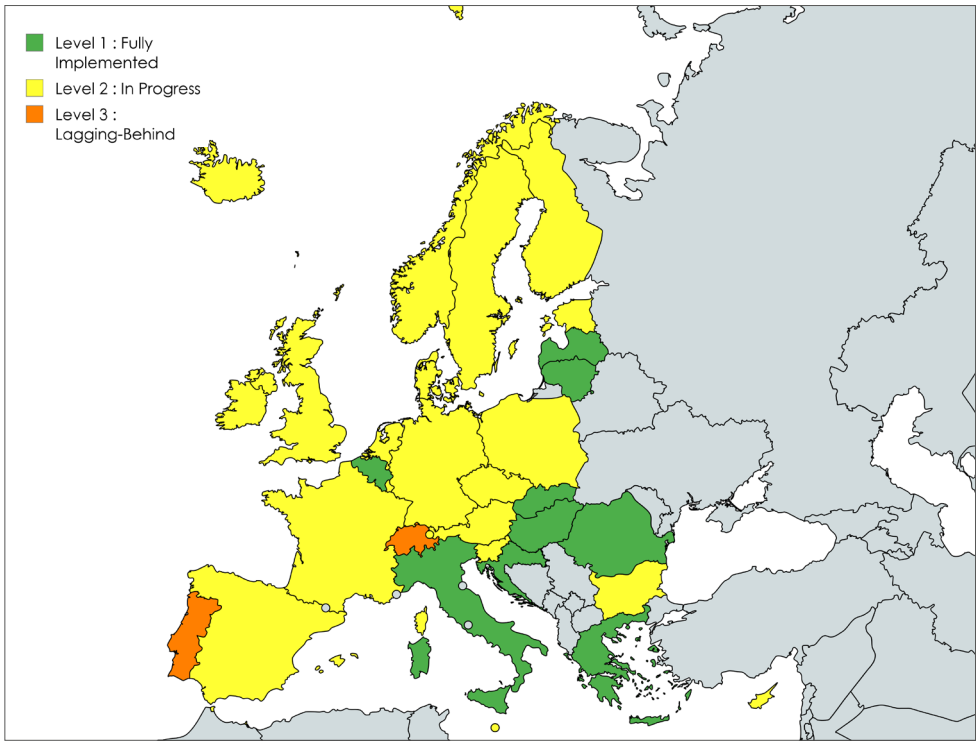

Figure1 : *European countries' NIS2 Transposition Status as of April 2025*

EU Member States were required to transpose NIS2 into national law by October 17, 2024. However, as of April 2025, many countries remain at different stages of the transposition process, with some having fully enacted the required legislation while others face delays. The scope of the document is not restricted to the European Union; it also includes the UK, Switzerland, Norway, Liechtenstein, and Iceland.

This report categorizes countries into three maturity levels based on their legislative progress:

- **Level 1: Fully Implemented –** Countries that have completed transposition, with enforcement mechanisms in place.
- **Level 2: In progress –** Countries that have published or approved draft laws and are in the final stages of transposition, but enforcement has not yet begun.
- **Level 3: Lagging Behind –** Countries with little to no progress, significant delays, or ongoing infringement procedures.

LEVEL 1 - COUNTRIES WITH NIS2 ALREADY IMPLEMENTED

Several EU Member States have fully transposed the NIS2 Directive into national law, establishing clear supervisory mandates, detailed compliance requirements, and enforcement frameworks. These countries have not only met the October 17, 2024, deadline but have also begun operationalizing the directive through sector-specific implementation and stakeholder engagement.

Country	Date of Transposition	National Authority
Belgium	April 26, 2024	Centre for Cybersecurity Belgium (CCB)
Croatia	February 15, 2024	Croatian National CERT
Greece	November 29, 2024	National Cyber Security Authority
Hungary	December 18, 2024	National Cyber Security Center
Italy	October 1, 2024	Agency for National Cybersecurity (ACN)
Latvia	September 1, 2024	Information System Authority (ISA)
Lithuania	October 18, 2024	National Cyber Security Centre (NKSC)
Romania	January 2025	Romanian National Cybersecurity Authority
Slovakia	January 2025	National Security Authority (NBU)

Table1 : *Countries with NIS2 already implemented*

BELGIUM

Law: Law of April 26, 2024
Status: Fully Implemented – entered into force October 18, 2024
National Authority: Centre for Cybersecurity Belgium (CCB)[1]

Belgium was among the earliest adopters of NIS2, finalizing its transposition through the Law of April 26, 2024, which came into force the same day. The Centre for Cybersecurity Belgium (CCB) has been granted wide-ranging powers to oversee compliance, conduct audits, issue corrective measures, and impose financial penalties for violations. Under this law, essential and important entities are required to implement proportionate technical and organizational measures, including risk analysis, access control, and supply chain cybersecurity checks. Incident notification must occur within 24 hours of becoming aware of an incident, followed by a more detailed report within 72 hours. Belgium also mandates close collaboration with sectoral CSIRTs and maintains a national registry of critical entities.

CROATIA

Law: Cyber Security Act
Status: Fully Implemented – entered into force February 15, 2024
National Authority: Croatian National CERT

Croatia's Cyber Security Act, adopted on February 15, 2024, fully aligns with NIS2 obligations and significantly strengthens the national cybersecurity regime. The Act introduces detailed incident management protocols, requiring entities to report incidents within 24 hours and classify them by severity. It mandates cybersecurity risk management strategies and places emphasis on supply chain security, including third-party risk assessments and contractual enforcement of cybersecurity clauses. Sectoral authorities and the Croatian National CERT work in tandem to offer guidance, conduct technical inspections, and ensure preparedness. The law also obligates operators in essential sectors to establish dedicated cybersecurity teams and conduct regular training and internal audits [2].

GREECE

Law: NIS2 Implementation Law
Status: Fully Implemented - entered into force November 27, 2024
National Authority: National Cybersecurity Authority of Greece

Details:
Greece has begun transposing the NIS2 Directive but has not yet finalized the law. The expected date for the full implementation is set for 2025. The National Cybersecurity Authority of Greece will be the responsible authority overseeing the implementation and enforcement of the NIS2 Directive. The country has already begun consultations with stakeholders, and draft laws are being discussed at the parliamentary level [3].

HUNGARY

Law: Cybersecurity Certification and Supervision Act
Status: Fully Implemented – entered into force mid-December 2024
National Authority: National Cybersecurity Center

Hungary's legislative response to NIS2 is the Cybersecurity Certification and Hungary's legislative response to NIS2 is the Cybersecurity Certification and Supervision Act, which came into effect in late 2024. This law emphasizes the creation of a national cybersecurity certification scheme that ensures service providers meet minimum cybersecurity requirements before operating in sensitive sectors. The Act mandates regular self-assessments, submission of compliance

documentation, and on-site inspections by the National Cybersecurity Center. It also introduces a national registry for essential entities and obligates periodic vulnerability assessments. Service providers in critical sectors such as energy, health, and digital infrastructure must undergo external audits at regular intervals [4].

ITALY

Law: Legislative Decree of October 1, 2024
Status: Fully Implemented - entered into force October 1, 2024
National Authority: Agency for National Cybersecurity (ACN)

Italy implemented NIS2 via a Legislative Decree effective October 1, 2024, administered by the Agency for National Cybersecurity (ACN). The decree sets out sector-specific minimum-security standards and obliges operators of essential and important services to align with ACN's technical implementation guidelines. The law requires entities to submit annual compliance declarations and conduct threat landscape reviews. ACN also maintains a national framework for incident categorization and provides centralized response coordination during major incidents. In addition, the decree strengthens public-private partnerships to facilitate cyber threat intelligence sharing across sectors [5].

LATVIA

Law: Cybersecurity Law (October 2024)
Status: Fully Implemented - entered into force October 1, 2024
National Authority: National Cyber Security Centre (NKSC)

Latvia's NIS2 transposition was finalized with the passing of the Cybersecurity Law, expected to take effect in October 2024. The National Cyber Security Centre (NKSC) will monitor compliance and offer support to critical sectors. Latvia's law emphasizes risk management and incident reporting requirements, and it mandates entities to register with the NKSC. There are also provisions for sector-specific cybersecurity measures and collaboration with sectoral CSIRTs [6].

LITHUANIA

Law: Law on Cyber Security (October 18, 2024)
Status: Fully Implemented - entered into force October 18, 2024
National Authority: National Cyber Security Centre (NKSC)

Lithuania enacted amendments to its Law on Cyber Security on October 18, 2024, effectively bringing it in line with NIS2 requirements. The legislation enforces strict supply chain oversight, requiring all essential and important entities to conduct due diligence on ICT service providers and maintain traceable procurement documentation. Entities must register in the national cybersecurity database, which is maintained by the National Cyber Security Centre (NKSC). The law introduces graded compliance obligations based on entity size and risk exposure. It also includes provisions for the continuous monitoring of digital infrastructure and mandates the use of cybersecurity maturity assessment tools [7].

ROMANIA

Law: Government Emergency Ordinance 155/2024 (GEO 155/2024)
Status: Fully Implemented — entered into force since 1 January 2025
National Authority: National Cyber Security Directorate

Romania has initiated the transposition of the NIS2 Directive, with an expected completion date in 2025. The National Cyber Security Directorate will be responsible for monitoring the implementation and enforcing cybersecurity regulations. Romania's approach focuses on developing sector-specific frameworks for critical infrastructure sectors and ensuring they meet the cybersecurity requirements stipulated by the directive [8].

SLOVAKIA

Law: Amendment to Act No. 69/2018 Coll. on Cybersecurity by Act No. 366/2024 Coll.
Status: Fully Implemented –entered in force since 1 January 2025
National Authority: National Security Authority (NBÚ)

Details:
The Amendment extends Slovakia's cybersecurity regime to cover approximately 3,500 entities—including public-administration bodies and third-party suppliers—and replaces the old identification criteria with a clear, exhaustive list of "essential" and "important" organizations. Each covered entity must register with NBÚ by 1 April 2025 and appoint a dedicated cybersecurity manager by 1 October 2025. Within six months of registration, organizations must establish a documented risk-management framework and, thereafter, undergo independent security audits every two years to ensure that technical and organizational controls are effective. For incident handling, entities must send an initial notification to NBÚ within 24 hours of detecting a significant cybersecurity event and follow up with a full report within 72 hours; further updates are then provided through NBÚ's centralized information system to coordinate response and lessons learned [9].

LEVEL 2 - COUNTRIES WITH NIS2 IMPLEMENTATION IN PROGRESS

These countries are actively working toward transposing the NIS2 Directive but are at varying stages of legislative maturity. Some have published draft laws or initiated parliamentary debates, while others are still conducting consultations or forming implementation strategies. Although enforcement has not yet begun, national authorities have started preparing guidance and engaging with critical sectors. Progress is often slowed by administrative delays, coordination hurdles, or legislative backlogs.

Country	Phase	Expected date of transposition	National Authority
Austria	Draft Submitted	TBD	Federal Chancellery (*Bundeskanzleramt*)
Bulgaria	Draft Submitted	TBD	State e-Government Agency
Cyprus	Draft Submitted	TBD	Ministry of Research, Innovation and Digital Policy
Czech Republic	Draft Submitted	Q3 - 2025	National Cyber and Information Security Agency (NÚKIB)
Denmark	Public Consultation	July 1, 2025	Danish Centre for Cyber Security (CFCS)
Estonia	Draft Under Discussion	TBD	Information System Authority (RIA)
Finland	Draft Submitted	Q3 - 2025	National Cyber Security Centre (NCSC-FI)
France	Draft Submitted	Q3 - 2025	*Agence nationale de la sécurité des systèmes d'information* (ANSSI)
Germany	Draft Submitted	TBD	Federal Office for Information Security (BSI)
Ireland	Draft Submitted	TBD	National Cyber Security Centre (NCSC)
Luxembourg	Draft Submitted	Q4 - 2025	*Institut Luxembourgeois de Régulation* (ILR)
Malta	Draft Submitted	TBD	Malta Information Technology Agency (MITA)
Netherlands	Draft Submitted	Q3 - 2025	*Rijksinspectie Digitale Infrastructuur* (RDI)
Poland	Draft Submitted	TBD	Ministry of Digital Affairs
Slovenia	Draft Submitted	May 2025	Information Security Administration
Sweden	Draft Submitted	H2 - 2025	Swedish Civil Contingencies Agency (MSB)
Iceland	Draft Submitted	TBD	Ministry of Infrastructure
Liechtenstein	Draft Submitted	TBD	Office for Communications
Norway	Draft Submitted	TBD	Norwegian National Security Authority (NSM)
Spain	Draft Submitted	Q3 - 2025	National Cryptologic Center (CCN)
United Kingdom	Draft Under Discussion	TBD	National Cyber Security Centre (NCSC – UK)

Table2 : *Countries with NIS2 implementation in progress*

AUSTRIA

Law: NIS2 Transposition Law
Status: In Progress - Draft Submitted
National Authority: Federal Ministry for Digital and Economic Affairs

Austria has initiated the process of transposing the NIS2 Directive and expects to complete the transposition in 2025. The Federal Ministry for Digital and Economic Affairs will oversee the implementation. Austria's draft law includes provisions for risk management, incident response, and sector-specific cybersecurity measures (Federal Ministry for Digital and Economic Affairs, 2024 [10]).

BULGARIA

Law: Cybersecurity Law
Status: In Progress - Draft Submitted
National Authority: State Agency for National Security (SANS)

Bulgaria is in the process of transposing the NIS2 Directive with full implementation expected by 2025. The State Agency for National Security (SANS) is the national authority responsible for implementing and enforcing the law. Bulgaria's draft law focuses on cybersecurity risk assessments, incident reporting, and ensuring compliance across critical sectors [11].

CYPRUS

Law: Cybersecurity Law
Status: In Progress - Draft Submitted
National Authority: Cyprus National CERT

Cyprus plans to integrate NIS2 by amending its existing Security of Networks and Information Systems Law (89(I)/2020). A formal public consultation on the amendment closed on September 29, 2023, after which the draft was submitted to Parliament. Although the amendment was expected to enter into force on October 18, 2024, it remains under parliamentary review, with no new enactment date confirmed. The DSA—located at *Helioupoleos* 12, Nicosia—will serve as both the single point of contact and the competent authority for digital service providers and operators of essential services. Cyprus was among the 23 Member States the Commission flagged for missing the transposition deadline in its Letter of Formal Notice of November 28, 2024 [12].

CZECH REPUBLIC

Law: NIS2 Transposition Law
Status: In Progress - Draft Submitted
National Authority: National Cyber Security Centre [13]

The Czech government approved its NIS2 transposition bill on July 17, 2024, submitting it to the Chamber of Deputies. This bill revises the national Cybersecurity Act to expand sectoral coverage, codify a 24-hour initial incident notification and a 72-hour detailed report, and introduces three implementing decrees clarifying security rules, registration procedures, and supervisory powers. Following passage by the lower house, it will proceed to the Senate and require the President's signature. NÚKIB is coordinating stakeholder feedback and parliamentary hearings; final adoption is anticipated in the third quarter 2025 [14][15].

DENMARK

Law: Draft NIS2 Transposition Act
Status: In Progress - Public Consultation
National Authority: Danish Centre for Cyber Security (CFCS)

Denmark published a draft law in July 2024, opening a public consultation on its proposed amendments to the Act on Digital Infrastructure Security. The CFCS is leading the legislative process, which will introduce mandatory risk-management requirements, 24/72-hour incident reporting timelines, and strengthened supply-chain security obligations for essential and important entities. Final parliamentary approval is expected by mid-2025 [16].

ESTONIA

Law: Draft amendment to the Cybersecurity Act published December 9, 2024
Status: In Progress - Draft Under Discussion
National Authority: Information System Authority (RIA)

Estonia, traditionally seen as a frontrunner in digital innovation, has surprisingly lagged in the transposition of NIS2. The Estonian Information System Authority (RIA) has acknowledged delays due to political transitions, limited legislative capacity, and ongoing institutional restructuring [17]. Although Estonia has an existing cybersecurity legal framework compliant with NIS1, it has yet to initiate the necessary reforms to meet the expanded requirements of NIS2. These include broader sectoral coverage, enhanced incident reporting timelines, and strengthened supervision mandates. As of April 2025, no public consultations or legislative drafts have been announced.

FINLAND

Law: Proposed amendments to the Cybersecurity Act (draft April 2025)
Status: In Progress - Draft Submitted
National Authority: National Cyber Security Centre Finland (under Traficom)

Finland has initiated stakeholder consultations and internal assessments but has not yet presented a draft law for public or parliamentary review. According to the Finnish Transport and Communications Agency (*Traficom*), the delay is due in part to the complex integration of NIS2 requirements into Finland's existing sector-specific regulatory regimes [18]. The National Cyber Security Centre Finland (NCSC-FI) is expected to play a central supervisory role, but questions remain around enforcement mechanisms and cross-sector coordination. Finland's proactive cybersecurity posture in other areas contrasts with its current lag in transposition, raising concerns about timing and operational readiness.

FRANCE

Law: Resilience of Critical Infrastructures and Cybersecurity Bill
Status: In Progress - Draft Submitted
National Authority: *Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI)

France's transposition of the NIS2 Directive is being implemented through the ''*Projet de loi relatif à la résilience des infrastructures critiques et à la cybersécurité* '' (Bill on Resilience of Critical Infrastructures and Cybersecurity). This comprehensive legislation expands the scope of covered sectors to include wastewater management, space, and postal services. The bill introduces mandatory cyber incident simulations and sector-specific training programs coordinated by ANSSI. It mandates operators to submit cybersecurity preparedness plans, participate in sectoral cyber exercises, and align with national risk assessment strategies. ANSSI will be responsible for central monitoring and enforcement, supported by sectoral regulators. Entry into force is expected by mid-2025, following further debates in the French Senate [19].

GERMANY

Law: NIS2 Implementation and Cybersecurity Enhancement Act
Status: In Progress - Draft Submitted
National Authority: *Bundesamt für Sicherheit in der Informationstechnik* (BSI)

Germany's NIS2 Implementation and Cybersecurity Enhancement Act (*NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz*) was published in draft form and is undergoing final committee reviews. The legislation introduces enhanced supervisory powers for BSI, including authority to conduct unannounced inspections and impose administrative penalties for non-compliance.

It mandates third-party security audits, regular vulnerability scans, and reporting of supply chain incidents. Additionally, Germany places significant emphasis on securing data center infrastructure, especially in the context of cloud services and government IT systems. Entities will be required to provide cybersecurity strategy reports and maintain active communication with sectoral regulators and the BSI. Final parliamentary approval is expected by the early second quarter 2025 [20].

IRELAND

Law: National Cyber Security (Amendment) Bill
Status: In Progress - Draft Submitted
National Authority: National Cyber Security Centre (NCSC-IE)[21]

Ireland has committed to transposing the NIS2 Directive and has launched preliminary consultations led by the Department of the Environment, Climate and Communications (DECC) [21]. The National Cyber Security Centre (NCSC), which currently oversees NIS1 enforcement, is preparing to assume expanded supervisory responsibilities under NIS2. As of April 2025, no formal draft legislation has been published. The government is conducting internal reviews to address challenges related to the classification of essential entities, reporting timelines, and the cybersecurity oversight of multinational cloud providers based in Ireland. Industry stakeholders have requested clarity regarding risk assessment standards and thresholds for incident notification. Concerns have also been raised about the adequacy of NCSC's operational capacity to fulfill its enhanced role.

LUXEMBOURG

Law: Draft Law No. 8364 (filed March 13, 2024)
Status: In Progress - Draft Submitted
National Authority: *Institut Luxembourgeois de Régulation* (ILR)

ILR's draft, currently under parliamentary review, amends four existing laws to transpose NIS2. It designates ILR as the supervisory authority, grants it audit and enforcement powers, and imposes 24/72-hour reporting deadlines. The banking sector will be overseen by the CSSF, and the HCPN will manage cyber crisis coordination. Adoption is expected by late 2025 [22].

MALTA

Law: Cybersecurity Act (Draft)
Status: In Progress - Draft Submitted
National Authority: Malta Information Technology Agency (MITA)

Malta's draft Cybersecurity Act was published for consultation in March 2025. It extends NIS2 obligations to digital service providers and critical infrastructure, introduces a centralized incident-reporting platform, and establishes sectoral cybersecurity frameworks. MITA is leading stakeholder workshops ahead of parliamentary table [23].

NETHERLANDS

Law: Cyber Security Act (*Cyberbeveiligingswet* – Cbw), replaces the existing Wbni
Status: In Progress - Draft Submitted
National Authority: *Nationaal Cyber Security Centrum* (NCSC)

The Netherlands is in the final stages of enacting its new *Cyberbeveiligingswet* (Cbw), which will replace the current Wbni law to fully comply with the NIS2 Directive. The draft legislation broadens the number of covered sectors and includes both essential and important entities, with obligations tailored to sector-specific risks. Key features of the law include clarified incident reporting chains, obligations to notify both the *naal Cyber Security Centrum* (NCSC) and sectoral authorities, and requirements for continuous threat monitoring. The law also introduces a centralized compliance registry managed by *Rijksinspectie Digitale Infrastructuur* (RDI) and mandates cybersecurity maturity evaluations based on EU-wide methodologies. The final adoption is expected in third quarter 2025, following stakeholder consultation and parliamentary approval [24].

POLAND

Law: Amendments to the National Cyber Security System Act (draft published March 2025)
Status: In Progress - Draft Submitted
National Authority: Ministry of Digital Affairs

Poland's draft amends its 2018 Cyber Security System Act to align with NIS2, introducing new categories of essential entities, tightening incident-reporting timelines, and mandating regular risk assessments. The Ministry expects parliamentary approval by mid-2025 [25].

SLOVENIA

Law: ZInfV 1 Draft Law (approved April 10, 2025)
Status: In Progress - Draft Submitted
National Authority: Information Security Administration (ISA) / SIRT Gov

Slovenia's government passed the ZInfV-1 draft under an urgent procedure in April 2025. It establishes ISA as the competent authority, sets a 24/72-hour reporting regime, and requires critical entities to implement risk-management frameworks. The National Assembly is expected to ratify the law by May 2025 [26].

SWEDEN

Law: Draft Cybersecurity Act (based on SOU 2024:18)
Status: In Progress – Draft Submitted
National Authority: Swedish Civil Contingencies Agency (MSB) [27]

The forthcoming law will align Sweden with NIS2's expanded sectoral scope by defining "essential" and "important" entities uniformly across Member States. It mandates that covered entities implement risk-management frameworks, conduct regular security assessments, and notify the MSB of significant cyber-incidents within 24 hours of becoming aware, followed by a detailed report within 72 hours. Secondary regulations are expected to set technical requirements for supply-chain security and incident-response coordination. MSB and PTS will publish guidance and maintain national registries of operators in scope [28][29].

ICELAND

Law: Draft Cybersecurity Act
Status: In Progress – Draft Submitted
National Authority: CERT-IS (Icelandic National CERT) [30]

Iceland's draft National Cyber Security Act, published January 15, 2025, seeks to transpose the EU NIS2 Directive by extending obligations to operators of essential and important services[31]. Despite missing the October 17, 2024 deadline, the government launched a public consultation that closed March 20, 2025, to refine risk-management, incident-reporting, and governance provisions. The European Commission opened infringement proceedings in December 2024, issuing a formal notice urging accelerated adoption under Article 258 TFEU [32]. Parliamentary committee debates are scheduled for May–June 2025, with full adoption anticipated by July 2025 and entry into force by August 2025. In the interim, Iceland's Cybersecurity Centre has issued non-binding guidelines to help entities align with forthcoming NIS2 requirements.

LIECHTENSTEIN

Law: Draft Digital Security Act (EEA alignment)
Status: In Progress – Draft Submitted
National Authority: Office for Communications (AK)

Liechtenstein published its draft Digital Security Act in February 2025. The Office for Communications will serve as the supervisory authority, enforcing NIS2-style obligations on EEA-relevant entities and managing incident notifications. Final adoption is anticipated in the fourth quarter 2025 [33].

NORWAY

Law: Digital Security Act
Status: In Progress – Draft Submitted
National Authority: Norwegian National Security Authority (NSM)

Norway's draft Digital Security Act, released in March 2025, transposes NIS2 into EEA law. NSM will oversee essential and important entities, enforce 24/72-hour incident reporting, and conduct risk-based audits. Public consultation closes in May 2025 [34].

SPAIN

Law: Draft Law on Cybersecurity Coordination and Governance
Status: In Progress – Draft submitted: Third quarter 2025
National Authority: *Instituto Nacional de Ciberseguridad* (INCIBE)

Spain has taken preliminary steps toward NIS2 transposition through a multi-phase strategy coordinated by the *Instituto Nacional de Ciberseguridad* (INCIBE) and the Ministry of Economic Affairs and Digital Transformation [35]. The Spanish Ministry of Interior approved and published on 17 January 2025 the draft Law on Cybersecurity Coordination and Governance, processed under an urgent procedure to implement NIS2. INCIBE will oversee incident notifications, which must occur within 24 hours, with follow-up reports within 72 hours, and the appointment of information security officers is mandated. Final parliamentary approval is expected by mid-2025 after sectoral consultations and ministerial input.

UNITED KINGDOM

Law: Cyber Security and Resilience Bill
Status: In Progress – Draft Under Discussion
National Authority: National Cyber Security Centre (NCSC – UK) [36]

Although the United Kingdom is no longer part of the EU, it continues to align its national cybersecurity policy with EU developments. In 2023, the UK government held a public consultation on proposals to update the Network and Information Systems (NIS) Regulations 2018. On 1 April 2025, the Department for Science, Innovation and Technology published a Policy Statement detailing the Bill's intent to extend regulation to managed service providers, mandate 24/72-hour reporting timelines, and grant enhanced enforcement powers to the National Cyber Security Centre (NCSC) and sectoral regulators. The Bill is expected to be formally introduced to Parliament later in 2025, with final enactment anticipated by year-end [37].

LEVEL 3 - COUNTRIES WITH NIS2 IMPLEMENTATION STILL LAGGING BEHIND

Portugal and Switzerland have yet to complete their NIS2 transposition, exposing them to potential enforcement action. Portugal's draft decree-law stalled after Parliament dissolved post-consultation on December 31st, 2024, with no final vote or notification to the Commission. Switzerland's amended Information Security Act and Cybersecurity Ordinance took effect on April 1st, 2025, but essential secondary rules on risk management and incident reporting remain unpublished. Both must now finalize their implementing regulations to close compliance gaps.

Country	Phase	Expected date of transposition	National Authority
Portugal	Draft Paused	Mid-2025	Portuguese National Cybersecurity Centre (CNCS)
Switzerland	Draft Under Discussion	2026	Swiss National Cyber Security Centre (NCSC – CH)

Table3 : *Countries with NIS2 transposition lagging behind*

PORTUGAL

Law: Draft Cybersecurity Coordination Decree-Law
Status: Draft Paused
National Authority: Portuguese National Cybersecurity Centre (CNCS) [38]

The Portuguese Government submitted a Draft Decree-Law to transpose the NIS2 Directive, revising Law 46/2018 (Legal Framework for Cyberspace Security) and Decree-Law 65/2021. The draft was approved by the Council of Ministers on 7th February 2025 and published for parliamentary debate. The draft law completed public consultation on 31 December 2024, receiving 149 contributions. It was set for a parliamentary vote on 20 March 2025, but the government's collapse and dissolution of parliament have paused the process. A new government after the 18th May 2025 elections must reintroduce the draft.
During public consultation, CNCS signaled it will enforce stricter risk-management requirements, 24-hour initial incident notifications and 72-hour detailed reports, and expanded supply-chain security checks. The draft grants CNCS enhanced audit and sanction powers—up to €1 million fines—and codifies a national registry of essential and important entities. CNCS has already begun issuing preparatory guidance and running sectoral workshops to help organizations align with forthcoming obligations.

SWITZERLAND

Law: Draft Cybersecurity Framework (in development)
Status: Draft Under Discussion
National Authority: National Cyber Security Centre (NCSC – Switzerland) [39]

Switzerland, though not an EU Member State, is actively working on revising its national cybersecurity legislation to reflect principles embedded in the NIS2 Directive. The Federal Council mandated the creation of a national cybersecurity law, which is currently under interdepartmental coordination and is expected to enter a public consultation phase by mid-2025. The Swiss National Cyber Security Centre (NCSC) is leading efforts to strengthen obligations for operators of critical infrastructure and essential services, covering sectors such as energy, health, transport, and digital services. The proposed law aims to enhance incident notification timelines, promote risk-based security measures, and introduce a centralized registry for essential entities. Switzerland's strategic goal is to ensure interoperability with EU cybersecurity frameworks to support cross-border digital cooperation [40].

EUROPEAN COMMISSION ENFORCEMENT ACTIONS

As of March 2025, the European Commission has launched infringement procedures against 23 Member States for failing to meet the NIS2 transposition deadline. These procedures can lead to financial penalties unless states provide a credible roadmap to compliance.

CONCLUSION: THE ROAD AHEAD

European countries are at different stages in implementing the NIS2 Directive. Some have already completed transposition into national law, while others have made only limited progress. Organizations are facing a complex mosaic of legal obligations, risk-management mandates, and incident-reporting deadlines.

Cyris360's core expertise in Governance, Risk & Compliance (GRC) directly addresses these very challenges: by establishing an ISO/IEC27001-compliant Information Security Management System (ISMS) that aligns with NIS2's Articles 20 (governance) and 21 (risk management), and by embedding robust incident-response processes that dovetail with NIS2's 24/72-hour notification requirements, your organization can achieve both regulatory compliance and operational resilience.

Implementing ISO/IEC 27001 provides a proven, auditable framework for:

- **Systematic Risk Assessment** - mirroring NIS2's risk-management measures through ISO/IEC27001's risk-assessment (Section 8.2) and treatment (Section 8.3) requirements.
- **ICT Readiness for business continuity** – leveraging the organizational control A5.30 with additional guidelines from ISO/IEC27031.
- **Incident Management** - leveraging incident management controls A5.24-A5.27 with additional guidelines from ISO/IEC27035 to meet NIS2's strict reporting timelines and CSIRT coordination requirements.
- **Supply Chain Security** - applying supplier-relationship controls A5.19-A5.31 with additional guidelines from ISO/IEC27036 to satisfy NIS2's supply-chain obligations.
- **Continuous Improvement** – utilizing the requirements from chapter 10 and the Plan-Do-Check-Act cycle to prepare for NIS2's periodic audits and ever-evolving threat landscape.

By partnering with Cyris360, you leverage our proven Cyber Risk Framework (CRF) and hands-on ISO/IEC 27001 implementation services, that re already trusted by leading brands, to transform NIS2 compliance from a regulatory burden into a strategic asset. We'll guide you through every step: from gap assessments and roadmap development, through control implementation and documentation, to internal audits and certification readiness. The result is a unified cybersecurity posture that meets NIS2 obligations, enhances stakeholder trust, and drives business growth.

Ready to bridge the gap between NIS2 and ISO/IEC 27001?
Contact Cyris360 today to turn regulatory requirements into resilient, competitive advantage.

REFERENCES

[1] Centre for Cybersecurity Belgium (CCB). NIS2 Regulation Overview. Retrieved from: https://ccb.belgium.be/regulation/nis2
[2] Croatian National CERT. Cyber Security Act Implementation. Retrieved from: https://www.cert.hr
[3] National Cybersecurity Authority (NCSA) of Greece. Profile. Retrieved from: https://cyber.gov.gr/en/
[4] Ministry of Technology and Industry – Hungary. NIS2 Transposition Update. Retrieved from: https://kormany.hu/hungary-nis2
[5] *Agenzia per la Cybersicurezza Nazionale* (ACN). Italy's Legislative Decree on NIS2. Retrieved from: https://www.acn.gov.it
[6] Information System Authority (ISA) – Latvia. NIS2 Implementation Status. Retrieved from: https://www.cert.lv
[7] National Cyber Security Centre (NKSC) – Lithuania. NIS2 Law Overview. Retrieved from: https://nksc.lrv.lt
[8] *National Cyberint Center* – Romania. NIS2 Transposition Overview. Retrieved from: https://www.cyberint.ro
[9] National Security Authority (NBU) – Slovakia. Cybersecurity Legislation. Retrieved from: https://www.nbu.gov.sk
[10] Federal Chancellery (Bundeskanzleramt). NIS2 Directive, Transposition in Austria. Retrieved from: https://www.nis-2-directive.com/Transposition/Austria.html
[11] State e-Government Agency – Bulgaria. NIS2 Transposition Draft. Retrieved from: https://www.egov.bg
[12] Ministry of Research, Innovation and Digital Policy – Cyprus. Cybersecurity Law Draft. Retrieved from: https://dsa.cy/en/activities/nis-directive-implementation
[13] National Cyber and Information Security Agency (NÚKIB) – Czech Republic. NIS2 Legislative Process. Retrieved from: https://nukib.gov.cz
[14] Wavestone. NIS 2: Where are European countries in transposing the directive? Retrieved from: https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive/
[15] Orrick. NIS2: Where do European Countries Stand on Implementing Cybersecurity Strategies. Retrieved from: https://www.orrick.com/en/Insights/2024/10/NIS2-Where-do-European-Countries-Stand-on-Implementing-Cybersecurity-Strategies
[16] Danish Centre for Cyber Security (CFCS). NIS2 Implementation Timeline. Retrieved from: https://cfcs.dk
[17] Information System Authority (RIA). Estonia's NIS2 Transposition Status. Retrieved from: https://www.ria.ee
[18] National Cyber Security Centre Finland (NCSC-FI). NIS2 Draft Progress. Retrieved from: https://www.kyberturvallisuuskeskus.fi
[19] *Agence nationale de la sécurité des systèmes d'information* (ANSSI). France's NIS2 Legislative Proposal. Retrieved from: https://www.ssi.gouv.fr
[20] Federal Office for Information Security (BSI). Germany's NIS2 Draft Law. Retrieved from: https://www.bsi.bund.de
[21] National Cyber Security Centre Ireland (NCSC-IE). NIS2 Consultation Update. Retrieved from: https://www.ncsc.gov.ie
[22] *Institut Luxembourgeois de Régulation* (ILR). Luxembourg's NIS2 Legislative Draft. Retrieved from: https://www.ilr.lu
[23] Malta Information Technology Agency (MITA). NIS2 Compliance Update. Retrieved from: https://mita.gov.mt
[24] *Rijksinspectie Digitale Infrastructuur* (RDI). *Netherlands Cyberbeveiligingswet* (Cbw). Retrieved from: https://www.rdi.nl
[25] Ministry of Digital Affairs – Poland. NIS2 Implementation Process. Retrieved from: https://www.gov.pl/cyfryzacja
[26] Information Security Administration – Slovenia. Cybersecurity Law Draft. Retrieved from: https://www.gov.si/drzavni-organi/ministrstva/mju
[27] Swedish Civil Contingencies Agency (MSB). NIS2 Transposition Plan. Retrieved from: https://www.msb.se
[28] European Commission. Implementation of the *NIS2 Directive in Sweden*. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-sweden
[29] European Commission. *Implementation of the NIS2 Directive in Sweden – Points of Contact*. Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-sweden
[30] CERT-IS. Iceland's NIS2 EEA Incorporation. Retrieved from: https://www.stjornarradid.is
[31] Government of Iceland. Draft National Cyber Security Act. Retrieved from: https://www.government.is/draft-cyber-act
[32] European Commission. Formal Notice to Iceland on NIS2 Transposition. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2025
[33] Office for Communications – Liechtenstein. Cybersecurity Strategy and NIS2. Retrieved from: https://www.llv.li
[34] Norwegian National Security Authority (NSM). NIS2 Directive Implementation. Retrieved from: https://www.nsm.no
[35] Instituto Nacional de Ciberseguridad (INCIBE). Spain's NIS2 Compliance Overview. Retrieved from: https://www.incibe.es
[36] National Cyber Security Centre – UK (NCSC-UK). Networks and Information Systems (NIS) Directive. Retrieved from: https://www.ncsc.gov.uk/collection/board-toolkit/principle-b-strategy/cyber-security-regulation-and-directors-duties-in-the-uk
[37] Hunton Andrews Kurth. UK Government Sets Out Scope for Cyber Security and Resilience Bill Retrieved from: https://www.hunton.com/privacy-and-information-security-law/uk-government-sets-out-scope-for-cyber-security-and-resilience-bill?utm_source=chatgpt.com
[38] Portuguese National Cybersecurity Centre (CNCS). Status of NIS2 Transposition. Retrieved from: https://www.cncs.gov.pt
[39] Swiss National Cyber Security Centre (NCSC – CH). Federal Department of Defence, Civil Protection and Sport (DDPS). Retrieved from: https://www.ncsc.admin.ch/ncsc/en/home.html
[40] ECSO. NIS2 Directive Transposition Tracker. Retrieved from: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

CYRIS360

BARE
CYBERSECURITY

Info@cyris360.com
www.cyris360.com
+31 10 32 161 32