Implementing the NIS 2 Directive: Towards Harmonisation or Further Fragmentation?

Federica Casarosa[1 †*], Giovanni Comandé [1, †]

[1] *Sant'Anna School of Advanced Studies, Piazza dei Martiri 33, 56127 Pisa, Italy*

Abstract

This paper examines the harmonisation process in cybersecurity within the European Union, focusing on the transition from the NIS Directive to NIS 2 in selected Member States. The effectiveness of harmonisation depends on national implementation choices, which remain highly discretionary. A comparative analysis of Italy, Belgium, Hungary, and Slovakia reveals divergences in reference standards, integration with adjacent legal frameworks, and supply chain risk management. While technical convergence around international standards is evident, implementation practices remain fragmented. ENISA's non-binding methodological tools represent a preliminary step toward a shared technical vocabulary. Nonetheless, achieving full harmonisation requires a systemic approach, encompassing regulatory integration and institutional cooperation, and recognising cybersecurity as a foundational component of the European digital space.

Keywords

legal harmonization, NIS 2 Directive, International standards, Risk management, healthcare

1. Introduction

Over the past 10 years, the European legislator has devoted increasing attention to cybersecurity. On the one hand, this is the result of a progressive expansion of knowledge about the use of IT infrastructures; on the other hand, the rise in successive attacks has highlighted the need for measures to harmonise the level of protection across all European states.[1]

Cybersecurity, in fact, emerges as an autonomous area that partially overlaps with other policy domains, such as combating cybercrime, protecting personal data, and ensuring the security of electronic communications.[2] In particular, initiatives aimed at coordinating critical infrastructure—now increasingly digitalised [4]—have revealed that national strategies remain heterogeneous and fragmented. This posed clear risks in ensuring an adequate level of protection against external attacks. On these grounds, work began on a proposal for a directive dedicated explicitly to cybersecurity, understood at the time as "the ability of a network or

* Joint National Conference on Cybersecurity (ITASEC & SERICS 2026), February 09-13, 2026, Cagliari, IT.
1* Corresponding author.
† These authors contributed equally.
Federica.casarosa@santannapisa.it (F. Casarosa); Giovanni.comande@santannapisa.it (G.Comandè).
0000-0002-5256-3505 (F. Casarosa); 0000-0003-2012-7415 (G. Comandè)

[1] The turning point can easily be attributed to the cyberattack suffered by Estonia's IT infrastructure in 2007, when a series of Distributed Denial of Service (DDoS) attacks managed to paralyze the country's infrastructure at a national level [1],[2].

[2] However, it is important to note that measures related to the security of information systems were already present in the early 1990s, but at that time they focused mainly on defining security and interoperability standards for infrastructures within the framework of the information society [3].

information system to withstand, with a given level of confidence, accidental events or malicious actions" [5].

The growing exposure of the European Union to cyber threats made the adoption of shared, harmonised regulatory measures essential to guarantee a uniform level of security across Member States. In this context, the NIS Directive represented the first attempt to build a common reference framework. However, the difficulties encountered in its implementation and the persistent regulatory fragmentation highlighted the inability to achieve the intended objectives, necessitating a substantial revision. The NIS 2 Directive, adopted in 2022, aims to overcome these critical issues by introducing stricter obligations and greater clarity in defining the entities involved. With the implementation deadline set for 18 October 2024, it is now possible—one year later—to formulate an initial comparative assessment of the choices made by individual states. In particular, two key aspects will be analysed to measure the degree of harmonisation achieved: the nature of the requirements imposed on essential and important operators, and the approach to risk management throughout the supply chain.

The selection of these two aspects is based on one of the project Fit4MedRob's research focuses: the development of healthcare and personal care robots in line with the legal requirements of the European system.[3] The project aims to develop robots/systems capable of providing physical rehabilitation and personal care treatments. This result exploits the latest technological developments, hosting sensors and computational reasoning that collect data from the environment or patients and translate them into actions. The development of these technologies is driven by collaboration among research institutions, healthcare providers, and laboratories. Given that all these actors fall within the scope of the NIS 2 directive, it is of utmost importance that the cybersecurity requirements be comparable and harmonised across Member States to ensure smooth collaboration among partners and reduce duplication and conflicts arising from different national standards.

This is even more important given the cyber threats to the healthcare sector, which has become one of the most vulnerable domains due to the acceleration of digitalisation of medical infrastructures and the widespread adoption of connected devices [6]. ENISA's reports consistently identify healthcare as a high-risk sector under the NIS framework, noting that hospitals and healthcare providers face a disproportionate number of cyber incidents compared to other critical sectors [7]. Moreover, a distinctive feature of healthcare is its dependency on complex supply chains that also include specialised vendors and manufacturers of medical devices. The vulnerabilities in these components can propagate across networks, creating systemic risks that compromise both operational continuity and patient safety. The NIS 2 Directive's requirement to address supply chain risks, therefore, assumes particular significance in this context, as it indirectly extends cybersecurity obligations to entities not formally covered by the directive, such as small and niche suppliers critical to medical operations. Given that cybersecurity failures can directly impact patient safety and the continuity of medical services, it is crucial to verify the current approaches adopted by Member States to determine whether and how cybersecurity measures can help protect health data and maintain trust in digital health systems. This contribution is the starting point of the research activity and will provide the overall framework, which in the future will be developed and adapted to the specificities of the health sector.

[3] 'Fit4MedRob - Fit for Medical Robotics' Grant (# PNC0000007), project funded by the Italian Ministry of University and Research, under the complementary actions to the NRRP. See more at https://www.fit4medrob.it/.

The analysis will then present the modifications that have been adopted with the NIS 2 Directive (sect. 2), focusing then on the national choices regarding the technical and organisational measures adopted (sect. 3). Specific attention will then be given to the supply chain control imposed on essential and important entities (sect. 4), followed by conclusions (sect. 5).

2. Harmonisation Measures in the Field of Cybersecurity

The first horizontal cybersecurity legislation was Directive 2016/1148 (NIS Directive), which aimed to establish a high and common level of security for networks and information systems across the European Union, thereby improving the functioning of the internal market. The choice to intervene through a directive clearly demonstrated the difficulties of regulating a complex sector in which individual countries' sensitivity regarding security decisions is particularly high. Indeed, this choice, on the one hand, left Member States broad discretion in implementation methods; on the other hand, it preserved the possibility of adopting more specific sectoral rules at the European level. As a result of the choice to adopt minimum harmonisation, each country has enjoyed a certain degree of flexibility in implementing the objectives in its national laws, without permitting measures less stringent than those outlined in EU legislation, for instance, allowing Member States to expand the list of sectors or entities covered by the legislation, or to set stricter deadlines for incident reporting.

Although the European Union had high hopes for achieving the objectives set by the NIS Directive, less than a year before the implementation deadline (May 9, 2018), the Commission began to express doubts about the results obtained [8]. While acknowledging the rapid developments in the sector, what clearly emerged was the diversity of approaches and the often high degree of decentralisation at the national level [9], [10], [11], [12], [13], [14]. In particular, the document identified three main areas of difficulty. The first problem was the low level of resilience achieved by businesses and all entities covered by the legislation. This was attributed to the limited number of sectors covered by the legislation, which meant fewer operators were subject to minimum security obligations, further increasing complexity as many states extended the regulation's scope. The second problem was the existence of different levels of resilience among Member States and sectors, resulting from inconsistencies in the procedures for identifying operators of essential services within the same industry, leading to discrepancies between Member States. In addition to difficulties in determining which entities are subject to the regulation, implementing the measures proved complex due to the broad discretion left to Member States. Security measures varied significantly, as did the thresholds for assessing compliance with criteria for incident notification to the competent authority. National authorities themselves, in the absence of precise standards to follow, adopted very different measures in exercising their oversight, even with the same number of violations detected. Finally, the third problem was the low level of awareness of cybersecurity issues among all stakeholders, which limited response capacity. In particular, Member States failed to establish adequate systems for sharing information on potential and actual cybersecurity threats among themselves.

These critical points represented the main areas of intervention in the reform process that led to the adoption of the NIS 2 Directive (Directive 2022/2555). Indeed, the European legislator's choice is guided by two objectives: limiting the excessive discretion left to Member States and

reducing the fragmentation of protection measures. This is reflected concretely in greater clarity regarding the scope of application, which no longer depends on states' discretionary choices but on an objective criterion for identifying essential and important entities.[4] Therefore, all medium-sized entities fall within the scope of the directive, along with a series of exceptions for companies offering services classified as essential (such as qualified trust service providers and top-level domain registries, as per Articles 3(b)-(g) of the NIS 2 Directive). Another harmonisation measure concerns the definition of a more detailed set of guidelines regarding security requirements that both essential and important entities must adopt to comply with the regulation. In fact, the previous distinction between operators of essential services and digital service providers was clearly outdated [16], [10], given the interactions among entities operating in national markets. However, the system adopted by the NIS 2 Directive remains based on a dual regime; this distinction does not affect the applicable requirements or procedures for notifying security incidents, focusing instead on the discretion allocated to supervisory authorities for potential audit activities and the resulting sanctions (in particular in articles 32 and 33 NIS 2 Directive).

The NIS 2 Directive set October 18, 2024, as the deadline for national implementation, allowing nearly two years to define national strategies and revise the previous regulatory framework for cybersecurity. However, only half of the Member States had completed this process one year before the scheduled deadline.[5] Among the most compliant countries are Belgium, Cyprus, Croatia, Denmark, Finland, Greece, Italy, Latvia, Lithuania, Romania, Slovakia, Slovenia, and Hungary. In the remaining states, only draft laws exist, still at various stages of approval. The Commission, therefore, has initiated a process that could lead to infringement proceedings against Member States that are still lagging behind. At the time of writing, the Commission had sent a first letter of formal notice to 23 States that had not transposed the Directive within the deadline (October 2024), followed by a reasoned opinion for the 19 states still non-compliant, including a formal request to comply with the legislation (May 2025). The Commission is currently evaluating whether to refer the matter to the Court of Justice.

In light of the ongoing process, it is possible to assess whether current legislative measures already indicate progress toward achieving the goal of harmonising the level of cybersecurity protection, and, potentially, the presence of prevailing models that could foster cross-border adoption among Member States. To concretely evaluate this outcome, for this analysis, two aspects will be compared: (1) the adoption of uniform requirements for regulatory compliance (art. 21 NIS 2 Directive), and (2) the control mechanisms applied to the supply chain (art. 21 (2) (d) NIS 2 Directive). These aspects represent innovations compared to the previous regulatory framework, on which Member States retain a degree of discretion regarding implementation methods.

The analysis will cover four countries selected from those that, by January 2025, had implemented the NIS 2 Directive. This allowed us to verify in greater detail the choices of each Member State, including national regulatory interventions. The choice fell on the first state implementing the NIS 2 Directive, namely Hungary, and the last in the selected period, namely

[4] For a critique of the choice of such a purely quantitative criterion for identifying the scope of application and the related challenges within the supply chain, see [15].

[5] See the updated list at https://ecs-org.eu/activities/nis2-directive-transposition-tracker/ and https://www.openkritis.de/eu/eu-nis-2-member-states.html.

Slovakia. Then, Italy and Belgium were selected based on the information available on the ECSO platform, which highlighted interesting elements in both countries' implementation strategies.

3. Cybersecurity Measures for Essential and Important Entities

Under Article 21 of the NIS 2 Directive, Member States must ensure that essential and important entities have adopted "appropriate and proportionate technical, operational, and organizational measures to manage the risks posed to the security of the network and information systems that these entities use in their operations or in the provision of their services, as well as to prevent or minimize the impact of incidents on the recipients of their services and on other services." Specifically, paragraph two of the article outlines the minimum content of such measures, including risk analysis and information system security policies; incident management; business continuity; supply chain security; security of acquisition, development, and maintenance of network and information systems, including vulnerability management and disclosure; strategies and procedures for assessing the effectiveness of cybersecurity risk management measures; basic cyber hygiene practices and cybersecurity training; policies and procedures related to the use of encryption and, where applicable, cryptography; human resource security; and the use of multi-factor or continuous authentication solutions.

Although the level of detail in the regulation is much higher than that provided under the original NIS Directive, Member States still retain discretion regarding the specific requirements that operationalise the minimum content set out in the directive. This must also be considered in relation to pre-existing international standards available on the market, which offer market operators—classified as essential or important entities—a degree of uniformity and alignment with the state of the art [17], [18], [19], [20]. In other words, the regulatory landscape must not only address "legal" requirements but also align with internationally established cybersecurity postures and technical frameworks. In this regard, numerous international frameworks play a central role, among which the most relevant are the ISO/IEC 27000 series and subsequent standards,[6] NIST standards,[7] IEC standards,[8] and COBIT standards.[9] While these standards are largely convergent, they exhibit non-negligible implementation and semantic differences,

[6] The ISO/IEC 27000 family of standards includes information security standards published by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). The series provides guidelines for managing information security within the context of a global Information Security Management System (ISMS), similar in concept to quality assurance management systems (part of another family of standards, the ISO 9000 series). The scope of the series is deliberately broad, not limited to privacy, confidentiality, and cybersecurity. It applies to organisations of all types and sizes. All organisations are encouraged to assess their information risks and address them (using specific controls) according to their needs. Given the dynamic nature of risk and information security, the ISMS concept incorporates feedback and continuous improvement activities to respond to changes in threats, vulnerabilities, and incident impacts. Refer to the objectives outlined by ISO/IEC JTC 1 (Joint Technical Committee 1) SC 27 (Subcommittee 27), which is responsible for developing the standards' content: https://www.iso.org/committee/45306.html.

[7] The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce whose mission is to promote American innovation and industrial competitiveness. The two most relevant standards for cybersecurity are the Cybersecurity Framework and NIST 800-53 rev. 5. The first is a standard initially published in 2014 and updated in 2024, developed in response to growing cyber threats and the need for standardised practices. The CSF provides a risk-based approach to managing cybersecurity risks. It is structured around five core functions: Identify, Protect, Detect, Respond, and Recover, each representing a critical phase in cybersecurity risk management. The second provides a catalogue of privacy and security controls for information systems. Initially, the standard was used only for federal agencies; however, the latest version (rev. 5) has adopted an approach that allows general application. See respectively: https://www.nist.gov/cyberframework and https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

underscoring their significance in each regulatory adaptation. Nevertheless, an analysis of legislative measures reveals a disparity of approaches, mixing interventions that directly correlate the requirements set out in the directive with (parts of) security frameworks developed purely at the national level, others where international standards are mentioned and considered equivalent, and still others proposing hybrid standards combining international frameworks with national specificities.

For example, in Slovakia, Act No. 366/2024, which amends and supplements Act No. 69/2018 on cybersecurity, is the implementing legislation for the NIS 2 Directive.[10] In the text, Article § 5 identifies the security measures applicable to essential and important entities and describes the minimum content required by the Directive. Specifically, it differentiates between aspects related to organisational principles of cybersecurity, resource and risk management, technical and procedural measures, and, finally, training and awareness. Although the legislation introduces a provision dedicated to cybersecurity certification systems (Article § 5a), the reference in Slovak law only concerns standards adopted under the Cyberesecurity Act (Regulation 2019/881), without mentioning international standards, thus failing to provide adequate space for intra-European coordination [21].

Conversely, the decree of the Hungarian Supervisory Authority for Regulated Activities (SZTFH) No. 1/2025. (I. 31.) On the rules for conducting a cybersecurity audit and the maximum fee for a cybersecurity audit,[11] dated January 31, 2025, the framework adopts a national standard explicitly based on the NIST 800-53A rev. 5 standard, "Assessing Security and Privacy Controls in Information Systems and Organisations". However, the Hungarian authority's intervention applies the international standard in a more binding, less flexible manner than initially intended. In particular, Annex 5 of the decree provides the structure of the audit activity. It identifies a rigidly defined set of checks based on interviews, document reviews, and practical tests (functional or configuration). Thus, the Hungarian approach establishes a fixed and standardised structure, whereas the NIST 800-53A rev. 5 framework, from which it draws, allows for an adaptable structure tailored to organisational needs. The same rigidity is evident in the handling of evidence, which is mandatory: failure to present documentation automatically results in a non-compliance judgment.

The Italian approach is similar to the Hungarian one, taking the NIST standard as a reference point but focusing on the NIST Cybersecurity Framework v. 2.0. In Italy, technical specifications are also defined by the competent authority: Determination No. 164179 of the National

[8] The IEC 62443 standard consists of a series of rules concerning the security of operational technology in automation and control systems. The series is divided into several sections that describe the technical and process aspects of automation and control system security. The standard, published by the International Electrotechnical Commission (IEC), is based on six general categories: General, Policies and Procedures, System, Component, Profiles, and Assessment. See https://www.iec.ch/blog/understanding-iec-62443.

[9] COBIT (Control Objectives for Information and Related Technologies) is a framework created by the Information Systems Audit and Control Association (ISACA) for managing and governing information technologies. The framework focuses on enterprise structure and defines a set of generic processes for IT management, with each process defined along with its inputs and outputs, key activities, process objectives, performance measures, and a basic maturity model. See https://www.isaca.org/resources/cobit.

[10] Zákon č. 366/2024 Z. z. (Act No. 366/2024 Coll.) of December 12, 2024, amending the cybersecurity law. Official English translation available at: https://www.nbu.gov.sk/data/att/3326.pdf.

[11] See the text of the decree at: https://njt.hu/jogszabaly/2025-1-20-8K. The decree is part of the process of implementing the NIS 2 Directive in Hungary, defined at the legislative level by Act LXIX of 2024 on cybersecurity in Hungary ("Cybersecurity Act"), adopted on December 20, 2024, which repeals previous regulations. See the full text of Act LXIX of 2024 in the official English translation at: https://njt.hu/jogszabaly/en/2024-69-00-00.

Cybersecurity Agency (ACN) dated April 14, 2025, establishes the basic methods and specifications for fulfilling the obligations under Articles 23, 24, 25, 29, and 32 of Legislative Decree No. 138 of September 4, 2024, implementing the NIS 2 Directive.[12] As stated in the determination, ACN's security measures are based on the National Framework for Cybersecurity and Data Protection (NFCDP), in its latest 2025 version.[13] This framework closely follows the structure of the NIST standard, incorporating the latest revisions adopted in December 2024. However, it is noteworthy that the text also includes technical measures derived from the application of Regulation (EU) 2016/679 on the protection of personal data (GDPR): for example, within the Identify and Protect functions, the NFCDP includes a category dedicated to Data Management for the classification, inventory, and management of personal data, and another dedicated to Data Security for the protection of data in transit and at rest, with direct reference to the measures required by the GDPR. This "variant" is a positive indicator because it signals an integration path between regulatory compliance requirements. The presence of alternative standards on the market, which employ different methodologies and security measures, has prompted ACN to establish a working group with national experts to define a "methodological bridge" between the requirements of ISO/IEC 27001 and those mandated by the NIST Cybersecurity Framework.[14] The result of this effort is the UNI/PdR 174:2025 standard, adopted by the Italian standardisation body on April 30, 2025.[15] This standard provides a mapping of requirements and measures, identifying terminological and methodological alignment between different standards. In this way, organisations already certified under ISO standards can determine how to extend their information management systems to meet the requirements of the NFCDP, thereby documenting the security measures required by the NIS 2 Directive without duplicating related economic and management burdens.

The approach adopted by the Belgian legislator, however, is different. Belgium implemented the NIS 2 Directive through the Law of April 26, 2024, which establishes a framework for the cybersecurity of network and information systems of public interest for public security purposes.[16] This was followed by the Royal Decree implementing the law of April 26, 2024.[17] The implementing measure, however, does not specify the technical measures to be adopted to ensure compliance with national legislation. Instead, Article 5 § 1 provides that essential entities

---

[12] Determination of the Director General of the National Cybersecurity Agency pursuant to Article 31, paragraphs 1 and 2, of Legislative Decree No. 138 of September 4, 2024, adopted according to the procedures set out in Article 40, paragraph 5, letter l), available at: https://www.acn.gov.it/portale/documents/d/guest/detacn_nis_specifiche_2025_164179_signed.

[13] National Framework for Cybersecurity and Data Protection – 2025 Edition (v2.1), available at: https://www.cybersecurityframework.it/.

[14] See the project presentation at: https://www.acn.gov.it/portale/w/uni/pdr-174-2025-pubblicata-la-nuova-prassi-di-riferimento-a-supporto-dei-soggetti-nis-certificati-iso-27001.

[15] UNI/PdR 174:2025 "Management System for Cybersecurity and Information Security Harmonized with UNI CEI EN ISO/IEC 27001 and the NIST CSF 2.0 Framework – Requirements," available at: https://store.uni.com/uni-pdr-174-2025.

[16] Law establishing a framework for the cybersecurity of networks and information systems of general interest for public security, 26 April 2024, available at: https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2024-05-17&lg_txt=f&pd_search=2024-05-17&s_editie=1&numac_search=2024202344&caller=sum&2024202344=4&view_numac=2024202344nx2024202344f.

[17] Royal Decree implementing the law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security, 9 June 2024, available at: https://www.ejustice.just.fgov.be/cgi/article.pl?language=fr&sum_date=2024-06-24&lg_txt=f&numac_search=2024005260.

See the presentation and text of the standard at: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework.

are free to choose between two options: the ISO/IEC 27001 standard and the national cybersecurity authority's standard. This means that technical compliance with either standard is also recognised as a presumption of compliance with the NIS 2 Directive. The Centre for Cybersecurity Belgium (CCB) immediately began drafting this standard in accordance with the requirements of Article 4 of the Royal Decree. The result is the Cyber Fundamentals Framework (CyFun®),[18] which includes a set of concrete measures for data protection, reducing the risk of common cyberattacks, and increasing an enterprise's cyber resilience.

Moreover, the CyFun standard mirrors the structure of European-level certification schemes, differentiating into three assurance levels: basic, important, and essential. The contents of the standard are based on an integration of various international standards: the NIST Cybersecurity Framework, ISO/IEC 27001,[19] CIS Controls,[20] and IEC 62443. It is important to note that the standard is developed based on the security measures required by the NIS 2 Directive, without integrating them with those necessary for GDPR compliance, as seen in the Italian framework. This difference between the Italian and Belgian models reflects two distinct approaches: while the Italian path seeks to maintain harmony with the primary international reference in the Western world, beginning to design a holistic vision for compliance with European regulations, the Belgian approach tends to position itself as an exclusive model dedicated to NIS 2 implementation.

The CCB manages the scheme framework and all associated documents as the Primary Scheme Owner. However, although CyFun is a Belgian framework, the authority hopes it will be recognised at the European level. Indeed, this process of expanding the scope of the standard is already underway: the Romanian National Cybersecurity Directorate (DNSC) is defining how CyFun can be qualified as an operational framework compatible with the implementation of the security measures required by national legislation.[21] The same is expected to happen in Ireland, as the Irish National Cyber Security Centre (NCSC) has formally included it among the reference models for implementing risk management measures required by NIS 2, alongside

[18] See the presentation and text of the standard at: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework.

[19] In fact, the text refers to numerous ISO standards: ISO/IEC 17000 Conformity assessment – Vocabulary and general principles, ISO/IEC 17021-1 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements, ISO/IEC 17029 Conformity Assessment – General principles and requirements for validation and verification bodies, ISO 19011 Guidelines for auditing management systems, ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary, ISO/IEC 27002 Information security, cybersecurity and privacy protection – Information security controls, ISO/IEC 27006-1 Information security, cybersecurity and privacy protection – Requirements for bodies providing audit and certification of information security management systems, ISO/IEC 27007 Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing. See CyberFundamentals Framework – Conformity Assessment Scheme, 7 March 2025, available at: https://atwork.safeonweb.be/sites/default/files/2025-07/CAS%20CyberFundamentals_Version%202025-03-07.pdf, p. 5.

[20] CIS Controls represent baseline configuration guidelines and recommended procedures for secure system configuration. Each guideline refers to one or more CIS Controls developed to help organizations improve their cybersecurity defense capabilities. See https://www.cisecurity.org/controls.

[21] Implementation in Romania took place with Government Emergency Ordinance No. 155 of 30 December 2024 on establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace (available at: https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121), followed by Law No. 124 of 7 July 2025 approving Government Emergency Ordinance No. 155/2024 on establishing a framework for the cybersecurity of networks and information systems in the national civil cyberspace (available at: https://legislatie.just.ro/public/DetaliiDocument/299675).

ISO/IEC 27001 and the NIST Cybersecurity Framework, pending the implementation of national legislation.[22]

What emerges from this picture is the fragmentation of national approaches, presented in Table 1, underscoring the crucial importance of international standards, particularly those established by NIST and ISO. However, even though these standards are frequently cited—if not used as a presumption of compliance—the variability of recognition and possible ambiguities in interpretation by Member States create a system that may appear (relatively) straightforward for companies operating nationally but is highly complex for entities operating cross-border [7].

Table 1

Comparison of cybersecurity measures for Essential and important entities

Country	Standards referred to	Approach
Slovakia	EU Cybersecurity Act standards only	Minimum content, national-centric
Hungary	NIST 800-53A rev5	Rigid audits, mandatory evidence
Italy	NIST CSF 2.0, GDPR, ISO↔NIST mapping	Integrated cybersecurity + GDPR model
Belgium	CyFun (NIST+ISO+CIS+IEC)	Dual-path: ISO or CyFun

The availability of a "translation" tool for standards would meet the needs of businesses without imposing common security measures or standardised evaluation criteria. An effort in this direction is evident in the strategies adopted by the Italian and Belgian cybersecurity authorities. However, the Italian model has focused only on comparing ISO 27001 standards with the NIST Cybersecurity Framework. In contrast, the Belgian model has achieved a broader goal by integrating more relevant standards into the new CyFun framework. A drawback of the Belgian solution is that it has concentrated on cybersecurity in the strict sense, without coordinating with the area that converges (though not completely overlaps) with it—namely, personal data protection. This is precisely the added value of the Italian system.

An effort toward a "dialogue" between models adopted at the national level can be found in ENISA's recent initiative dedicated to implementing measures under the NIS Directive in light of the Commission's Implementing Regulation 2024/2690. The text,[23] currently still under consultation, provides guidance to support stakeholders in implementing the technical and methodological requirements set out in Article 2 and the annex of the Commission's

[22] See the draft of the NIS 2 Risk Management Measures Guidance, presented on 4 June 2025 by the NCSC, available at: https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf. The text is qualified as "draft" pending approval of the National Cybersecurity Bill.

[23] ENISA, NIS 2 Implementing Guidance – On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555, presented for public consultation on 26 June 2025, available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

implementing regulation. Specifically, ENISA's document contains practical advice on parameters to consider for compliance with requirements, examples of supporting evidence, and a mapping that correlates each requirement with European and international standards and national frameworks. Although ENISA clearly states that this mapping does not represent equivalence between standards, it serves as a starting point that highlights similar cybersecurity requirements across different models. The document currently considers four international standards[24] and an equal number of national standards[25] without establishing new standards or duplicating existing ones. This approach could be expanded by progressively integrating the choices of all Member States to facilitate comparison of the requirements provided.

4. Supply chain control

A closely related aspect is that of supply chain control from a cybersecurity perspective. As anticipated, one of the requirements set out in Article 21 regarding security measures to be adopted by essential and important entities is "the security of the supply chain, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers". The Directive does not specify the tools or means by which essential and important entities must implement this obligation, leaving it to the entities themselves to verify whether organisations in their supply chain ensure an adequate and proportionate level of security. This aspect acquires an increasing importance in the healthcare sector, where the dependency on complex supply chains that include both research and development areas (for instance biologists, vaccinologists or other laboratories), distributors (such as logistics and delivery service providers), vendors and manufacturers of medical devices, as well as other providers (such as pharmacies, assisted living, etc.) is the rule. ENISA stresses that vulnerabilities in these components can propagate across networks, creating systemic risks that compromise both operational continuity and patient safety. The NIS 2 Directive's requirement to address supply chain risks, therefore, assumes particular significance in this context.

As a result, the supply chain control obligation can be perceived from two perspectives: on the one hand, the entities concerned may impose cybersecurity risk management measures on organizations in their supply chain (such as suppliers and subcontractors) and supervise them; on the other hand, it implies that entities not falling within the scope of NIS 2 may be prompted to adopt cybersecurity risk management measures to enter the market.

Table 2

Comparison on supply chain control

[24] The text takes into account the following: ISO/IEC 27001:2022, ISO/IEC 27002:2022, NIST Cybersecurity Framework 2.0, ETSI EN 319 401 V2.2.1 (2018-04), CEN/TS 18026:2024.

[25] National standards include those of Belgium, Finland, Germany, Greece, and Spain, based on information provided by the NIS Cooperation Group's security measures working group.

Country	Contractual Obligations	Risk Management Measures	Extension to Suppliers
Slovakia	Mandatory clauses: equal security + notification duties	Supplier risk assessments + audit rights	Strong indirect extension via contracts
Italy	Mandatory clauses + due diligence requirements	Full lifecycle monitoring, supplier criticality	Very strong indirect extension across supply chain
Belgium	Only mandatory at the highest assurance level	Tiered guidance; voluntary uptake for others	Moderate extension, depends on the assurance level

This double perspective is clearly reflected in the choices made by national legislators on this issue, highlighting interventions that are particularly invasive in relation to the contractual choices of the entities concerned, as described in Table 2. For example, Slovak legislation introduces specific rules dedicated to managing cybersecurity in the supply chain (Article § 19 (2)), requiring essential entities to include in their risk assessment those associated with their suppliers. This is linked to an obligation for the essential entity to stipulate, in contracts with suppliers, security measures and notification obligations equivalent to those applied internally. The essential entity can verify compliance with these measures through audit systems.

A similar approach is also provided by the NFCDP, recognised by ACN in the Italian system. In particular, the "Govern" section includes a series of specific controls for the supply chain (GV.SC). Not only are entities required to establish objectives, policies, and risk management processes for the supply chain, which must be communicated and coordinated with suppliers, customers, and partners, but they must also integrate supply chain risk management into their overall risk management strategy and differentiate suppliers based on their criticality. Furthermore, cybersecurity requirements must be incorporated into contracts and agreements with suppliers and third parties, and due diligence checks must be conducted to mitigate risks before formal relationships are established. For example, the following elements can be verified in advance: assessment of the supplier's security policies, verification of compliance with international standards, analysis of risks related to supplied software, hardware, or services, checking for known vulnerabilities in products or services, requesting security audits or certifications, evaluation of business continuity and disaster recovery plans of the supplier, control of the origin and integrity of components, reputational monitoring, and review of past security incidents. Moreover, during relationships with such suppliers, entities are required to monitor supply chain security practices throughout the lifecycle of products and services (see GV.SC-01 to GV.SC-10 of the NFCDP).

The Belgian system, on the other hand, does not directly require all concerned entities to include contractual clauses to manage cybersecurity risk in the supply chain. The CyFun framework differentiates three assurance levels: basic, important, and essential. Only at the highest, most critical level are controls provided that explicitly require entities to include contractual clauses with suppliers and third parties, requiring them to implement adequate

measures to meet the objectives of the entity's cybersecurity policy.[26] In addition, the CCB recommends that all entities not within the scope of the NIS 2 Directive adopt adequate and proportionate risk management measures to prepare for the possibility of being part of the supply chain of an entity within its scope of application. In this case, they may refer to CyFun to identify and implement the concrete measures that might be required of them.

The requirement concerning supply chain control may serve as a tool to extend, through contractual mechanisms, the obligations of the NIS 2 Directive well beyond the boundaries defined by its scope of application. Although the Directive explicitly excludes small and micro-enterprises from its scope, these businesses constitute the backbone of the European market, making it likely that a large portion of them will be part of the supply chains of essential or important entities, as they often provide niche products or services. Therefore, it's hard to imagine these enterprises remaining entirely outside the reach of cybersecurity measures. While some national models, including the Italian one, specify a prioritisation criterion for companies based on their criticality, it is easy to foresee that niche suppliers will be indirectly incorporated into the NIS 2 framework.

Moreover, the NIS 2 Directive does not specify the type of security measures required for the supply chain, stating that the multi-risk management approach must include "the security of the supply chain, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers," where the term "including" leaves room for other types of measures [22].

5. Conclusions

The analysis of the regulatory harmonisation process in cybersecurity at the European level, from the NIS Directive to the adoption and implementation of the NIS 2 Directive, reveals a complex and somewhat ambiguous picture. The European legislator's intention to strengthen Member States' cyber resilience through the introduction of standard minimum requirements and a clearer system of obligations and responsibilities for essential and important entities is reflected in NIS 2, which represents a more mature regulatory expression compared to its predecessor. However, the effectiveness of the harmonisation process largely depends on the implementation choices of individual Member States, which still retain significant discretion in defining operational measures, technical requirements, and control mechanisms.

The comparison between national models adopted by countries such as Italy, Belgium, Hungary, and Slovakia highlights at least three levels of divergence that affect the scope and effectiveness of the desired harmonization: (1) the selection and adaptation of reference standards, (2) the level of integration with adjacent regulations (such as personal data protection), and (3) the extension of obligations along the supply chain, even beyond entities formally included in the Directive.

From a technical perspective, there is a gradual convergence toward adopting widely recognised international standards, particularly the NIST Cybersecurity Framework and the ISO/IEC 27000 series, which serve as a common basis for defining security measures. However, convergence on content does not yet translate into actual harmonisation of implementation practices. The Italian case, with the creation of the National Framework for Cybersecurity and

[26] See CyberFundamentals – ESSENTIAL, Version: 01.03.2023, available at: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework. In particular, controls ID.SC-1 to ID.SC-5.

Data Protection and the development of the UNI/PdR 174:2025 standard, demonstrates an explicit attempt to establish methodological bridges between different standards, facilitating organisations' transition across compliance models. This approach demonstrates an integrated vision that considers not only cybersecurity in the strict sense but also coherence with the European regulatory framework on personal data protection.

Conversely, the Belgian experience, with the development of the CyFun framework, offers an interesting alternative: a national model that integrates multiple international standards (NIST, ISO, IEC, CIS) while remaining focused exclusively on cybersecurity. The lack of coordination with other regulatory areas, such as data protection, is a potential weakness, especially for operators that must comply with multiple regulations simultaneously. This confirms that, although a common technical "substrate" exists at the European level, developing a truly shared "regulatory language" still requires significant integration work among the different legal and regulatory cultures of individual states.

Furthermore, supply chain management emerges as one of the key factors determining the actual scope of NIS 2 beyond its formal boundaries. The obligation for essential and important entities to assess and monitor risks along the supply chain represents, in practice, an indirect mechanism for extending the Directive's scope to entities not formally included within it. This is particularly relevant for the European economic fabric, strongly characterised by small and micro-enterprises operating in strategic and highly specialised sectors. Slovak legislation, which explicitly requires the inclusion of cybersecurity clauses in supplier contracts, and the Italian model, which integrates supply chain risk management into a structured security governance system, represent examples of approaches oriented toward holistic risk management. Conversely, the Belgian model reserves more stringent obligations only for entities classified as essential and adopts a gradual approach based on assurance levels.

In light of the above, it can be stated that the circulation of implementation models remains only partially achieved. While there is increasing reliance on the same technical references, the diversity of application methods remains an obstacle to creating a single, accurate cybersecurity market. ENISA's initiative, with the publication of methodological guidelines and mapping tools between international standards, represents a first concrete step toward creating a shared technical vocabulary that can facilitate interoperability among different national models and support businesses operating across borders. However, the absence of a legal mandate for these tools limits their effectiveness, making it desirable to strengthen central coordination and, if necessary, evolve toward more stringent harmonisation in particularly sensitive sectors.

In conclusion, the effective harmonisation of the European cybersecurity framework depends not only on formal legislation but, above all, on implementation practices, integration between regulatory areas, and institutional cooperation between national authorities and European bodies. The dual foundation of this process—technical, represented by shared security frameworks, and value-based, centred on protecting fundamental rights and critical infrastructures—requires a systemic vision that considers cybersecurity not as an isolated domain but as an integral part of the European integration project and the defence of its shared digital space.

Acknowledgements

The research was supported by the Italian Ministry of University and Research, under the complementary actions to the NRRP 'Fit4MedRob - Fit for Medical Robotics' Grant (# PNC0000007).

Declaration on Generative AI

During the preparation of this work, the authors used the following tools: Copilot to translate Slovak and Hungarian legislation into English, then the authors reviewed and verified the content through literature review; Grammarly to grammar and spelling check, paraphrase, and reword, after using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] M. Lesk, The New Front Line: Estonia under Cyberassault, in IEEE Security & Privacy, 2007, vol. 5, no. 4, pp. 76–79.

[2] S.J. Shackelford, Estonia Two-and-A-Half Years Later: A Progress Report on Combating Cyber Attacks, Journal of Internet Law, 2010, available at: https://ssrn.com/abstract=1499849.

[3] F. Gaggero, L'azione normativa del governo in materia di cybersecurity, in F. Bailo and M. Francaviglia (eds), Bilanci e prospettive intorno ai poteri normativi del governo, Naples, 2003, pp. 347–374.

[4] European Commission, Communication on Critical Information Infrastructure Protection – Achievements and Next Steps: Towards Global Cyber-Security, 2009.

[5] European Commission, Communication, on Network and Information Security: Proposal for a European Policy Approach, 2001.

[6] European Commission - Joint Research Centre, Cyber security in the health and medicine sector: A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings, 2024. Publications Office. https://data.europa.eu/doi/10.2760/693487

[7] European Cyber Security Organization, White Paper on NIS 2 Implementation: Challenges and Priorities, 2025, available at: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf.

[8] European Commission, Commission Staff Working Document Impact Assessment Report – Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148, December 16, 2020, SWD(2020) 345 final.

[9] J.D. Michels, and I. Walden, Beyond "Complacency and Panic": Will the NIS Directive Improve the Cybersecurity of Critical National Infrastructure?, 2020.

[10] S. Schmitz-Berndt, Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. Journal of Cybersecurity, 2023, 9(1), tyad009. https://doi.org/10.1093/cybsec/tyad009

[11] P. Contreras, The Transnational Dimension of Cybersecurity: The NIS Directive and Its Jurisdictional Challenges. In C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H.

Hindy, & M. G. Jaatun (Eds.), Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Nature Singapore, 2023, pp. 327–341).

[12] C. Gaie and M. Mueck, Introduction to the Networks and Information Systems 2 (NIS2) Directive. In M. Mueck & C. Gaie (Eds.), European Digital Regulations, Springer Nature Switzerland, 2025, Vol. 265, pp. 161–180).

[13] T. Sievers, Proposal for a NIS directive 2.0: Companies covered by the extended scope of application and their obligations. International Cybersecurity Law Review, 2021, 2(2), 223–231.

[14] A. Gruber, and N. Ségur-Cabanac, Necessary or premature? The NIS 2 Directive from the perspective of the telecommunications sector. International Cybersecurity Law Review, 2021, 2(2), 233–243.

[15] F. Casarosa, and G. Comandé, Private Law Perspectives of Cybersecurity. In AA.VV (Ed.), Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024), Salerno, Italy, April 8–12, 2024. 2024, CEUR.

[16] D. Markopoulou, V. Papakonstantinou, and P. De Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 2019, 35(6), 105336

[17] S. de Nitto, Regolazione per standard: Un valore aggiunto? Federalismi.it, 2022, 19, 81.

[18] I. Kamara, European cybersecurity standardisation: A tale of two solitudes in view of Europe's cyber resilience. Innovation: The European Journal of Social Science Research, 2024, 37(5), 1441–1460.

[19] M. Rampášek, M. Mesarčík, and J. Andraško, Evolving cybersecurity of AI-featured digital products and services: Rise of standardisation and certification? Computer Law & Security Review, 2025, 56, 106093.

[20] F. Serini, La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana. Rivista italiana di informatica e diritto, 2024, 5(2), 41–76.

[21] J. Ristvej, M. Tonhauser, D. Chovanec, J. Kubás, B. Kollár, and Z. Zamiar, Cyber resilience conceptual model for European Union NIS2 standards implementation in Slovakia. Scientific Reports, 2025, 15(1), 26902

[22] M. Anon, The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things. SSRN Electronic Journal, 2024.