standICT.2026.eu

ICT Standardisation Observatory and Support Facility in Europe

Case Study 1

NIS2 Directive - Standards Challenges for a Unified Implementation

Axel Thévenet (OFE)

Funded by the European Union

February 2026

1. Introduction

The NIS2 Directive 2022/2025[1] was introduced to update Europe's cybersecurity framework, addressing developments in digitalization and the evolving nature of threats. Adopted by the Council of the EU in November 2022, the Directive came into force in January 2023.[2] It was proposed by the European Commission as part of a new EU cybersecurity strategy aimed at enhancing Europe's collective resilience.[3] Although the Directive does not mandate the drafting of new standards, Article 25 strongly encourages Member States (MS) to use relevant European and international standards and technical specifications for its implementation.

In comparison to the original NIS Directive, NIS2 applies to eight additional sectors, including public administrations and digital services such as social networks and data centers. Entities within its scope are divided into two categories: essential and important. Essential entities must meet supervisory measures as soon as NIS2 becomes effective in 2025, while important entities are under ex-post supervision. To facilitate transposition into national law, the scope of NIS2 defines entities' sizes, with small and micro-entities a priori excluded from direct compliance.[4]

As a horizontal regulation, the NIS2 Directive affects a wide range of sectors and involves many diverse stakeholders, both directly and indirectly. This includes traditional industries as well as software stakeholders and the IT industry, reflecting the broad scope of the Directive's impact. The development of harmonised standards for the NIS2 Directive can be seen as a precursor or first attempt to establish a horizontal framework of standards with significant software implications.

This case study draws on insights from two stakeholder interviews and publicly available sources; the perspectives reported here do not necessarily represent the full spectrum of views within the cybersecurity and standardisation community. It explores the implementation of the NIS2 Directive through existing standards, highlighting the role of Article 25 in encouraging Member States to use established European and international standards. It examines the challenges and opportunities in transposing the Directive into national laws, particularly focusing on the impact on medium-sized enterprises and the varying levels of cybersecurity maturity across different sectors. This highlights the challenges faced by the European Standardization System and regulators in listing or creating harmonized standards that are relevant across diverse sectors. It emphasizes the need to balance the inclusion of a wide range of stakeholders with the demand for speed and the delivery of quality standards.

1 **European Parliament and Council of the European Union**, *Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)*, Official Journal of the European Union, L 333/80, 27 December 2022, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555. NIS refers to "Network and Information System"

2 **European Parliament**, *Review of the NIS Directive*, available at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive.

3 **European Commission** (last updated 15.01.2025), NIS2 Directive: new rules on cybersecurity of network and information systems

4 Directive on measures for a high common level of cybersecurity across the Union - Factsheet NIS2

2. Implementing NIS2 through existing standards

Article 25 strongly encourages MS to use relevant European and international standards and technical specifications for NIS2 implementation. Cybersecurity standards experts consulted for this case study consider this reference to existing standards as overall positive to acknowledge existing standards rather than mandating new ones. Experts and relevant national authorities, as well as ENISA, are particularly highlighting ISO27001[5] as the standard of reference for NIS2. However, the experts also noted that more direct reference to specific standards and mechanisms would have been useful to leverage existing certifications in facilitating compliance.

More direct references to standards are likely to come through ENISA, the EU Cybersecurity Agency, as Article 25 mandates ENISA to draw up implementation advice in relation to existing standards. In November 2024, ENISA published a first draft of technical guidance for cybersecurity measures.[6] The draft includes a mapping correlating different European, international, and national standards frameworks that can inform NIS2 implementation. In this draft ENISA specifies that the implementing guidance is not meant to establish new standards, further emphasising that NIS2 compliance is to be assessed through existing standards.[7]

A practical example of the applicability of existing standards for NIS2 is the transposition of the Directive into Belgian law. Belgium has appointed the Center for Cyber Security (CCB) as the national authority for NIS2 and has based its law on the CCB's CyFun Standard, meaning that compliance with the CyFun framework, for instance through an ISO27001 certification will act as a presumption of compliance with NIS2.[8] CyFun is also included in ENISA mapping[9] and is being considered by other MS such as Luxembourg.[10] Another example is Spain, which has not yet transposed the directive into law, but the National Cryptologic Centre which is to support entities in Spain with NIS2 implementation has published a compliance guide specifying in which instances the Esqueme Nacional de Seguridad (ENS) certification, indicating compatibility with ISO27001, can be used for compliance with NIS2.[11]

5 ISO/IEC 27001 is an international standard for information security management systems (ISMS). It provides a framework for organisations to manage sensitive information through policies, controls, and procedures aimed at ensuring confidentiality, integrity, and availability. The standard adopts a risk-based approach, requiring regular assessments and improvements. Certification to ISO/IEC 27001 demonstrates adherence to best practices in information security, recognised globally across various industries.

6 In relation to the NIS2 Implementing Act, itself published by the Commission on 17 October 2024, see European Commission. (2024, October 17). *New rules to boost cybersecurity for the EU's critical entities and networks.* Available at: https://digital-strategy.ec.europa.eu/en/news/new-rules-boost-cybersecurity-eus-critical-entities-and-networks

7 European Union Agency for Cybersecurity (ENISA). (2024, November 7). *Asking for your feedback: ENISA technical guidance for the cybersecurity measures of the NIS2 Implementing Act.* Available at: https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act

8 Centre for Cybersecurity Belgium (CCB). (2024, April 26). *NIS2.* Retrieved from https://ccb.belgium.be/regulation/nis2

9 European Union Agency for Cybersecurity (ENISA). (2024, November 7). *Asking for your feedback: ENISA technical guidance for the cybersecurity measures of the NIS2 Implementing Act.* Retrieved from https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act

10 Wavestone. (2024, November 25). NIS 2: Where are European countries in transposing the directive? Retrieved from https://www.wavestone.com/en/insight/nis-2-european-countries-transposing-directive/?utm_source=mktg&utm_medium=news&utm_campaign=Riskinsight_EN_11_2024

11 Centro Criptológico Nacional (CCN). (2024, August 1). *NIS2 Directive.* Retrieved from https://www.ccn.cni.es/en/regulations/nis2-directive

3. NIS2 Implementation Challenges and Opportunities

Transposing the Directive into national law

NIS2 being a directive, the main challenge is the fragmentation of its implementation through different national laws. The two interviewees highlighted that the lack of a unified implementation framework across EU Member States will add to the compliance burden for entities in scopes, with different implementation measures and certification schemes required across Member States. Some experts further stress the compliance burden for small and micro businesses that are not directly in scope of the directive but are impacted through the supply chain requirements and might find themselves having to comply with different cybersecurity frameworks.

Both interviewees noted that, despite the reference to existing standards, delays and limited transparency in national transposition have made it difficult for stakeholders to see how standards will underpin presumption of compliance. They cautioned that without agreement across Member States on which standards to use, the reference in the Directive may have limited impact on improving clarity or on practically enhancing cybersecurity. These observations reflect the experience of the two interviewees and may not be universally shared among Member State authorities or industry actors.

One interviewee suggested that a regulation, rather than a directive, might have offered clearer and more uniform expectations. The other interviewee stressed the value of national flexibility under a directive. These views highlight that the choice between a regulation and a directive remains debated among stakeholders. At the same time, they noted that regulation, through its larger scope, would have increased the cost of compliance including on SMEs and that the choice of a directive referencing existing standards helps with the costs-benefits balance of compliance with cybersecurity measures for SMEs. These diverging views illustrate that the choice between a regulation and a directive remains debated among stakeholders.

Impact on Medium Size Businesses

Cybersecurity standardisation experts have expressed concerns as to the impact on medium-sized enterprises.[12] Caught in the scope of the directive, medium-size businesses are less likely to have in place the framework needed to manage information security or the expertise required to set it up - a challenge furthered by the fragmentation risk of aligning with different legal instruments across the EU.

Cybersecurity Maturity Levels

Interviewees raised concerns about a potential domino effect with broad consequences across the European industrial landscape is likely to be expected, in particular with concerns to service providers. This is related to existing discrepancies across different fields when it comes to maturity levels in information security. While entities that provide digital services are likely to see the NIS2 Directive as a small variation of the previous one and of existing standards, public services or sectors that are more traditionally oriented towards production have less experience with cybersecurity standards and little access to related information. Experts also noted the lack of information available regarding existing standards and how they can be leveraged, expressing concerns that most relevant national entities have yet to provide substantial guidance as to standards and certifications which can be used for compliance with the directive.

12 European DIGITAL SME Alliance. (2021, April 1). *Cybersecurity Update: DIGITAL SME's views on proposed EU law about Security of Network and Information Systems (NIS2 Directive).* Retrieved from https://www.digitalsme.eu/cybersecurity-update-digital-smes-views-on-eu-law-about-security-of-network-and-information-systems-nis2-directive/

4. Conclusion

The NIS2 Directive exemplifies the use of existing standards to streamline compliance and reduce fragmentation across the EU. By encouraging the adoption of established standards like ISO27001, it offers a unified approach to cybersecurity that can ease the compliance burden on medium-sized enterprises and promote consistency across diverse sectors. However, challenges remain in ensuring transparency and agreement on standards implementation across Member States, highlighting the need for continued collaboration and guidance to fully realize the Directive's potential.

standICT.2026.eu

ICT Standardisation Observatory and Support Facility in Europe

Disclaimer

This case study has been developed for informational purposes only and does not represent any official position of the European Commission. It is part of a broader series of case studies launched under StandICT.eu to explore emerging challenges and developments in the ICT standardisation landscape. The series aims to stimulate critical reflection and discussion among stakeholders on topics of strategic relevance to the European and global standardisation ecosystem. The views expressed are those of the authors and interviewees and do not necessarily reflect the views of the European Commission, any SDOs or any affiliated organisation.

Funded by
the European Union