LUND UNIVERSITY

SCHOOL OF ECONOMICS AND MANAGEMENT

# EU Cybersecurity obligations for healthcare providers

## The NIS 2 Directive, the Cybersecurity Act, and the Emerging EU Certification Framework

**Daniel Simfors, Mathilda Helander**

DEPARTMENT OF BUSINESS LAW

Master's Thesis in European and International Trade Law

15 ECTS

HARN63

Spring 2026

# Contents

# Abstract

The purpose of this thesis is to examine the extend of cybersecurity obligations imposed on healthcare providers under EU law. To achieve this, the research questions focus on selected parts of the NIS 2 Directive and the Cybersecurity Act. Particular attention is afforded cybersecurity risk-management measures required under Article 21 of the NIS 2 Directive, as well as the role of certification schemes established under the Cybersecurity Act. The thesis further considers the recently proposed Cybersecurity Act 2, with its targeted amendments to the NIS 2 Directive, in order to assess the future development of EU cybersecurity regulation within the healthcare sector.

The thesis finds that neither the NIS 2 Directive nor the Cybersecurity Act establishes a fully cohesive or horizontally applicable cybersecurity framework. Nevertheless, the NIS 2 Directive achieves an important regulatory foundation, requiring healthcare providers to implement appropriate technical, operational, and organisational cybersecurity measures. Examples include secure medical devices, protecting its physical environment, and cybersecurity training for staff. At the same time, healthcare providers retain considerable discretion in determining which of those measures are suitable in practice.

By contrast, the regulatory significance of certification schemes under the Cybersecurity Act remains limited. The certification framework operates largely on a voluntary basis and predominantly targets manufacturers of digital solutions. From the forward-looking perspective, the proposed Cybersecurity Act 2 indicates a significant strengthening of EU certification. It suggests a shift toward more market-oriented perspectives, introduces cyber posture assessments, and enhanced operational supply-chain security. Whether these developments will produce a more functionable cybersecurity framework within the healthcare sector, remains to be determined.

**Keywords**: EU Cybersecurity law, Healthcare, NIS 2 Directive, Cybersecurity Act, ICT certification.

# Abbreviations

| | |
|---|---|
| AVA_VAN | Vulnerability Analysis |
| CJEU | Court of Justice of the European Union |
| CSA | Regulation (EU) 2019/881 of the European Parliament and of the Council on 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) |
| CSA 2 | Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) |
| CSIRT | Computer Security Incident Response Team |
| ECCF | European Cybersecurity Certification Framework |
| EHDS | European Health Data Space Regulation |
| ENISA | European Network and Information Security Agency |
| EUCC | European Union Cybersecurity Certification |
| ICT | Information and Communication Technology |
| ICT-PSP | Information and Communication Technology Products, Services and Processes |
| IoT | Internet of Things |
| ISMS | Information Security Management Systems |
| ISO/IEC | International Organisation for Standardisation and the International Electrotechnical Commission |
| NIS 2 | Directive (EU) 2022/2555 of the European Parliament and og the Council 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 (NIS 2 Directive) |
| MSSP | Managed Security Service Provider |

# 1 Introduction

## 1.1 Background

Any attempt at addressing cybersecurity within the European Union (EU) is a difficult endeavour.[1] Information and network systems permeate almost every aspect of modern life and are a cornerstone of societal welfare.[2] Globally, access to a digital information ecosystem has enabled social networks, the exchange intangible information, the organisation of lives, and the growth of businesses.[3] While this interconnectivity creates significant economic opportunities, it also exposes us to digital vulnerabilities.[4] In today's society, disruptive cyberattacks repeatedly affect critical infrastructure in the Union.[5] In response to this increasingly sophisticated cyberthreat landscape, new cybersecurity strategies have been introduced by the European Commission.[6] These focus on protecting essential services such as healthcare, energy, transport and digital infrastructure, while also addressing the growing risks associated with connected devices and emerging technologies.[7]

Healthcare in particular has benefited from innovations such as electronic health records, telemedicine and AI-driven diagnostics.[8] At the same time, it is one of the most frequently targeted fields for cyberattacks of any critical sector, where more than half of these attacks involve ransomware.[9] The EU is therefore taking action to protect healthcare as critical infrastructure through an action plan built on existing legislation, with the aim of ensuring that healthcare systems, institutions and connected medical devices are resilient against cyberthreat and that patient safety and trust are protected.[10] Accordingly, this thesis focuses on the healthcare sector,

[1] Antonio Segura Serrano (ed), '*The EU's Cybersecurity policy: results and context* in *Global Cybersecurity and International Law'* (Routledge 2024) chap. 9, 154.

[2] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151/15, recital 2. See also European Commission, 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' COM(2016) 410 final, 2.

[3] Krzysztof Świtała, '*Opportunity Makes the Thief. A Risk Analysis and Vulnerability Identification Approach Information Security Management Systems as a Method of Countering Cybercrimes*', vol. 60, no. 1 (Review of European and Comparative Law 2025) 190-191.

[4] Directive (EU) 2022/2555 of the European Parliament and of the Council 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) [2022] OJ L 333/80, recital 2.

[5] Roderick Parkes, '*Nuts and Bolts: Safeguarding the critical infrastructure of the Union* in Daniel Fiott (ed), *Protecting Europe: The EU's Response to Hybrid Threats'* (European Union Institute for Security Studies 2019) 23-24.

[6] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint communication, 'Strengthening EU Economic Security' JOIN(2025) 977 final, 3.

[7] European Commission, 'EU Cybersecurity Strategy' (New Cybersecurity Strategy) <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy> accessed May 21 2026.

[8] European Commission, 'European action plan on the cybersecurity of hospitals and healthcare providers' (EU plan for healthcare providers) <https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en> accessed 22 May 23 2026.

[9] European Union Agency for Cybersecurity (ENISA), 'Cyber Hygiene in the Health Sector' (ENISA Cyber Hygiene) <https://www.enisa.europa.eu/publications/cyber-hygiene-in-the-health-sector> accessed 23 April 2026.

[10] New Cybersecurity Strategy, *op cit.*, 1.

with the scope limited to the horizontal common denominators and minimum obligations arising from the acts selected below and their associated material.

Before proceeding, it's important to emphasise that the complexity of cybersecurity extends beyond its technical dimensions. From a legal perspective, cybersecurity within the EU is characterised by a fragmented regulatory landscape consisting of sector-specific legislation,[11] standardisation efforts,[12] legislative proposals,[13] and IT infrastructure policies.[14] Consequently, cybersecurity cannot be understood as an autonomous field of law.[15] Rather, it intersects with data protection law, competition law, and even fundamental rights.[16] The rationale behind cybersecurity protection also differs. Some measures are ex-ante, focusing on prevention and detection, while others are ex-post, focusing on response and recovery.[17] This distinction shapes the legislative architecture. Some legal acts impose technical requirements of products,[18] other regulate specific sectors,[19] and others address cybersecurity functionality through instruments such as certification schemes.[20]

## 1.2 Purpose and research questions

The purpose of this paper is to describe and analyse the extent of cybersecurity obligations imposed on healthcare providers within EU cybersecurity law, according to selected parts of Directive 2022/2555 (NIS 2) and Regulation EU 2019/881 (CSA). To accomplish this, the questions set out below will be used.

Question 1: What do cybersecurity risk-management measures and reporting obligations as held within the NIS 2 Directive (EU 2022/2555), entail for healthcare providers?

Question 2: To what extent does the certification framework established by the Cybersecurity Act (EU 2019/881), affect the cybersecurity obligations of healthcare providers?

[11] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (Cybersecurity Act 2)' COM(2026) 11 final, 2-3.

[12] NIS2 Directive, *op cit.*, recital 81.

[13] Segura Serrano, *Global Cybersecurity and International Law, op cit.*, 156.

[14] Joint Communication, 'Strengthening EU Economic Security', *op cit.*, 1-2.

[15] NIS2 Directive, *op cit.*, recital 4-6.

[16] *Ibid*, recital 14,70, 119.

[17] *Ibid*, recital 122.

[18] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 13 December 2023 laying down horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 (Cyber Resilience Act) [2024] OJ L 2847, Art. 6.

[19] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act) [2022] OJ L 333/1, Art. 1.

[20] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC Implementing Regulation) [2024] OJ L 482/1, Art. 2.

Question 3: How does the proposed Cybersecurity Act 2, and its targeted amendments to the NIS 2 Directive, reshape the cybersecurity framework applicable to healthcare providers?

## 1.3 Delimitations

This thesis will not in detail examine the institutional organisation and operational activities of EU cybersecurity bodies such as ENISA, the CSIRTs Network, and EU-CyCLONe. However, two deviations are in order. First relates to ENISA's enhanced role in the proposed Cybersecurity Act 2, and its targeted revision of the NIS 2 directive. The second relates to IoT in the chapter relating to supply chain security, as it otherwise is not of central focus.

Furthermore, this examination will not focus on member state enforcement mechanisms of cybersecurity breaches or legal questions concerning jurisdiction and territoriality.

## 1.4 Method and materials

To answer the research questions, this thesis employs a legal dogmatic method. The method is characterised by analysing, describing and explaining the law in a in a given legal setting *de lege lata*.[21] For the purposes of this thesis, this means determining the cybersecurity obligations imposed on healthcare providers according to the selected EU legal acts. As this thesis explores requirements posed by EU law, the interpretative tools commonly used by the Court of Justice of the European Union (CJEU) are included.[22] These utilise textual, contextual, and teleological means of interpretation.[23] The textual approach requires looking at what words are meant to convey in a literal sense, which further holds that whenever the provision in question is clear and precise, it may not be replaced by any other interpretative tool. [24] This is followed by the contextual approach, which accepts the operational functionality of the provisions as it forms part of a broader systematic framework.[25] This systematic approach considers the legislator a rational actor who assume that the provisions form part of a coherent legal order which in turn dictates the outcome in a given legal setting.[26] However, this is not to be equated to a narrow and consistent interpretation which would risk conflict with the legal area it takes part in.[27] Lastly, the teleological approach serves to interpret the provision in light of its purpose and objective.[28] This will require balancing the various objectives in a

[21] Jan M Smits, *'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research*' (Maastricht European Private Law Institute Working Paper No 2015/06, 2015) 8.
[22] Koen Lenaerts and José A. Gutiérrez-Fons, *'To say what the law of the EU is: Methods of Interpretation and the European Court of* Justice' Academy of European Law (AEL 2013/9).
[23] *Ibid*, 3-5.
[24] *Ibid.*
[25] *Ibid*, 6-9, 13-18.
[26] *Ibid*, 13.
[27] *Ibid*, 14.
[28] *Ibid*, 24-28.

provision against each other, since the language is purposely broad, and thereafter determine the most balanced outcome.[29]

Crucially, the *sui generis* aspect of EU cybersecurity does partly challenge the traditional methodological approach of a dogmatic inquiry. Much of the material surrounding the chosen acts are proposals, action plans, working documents and law journals.[30] Even standards developed jointly by the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC), while explicitly referenced as representing the state of the art, are not strictly legally binding.[31] Nonetheless, this does not render a legal dogmatic method unsuitable. Rather, these sources are anchored in the acts chosen and form part of a broader context in which EU cybersecurity law operates. It is therefore a fitting method to achieve the desired end.

This thesis will also include the recently proposed Cybersecurity act 2 (CSA 2) with a targeted revision of the NIS 2 Directive. This provides valuable insights into the current EU cybersecurity ecosystem. Again, while not legally binding, it provides indispensable guidance for healthcare providers future obligations and is thus to be included. Finally, while the acts frequently target *member states* to act and refrain from certain behaviour, the mandatory requirements ultimately depend on the actions of services providers. These objectives can thus only materialise through their own actions.

## 1.5 Outline

Following this introductory Chapter, Chapter two examines the NIS 2 Directive and answers the first research question by analysing the directive's scope, the cybersecurity risk-management measures and reporting obligations it imposes, and the proposed targeted amendments relevant to healthcare providers. Chapter three examines the Cybersecurity Act and answers the second research question by assessing the certification framework, the role of Information and Communication Technology (ICT) standardisation, and the extent to which certification influences the cybersecurity obligations of healthcare providers. It also examines the proposed Cybersecurity Act 2 and what it entails for healthcare providers. Research question three is answered throughout Chapter two and three. The thesis concludes with Chapter four which synthesises the preceding analysis and assesses whether the NIS 2 Directive along with the Cybersecurity Act provides a coherent and workable regulatory framework for healthcare providers.

[29] *Ibid.*
[30] NIS2 Directive, *op cit.*, recital 2.
[31] *Ibid*, recital 79-82.

# 2 The NIS 2 Directive

## 2.1 Introduction

Directive 2016/1148 (NIS1) laid down the groundwork for cybersecurity in the EU and represented a significant mind-shift in relation to information security.[32] However, it still contained inherent gaps allowing for national discrepancy and left providers of essential services, such as healthcare entities, practically untouched.[33]

Directive 2022/2555 (NIS 2) was therefore formally adopted by the European Parliament with the ambition to accelerate the levels of cybersecurity within the Union.[34] Compared to its predecessor, it sets out a wider scope, clearer rules and stronger supervision tools for the Member States.[35] It establishes a baseline for cybersecurity protection from a more "ex-ante risk-management perspective" common to regulating other fields of digital technology,[36] without hampering already applicable, or future, sector-specific cybersecurity law.[37] The directive aims to more robustly anchor cybersecurity in fundamental rights,[38] and emphasises the physical and environmental security of network and information systems.[39] Similarly to the CSA, it stresses the need to refine cybersecurity infrastructure to battle cybersecurity attacks,[40] addresses supply chain and third-party reliance,[41] and recognises the significance of international standardisation.[42] Hence, this Chapter will also cover relevant parts of standardisation as contained in the ISO-27000 family.

In January 2026 the European Commission made its most recent efforts in refocusing the cybersecurity agenda on strengthening resilience and capabilities across the Union.[43] The new cybersecurity package was introduced with the intentions to further simplify compliance with the EU's cybersecurity rules and risk-management

[32] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [2016] OJ L194/1, recital 5.

[33] NIS2 Directive, *op cit.*, recital 2,4, 6, Art. 21.

[34] European Commission, 'NIS2 Directive: securing network and information systems' <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> accessed 17 April 2026.

[35] *Ibid*.

[36] Giovanni De Gregorio, Pietro Dunn, *'The European risk-based approaches: Connecting dots in the digital age*' (2022) 59 Common Market Law Review, Issue 2, 473.

[37] NIS2 Directive, *op cit.*, recital 22-23, Art. 4-5.

[38] *Ibid*, recital 70.

[39] *Ibid*, recital 79.

[40] *Ibid*, recital 54.

[41] *Ibid*, recital 56, 85.

[42] *Ibid,* recital 58, 81.

[43] European Commission, 'Commission strengthens EU cybersecurity resilience and capabilities' <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive> accessed 17 April 2026.

requirements. Part of this proposed package are targeted amendments to the NIS 2 Directive,[44] which will be addressed in Chapter 2.4.

## 2.2 Definitions and scope

The NIS 2 Directive obliges entities to implement cybersecurity risk-management and reporting measures.[45] To fall within the directive's scope, entities which provide their services in the EU are covered if they are deemed medium-sized and larger i.e. above 50 employees with an annual overturn above EUR 10 million.[46] In addition to size, the providing entity must also be included in Annex I as operating in a critical sector.[47] Notwithstanding this, certain obligations will apply to entities *regardless* of their size.[48] These often refer to service providers which by the member states are determined as sole providers of important services, hold critical positions, or are public administration entities etc.[49]

The directive also makes a distinction between essential and important entities, which affects their compliance, administrative burdens, and is to be settled according to its size and influence.[50] To be classified as an essential entity, various avenues are available, similar to the classifications above.[51] If not captured by any of these, the entity will instead be deemed important.[52]

The NIS 2 Directive transposes many of the definitions already contained in the CSA.[53] However, it also provides a definition for *security* of network and information systems and holds that it refers to the ability for the system to resist events that may compromise the availability, authenticity, integrity or confidentiality of data, relating to those network and information systems.[54]

Finally, and most importantly, in order to comply with their cybersecurity risk-management and reporting obligations, Article 21 holds that member states must ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to their network and information systems for its use, performance of service, prevention, and minimisation of impact of incidents.[55] They must also notify relevant national authorities in case of significant incidents. In practice, determining what steps will lead to a more secure information system remains with the entity itself.[56] Generally,

[44] European Commission, 'Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act' <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act> accessed 17 April 2026.

[45] NIS2 Directive, *op cit.*, Art. 1.2.

[46] *Ibid*, Art. 2. 1.

[47] *Ibid*.

[48] *Ibid*, Art. 2. 2.

[49] *Ibid*, Art. 2. 2. (b), 3. See also recital 8-9.

[50] Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124/36, Annex I. See also NIS2 Directive, *op cit.*, recital 7, 15.

[51] NIS2 Directive, *op cit.*, Art. 3.1 (a-f)

[52] *Ibid*, Art. 3. 2.

[53] *Ibid*, Art. 6. 2.

[54] *Ibid*, Art. 6. 2. 2.

[55] *Ibid*, Art. 21.

[56] *Ibid*, recital 77.

the security level sought is to be aligned with the risks posed, which requires considering the state-of-the-art, costs, social and economic impact, and making a general proportionality assessment.[57] This is to be determined according to the following categories which includes but is not limited to; information system security policies, incident handling, supply chain security, network and information systems acquisition and maintenance, cryptography and encryption policies, and asset management.[58]

## 2.3 Relevant cybersecurity measures

Given that Article 21 of the NIS 2 Directive formulates cybersecurity risk-management measures broadly, guidance must be derived from other sources. The division of cybersecurity risk-management measures into technical, operational and organisational measures does however offer a useful guide for understanding how secure networks can be achieved. For this, standards can be utilised, which primarily encompasses the ISO/IEC 27000 information system family.[59] The 27000 family is widely conceptualised to create a holistic framework to improve conditions for all types of Information Security Management Systems (ISMS).[60] ISO/IEC 27001:2022[61] and 27002:2022[62] serve as the backbone of generic information security, which draws upon implementing controls. Controls is the term used to describe *inter alia* relevant policies, procedures, and organisational structures which serve to maintain a secure information network and mitigate cyberthreats.[63] For our examination, ISO 27799:2026 is most relevant as it relates to the healthcare sector and will be addressed later.[64]

While EU certification schemes are to be explored in Chapter 3, it's important to emphasise that the NIS 2 Directive itself contains explicit references to the certification schemes as established by the CSA.[65] It holds that member states may require essential and important providers to demonstrate compliance by using digital solutions that are EU-certified.[66]

## 2.4 Supply chains

Beyond the standards of the ISO family, the crucial perspective of supply chains must also be considered.[67] Weaknesses in supply chains represents a large portion of

[57] *Ibid*, Art. 21. 1. 2.

[58] *Ibid*.

[59] Ibid, recital 58-59, 79, Art. 25.

[60] International Organisation for Standardisation, '*ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls (ISO 27002:2022)'* (ISO/IEC 2022) Introduction 0.1.

[61] International Organisation for Standardisation, *'ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO 27001:2022)'* (ISO/IEC 2022).

[62] ISO 27002:2002, *op cit.,* related international standards 0.7.

[63] *Ibid*.

[64] International Organisation for Standardisation, '*ISO 27799:2026 Health informatics - Information security, cybersecurity and privacy protection in health - Information security management in health using ISO/IEC 27002 (ISO 27799:2026)*' (ISO/IEC 2026).

[65] NIS2 Directive, *op cit*., Art. 24.

[66] *Ibid*, recital 77-79.

[67] NIS2 Directive, op cit., Art. 21.

all attacks leading to data breaches.[68] In a top position of the supply chain, the NIS 2 Directive requires a healthcare provider (or other essential service provider), to meticulously identify all potential risks of each partner and include them when drawing up their cyber risk-management plan, as every contractor will themselves be included and subject to the rules of the NIS 2 Directive, if the "top" entity is.[69] If failing to appropriately mitigate supply-chain cybersecurity risks, the service providers itself will bear primary responsibility for failure to comply.[70] Importantly, one must also remember that several suppliers can "co-exist" at once when developing a component containing digital information.[71] For example, within IoT, one product can have a significant amount of varied software and hardware parts.[72]

This upstream and downstream inclusion of different actors along the supply-chain significantly impacts business interactions.[73] For example, in a situation where the product or service is widely used, substitution of a downstream actor might be preferred. While appearing to be negative for downstream actors, it does also generate incentive to meet cybersecurity objectives and standards, which sets them apart from other competitors.[74] For the upstream actors, one particular challenge relates to the practical determination of risk.[75] While they frequently demand transparency and detailed reporting from their supply chains, there is issues of overlapping digital systems and practical processes, making their compliance with cybersecurity obligations harder to understand. This could potentially be simplified through a cybersecurity clause being included in supplier contracts. [76]

## 2.5 Proposal for targeted amendments of the NIS 2 Directive

The recently proposed targeted amendments of the NIS 2 Directive seek to align the NIS 2 with the overarching CSA 2 revision package and to address the complexity and fragmentation of cybersecurity-related policies by clarifying obligations and ease compliance.[77] It suggests targeted interventions to simplify implementation, increase legal certainty and enhance collective response efforts. It contains a revised mandate of ENISA, elaborates on the European cybersecurity certifications, and introduces new definitions.[78]

Among these definitions is the introduction of a new category of *small mid-cap enterprises,* as held in the 2025 Commission Recommendation on the definition of

[68] Andrej Savin, '*NIS2 & Cybersecurity in Practice: Compliance in Practice Compliance* Challenges', vol. 17, no. 69, (International In-house Counsel Journal 2024), 9345.

[69] *Ibid,* 9345-9345.

[70] NIS2 Directive, o*p cit.*, Art. 21, 2. (d).

[71] Mattis van't Schip, '*The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things'*, vol.15 no. 1 (European Journal of Law and Technology 2024), 4.

[72] *Ibid*, 6.

[73] Andrej Savin, op cit., 9345.

[74] *Ibid*, 9345.

[75] *Ibid*.

[76] *Ibid,* 9346.

[77] European Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the Proposal for the Cybersecurity Act 2 (Targeted amendments of NIS2)' COM(2026) 13 final, 1-5.

[78] *Ibid,* 10-15.

small mid-cap enterprises.[79] It would cover entities with fewer than 750 employees and less than EUR 150 million in annual turnover.[80] In such a case, they would be designated as important entities rather than essential, thereby reducing their compliance requirements and the supervision burden on competent authorities.[81] Another new definition requires states, as part of their national cybersecurity strategy, to adopt ”post-quantum cryptography” mitigating measures.[82] In essence, post-quantum cryptography are algorithmic tools put in place in cybersecurity environments in order to withstand attacks from stronger quantum computers.[83]

Another suggestion relates to the collection and harmonised reporting on data of ransomware attacks.[84] Computer Security Incident Response Teams (CSIRTs) and competent authorities may request detailed information from victims of ransomware attacks, including whether a ransom was paid, the amount and the recipient, in order to support intelligence for law enforcement.[85] More consistent reporting would give authorities better insight into ransomware activity and could make future interventions more targeted and effective while ensuring that reporting them does not automatically result in increased liability or deterrent penalties.[86]

To further ease compliance, the NIS 2 amendments also assign ENISA an expanded supervisory role. ENISA is tasked with supporting Member States in supervising entities operating in multiple countries, facilitating mutual assistance and improving oversight of entities within the ambit of the NIS 2 Directive.[87] It is also expected to conduct annual comprehensive analyses of cross-border cybersecurity risks and may recommend the establishment of joint examination teams for high-risk entities.[88] The certification recognition in Article 24 of the NIS 2 Directive is also afforded an extension. Member states may now require important and essential entities to obtain a certificate on the *cyber posture* under a particular certification scheme.[89] Where such certification is granted according to a particular implementing act, competent authorities may not impose certain additional compliance measures. Again, this will be revisited in Section 3.

Finally, while the proposal broadly recognises supply chain security as being of crucial importance, for instance acknowledging the unreasonable surge of entities requesting extensive and repeated information from their suppliers, it does not provide for an explicit amendment provision.[90] Instead, it opts for the Commission to adopt future guidelines.[91]

---

[79] European Commission, ’Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises‘ [2025] OJ L, 2025/1099, Annex 2.

[80] *Ibid*.

[81] Targeted amendments of NIS2, *op cit.*, 5.

[82] *Ibid*, recital 8. Art. 5.5.

[83] National Institute of Standards and Technology, ‘What Is Post-Quantum Cryptography?‘ <https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography> Accessed 22 May 2026.

[84] Targeted amendments of NIS2, *op cit.*, recital 10

[85] *Ibid*.

[86] *Ibid*, Art. 5(8).

[87] *Ibid*, 5.

[88] *Ibid*, 15.

[89] *Ibid*, Art. 5. 9. 4.

[90] *Ibid*, 5. See also recital 9.

[91] *Ibid*.

## 2.6 Healthcare providers

For healthcare providers, ISO 27799:2026 contains more precise sector-specific guidance on how to ensure cybersecurity risk-compliance and transposes the broader structure of ISO 27002:2022.[92] It emphasises a structured approach based on risk assessment, comprehensive policy frameworks and regular auditing to ensure cybersecurity risk-compliance within healthcare organisations.[93]

From the technical and operational standpoint, it includes requirements such as use of medical devices and Internet of Things (IoT),[94] maintaining and updating software,[95] and preservation and protection of personal data.[96] From the organisational and managerial perspective, it ranges from the security of interacting with patients by several different kinds of health professionals,[97] decision-making by top management,[98] to the concern of information flow within or between organisations.[99] Additionally, there is also the requirement to maintain a safe physical environment and people controls. For instance, enabling organisations to provide its services even in the event of a natural disaster, and have medical staff practice cyber security hygiene measures.[100] This will now be explored in greater detail.

For technical controls, key features include requirements for medical devices and digital clinical equipment, secure authentication, malware protection, configuration management, information deletion, data masking, and web filtering.[101] For medical IoT, the importance of incorporating cybersecure health software in medical devices such as pacemakers, MRI-machines, surgical robots, and defibrillators, cannot be overstated.[102] Secure authentication holds that two-factor authentication should be used for systems that operate personal healthcare data.[103] Malware protection ensures that the blocking of malicious websites and detection of unauthorized software is possible. Conversely, over-blocking caused by anti-malware software must be duly observed so that it does not interfere with the actual functioning of medical devices.[104] Configuration management involves maintaining secure interoperability of health record systems and medical devices, including clarifying potentially overlapping responsibilities associated with those devices.[105] Information deletion and data masking refers to the fact that information should be deleted when no longer required to avoid unnecessary data exposure,[106] whereas data masking concerns

[92] ISO 27799:2026 General 4.1. See also Introduction 0.1, 0.3.
[93] *Ibid*.
[94] *Ibid,* Annex C 5.2.1.
[95] *Ibid*, Scope 1.
[96] *Ibid*, 5.9. See also Personal health information 3.1.4.
[97] *Ibid*, Segregation of duties 5.3.
[98] *Ibid*, Policies for information security 5.1.
[99] *Ibid,* Context and background 0.2 (d).
[100] *Ibid*, Context and background 0.2 (g). See also Chapter 6.
[101] *Ibid*, Technological Controls, chapter 8, 28-33.
[102] Ibid, Annex C 5.3.
[103] *Ibid*, Secure authentication 8.5.
[104] ISO 27002:2022, *op cit.*, 8.7 (a-f).
[105] ISO 27799:2026, *op cit.*, Configuration Management 8.9.
[106] ISO 27002:2022, *op cit.*, Information deletion 8.10.

pseudonymisation techniques that can be used as a protection measure.[107] Web filtering is a common tool for blocking content outside the medical context which is inappropriate. However, in the medical context, material such as anatomical images and terms relating to drug use may be necessary and should therefore not be censored.[108] Similarly to ISO 277996:2026, ENISA has also published the practical guide "Cyber hygiene in health sector" which outlines other technical practices which healthcare providers should adopt to safeguard its network and information systems. It highlights the need for monitoring admin privileges and the support for strong passwords, the deployment of firewalls and removal of outdated software, use of encryption standards, and maintenance of safe health apps for mobile units.[109]

Operational risk compliance is not granted its own section in ISO 27799:2026. However, it is more widely envisaged in the overall organisational structure which concerns day-to-day implementation, maintenance, and review of controls across healthcare information systems. ISO 27002:2002 established that each organisation is to establish their own information security policy.[110] This must be accepted by the very top management and relevant parties,[111] and include requirements such as; projected information risks, strategies, and relevant contracts.[112] It should also make statements relating to areas such as; information transfer, backups, and lessons learned from previous information security events.[113]

In ISO 27799:2026, this further extends to have healthcare providers ensure that due caution is granted requirements relating to personal health information, with its associated legal and ethical responsibilities.[114] It also requires regular revision of its policy contents, since such policies are guided by the continuously developing rights of subjects of care and their right of accessing their own health data.,[115] the fact that several medical institutions nowadays are involved the provision of medical services,[116] and the general breadth of health information and medical digitisation.[117] Additionally, and similarly to concerns regarding supply chains, it highlights maintenance of information security policy for arrangements regarding temporary staff.[118] This is not limited only to clinical staff but may include personnel from inspection bodies and administrative services.[119]

Generally, ISO 27799:2026 also broadly considers operational risk compliance through the lens of environmental, infection-control, building-management, and physical security systems.[120] It recognises the practical realities of healthcare delivery: information must remain available across hospital, clinics, cloud-based

[107] *Ibid*, 27002:2022, Data masking 8.11.
[108] ISO 27799:2026, *op cit.*, Web filtering 8.23.
[109] ENISA Cyber Hygiene, *op cit.*, 4-8.
[110] ISO 27799:2026, *op cit.*, Policies for information security 5.1.
[111] ISO 27002:2022, *op cit.*, 5.1.
[112] *Ibid*.
[113] *Ibid*.
[114] ISO 27799:2026, *op cit.*, 5.1. (d)
[115] *Ibid,* 5.1 (maintenance) (c).
[116] Ibid, 5.1 (maintenance) (e).
[117] *Ibid*, 5.1. (maintenance) (a).
[118] *Ibid*, 5.1. (maintenance) (g).
[119] Ibid, 5.1. (maintenance) (g) 2-3.
[120] *Ibid,* C Annex 45-47.

environments, and other settings, often on continuous 24-hour basis. For that reason, operational compliance requires more than periodic checks; it requires systematic control of how information is stored, accessed, transferred, and protected in routine operations, as well as how the organisation responds to incidents and keeps its controls aligned with changing risks and service demands.[121]

ISO 27799:2026 also includes controls relating to people.[122] This requires organisations to screen all individuals through the use of *e.g.* identify verification, and that they put in place mandatory obligations so that staff actually report cybersecurity breaches.[123] It also includes more imposing and disciplinary measures.[124] These processes should be used as a deterrent tool, as well as ensuring that for serious violations, individuals are reported to relevant authorities.[125] When changes of employment happen, or any other type of naturally occurring ”rotation” within a premise, organisations should also make sure that no unnecessary access to health data remains.[126] The same applies to changes of security passes so that no unauthorised personal can gain access to the premises.[127] Another crucial feature concerns remote working.[128] Performance of healthcare services may even take on cross-border perspectives, as medical professionals may for example review medical documents when abroad.[129]. In such context, particular care must be undertaken by the healthcare provider in question.[130] Finally, this compliments the final point in regard to people controls. Namely, security event reporting.[131] Organisations should arrange and enable for reporting to take place at the earliest opportunity possible.[132] There shall be no repercussions for staff and if needed, organisations should make available anonymous reporting functions.[133] This will also require the healthcare provider to disclose for subjects of care if their data has been leaked.[134]

With the introduction of the NIS 2 Directive, the focus on cyber resilience has also transitioned from the technical, to the managerial aspects in the boardroom.[135] In ISO 27799:2026, organisational cybersecurity compliance is framed as a governance issue rooted in high-level policy, accountability and oversight. In practice, this means that information security policy should be approved at the highest management level, kept under regular review, and defined broadly enough to cover the organisation’s legislative, regulatory, and contractual obligations, including

[121] *Ibid*, Classification of information 5.12, Labelling of information 5.13.
[122] *Ibid,* People controls 6.1.
[123] *Ibid,* Information security awareness, education and training 6.3.
[124] *Ibid,* Disciplinary process 6.4, Responsibilities after termination or change of employment, 6.5.
[125] *Ibid*.
[126] *Ibid*.
[127] *Ibid*.
[128] *Ibid,* Remote working 6.7.
[129] *Ibid.*
[130] *Ibid*.
[131] *Ibid*, Information security event reporting 6.8.
[132] *Ibid*.
[133] *Ibid*.
[134] *Ibid*.
[135] Mark Sharron, ‘NIS Article 20 Explained: Turning Board Accountability into Cyber Resilience’ (ISMS.online, 31 October 2025) https://www.isms.online/nis-2/articles/20-management-and-board-responsibility-for-cybersecurity/ accessed 24 May 2026. See also NIS2 Directive, *op cit.*, Art. 20.

obligations related to personal health information.[136] Top management may also have to undergo training if need be and promote proactive and strategic "business continuity plans".[137] It could even hold individuals personally liable for breaches and requires repeated rolling evidence of compliance, not occasional.[138] The standard also emphasises clear role allocation where healthcare organisations should designate clear responsibility roles for information security, which should benefit from pre-existing advisory structures that coordinate security work across functions such as ICT, medical engineering, governance and compliance.[139] A means of achieving this is to include key information officers into top management.[140] Naturally, instead of spending significant resources training executives, promotion could be used to help achieve these goals. This is particularly relevant in healthcare, where responsibility for security and safety often distributes across different professional groups, and where decisions affecting electronic health record systems, medical devices incorporating health software, and other digital equipment can have both clinical and security consequences.[141]

To further accomplish this, suggestions have been compiled which stress that cybersecurity should be thought of as a "strategic business risk consideration".[142] It requires that management fully grasp the broader implications of strategic risk planning, that cybersecurity mitigation measures may produce spillover effects into other areas such privacy law, which may come to effect privacy concerns of its staff.[143] Beyond the top management, board members should also have access to expert help and be assisted by external advisors when needed.[144] Overall, there should be greater collaborative efforts that synthesize efforts made by management and, efforts made by the IT-side of a business enterprise.[145]

Physical controls are related to the operational requirements above but focuses more closely on maintenance of physical integrity of its facilities. For example, that physical entry points should be treated with particular caution.[146] This extends to ensuring sensitive health information is not displayed to unauthorised personnel.[147] Workstations should be cleared when not in use, in conjunction with automatic log-out processes.[148] Hardware and physical storage media such as SIM-cards, USB-sticks and even printers may all contain confidential health information. Thus, they should have maintenance and disposal protocols in place.[149]

---

[136] ISO 27799:2026, *op cit.*, Information Security Roles and responsibilities 5.2.

[137] NIS2 Directive, *op cit.*, Art. 21. 2. (c).

[138] Annika Galle and Hélène Vletter-van Dort, '*From Cybersecurity to Cyber Resilience in the Board Room: Key Steps for Supervisory Board Members and Non-executives*' (6 International Cybersecurity Law Review 2025) 221-223.

[139] ISO 27799:2026, *op cit.*, Segregation of duties 5.3, Management responsibilities 5.4, Threat intelligence 5.7.

[140] Andrej Savin, *op cit.*, 9347.

[141] ISO 27799:2026, *op cit.*, Context and background 0.2, Audience and users 0.3.

[142] Andrej Savin, *op cit*., 9347.

[143] *Ibid,* 9347 (2).

[144] *Ibid,* 9347 (3).

[145] *Ibid,* 9347 (4).

[146] ISO 27799:2026, *op cit.*, Physical entry 7.2.

[147] *Ibid.*

[148] *Ibid*, Clear desk and clear screen 7.7.

[149] *Ibid*, Storage Media 7.10, Equipment Maintenance 7.13.

## 2.7 Conclusion

The NIS 2 Directive represents an ambitious undertaking to raise the baseline of cybersecurity protection across the Union through its increased obligations for providers of essential services. However, while Article 21 is supplemented by standards and proposed targeted amendments, there is still a lingering absence of cohesion for healthcare providers.

First, the inherent scope of NIS 2 Directive creates persistent uncertainty regarding how healthcare providers are to be categorised. While large-scale actors in high-criticality sectors are clearly essential, some of them are smaller operators offering limited health services online. These actors should logically benefit from lessened administrative burdens but may nonetheless be classified as sufficiently essential according to a member state no matter size or influence. In such a case, the mandatory obligations remain, leaving smaller operations without having prepared or sufficiently allocated their resources. Moreover, they must nonetheless comply with internationally recognised standards and may fall foul to other niche-sector specific legal requirements. This must also be viewed in light of the potential new mid-cape enterprise definition and the general proportionality assessment which is to be dictated by member states. This collectively creates significant legal uncertainty and may ultimately undermine a functioning internal market and reasonable expectations.

Another perspective concern supply chain vulnerability. The NIS 2 Directive now strongly emphasises responsibly for service providers to take ownership of third-party cybersecurity weaknesses all along the supply chain. Cybersecurity risk-assessment cannot be contractually outsourced to avoid legal responsibility. This includes even seemingly miniscule parts of IT infrastructure which can constitute the initial “compromising vessel” for allowing unauthorised access. Holding providers of essential services accountable for production fault in the constituent elements of a digital solution, may present absurd outcomes.

Finally, despite the above tensions, certain technical, operational and organisational benchmarks emerge as particularly essential. These are predominantly derived from Article 21 of the NIS 2 Directive, ISO 27799:2026 and the NIS 2 targeted amendments. For instance, the maintaining of safe network systems and patient health data records, ensuring safe practical use and development of medical devices, enabling proper risk management handling and incident response policies, and reliably maintain physical security and operational resilience. From the future perspective, upcoming challenges will include addressing refined cryptography requirements, broader harmonised ransomware reporting and closer operational collaboration with ENISA. If healthcare providers can ensure the above, and align their expectations correctly, they are well on their way of providing a cybersecure and compliant data health network ecosystem.

# 3 Cybersecurity Act and Information Communication Technology standardisation

## 3.1 Introduction

The Cybersecurity Act, as the NIS 2 Directive, sets out to create a high level of cybersecurity within the Union through increased trust, coherence and cyber resilience.[150] It holds cybersecurity to reflect those activities necessary to protect network and information systems.[151] Network and information systems are in turn defined as an electronic signal transmissions system,[152] where any group of devices perform digital data processing automatically. The definition can also refer to digital data being stored, processed, under this first categorisation, for purposes of their operation, use, and protection.[153] ICT, on the other hand, is a term which has developed to cover technologies capable of storing, communicating, and retrieving digital information.[154]

Prior to the CSA, the standardisation of ICT had already been identified as a crucial tool for establishing a functioning digital single market.[155] Standardisation would therefore allow for improved interoperability between digital products, lower market entry barriers, combat supply chain weaknesses, and harmonise cybersecurity evaluation methodologies.[156]

Building on the concept of ICT standardisation, the CSA sets out to remove overlapping certification schemes for ICT solutions, increase cross-border cooperation, introduce educational “cyber-hygiene-thinking" efforts, incentivise cybersecurity “by design and default” for manufacturers, and create greater transparency.[157] These objectives are included in its two central pillars.[158] The first

[150] Cybersecurity Act, *op cit.,* recital 7, 66-68.

[151] *Ibid*, Art. 2. 1.

[152] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L 108/33, art. 2.

[153] NIS2 Directive, *op cit.,* Art. 6.

[154] International Telecommunication Union (ITU), ‘Information and Communication Technology Revolution‘ <https://www.itu.int/ITU-D/tech/FORMER_PAGE_IMT2000/Revised_JV/IntroducingIMT_item1.html> accessed 2 May 2026.

[155] European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: ICT Standardisation Priorities for the Digital Single Market’ COM(2016) 176 final 2-3.

[156] *Ibid,* see also European Commission, ‘Commission Staff Working Document: Union Rolling Work Programme for European cybersecurity certification’ (URWP Working document for European cybersecurity certification) SWD(2024) 38 final, 3-4, and Cybersecurity Act, *op cit.*, recital 11.

[157] Cybersecurity Act, *op cit.,* recital 9, 12-13, 40, 54, 66, 69.

[158] *Ibid*, Art. 1.

establishes the tasks and functions of ENISA. The second establishes a certification scheme for ICT products, services and processes.[159]

## 3.2 European Certification schemes

ICT products, services and processes (ICT-PSPs) are often collectively considered in the CSA. ICT products are defined as those constituent elements which make up a network and information system.[160] An ICT service is a service consisting mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.[161] Finally, an ICT process refers to activities performed to design, develop, deliver or maintain an ICT product or ICT service.[162]

An ICT-PSP certification scheme shall serve to raise the overall level of cybersecurity protection in the EU and harmonise the certification approach, ensuring that ICT-PSPs comply with specific security requirements.[163] It aims to foster trust among customers to make more informed choices.[164] For instance, data shall be protected from unauthorised access and destruction,[165] it should enable authorised personal to access the data and reliably be able to document who, when and where data was accessed.[166] It also contains obligations to ensure that vulnerabilities can be located, identified, and that updates are secure.[167]

To achieve this, the CSA established the Union Rolling Work Programme which is to determine *strategic priorities* that are relevant for EU ICT cybersecurity certification schemes.[168] Beyond standards, the group has highlighted the priority of security-by-design, qualified risk-based assurance levels, coherence and international cooperation.[169] Security-by-design means that the ICT-PSPs are to be encouraged by the CSA certification framework to integrate appropriate cybersecurity measures in every step of development of the ICT solution. Starting from the initial developing stage and throughout the entity's whole lifecycle, so that that cyberattacks can be anticipated and minimised.[170] Risk-based assurance levels provide a basis of credibility that an ICT-PSP meets the requirements of a particular EU certification.[171] These levels should be equivalent to the rigorousness of the evaluation methodology performed and be proportionate to the risk associated with the intended use of the ICT-PSP, based on likelihood of an incident and its impact.[172] Here, the manufacturer of the ICT-PSP chooses a specific security level to target in

[159] *Ibid*, Art. 1. 1 (b).
[160] *Ibid*, Art. 2. 12.
[161] *Ibid*, Art. 2. 13.
[162] *Ibid*, Art. 2. 14.
[163] *Ibid*, Art. 46. 1-2.
[164] European Union Agency for Cybersecurity (ENISA), 'EUCC - European Cybersecurity Scheme on Common Criteria (ENISA EUCC)' <https://certification.enisa.europa.eu/browse-topic/eucc_en> accessed 2 May 2026.
[165] Cybersecurity Act, *op cit.,* Art. 51. (a-b).
[166] *Ibid*, Art. 51. (e-f).
[167] *Ibid*, Art. 51. (d), (g).
[168] *Ibid*, Art. 47. 1.
[169] URWP Working document for European cybersecurity certification, *op cit.*, 3-6.
[170] *Ibid*, 4.
[171] Cybersecurity Act, *op cit.,* recital 86, Art. 52.
[172] EUCC Implementing Regulation (EU) 2024/482, *op cit.,* recital 12-13. See also Cybersecurity Act, *op cit.,* Art. 52. 1.

its application of a particular certification, going from ”basic“, to ”substantial”, and finally ”high”.[173] The ICT-PSP is then put through a series of tests and measures corresponding to the level chosen.[174]

This is best highlighted in practice by the first implementing regulation enacted under the Cybersecurity Act.[175] It makes use of the international renowned common criteria framework ISO/IEC 15408[176] and creates the European Common Criteria-based cybersecurity certification scheme (EUCC), which holds that *all* ICT *products* which submits for certification must meet certain targets.[177] It utilises the Vulnerability Analysis family (AVA_VAN) of the common criteria called components which determines how strong an ICT product is.[178]

In the context of the Implementing Regulation, these components are translated into the assurance levels mentioned, where AVA_VAN levels 1-2 correspond to “substantial” and AVA_VAN levels 3-5 represents “high”.[179] For non-complex or low-risk ICT-PSPs, corresponding to assurance level ”basic”, a “conformity self-assessment" is permitted.[180] This level may refer to ICT solutions such basic cloud storage or email service platforms.[181] For assurance level ”substantial” to be issued for the certificate, the ICT-PSP provider must implement the required security obligations and be able to withstand an attacker with limited skills and resources.[182] This corresponds to ICT solutions like certain hospital network infrastructure (e.g. routers and access management systems).[183] The final level ”high” refers to an ability to resist elaborate, state-of-the-art attacks that are carried out by well-resourced actors.[184] Consider for instance surgical IoT systems and emergency health database back-ups.[185]

## 3.3 Proposal for Cybersecurity Act 2

Since the adoption of the CSA in 2019, the geopolitical context has become more complex.[186] Ongoing global and regional conflicts have contributed to a rise in cyberattacks, as reflected in ENISA’s 2024 Threat Landscape report.[187]

---

[173] Cybersecurity Act, *op cit.,* recital 88-90.

[174] *Ibid*, Art. 52. 6-7.

[175] EUCC Implementing Regulation 2024/482.

[176] International Organisation for Standardisation, ’*ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components (ISO 15408-3:2022)*’ (ISO 2022).

[177] EUCC Implementing Regulation 2024/482, *op cit.*, Art. 1-5.

[178] ISO 15408-3:2022, *op cit.*, 135-141.

[179] EUCC Implementing Regulation 2024/482, *op cit.*, Art. 4. 2-3.

[180] Cybersecurity Act, *op cit.,* recital 79.

[181] International Organisation for Standardisation, ’*ISO/IEC 15408-3:2024 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Security assurance components (ISO 15408-3:2024)‘* (ISO 2024), 136-137. See also Cybersecurity Act, *op cit.*, Art. 52 (5).

[182] Cybersecurity Act, *op cit.,* art. 52 (6), recital 89.

[183] ISO 15408-3:2024, *op cit.*, 138. See also Cybersecurity Act, *op cit.*, Art. 52 (6).

[184] Cybersecurity Act, *op cit.*, Art. 52. (7), recital 90. See also EUCC Implementing Regulation 2024/428, *op cit.*, recital 12.

[185] ISO 15408-3:2024, *op cit.*, 140. See also ISO 27799:2026, *op cit.*, 45.

[186] Cybersecurity Act 2, *op cit.*, 1.

[187] European Union Agency for Cybersecurity (ENISA), *’ENISA threat Landscape 2024*‘ (2024) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> accessed 18 May 2026.

Cybersecurity is therefore framed not merely as a technical issue, but a strategic defence concern with greater implications for democracy and the economy.[188] This view is echoed in Mario Draghi's 2024 report "The future of European Competitiveness", which calls for greater simplification, harmonisation, as well as stronger cross-border cooperation within the EU and among EU cybersecurity agencies.[189]

This progressively hostile environment has exposed limitations in the original cybersecurity framework where new emerging technologies such as artificial intelligence and quantum computing are reshaping the cybersecurity environment.[190] The ambition of the revision of CSA, is therefore to ensure greater coherence between the legal acts and provide the necessary tools to make the cybersecurity framework functioning for today's challenges.[191]

In response, the European Commission has announced a new cybersecurity package.[192] A central element of the package is the Cybersecurity Act 2, which intends to replace the CSA.[193] The proposal identifies four key shortcomings in the existing framework. First, it broadly finds a gap between the current cybersecurity policy framework and the actual needs of stakeholders operating in the cybersecurity environment.[194] Second, implementation of the European Cybersecurity Certification Framework (ECCF) has stalled, with few cybersecurity scheme operational nearly five years after adoption.[195] Third, in spite of the efforts of the CSA, the compliance landscape remains complex and fragmented, with overlapping horizontal and sector-specific rules.[196] Fourth, the proposal highlights growing risks arising from non-technical factors, including "technical sovereignty" and control exercised by third-country suppliers over critical ICT infrastructure.[197]

To address this, the Commission intents to substantially strengthen the mandate of ENISA, significantly improve and simplify the ECCF, and establish a trusted supply chain framework.[198] This second objective is a major reform of the original CSA and extends, beyond ICT-PSPs, the EU certification framework to include managed security services (MSSPs) and cyber posture of entities.[199] MSSPs are third-party actors which supply its customers with security systems management and thus perform vulnerability assessments, monitoring, and incident response etc.[200] These actors are becoming increasingly intertwined with the operations of its customers,

---

[188] *Ibid*, 6.

[189] Mario Draghi, *'The Future of European Competitiveness – Part B: In-depth Analysis and Recommendations*' (European Commission 2024), 75.

[190] Cybersecurity Act 2, *op cit.*, recital 42.

[191] *Ibid*, 2-4

[192] European Commission, 'Proposal for a Regulation for the EU Cybersecurity Act' <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act> accessed May 21, 2026.

[193] Cybersecurity Act 2, *op cit.*, 1.

[194] *Ibid*.

[195] *Ibid*, 8.

[196] *Ibid*, 2.

[197] *Ibid*, 12.

[198] *Ibid*, Art. 1.

[199] *Ibid*, recital 79-82, Art. 71.

[200] IBM, 'What is a Managed Security Service Provider (MSSP)?' (IBM Think) <https://www.ibm.com/think/topics/managed-security-service-provider> accessed 21 May 2026.

and as such carry particular responsibility for ensuring customers' cybersecurity risk management.[201] Cyber posture is a newer concept and relates to an entity's ability to demonstrate compliance of other cybersecurity legal acts, for instance indicating an ability to withstand cybersecurity attacks.[202]

Moreover, the general obligations of the EU certification framework are considerably revamped. Beyond ensuring that certified ICT-PSPs protect the common integrity, authenticity and accessibility of data according to the original CSA,[203] providers are now *inter alia* required to monitor *all* relevant internal activity of the certified entity, protect the availability of essential and basic functions (even after an incident), regularly test the ICT-PSP, remediate vulnerabilities without delay, and share information about potential vulnerabilities.[204] ICT-PSP providers are now even obliged to provide their users with more service-oriented supplementary information. This includes informing the user of the intended purpose of the ICT-PSP, guide and assist the user to ensure proper configuration and operation of the ICT-PSP and describe its potential vulnerabilities.[205]

Lastly, it introduces the trusted ICT supply chain framework as a security mechanism to address *non-technical* risks in the supply chains of critical sectors.[206] This is to be understood as a practical and coordinated function which sets out to defend the Union against high-risk threats to ICT supply chains.[207] When such a threat is identified (by the Commission or three Members States), a security risk assessment shall be performed,[208] which may lead to an ICT supplier to be prohibited from participating in the development of standards, applying for an EUCCF, and partake in Union programmes.[209] The proposal even confers power to the Commission to conclude that a third country poses serious risks to ICT supply chains, leading to similar blockades.[210]

## 3.4 Healthcare providers

For healthcare providers, most of its digital solutions provided are ICT-PSPs captured by the definition in the CSA.[211] For the health space in particular, successful digitisation would dramatically improve how healthcare is provided to patients.[212] For example, a patient health record exchange format could ensure seamless

[201] Cybersecurity Act 2, *op cit.*, recital 82.
[202] *Ibid*, recital 93, Art. 2 (29).
[203] Cybersecurity Act, *op cit.*, Art. 51 (a-d).
[204] Cybersecurity Act 2, *op cit.*, Art. 80.
[205] *Ibid*, Art. 84.
[206] *Ibid*, Art. 98.
[207] *Ibid*, Title IV, Art. 99. 3.
[208] *Ibid*, Art. 98-99.
[209] *Ibid,* Art. 100. 4. (a-f).
[210] *Ibid*.
[211] See Section 3.2.
[212] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society (Digital Transformation of Health and Care') COM(2018) 233 final, 1.

movement of cross-border health data for each EU citizen.[213] Other suggestions relate to the promotion of research initiatives and biobanks where the pooling of collective resources could help achieve personalised treatment and use of E-health solutions.[214]

To guarantee this functions properly in practice, the digital systems must be reliable and secure.[215] This is also where ICT-standardisation re-appears. In the multi-stakeholder 2023 Union Rolling plan for ICT standardisation[216] a vast amount of material relating to the health sector was compiled. It includes the European Health Data Space (EHDS) Regulation,[217] which not only realises the above health data sharing efforts, but also sets out to create mandatory certification schemes for electronic health record systems.[218] Other measures concern standardisation projects requiring medical devices and clinical IoT to uphold security throughout the products lifecycle.[219]

From the perspective of the ongoing CSA 2 proposal, the health sector will mainly be impacted through the certification scheme introduced for cyber posture and MSSPs, trusted ICT supply chain framework, enhanced operational support from ENISA (such as digital simplification of reporting), and addressing the cybersecurity skills shortage among individuals.

By considering the cyber posture of entities to be certification-relevant activities, it will help healthcare providers to use a *single* European cybersecurity certificate to demonstrate compliance with the risk-management obligations of *several* horizontal instruments such as the GDPR, Cyber Resilience Act, and NIS 2 Directive.[220] This approach is designed to simplify regulatory requirements for entities providing services across several Member States, significantly lower compliance costs and unlocking resources for operational preparedness.[221] Where a specific union legal act provides for it, these certificates can confer a presumption of conformity with legal requirements, making supervision less burdensome.[222]

The trusted supply chain mechanism would help identify key ICT assets in critical ICT supply chains, such as medical devices or crucial data processing systems in the healthcare sector.[223] Healthcare providers may be prohibited from using, installing or integrating ICT components from suppliers in these key assets who are deemed to

[213] Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format [2019] OJ L 39/18, See also 'Digital Transformation of Health and Care' *op cit*., 6-7.

[214] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L 88/45, art 14. See also 'Digital Transformation of Health and Care' *op cit*., 7-8.

[215] 'Digital Transformation of Health and Care', *op cit.*, 1-3.

[216] European Commission, 'Rolling Plan for ICT Standardisation 2023 (ICT rolling plan)' (Publications Office of the European Union 2023), 113.

[217] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (EHDS) [2025] OJ L, 2025/327.

[218] *Ibid*, recital 7, 43, Art. 24.

[219] ICT rolling plan, *op cit.*, 114.

[220] Cybersecurity Act 2, *op cit.*, recital 79-80.

[221] *Ibid*, 3.

[222] *Ibid,* Art. 78(1).

[223] *Ibid*, Art. 98.

be at high-risk.[224] If a healthcare provider would be using components from a supplier later designated as high-risk, they would be subject to transition periods for phasing out those components.[225]

With a reinforcement of ENISA's mandate, it would offer early alert service specifically for entities in sectors of high criticality. The service shares information on potential or ongoing significant cyber threats indicators and provide mitigation recommendations.[226] The commission recognises that ransomware is a core threat and empowers ENISA to establish a helpdesk to assist individual healthcare providers in preparing for, responding to, and recovering from ransomware incidents. Healthcare providers would benefit from enhanced "situational awareness sharer" through regular technical reports on trends in cyber threats and incidents, made available by ENISA, that analyse maturity levels of sectors and specific challenges within the critical sectors.[227] Finally, the CSA 2 suggests a union-integrated framework for individual cybersecurity skills development. Similar to an ICT-scheme, such attestation would enable employers to more easily hire cybersecurity professionals and generally strengthen their cybersecurity competence.[228]

## 3.5 Conclusion

The phasing-out of national certification schemes is reasonable to avoid internal market fragmentation and preserve a functional digital single market. To incentivise cybersecurity developers to "by-design" manufacture products in line with pre-existing certification models and strive for technical interoperability is therefore well founded. The EUCC in particular serves as the first example of the ongoing work of standardising such certification schemes. Traditionally, EU certifications such as the implementing act have been targeted at IT-developers and not the essential entities themselves (e.g. healthcare providers). However, as suggested by the CSA 2 proposal, future certification will not only concern the proliferation of technical ICT standardisation relevant for manufacturers, but will come to include cyber posture perspectives, more in line with the NIS 2 Directive and other ISO-standards. How this is to play out in practice for essential service providers remains unclear.

Another crucial factor is the access and management of health data which sits at the very core of creating a cybersecure healthcare environment. Many of the issues highlighted within the healthcare space concerns issues of personal data protection, IoT, or access to technology. This renders cybersecurity obligations for healthcare providers overall unclear and further reinforces that cybersecurity is difficult to conceive of in isolation, and that the CSA struggles in formulating clear and directly applicable obligations. While certainly intentional owing to its limited intended

[224] *Ibid*, Art 103.
[225] *Ibid*.
[226] *Ibid*, Art. 12.
[227] *Ibid*, recital 34.
[228] *Ibid*, recital 46, art. 19.

target group, it still fails in the overall objective of creating a more coherent, capable and safe cybersecurity framework.

In light of the above, it is reasonable to question whether the CSA actually imposes tangible obligations for healthcare providers. However, the framework still differentiates between varying assurance levels, taking the severity of ICT-PSPs in different sectors into account. For EU certifications, it is highly unlikely that manufacturers of healthcare ICT-PSPs would be considered carrying out low risk activities allowing for any conformity self-assessment corresponding to a 'basic' assurance level in the CSA. Instead, activities will be considered substantial or high. As a consequence, healthcare providers should instead view the CSA as an informed procurement tool, which simplifies ways of picking a trustworthy ICT providing partner. This holds especially true in view of the CSA 2. The CSA 2 also strongly promotes that healthcare providers are to increase digital literacy among its workers through educational efforts. It will also allow for stronger partnerships to form between ENISA and healthcare providers through simplified response and information sharing services, with a trusted supply chain ICT framework granting even further preventative and enforceable cross-border mechanisms.

# 4 Summary

Cybersecurity as a legal field is fundamentally different from other traditional areas of law. The preceding chapters demonstrate that cybersecurity within the EU has evolved from a technical niche into an intricate web of responsibilities in which relevant actors must navigate sector-specific legal requirements, technical standards, policy guidance and certification mechanisms in order to implement "appropriate and proportionate" cybersecurity measures. This inevitably creates complexity, particularly because cybersecurity threats evolve far more rapidly than legislative frameworks do.

Within healthcare, the complexity of cybersecurity requires a careful distinction between legally binding obligations and non-binding guidance. While the NIS 2 provides more concrete requirements, the direct applicability of certification schemes for healthcare providers under the CSA remains comparatively uncertain. According to obligations prescribed in Article 21 of the NIS2 Directive, alongside standard ISO 27799:2026, healthcare providers are to implement relevant technical, physical, and organisational cybersecurity risk-management measures. The standard explores several of these, for instance holding that technical measures relate to safe medical IoT and encryption policies, organisational measures concern protection of physical environments, since emergency services must remain continuously operational, even in the event of a cyberattack. Finally, organisational measures have elevated the role of management. Cybersecurity concerns have now become an issue of corporate accountability and strategic management.

Under the NIS 2 framework, the expansion of supply-chain responsibility also represents one of the most challenging aspects for healthcare providers. Modern healthcare infrastructure depends heavily on external suppliers. For example, a medical device containing an inherent digital vulnerability from the manufacturer, would nonetheless result in responsibility for the healthcare provider. Although a certification ICT-PSP solution under the CSA may mitigate such risks, certification largely remains voluntary and is stringently focused on the manufacturers. This may produce significant disproportionate outcomes where healthcare providers are expected to account for vulnerabilities deeply embedded within third-party technologies. Similar tensions also stem from definitional ambiguities within EU cybersecurity law. For example, it remains unclear whether the distinction between important and essential entities produces meaningful practical differences, and how the emerging notion of cyber posture is to be understood in practice.

In many respects, the proposed Cybersecurity Act 2 represents an attempt to address these structural gaps. However, the NIS 2 Directive and CSA are fundamentally intended for different target groups, rendering the overlap between the acts somewhat uncertain. Simultaneously, while the proposal signals a more streamlined and harmonised direction, it also focuses on increasingly politicised areas such as limiting reliance on unreliable third-country supply chains and strengthening technological sovereignty.

Despite these tensions, the demand for demonstrable technical conformity and recognised assurance will unquestionably continue to rise. In such a context, it is highly probable that *if* a healthcare provider chooses an uncertified ICT-PSP solution for clinical application, it may face considerable evidentiary pressure in demonstrating that its cybersecurity measures satisfy the "state-of-the-art" requirement. Ideally, this will gradually incentivise healthcare providers to adopt certified ICT solutions more systematically, which indirectly strengthens supply-chain security in line with the objectives of the NIS 2 Directive. In this sense, the CSA functions less as a direct source of mandatory obligations, and more as an informed procurement tool helping healthcare providers to choose a trusted ICT partner.

Ultimately, the examined legal acts do not fully accomplish coherent horizontal cybersecurity obligations for healthcare providers. Technical specificities may therefore be better addressed through future implementing acts or national healthcare legislation. However, the NIS 2, CSA, and proposed CSA 2 collectively establish the trajectory of future EU cybersecurity compliance. Healthcare providers that neglect to align their digital infrastructure and risk-management practices with this emerging regulatory direction, risk becoming increasingly exposed to both legal and operational cybersecurity challenges.

# References

## Official documents

### EU Legal Acts and recommendations


Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L 108/33, (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021).

Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L124/36, (eur-lex.europa.eu/eli/reco/2003/361/oj/eng).

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare [2011] OJ L88/45, (eur-lex.europa.eu/eli/dir/2011/24/oj/eng).

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) [2016] OJ L194/1, (eur-lex.europa.eu/eli/dir/2016/1148/oj/eng).

Commission Recommendation (EU) 2019/243 of 6 February 2019 on a European Electronic Health Record exchange format [2019] OJ L39/18, (eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0243).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15, (eur-lex.europa.eu/eli/reg/2019/881/oj/eng).

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act) [2022] OJ L333/1, (eur-lex.europa.eu/eli/reg/2022/2554/oj/eng).

Directive (EU) 2022/2555 of the European Parliament and of the Council 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) [2022] OJ L333/80, (eur-lex.europa.eu/eli/dir/2022/2555/oj/eng).

Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [2024] OJ L482/1, (eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02024R0482-20251229).

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and

Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L 2847, (eur-lex.europa.eu/eli/reg/2024/2847/oj/eng).

Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (EHDS) [2025] OJ L 2025/327, (https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng).

Commission Recommendation (EU) 2025/1099 of 21 May 2025 on the definition of small mid-cap enterprises [2025] OJ L, 2025/1099, (eur-lex.europa.eu/eli/reco/2025/1099/oj/eng).

### EU Commission Publications

Draghi M, 'The Future of European Competitiveness - Part B: In-depth Analysis and Recommendations (European Commission 2024), (commission.europa.eu/topics/competitiveness/draghi-report_en).

European Commission, 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' COM(2016) 410 final, (eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0410).

European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: ICT Standardisation Priorities for the Digital Single Market' COM(2016) 176 final, (eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:176:FIN).

European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society (Digital Transformation of Health and Care') COM(2018) 233 final, (eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0233).

European Commission, Rolling Plan for ICT Standardisation 2023 (Publications Office of the European Union 2023), (https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2023)

European Commission, 'Commission Staff Working Document: Union Rolling Work Programme for European cybersecurity certification' SWD(2024) 38 final, (certification.enisa.europa.eu/system/files/2024-03/SWD_2024_38_F1_STAFF_WORKING_PAPER_EN_V3_P1_3268229_8D9PyZAu7Q8rfTyMp2OkTXgP4_102292.PDF).

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament and the Council: Strengthening EU Economic Security, JOIN(2025) 977 final,(eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020).

European Commission, 'Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the Proposal for the Cybersecurity Act 2 COM(2026) 13 final, (eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837).

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the

European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (Cybersecurity Act 2)' COM(2026) 11 final,(eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837).

### ENISA reports

European Union Agency for Cybersecurity (ENISA), 'Cyber Hygiene in the Health Sector', (www.enisa.europa.eu/publications/cyber-hygiene-in-the-health-sector).

European Union Agency for Cybersecurity (ENISA), 'EUCC - European Cybersecurity Scheme on Common Criteria' (certification.enisa.europa.eu/browse-topic/eucc_en).

European Union Agency for Cybersecurity (ENISA), 'ENISA threat Landscape 2024' (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> accessed).

### Standards

International Organisation for Standardisation and International Electrotechnical Commission, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 2022), (iso.org/standard/27001).

International Organisation for Standardisation and International Electrotechnical Commission, 'ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls' (ISO/IEC 2022), (iso.org/standard/75652.html).

International Organisation for Standardisation and International Electrotechnical Commission, 'ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components' (ISO/IEC 2022), (iso.org/standard/15408-3).

International Organisation for Standardisation and International Electrotechnical Commission, 'ISO/IEC 15408-3:2024 Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Security assurance components' (ISO/IEC 2024), (iso.org/standard/15408-3).

International Organisation for Standardisation and International Electrotechnical Commission, 'ISO 27799:2026 Health informatics - Information security, cybersecurity and privacy protection in health - Information security management in health using ISO/IEC 27002' (ISO/IEC 2026), (iso.org/standard/84647.html).

## Literature

### Books and Journal Articles

De Gregorio G and Dunn P, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (Common Market Law Review 2022), (doi.org/10.54648/cola2022032).

Galle A and Vletter-van Dort H, 'From Cybersecurity to Cyber Resilience in the Board Room: Key Steps for Supervisory Board Members and Non-Executive

Directors' (International Cybersecurity Law Review 2025), (doi.org/10.1365/s43439-025-00151-7).

Lenaerts K and Gutiérrez-Fons JA, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (Academy of European Law, AEL 2013/9, 2013), (hdl.handle.net/1814/28339).

Parkes R, 'Nuts and Bolts: Safeguarding the Critical Infrastructure of the Union' in Daniel Fiott (ed), Protecting Europe: The EU's Response to Hybrid Threats (European Union Institute for Security Studies 2019), (jstor.org/stable/resrep21143.6).

Savin A, 'NIS2 & Cybersecurity in Practice: Compliance Challenges' (International In-House Counsel Journal 2024), (heinonline.org/HOL/P?h=hein.journals/iihcj17&i=513).

Segura Serrano A (ed), 'The EU's Cybersecurity Policy: Results and context in Global Cybersecurity and International Law' (Routledge 2024), (doi.org/10.4324/9781003344124).

Smits JM, 'What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' (Maastricht European Private Law Institute Working Paper No 2015/06), (doi.org/10.1017/9781316442906.006).

Świtała K, 'Opportunity Makes the Thief. A Risk Analysis and Vulnerability Identification Approach in Information Security Management Systems as a Method of Countering Cybercrimes' (Review of European and Comparative Law 2025), (doi.org/10.31743/recl.18192).

Van't Schip M, 'The Regulation of Supply Chain Cybersecurity in the NIS2 Directive in the Context of the Internet of Things' (European Journal of Law and Technology 2024), (ejlt.org/index.php/ejlt/article/view/989).

## Other online sources

### Web-based material

European Commission, 'EU Cybersecurity Strategy' (digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy).

European Commission, 'European action plan on the cybersecurity of hospitals and healthcare providers' (health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/european-action-plan-cybersecurity-hospitals-and-healthcare-providers_en).

European Commission, 'NIS2 Directive: securing network and information systems' (digital-strategy.ec.europa.eu/en/policies/nis2-directive).

European Commission, 'Commission strengthens EU cybersecurity resilience and capabilities' (digital-strategy.ec.europa.eu/en/news/commission-strengthens-eu-cybersecurity-resilience-and-capabilities).

European Commission, 'Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act' (digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act).

European Commission, ’Proposal for a Regulation for the EU Cybersecurity Act’ (digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act).

IBM, What is a Managed Security Service Provider (MSSP)?’ (ibm.com/think/topics/managed-security-service-provider).

International Telecommunication Union (ITU), ‘Information and Communication Technology Revolution‘ (www.itu.int/ITU-D/tech/FORMER_PAGE_IMT2000/Revised_JV/IntroducingIMT_item1.html)

Mark Sharron, ‘NIS Article 20 Explained: Turning Board Accountability into Cyber Resilience’ (isms.online/nis-2/enforcement/board-liability/article-20/)

National Institute of Standards and Technology, ‘What Is Post-Quantum Cryptography?‘ (www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography).