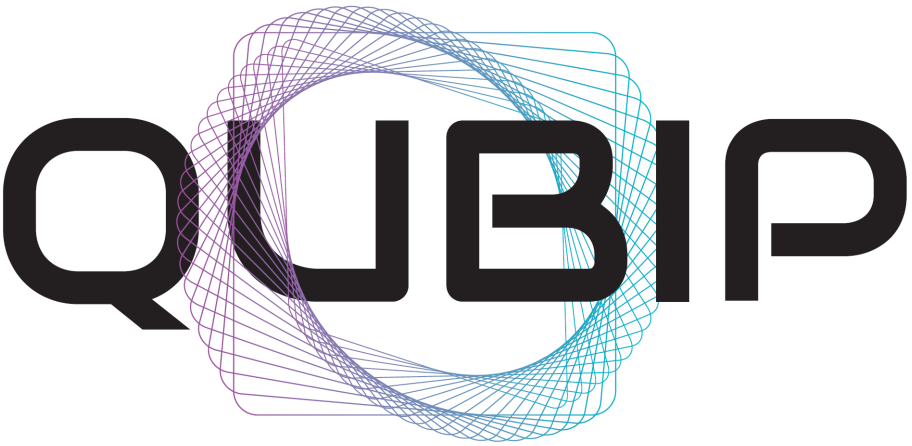
Horizon Europe



QUANTUM-ORIENTED UPDATE TO BROWSERS AND INFRASTRUCTURES FOR THE PQ TRANSITION (QUBIP)

Policy Brief No. 2
Regulating Quantum Computing

Deliverable number: D4.8

Version 1.0

(NOTE: this version is published for dissemination purposes only but it has not yet been formally accepted by the EC)

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Project Acronym:	QUBIP
Project Full Title:	Quantum-oriented Update to Browsers and Infrastructures for the PQ transition
Call:	HORIZON-CL3-2022-CS-01
Topic:	HORIZON-CL3-2022-CS-01-03
Type of Action:	HORIZON-IA
Grant Number:	101119746
Project URL:	https://www.qubip.eu
Start date:	1 September 2023
Duration:	36 months

Editor:	Alessandro Mantelero – POLITO
Deliverable nature:	Report (R)
Dissemination level:	Public (PU)
Contractual Delivery Date:	31 August 2025
Actual Delivery Date	30 September 2025
Number of pages:	46
Keywords:	Policy guidelines, regulatory framework, cybersecurity, post-quantum, cryptography
Contributors:	Antonio Pastor – TID
Peer review:	Verónica Fernández Mármol – CSIC David Martín-Sánchez – CSIC Javier Faba – UPM Antonio Lioy – POLITO
Approved by:	ALL partners

Table 1: Document revision history

Issue Date	Version	Comments
23/07/2025	0.1	Initial ToC
31/07/2025	0.2	First draft version, for internal review
31/08/2025	0.3	Second draft version
30/09/2025	1.0	Final version, for submission

Abstract

This document represents the Deliverable D4.8 of the Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition (QUBIP) project and contains the updated version of its Policy Brief, to be further updated in the final year of the project.

Given the nature of this document, in addition to its extended content, an Executive Summary is also included.

Note to the reader: given its nature as a policy brief and its focus on the regulatory issues, this deliverable adopts the common standards used in the legal context and in the legal policy briefs with regard to the use of footnotes, citations, abbreviations, etc.

Executive Summary

This Policy Brief provides an analysis of the vulnerabilities and inherent gaps in the current European Union (EU) regulatory framework, focusing on the challenges posed by the transitional phase towards Post-Quantum Cryptography (PQC). This phase is critical because legal requirements that are not oriented towards quantum-resistant solutions could lead to systemic risks. The risk analysis in this report does not consider entities that could be affected by the transition to quantum computing technologies. It is not a readiness assessment, either. This report is intended for rule makers and policymakers, and provides an evaluation of the current legal framework, highlighting potential weaknesses in two key areas:

- **Sectoral regulations in high-risk or critical industrial sectors**, already subject to specific regulatory obligations and vulnerable to quantum technologies;
- **Cross-sectoral general regulations**, that apply horizontally across sectors.

The key sectors analysed, which partially overlap with those classified as highly critical under the Network and Information Security 2 (NIS2) Directive, are finance, healthcare, energy, e-government, transportation and telecommunications. To evaluate the risks associated with quantum technologies within the current legal framework, two key variables were taken into account: **the likelihood of a quantum attack** (related to the sensitivity of the sector) and **the extent to which the applicable legal framework is prescriptive and ready to address quantum-related issues**. The risk analysis distinguishes among the following scenarios:

- (i) High-risk contexts: where quantum attacks are likely and systems/devices, as defined by legal requirements, are not quantum-resistant;
- (ii) Medium-risk contexts: where vulnerabilities exist, but quantum-resistant solutions can be implemented within the existing legal framework;
- (iii) Low-risk contexts: where there are no significant targets for quantum attacks and no need to define specific legal requirements.

The analysis of each regulated sector that could be affected by quantum technologies is summarised below.

Financial Sector

The financial sector is characterized by a high dependency on ICT systems and a high frequency of cyber-attacks. Threats include Distributed Denial of Service (DDoS) attacks, data breaches (often from supply chain attacks and social engineering), fraud, and ransomware. The regulatory framework is detailed. The **Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554)** imposes prescriptive requirements for financial entities that are required to continuously monitor and manage ICT systems to mitigate risk impact. This is done by adopting policies and tools that ensure resilience, availability, and high standards for data protection—covering integrity, confidentiality, and authenticity—whether data is at rest, in use, or in transit. The **Delegated Regulation (EU) 2024/1774** under DORA **explicitly acknowledges the threats posed by quantum computing** and mandates a flexible, risk-based approach to cryptographic threats. It requires financial entities to develop and implement a cryptographic policy, including criteria for the selection and usage of cryptographic techniques, as well as provisions for updates based on cryptanalysis developments. Under DORA, the context is classified as **medium/high** risk. The **Revised Payment Services Directive (PSD2)** requires Strong Customer Authentication (SCA) and security measures to protect credentials, with technical standards subject to regular revision to reflect technological advances. The

Markets in Crypto-Assets Regulation (MiCA) requires crypto-asset service providers to adopt security systems aligned with EU standards and to ensure the availability, authenticity, integrity, and confidentiality of data, in line with DORA and the General Data Protection Regulation (GDPR). Both PSD2 and MiCA are considered to present a **medium/low** risk in relation to quantum threats, due to their general provisions that allow for the implementation of quantum-resistant security measures.

Healthcare Sector

The healthcare sector is highly reliant on ICT systems (e.g., sensors, monitoring devices, electronic health records) and is among the most targeted by cyber attacks, with an increasing number of incidents, particularly ransomware attacks and emerging DDoS threats. The security of connected medical devices is of particular concern. The regulatory framework analysed includes **Regulation (EU) 2017/745 on medical devices (MDR)** and **Regulation (EU) 2017/746 on in vitro diagnostic medical devices (IVDR)**, which require risk management systems and cybersecurity measures (including protection against unauthorized access) based on the "state of the art". Quantum threats directly undermine current protections relying on classical cryptography. The **European Health Data Space (EHDS) (Regulation (EU) 2025/327)** establishes a framework for secure access to and interoperability of health data, requiring the use of secure processing environments with high technical and security standards and compliance with the GDPR. The regulatory framework in the healthcare sector is classified as **medium** risk with respect to quantum threats. There are no overly prescriptive cryptographic requirements that would hinder the adoption of post-quantum solutions, and the flexibility allows for their gradual integration.

Energy Sector

The digitalization of the energy sector increases its vulnerability to cyber threats, with electricity being the most dependent sub-sector. Incidents can cause widespread disruptions. The NIS2 Directive designates the energy sector as a critical infrastructure, imposing obligations for risk management and supply chain security. The **Delegated Regulation (EU) 2024/1366** introduced the first EU network code dedicated to cybersecurity in the electricity sector, setting out common minimum requirements and a review mechanism in the event of emerging threats. This regulation mandates common strategies, monitoring activities, reporting mechanisms, and crisis management procedures in response to cyberattacks. Entities with a high and critical impact must conduct risk assessments that consider potential cyber threats. This could include quantum threats, should they be recognised at the EU level. The common cybersecurity framework includes basic and advanced controls and a cybersecurity management system that must be verifiable. These controls can be revised to include post-quantum cryptography if future assessments identify quantum computing as a significant risk. The **Regulation (EU) 2024/1789** for the gas subsector updates the legal framework for natural gas, renewable gas, and hydrogen markets and includes clear cybersecurity provisions, empowering the Commission to adopt delegated acts to regulate cross-border gas and hydrogen cybersecurity aspects. Under the adopted risk assessment framework, the EU energy sector, as currently regulated, is classified as medium-risk in relation to the potential impact of quantum threats. The regulatory approach remains flexible and adaptive, emphasizing general cybersecurity principles and risk-based methodologies rather than imposing specific cryptographic standards.

E-Governance

In the realm of e-governance, attention is given to the **eIDAS Regulation (EU) 2014/910**, as updated by the **EU Digital Identity Framework Regulation (EUDI Regulation) (Regulation (EU) 2024/1183)**, which introduces the **European Digital Identity Wallet (EUDI Wallet)**. Current public-key cryptographic systems

(e.g., RSA, ECDSA) used in EUDI Wallet prototypes are vulnerable to quantum computing. The EUDI Wallet is considered an ideal starting point for introducing hybrid, quantum-resistant cryptographic tools (PQC), thanks to the flexibility and technological neutrality of the regulatory language. The regulation is built on the principle of "security by design" and includes advanced security features (e.g., end-to-end encrypted communication). Despite its current vulnerabilities, the EUDI Wallet's regulatory design and flexibility mean it is a proactive vehicle for the post-quantum transition, with a **medium/low** risk classification.

Transport Sector

The transport sector is heavily impacted by ransomware attacks and data-related threats. The analysed sub-sectors show varying levels of maturity. The **Regulation (EU) 2018/1139** recognises the increasing reliance on ICT and sets out essential requirements for information security. Systems and equipment must be designed to minimize risks from reasonably foreseeable threats, including both internal and external information security threats. The **Delegated Regulation (EU) 2022/1645** requires Information Security Management Systems (ISMS) with detailed technical and security measures, including risk assessments and incident response.

For the maritime sector, **Regulation (EC) 2004/725** addresses security (including cybersecurity) for EU-flagged vessels and port facilities. Security assessments must consider the protection of radio and telecommunications systems, including IT systems and networks, which are inherently vulnerable to cyber threats. Security plans must include procedures to protect sensitive information in both physical and digital formats. The **Directive 2005/65/EC** complements these measures by extending them to the entire port area, requiring appropriate measures to protect confidential information, implying the need for information security systems. The Regulation (EU) 2019/1239 establishes the European Maritime Single Window environment (EMSWe), a technologically neutral system enabling the Commission to update technical specifications and procedures to remain open to future technologies. Implementing Regulations (EU) 2023/204 and 2023/2790 define security measures for databases and information exchange systems, including identification, authentication (e.g., mutual TLS), authorization, traceability, accountability, and data integrity. Data confidentiality is ensured through encryption between the sender's access point and the Reporting Interface Module (RIM). Communication and message validation must include security measures to guarantee authenticity and non-repudiation. Processing of personal data must comply with the GDPR, and commercial/sensitive information must remain confidential. The identified risk level is **medium**, considering the balance between implemented technical security measures and the openness of some systems to remain technologically neutral.

Telecommunication Sector

The European telecommunications sector is a vital infrastructure highly dependent on digital technologies and increasingly vulnerable to quantum cybersecurity threats. Regulatory developments, particularly the **European Electronic Communications Code (EECC)**, the **NIS2 Directive**, and the **GDPR**, frame telecoms as critical infrastructure and mandate stronger cyber risk management. The European Commission's **Recommendation 2024/1101** for PQC jointly with recent strategy from NIS cooperation group, sets a coordinated roadmap for transitioning to quantum-safe systems by 2030, with initial goals in 2026. Despite this, the sector faces significant challenges due to network complexity, interdependence, and a lack of detailed quantum-safe implementation guidance for operators. According to the risk assessment framework adopted in this analysis, the telecommunications sector can be classified as **medium/high risk** context with respect to quantum threats. This classification reflects the high criticality of the sector, combined with a regulatory environment that is predominantly principles-based while also incorporating specific policy instruments that directly address quantum computing issues.

Cross-Sectoral Regulations

The analysis of cross-sectoral regulations reveals that the existing legal framework is rooted in classical cryptographic assumptions and provides limited—if any—guidance on mitigating the emerging challenges posed by quantum computing. The **GDPR (Regulation (EU) 2016/679)** remains the cornerstone for personal data protection but lacks a systemic vision of quantum threats. It emphasizes data integrity and security, promotes "privacy by design" (Art. 25), and requires appropriate technical and organizational measures (e.g., pseudonymization, encryption) in line with the "state of the art" (Art. 32). The **Data Act (Regulation (EU) 2023/2854)** reaffirms the principles of data minimization and privacy by design and by default, requiring adequate technical and organizational safeguards, including pseudonymization and encryption where processing poses significant risks to fundamental rights. It also highlights the protection of trade secrets, allowing the use of technical safeguards such as smart contracts and encryption to prevent unauthorized access or disclosure. Similarly, the **Data Governance Act (Regulation (EU) 2022/868)** promotes a secure and trustworthy data market, requiring high cybersecurity standards and measures to prevent unauthorized access to non-personal data (e.g., encryption). It recognizes pseudonymization and anonymization as appropriate measures. The **AI Act (Regulation (EU) 2024/1689)** includes general safety provisions, requiring high-risk AI systems to be designed for appropriate levels of accuracy, robustness, and cybersecurity, and to operate reliably throughout their lifecycle. It identifies specific attack vectors for AI and relies on the "state of the art" principle, allowing adaptation to technological advancements. It encourages the use of cryptography for privacy by design and cryptographic watermarking of synthetic content. Regarding the European cybersecurity framework, the **NIS2 Directive (Directive (EU) 2022/2555)** promotes the use of innovative technologies for threat detection and prevention and stresses the importance of advanced cryptographic systems. It requires entities to adopt technical, organizational, and operational measures that are continuously updated in response to evolving threats. The **Cybersecurity Act (Regulation (EU) 2019/881)** fosters a common level of cybersecurity and resilience in the EU, encouraging "security by design and by default," and requiring manufacturers to embed protective measures throughout the lifecycle of ICT products and services. It establishes a certification framework that ensures data confidentiality, integrity, and availability, and includes cybersecurity vulnerability management. The European Union Agency for Cybersecurity (ENISA) is tasked with providing guidance on encryption and anonymization based on current and emerging risk analysis. The assurance levels (with "high" requiring testing against sophisticated attacks) offer a mechanism for assessing security robustness. Finally, the **Cyber Resilience Act (Regulation (EU) 2024/2847)** establishes a horizontal regulatory framework for essential cybersecurity requirements in digital products, explicitly designed to adapt to emerging threats. It mandates "privacy-by-design" and requires digital products to protect data at rest and in transit using state-of-the-art encryption and other technical measures, ensuring data integrity against unauthorized manipulation. Both data protection and cybersecurity regulations impose quite broad security and cybersecurity requirements. Therefore, any regulatory response to the advent of quantum threats will likely need to be addressed through secondary legislation (e.g., implementing acts or delegated regulations), rather than amendments that alter the core structure of the primary legislative texts.

Contents

List of Acronyms

AI	Artificial Intelligence
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EC	European Commission
ECC	Elliptic-Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EEA	European Economic Area
EECC	European Electronic Communications Code
EHDS	European Health Data Space
EMSWe	European Maritime Single Window environment
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
EUDI	EU Digital Identity
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
ISMS	Information Security Management Systems
MiCA	Markets in Crypto-Assets Regulation
NIS2	Network and Information Security 2
PKI	Public-Key Infrastructure
PQC	Post-Quantum Cryptography
PSD	Payment Services Directive
PSD2	Revised Payment Services Directive
PSP	Payment Service Provider
QKD	Quantum Key Distribution
QUBIP	Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition
RIM	Reporting Interface Module
RSA	Rivest–Shamir–Adleman
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SCA&CSC	Strong Customer Authentication and Common and Secure Communication
SSL	Secure Socket Layer
TLS	Transport Layer Security

1 Introduction

This Policy Brief analyses the challenges posed to the existing EU legal framework by quantum computing technologies. The aim of this document is to identify the inherent vulnerabilities/shortcomings of the current EU regulatory framework in critical sectors, particularly in terms of their capacity to respond to the challenges of a future post-quantum scenario, especially in the fields of cybersecurity and data protection.

The risk analysis conducted in this report is therefore not focused on entities that could be affected by the transition to quantum computing technologies[1]. It is not a readiness assessment either. The report is addressed to rule makers and policymakers, providing them with an assessment of the existing legal framework to highlight any potential weaknesses and necessary changes and/or integrations.

Several EU regulations impose specific requirements in the domains of data processing and cybersecurity that may be undermined by quantum technologies, thus potentially rendering the current legal safeguards inadequate. From this perspective, the level of risk posed by quantum technologies depends on the technical safeguards mandated by law and the extent to which they may be challenged by quantum-based hacking. It is therefore crucial to address the risk that existing relevant legal provisions may become partially ineffective or even obsolete in the face of the development of quantum computing. The primary objective of this Policy Brief is to assess the vulnerabilities of the current EU legal framework in relation to critical sectors, focusing on the 'transition phase' toward post-quantum cryptography[2]. To achieve this objective, this policy brief adopts a methodology based on the analysis of relevant legislation across two main areas:

- **Regulated high-risk/critical sectors** – sectors already subject to specific regulations and identified as particularly vulnerable to the threat posed by quantum technologies;
- **Cross-sectoral general regulations** – overarching legal frameworks that apply across multiple sectors, such as the GDPR, the NIS2 Directive, and the AI Act.

In identifying the key sectors to be considered, we focused on those associated with the most critical issues/vulnerabilities, and potential negative impacts. This selection partially overlaps/aligns with the sectors classified as highly critical under the NIS2 Directive (Directive (EU) 2022/2555). These sectors include finance, healthcare, energy, e-government, transport, and telecommunications.

To assess the risks associated with quantum technologies within the existing regulatory framework, two key variables were considered:

- The **likelihood of a quantum attack**, which depends largely on the sensitivity of the sector;
- The **existing legal framework**, particularly the level of detail and prescriptiveness of the applicable regulations, vis-à-vis the challenges posed by quantum technologies.

It is essential to emphasize the logic underlying our risk assessment scale: more detailed and prescriptive regulation in a given sector is considered indicative of a higher level of risk. This is because such regulations often impose specific technical requirements, which may be more susceptible to quantum-based attacks, especially if these requirements do not foresee or allow for the integration of post-quantum cryptographic solutions. Conversely, more flexible and technology-neutral regulatory frameworks are considered to pose lower risk, as they allow for greater adaptability in adopting quantum-resistant measures.

Based on this approach, our risk assessment distinguishes between the following scenarios:

- (i) **High-risk contexts** – where quantum attacks are likely, and the systems/devices, as defined by legal requirements, will not be quantum-resistant.
- (ii) **Medium-risk contexts** – where vulnerabilities exist, but it is possible to implement quantum-

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

resistant solutions within the existing legal framework.

- (iii) **Low-risk contexts** – where there are no significant targets for quantum attacks, and no need to define specific legal requirements.

Our analysis is conducted by examining existing legal requirements in order to detect potential risks for legally protected interests. Therefore, the risk level is determined based on the technical protection required by law and the extent to which such protection might be undermined by quantum hacking. This analysis does not take into account Member State-level legislation but is conducted exclusively from the perspective of EU-level law.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2 Analysis of the Critical Sectors

The following sections provide an overview of the key sectors most impacted by quantum computing technologies, highlighting the specific regulatory vulnerabilities identified in each area.

The sectors taken into consideration are the following ones:

1. Financial: banks and financial market infrastructures are entirely dependent on ICT for their operations (including payments, risk management, interbank services and real-time trading). This sector is among the most targeted sectors for cyberattacks, being incidents extremely time-sensitive, with impacts that manifest almost immediately and can halt payments, affecting both businesses and individuals.
2. Health is highly dependent on ICT systems for core processes, including sensors, monitoring devices, AI solutions, and electronic health records, with minimal manual backup options. Its scope has significantly expanded under the NIS2 Directive, increasing its heterogeneity and complexity. It is among the most affected sectors by cyber incidents, with hospitals and healthcare providers particularly targeted. Given the high sensitivity of patient health data and the potentially devastating impact of cyberattacks on healthcare services, it is essential to ensure a rapid and effective response to protect patient safety and maintain the sector's critical functions.
3. Energy: the digital transformation of the energy sector in Europe is accelerating, increasing its vulnerability to cyber threats due to its growing reliance on ICT and interconnected systems. The electricity subsector is the most dependent on digital technologies. A major cybersecurity incident in this area could cause widespread disruptions, including power outages that would not only affect consumers directly but also disrupt other highly critical sectors such as telecommunications, where many systems rely on electricity. The gas subsector has a significant, though slightly lower, level of dependence. This subsector follows in terms of potential impact, reflecting its dominant role as an energy source for households across the EU.
4. E-governance: Public Administration is a sector particularly affected by cyber-attacks, accounting for 19% of all recorded events between July 2023 and June 2024. Despite its vital role in governance and service delivery to society, it is among the least mature sectors in terms of cybersecurity. The sector is newly regulated under the NIS2 Directive and remains in the early stages of alignment with its requirements. DDoS attacks were the primary threat (33% of all DDoS incidents), and it was the second most affected sector by data-related threats (12%). Malware (11%) and social engineering (10%) were also significant threats.
5. Transportation: it is the second most targeted sector in the ENISA Threat Landscape 2024, accounting for 11.19% of recorded events, with DDoS and ransomware attacks being the most prevalent threats. Cyber incidents in this sector are highly time-sensitive, and delays in response can have cascading effects on other sectors, including emergency services. The sector exhibits varying levels of maturity across its subsectors: maritime transport faces challenges related to outdated operational technology systems, making it vulnerable to cyberattacks, while air transport is the most digitally advanced.
6. Telecommunications: is considered a critical infrastructure sector in EU regulations. It is also affected by multiple ICT directives, as it transports data from other critical sectors. Among the regulations with an impact on this sector are the general ICT regulations, such as GDPR or NIS2, as well as other specific national-level regulations, such as lawful interception, which will be relevant for the Post-quantum transition.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2.1 Financial Sector

On 21 February 2025, the ENISA published a report analysing the cyber threat landscape of the European financial sector. The report reviews cyber incidents that affected the sector between January 2023 and June 2024, focusing on the main incidents observed in EU Member States and neighboring countries, as well as on organizations falling within the scope of the NIS2 Directive and the Digital Operational Resilience Act (DORA)[3] – the latter will be analysed in more detail below.

The current threat landscape in the European financial sector has experienced a diverse range of cybersecurity threats that can be described as follows: geopolitical events triggered spikes in DDoS attacks, mainly affecting European credit institutions (58%) and government websites related to finance (21%) leading to operational disruptions. While their direct impact was often limited, mitigation costs remained significant.

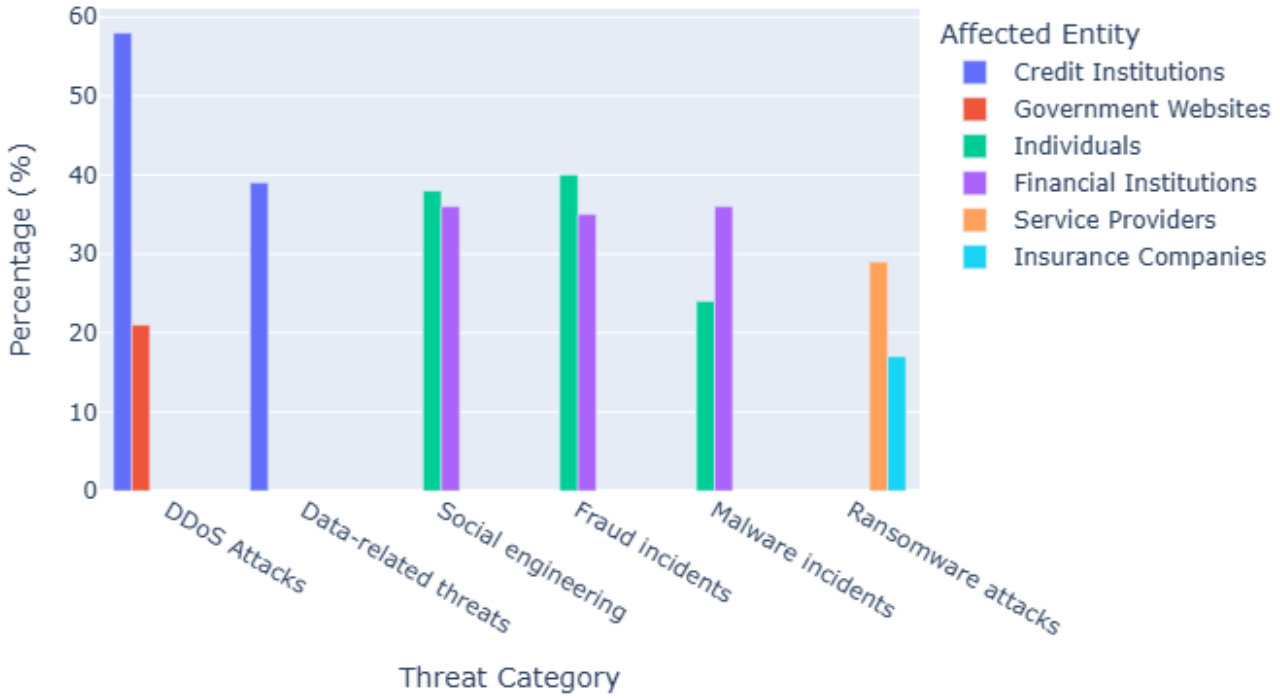


Figure 2.1: Cyber Threat Landscape in the EU Financial Sector.

Data-related threats, including breaches and leaks—often stemming from supply chain attacks and social engineering—have primarily affected credit institutions (39%), leading to financial losses, regulatory fines, and reputational damage. Social engineering tactics, such as phishing, smishing, and vishing, were widespread, targeting both individuals (38%) and financial institutions (36%). These attacks led to financial fraud (50%), large-scale financial crimes (28%), and the sale of sensitive data (19%). Fraud incidents accounted for 6% of total cases, with individuals (40%) and institutions (35%) being the main victims. The rise in crypto-related fraud, especially investment scams and illicit money laundering, is noteworthy.

Ransomware attacks predominantly affected service providers (29%) and insurance companies (17%), resulting in financial losses, data exposure, and operational downtime. Malware incidents - though less frequent (6%) - involved banking trojans and spyware targeting institutions (36%) and individuals (24%), with a notable surge in mobile banking trojans. Supply chain attacks primarily involved data breaches and ransomware, impacting digital, cloud, and payment service providers, resulting in data exposure (63%) and operational disruptions (26%). Additionally, 73% of incidents reported under the NIS Directive were non-malicious, primarily due to system failures (64%) and human error (9%). Threat actors include state-sponsored groups, cybercriminal organizations, and hacktivists, driven by ideological motives (54%) and

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

financial gain (41%). Affected assets included IT infrastructure (31%), operational systems (28%), personal data (25%), and business information (15%), with the main consequences being operational disruption (58%), data exposure (17%), and financial loss (13%)[4].

2.1.1 Analysis of the main regulations in the financial sector

Building on the points highlighted above and considering that the financial sector is a highly regulated domain — including its cybersecurity aspects — it is essential to examine the main regulatory frameworks governing the sector and assess their adequacy in addressing the challenges posed by quantum computing technologies.

At the end of 2022, the EU institutions adopted the Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554), which became applicable on 17 January 2025. It covers key areas such as ICT risk management, ICT incident management and reporting, testing of the operational resilience of ICT systems and management of ICT third-party risks with the aim of preventing and mitigating cyber threats. Moreover, it acts as lex specialis to the NIS2 Directive (Directive (EU) 2022/2555)[5] and to Article 11 and Chapters III, IV and VI of the Directive on the Resilience of Critical Entities (Directive (EU) 2022/2557)[6].

DORA recognises the systemic nature of cyber risks referred to in multiple recitals and articles. Some of its parts lay down rather prescriptive requirements. In this respect, Article 9 of the regulation, which addresses protection and prevention, is particularly relevant to the PQC transition[7] as it requires financial entities to continuously monitor and manage their ICT systems to reduce the impact of ICT-related risks.

These entities must also adopt security policies, procedures, and tools that ensure the resilience and availability of critical systems and maintain high standards for data protection, including data integrity, confidentiality, and authenticity—regardless of whether the data is at rest, in use, or in transit[8]. In addition, pursuant to Article 15 of DORA, the European Commission adopted a delegated regulation (Regulation (EU) 2024/1774[9]) on regulatory technical standards specifying ICT risk management tools, methods, processes, and policies to ensure further harmonisation thereof, which elaborates on many aspects of Article 9 of DORA.

Recital 9 of Regulation (EU) 2024/1774 acknowledges the threats posed by the development of quantum computing, stating that “Given the rapid technological developments in the field of cryptographic techniques, financial entities . . . should remain abreast of relevant developments in cryptanalysis and consider leading practices and standards. Financial entities . . . should hence follow a flexible approach, based on risk mitigation and monitoring, to deal with the dynamic landscape of cryptographic threats, including threats from quantum advancements”. Moreover, this delegated regulation sets out detailed cryptographic guidance. For example, in Section 4 (“Encryption and cryptography”), Article 6 (“Encryption and cryptographic controls”) obliges financial entities to develop and implement a policy on encryption and cryptographic controls[10]. We can therefore conclude that, with reference to DORA, the context falls within the medium-risk category.

Another relevant regulatory source is the Revised Payment Services Directive (PSD2), Directive (EU) 2015/2366 – which replaced the first Payment Services Directive (PSD), Directive 2007/64/EC - aimed at regulating payment services and payment service providers across the EU and the European Economic Area (EEA). The Directive emphasizes the need for payment services offered electronically to be made secure through the use of technologies that ensure secure user authentication and minimize the risk of fraud (Recital 95[11]). Article 97 establishes the obligation for payment service providers to apply Strong Customer Authentication (SCA)[12] at various stages of electronic payment processes and online account access, in order to protect the confidentiality and integrity of payment service users’ personalized security credentials. Article 98 of the Directive provides that the European Banking Authority (EBA) shall issue Regulatory Technical Standards (RTS) specifying the requirements for strong customer authentication, exemptions, the security requirements necessary to protect credentials, and requirements for common

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

and secure open communication standards between different payment service providers[13]. In line with this Article, EBA developed RTS on Strong Customer Authentication and Common and Secure Communication (SCA&CSC), which have been in effect since 14 September 2019[14].

Delegated Regulation 2018/389 requires Payment Service Providers (PSPs) to implement transaction monitoring mechanisms to detect unauthorized or fraudulent transactions. These mechanisms must be based on transaction analysis and take into account risk factors such as compromised or stolen authentication elements, the amount of each transaction, known fraud scenarios, the presence of malware, and abnormal use of devices or software provided by the PSP[15].

Payment service providers must ensure that the creation of personalized security credentials takes place in a secure environment, that such credentials are not stored in plain text, are masked from view, and are generated/transmitted within secure environments. Their creation, association with the user, delivery, renewal, and deactivation must follow secure procedures (e.g., SCA for secure remote user enrolment; secure delivery of credentials/devices, with mechanisms to verify their authenticity, etc.)[16].

SCA must be based on two or more elements classified into the categories of knowledge, possession, and inherence, resulting in the generation of an authentication code. This code is accepted only once by the payment service provider. The providers must adopt certain security measures to ensure that: no information about the SCA elements can be derived from the code, a new code cannot be generated from a previous one, and the code cannot be forged. In the event of authentication failure, it should not be possible to determine which element is incorrect. Communication sessions must be protected against data interception and manipulation[17].

Payment service providers shall adopt measures to mitigate the risk of acquisition, disclosure, or unauthorized use of elements of knowledge, possession, and inherence, and to prevent their duplication[18] The compromise of one SCA element must not affect the reliability of the others. If a multifunctional device (e.g., a smartphone) is used, measures must be implemented to mitigate associated risks (e.g., secure execution environments, tamper detection)[19]. Account Information Service Providers (AISPs), Payment Initiation Service Providers (PISPs), and PSPs issuing card-based payment instruments must be able to identify themselves to the Account Servicing Payment Service Providers (ASPSPs). To this end, they must use qualified certificates for electronic seals or website authentication (eIDAS certificates), which include specific attributes regarding their role and the competent registration authority[20].

ASPSPs must offer at least one interface that enables secure communication with Third-Party Providers (TPPs). These entities must apply secure encryption during data exchange over the Internet. TPPs must prevent access to, storage of, or processing of data for purposes other than the requested service[21]. Among the exemptions from the application of SCA provided by the Regulation – based on risk level, amount, frequency, and payment channel – particular mention should be made of the exemption under Article 10, which was later amended. This provision originally allowed for an optional exemption from SCA for access to account information (specifically, balance and transactions from the past 90 days, excluding sensitive payment data), provided that SCA was applied at the first access and at least once every 90 days thereafter. This exemption applied to both direct access and access via an Account Information Service Provider (AISP)[22]. The EBA had interpreted this and other exemptions as voluntary, giving ASPSPs the discretion to still require SCA, due to their responsibility for data protection. However, under Article 98(5) of PSD2 – which requires periodic review of the RTS to reflect technological developments – and due to the inconsistent application of this exemption in practice, on April 5, 2022, the EBA published a final report amending the RTS and introducing a new mandatory exemption[23]. With Delegated Regulation (EU) 2022/2360, it was established that when customers access their account information through an Account Information Service Provider (AISP), SCA is no longer required, provided that access is limited to the account balance and transactions from the last 90 days and does not involve the disclosure of sensitive payment data[24]. Conversely, when users access their online account information directly, the exemption from SCA remains optional for ASPSPs[25].

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

The PSD2 Directive also provides that Member States have to ensure that payment service providers establish a framework of mitigation measures and appropriate control mechanisms to manage operational and security risks. It also requires effective incident management procedures and the annual provision of an updated risk assessment to the competent authorities. It foresees that EBA will issue guidelines on security measures (Article 95 (3) [26]).

On 11 February 2025[27], EBA updated and narrowed the scope of its Guidelines on ICT and security risk management due to the implementation of the DORA. These changes aim to simplify the regulatory framework and avoid overlapping requirements. Under the revised Guidelines, only entities covered by DORA—such as credit institutions, payment institutions, account information service providers, and certain exempted entities—are now within its scope. The scope is limited to relationship management with users of payment services. However, PSD2 requirements on operational and security risk management, in force since 2018, still apply to payment service providers not covered by DORA, like postal giro institutions and credit unions. These providers may also be subject to additional national rules, depending on the decisions of national authorities. The updated Guidelines will apply by 20 May 2025 at the latest.

In line with the 2020 Digital Finance Strategy, the EU adopted a comprehensive legislative framework governing the issuance of crypto-assets as well as the provision of services related to crypto-assets. The Markets in Crypto-Assets Regulation (MiCA)[28], applicable since 30 December 2024, covers crypto-assets and the related services and activities that are not otherwise covered by other Union financial services legislation.

MiCA requires that issuers of crypto-assets and crypto-asset service providers adopt effective administrative arrangements to ensure that their security systems and protocols comply with EU standards. In particular, Article 34 (paragraphs 9–11) requires issuers of asset-referenced tokens to establish a business continuity policy and plans to ensure that, in the event of a disruption to their ICT systems and procedures, essential data and functions are preserved. If continuity cannot be maintained, they must be able to recover the data and resume operations without undue delay.

Issuers are also required to implement internal control mechanisms and effective risk management procedures, including safeguards for managing ICT systems in line with Regulation (EU) 2022/2554. This includes assessing any third-party providers involved in their operations. These procedures must be regularly evaluated and adjusted to address any vulnerabilities. Issuers must have appropriate systems and procedures in place to guarantee the availability, authenticity, integrity, and confidentiality of data. These systems must comply with Regulation (EU) 2022/2554 and the GDPR (Regulation (EU) 2016/679), ensuring the secure recording and storage of all relevant data generated during their activities.

Following the approach adopted in this risk assessment, it can be stated that the regulatory framework governing the financial sector can be considered a medium-risk context in relation to quantum threats. Although the principles-based approach does not pose obstacles to the adoption of quantum-safe technologies, the absence of explicit guidance or implementation measures specific to quantum computing leaves a regulatory gap in addressing emerging quantum-related risks.

2.2 Health Sector

On July 5, 2023, the ENISA published a report analysing the cyber threat landscape in the EU health sector[29]. Covering the period from January 2021 to March 2023, the report (see the table below, extracted from the report) highlights that EU healthcare providers were the most affected (53% of incidents), particularly hospitals (42%), followed by health authorities and agencies (14%), and the pharmaceutical industry (9%). What marked the threat landscape for the sector was the increase in ransomware attacks (54%) which in most cases (43%) led to data leakage (either data breaches or data theft) of patient information, including electronic health records, disruption of healthcare services (22%), and outages in non-health-related services (26%). Hospitals and primary care facilities were the most severely affected by data

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

breaches, resulting in closures of emergency departments, suspensions of surgeries, and delays in life-saving treatments. Ransomware remained a key threat in 2023, accompanied by an emerging wave of DDoS attacks targeting hospitals and health authorities. However, the overall impact of the latter remained limited.

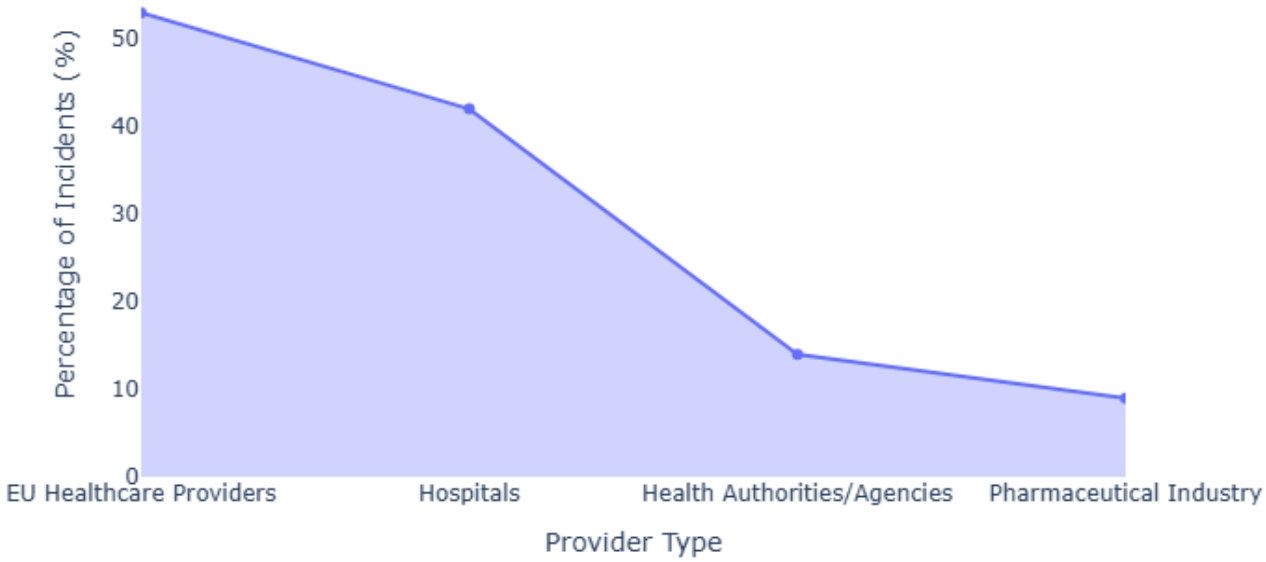


Figure 2.2: Cyber Incidents in the EU Health Sector (by Provider).

Similarly, malware accounted for only 5% of incidents (11 cases), mainly causing disruptions to services such as Internet access or email. Other significant causes of high-impact incidents included system failures (68%), human error (16%), and malicious actions (16%). The healthcare sector reported the highest number of incidents related to software and hardware vulnerabilities. Despite the sector's critical importance and the escalating threat landscape, many healthcare organizations remain insufficiently prepared to respond to cyberattacks. Research indicates that only 27% have a dedicated ransomware defence program in place, while 40% lack security awareness training for non-IT personnel[30].

A major concern highlighted by ENISA is the security of medical devices and the implications for patient safety and privacy. ENISA's Foresight Cybersecurity Threats for 2030[31] identifies targeted attacks using data from smart medical devices and wearables as a top future threat. Connected medical devices—used by 64% of healthcare organizations—pose emerging risks due to their sensitivity and critical role in patient care. Vulnerabilities in these devices can lead to severe consequences, such as misdiagnosis or treatment errors. Devices used in elderly care, mental health, or home-based care—like emergency buttons and remote monitoring tools—are particularly vulnerable. Their exploitation could endanger both patients and healthcare staff[32].

The continued use of unsupported medical devices lacking patches presents another critical challenge, as replacement options may be limited. During the pandemic, the rushed deployment of apps for testing and vaccination exposed additional vulnerabilities and sensitive data. As healthcare systems and devices become increasingly internet-connected, strong cybersecurity measures must be implemented. Currently, both the sector and its supply chain lag behind, with vulnerabilities being a major cause of incidents.

2.2.1 Analysis of the main regulations in the health sector

This section examines the two main European Union regulations governing medical devices: Regulation (EU) 2017/745 on medical devices (MDR)[33] and Regulation (EU) 2017/746 on in vitro diagnostic medical

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

devices (IVDR)[34]; and the Regulation (EU) 2025/327[35], establishing the European Health Data Space (EHDS), which lays the legal foundation for a secure, standardized, and interoperable framework for the use of health data across the European Union.

It is appropriate to jointly describe the existing regulatory framework in Europe concerning medical devices, consisting of the MDR and the IVDR, as the relevant provisions for the subject matter discussed here are largely analogous. A first reference point in both regulations is Article 10, which establishes the obligations of manufacturers regarding the design and manufacture of devices to ensure their safety and performance. Manufacturers must ensure that any devices they place on the market or put into service comply with the requirements of the Regulations. In particular, Article 10 of both regulations requires them to establish, document, implement, and maintain a risk management system, as described in the related Annex I, point 3. Annex I, which is present in both regulations and titled "General Safety and Performance Requirements", is one of the cornerstones of the regulatory framework. It stipulates that devices must be designed and manufactured in a manner that does not compromise the health or safety of patients, users, or other persons, ensuring an acceptable level of risk in relation to the intended benefits and consistent with the generally accepted state of the art.

Point 3 of Annex I requires manufacturers to establish and maintain a risk management system throughout the entire lifecycle of the device. This includes, for each device, the development of a risk management plan, the identification and analysis of known and foreseeable hazards, the estimation of risks associated with the intended use, the evaluation of information from production and post-market surveillance, and the adoption of control measures based on the recognized state of the art, in order to ensure that the residual risk, both individual and overall, is acceptable. In this context, the ability of future quantum computers to break current cryptographic algorithms must be considered among the foreseeable risks, particularly for devices that handle sensitive patient data.

Further references can be found in point 17 of Annex I of the MDR and point 16 of the IVDR, which address programmable electronic systems and software as integral parts of medical devices. These provisions impose requirements regarding the security, reliability, and performance of devices incorporating software, and require explicit cybersecurity measures, including protection against unauthorized access. The development and manufacture of such devices must also be based on the state of the art, and generally refer to the security, verification, and validation of the information handled by the software. Notably, point 17.4 (MDR) and point 16.4 (IVDR) explicitly require manufacturers to define the minimum requirements for hardware, network characteristics, and cybersecurity measures — including protection against unauthorized access — necessary for the software to function as intended. This represents the most direct cybersecurity obligation currently found in the MDR. Quantum threats directly undermine current protections against unauthorized access, which are based on classical encryption. These threats may also compromise device reliability and performance by targeting data or software integrity.

Finally, Article 10(4) in both regulations requires manufacturers to prepare and update technical documentation that demonstrates compliance with the requirements of the Regulation. This documentation must include the results of the risk management process[36] and the identification of applicable General Safety and Performance Requirements (GSPRs), as well as the solutions adopted to fulfil them (such as harmonized standards or common specifications)[37].

With regard to the European Health Data Space, it should be noted that Recitals already refer to the need for secure access to electronic health data, including in cross-border situations, with the consequent use of additional access mechanisms (e.g., tokens or access codes)[38]. Given the sensitivity of electronic health data, data users should not have unlimited access to such data. All access for the secondary use of requested electronic health data should occur through a secure processing environment.

To ensure the existence of robust technical and security safeguards for electronic health data, the body responsible for access to health data, or where applicable, the trusted data holder, should provide access to such data within a secure processing environment that complies with the high technical and security

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

standards established under this Regulation. The processing of personal data in such a secure environment should comply with Regulation (EU) 2016/679, including, where the secure environment is managed by third parties, the provisions of Article 28 thereof, and where applicable, Chapter V. The secure processing environment should reduce confidentiality risks related to such processing activities and prevent the electronic health data from being transmitted directly to the health data users.

The body responsible for access to health data or the data holder providing such a service should at all times retain control over access to electronic health data, and the access granted to health data users should be determined by the conditions of the data permit issued. It is appropriate for health data users to download only non-personal electronic health data from the secure processing environment, which does not contain any personal electronic health data. The secure processing environment thus constitutes an essential safeguard to protect the rights and freedoms of natural persons in relation to the processing of their electronic health data for secondary use.

The Commission should assist Member States in developing common security standards to promote the security and interoperability of various secure processing environments[39]. In this regard, Article 73 is entirely dedicated to secure processing environments, establishing that access to electronic health data may only be provided through an environment subject to technical and organizational measures and compliant with security and interoperability requirements. Paragraph 1 lists specific security measures[40]. The evolution of security threats, including those posed by quantum computing, may require these measures to be updated to ensure continued protection. Under paragraph 5, it is provided that the Commission shall, by no later than 26 March 2027, through implementing acts, establish technical and organizational requirements regarding information security, confidentiality, data protection, and interoperability for such environments.

Furthermore, manufacturers of Electronic Health Record (EHR) systems should demonstrate compliance with essential interoperability and security requirements by adopting common specifications. In this regard, Article 36 concerns common specifications and provides that the Commission may adopt, by no later than the end of March 2027, implementing acts to establish common specifications on various aspects, including technical specifications, standards and profiles for the exchange of electronic health data; requirements and principles relating to patient safety, the security, confidentiality, integrity and protection of electronic health data; specifications and requirements concerning identity management and the use of electronic identification. These common specifications must take into account the specificities of medical devices and high-risk AI systems (as per the MDR and IVDR), as well as state-of-the-art standards in the field of health informatics. Thus, in the future, the development of these common specifications may need to consider the vulnerabilities introduced by quantum computing and the need for post-quantum cryptography [41].

Annex II lays down essential requirements for the harmonized components of EHR systems and for products claiming interoperability with such systems, establishing that these components and products, including medical devices, must be designed and developed in such a way that the interoperability and security features of the system protect the rights of natural persons, in line with the system's intended purpose[42]. An EHR system intended for use by healthcare professionals must provide reliable mechanisms for their identification and authentication[43].

Applying the logic underpinning the risk assessment scale mentioned above, the regulatory framework governing the health sector can be classified as a medium-risk context in relation to quantum threats. There is no evidence of overly prescriptive cryptographic requirements that would hinder the adoption of post-quantum solutions. The flexibility afforded by the existing legal framework allows for the progressive integration of quantum-resistant measures.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2.3 Energy Sector

In the context of the ongoing digitalisation of the European energy sector, the European Commission has embraced a comprehensive and systemic approach to enhancing the cybersecurity of critical infrastructure. Through the 2022 Action Plan on the Digitalisation of the Energy System, the Commission aimed to integrate sector-specific initiatives within a broader, cross-sectoral cybersecurity framework. To this end, the NIS2 Directive designates the energy sector as one of the Union's critical infrastructures. It establishes binding obligations regarding risk management, supply chain security, and the implementation of technical and organisational measures to mitigate cyber threats.

In the electricity sector, the Commission – in cooperation with ACER, ENTSO-E, and the EU DSO Entity – signalled its intention to propose a delegated act for the adoption of a network code on the cybersecurity of cross-border electricity flows, pursuant to Article 59(2)(e) of the Electricity Regulation[44] [45]. This code is expected to include common minimum requirements, forward planning, continuous monitoring, effective communication protocols, and robust crisis management provisions, with the overarching goal of bolstering the resilience of the European electricity grid.

Already in 2019, the "Clean Energy for All Europeans" legislative package had laid the foundations for a transformative shift in the EU energy system, promoting efficiency and sustainability while placing a growing emphasis on cybersecurity — now recognised as a cornerstone of the sector's digital transformation. In the same vein, Regulation (EU) 2019/941 on risk preparedness in the electricity sector explicitly stipulates that malicious cyberattacks must be accounted for among the baseline risks in regional electricity crisis scenarios.

Similarly, with the proposed amendment to the Regulation on the Security of Gas Supply, the Commission seeks to align the gas sector with emerging threats, including those of a cyber nature. Upon adoption of this amendment, a dedicated delegated act is foreseen, addressing the cybersecurity of gas and hydrogen networks. This measure will complete the regulatory landscape, ensuring that cybersecurity is addressed in a coherent and coordinated manner across all branches of the European energy system[46].

2.3.1 Analysis of the main regulations in the energy sector

Delegated Regulation (EU) 2024/1366, published in May 2024 and entering into force on 13 June of the same year, established the European Union's first network code dedicated to cybersecurity in the electricity sector[47]. This regulation sets out a harmonized regulatory framework for the protection of cross-border electricity flows, introducing common minimum requirements, planning strategies, monitoring activities, reporting mechanisms, and crisis management procedures in response to cyberattacks[48].

Given the high degree of digitalization and interconnection of European electricity networks, the regulation acknowledges the need for shared regulatory tools within the Union to prevent and mitigate cybersecurity vulnerabilities. In this context, Transmission System Operators (TSOs) and Distribution System Operators (DSOs), to whom Regulation (EU) 2019/943 assigns specific responsibilities in the field of cybersecurity, are required to adopt common methodologies for risk assessment and management, including incident classification scales and proportionate mitigation measures[49]. The Agency for the Cooperation of Energy Regulators (ACER) plays a central role in monitoring the implementation of the prescribed measures. Every three years, it must publish a report on the effectiveness of the policies adopted by high-impact and critical-impact entities, assessing the need for regulatory updates, the identification of new priorities, or adjustments in light of technological developments[50].

In this regard, the regulation also provides a review mechanism in case of emerging threats: if quantum computing were to pose a significant cybersecurity threat to the sector, this section could provide a mechanism to review and update the regulation accordingly. The regulation mandates the drafting of a cross-border electricity cybersecurity risk assessment report, which must include an analysis of current

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

cyber threats, with a particular focus on emerging threats and risks to the electricity system[51]. In this context, quantum computing could be considered an emerging threat and, if so, would need to be addressed in the report. High-impact and critical-impact entities are required to carry out risk assessments that account for potential cyber threats, including those identified in the latest cross-border cybersecurity risk assessment[52]. Therefore, if risks related to quantum computing are recognized at Union level, they must be considered in the cybersecurity strategies adopted by these entities.

The regulation establishes a common cybersecurity framework for the electricity sector, consisting of both basic and advanced cybersecurity controls, a mapping matrix, and a cybersecurity management system[53]. These controls are defined based on the risks identified in earlier risk assessment reports[54] and include specific measures to protect information exchanged across systems, as required under Article 46. Their implementation must be verifiable through audits or national verification mechanisms. Responsibility for developing proposals for these controls lies with TSOs, in cooperation with the EU DSO[55]. These controls must be auditable, either via national systems or through independent third-party audits. The initial version of these controls is based on cybersecurity risks identified at the Union level and includes safeguards for the protection of shared information[56] Entities identified as high-impact or critical-impact must implement these controls when defining their entity-level risk mitigation plans. If future assessments highlight risks stemming from quantum computing, the basic and advanced controls may be revised accordingly, for example, through the adoption of post-quantum cryptography.

These entities are also required to establish a cybersecurity management system covering all assets within their designated perimeter. After submission of the initial draft of the cybersecurity risk assessment (Article 19(4)), TSOs, ENTSO-E, and the EU DSO are tasked with developing proposals for additional cybersecurity controls in the supply chain, which build on and complement the controls defined under Article 29. These supply chain controls address critical areas, including background checks on supplier personnel (with identity verification in line with Regulation (EU) 2016/679), secure design and manufacturing processes, supplier access to operational assets, contractual safeguards, criteria for supplier selection, and diversification of supply chains. Basic controls also include procurement requirements that incorporate cybersecurity specifications. These may cover secure design of IT and network systems—particularly those handling untrusted devices—obligations to subcontractors regarding data protection, traceability of cybersecurity requirements, support for updates, and the right to audit suppliers' cybersecurity measures.

To ensure the confidentiality, integrity, availability, and non-repudiation of information shared under the regulation, protective measures must be implemented. These include anonymizing data prior to disclosure and restricting access exclusively to individuals who meet specified criteria. By 13 June 2025, ACER, following consultation with ENISA, national authorities, ENTSO-E, and the EU DSO, must issue guidance on the communication mechanisms to be used by all relevant entities (Article 2(1)). This includes recommended flows of information exchange and methods for anonymizing and aggregating data in accordance with the regulation. By the same date, ENTSO-E, in cooperation with the EU DSO, is required to compile a provisional list of relevant European and international standards and national legislation that are applicable to the cybersecurity of cross-border electricity flows[57]. This list, informed by inputs from competent authorities, must include: European and international standards and national laws providing guidance on cybersecurity risk management at the entity level; and cybersecurity controls equivalent to those likely to be adopted as part of the regulation's basic and advanced controls.

According to what has been observed so far, the digitalisation of infrastructure within the European energy landscape is exposing energy networks to new and more complex vulnerabilities, particularly in terms of cybersecurity. In this context, the European Commission has adopted Regulation (EU) 2024/1789[58], which significantly updates the regulatory framework for the internal markets of natural gas, renewable gas, and hydrogen, including clear provisions on cybersecurity. While, as we have seen, the EU has already implemented advanced measures in the electricity sector—such as a dedicated network code for the cybersecurity of cross-border electricity flows—the gas sector has so far shown a clear regulatory gap.

The regulation addresses this issue by granting the European Commission the power to adopt delegated

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

acts to develop network codes that regulate cybersecurity aspects of cross-border flows of natural gas[59] and hydrogen[60]. These codes, which are still under development, are expected to include: common minimum cybersecurity requirements; mechanisms for preventive planning and continuous monitoring; and guidelines for threat communication and crisis management. Although there are already network codes in place for gas concerning interoperability and data exchange[61], gas balancing in transmission networks[62], capacity allocation mechanisms in gas transport systems[63], and transportation tariffs[64], none of them currently address cybersecurity directly.

According to the risk assessment framework adopted here, the European energy sector, as currently regulated, can be classified as a medium-risk context in terms of the potential impact of quantum threats. While the sector is clearly designated as critical infrastructure and is subject to a complex and evolving regulatory framework—particularly in the electricity domain—the regulations in force, including the recently adopted Delegated Regulation (EU) 2024/1366, maintain a flexible and adaptive approach. Rather than mandating specific cryptographic standards, the regulatory instruments emphasize general cybersecurity principles, risk-based methodologies, and forward-looking review mechanisms capable of responding to technological developments, including quantum computing. Importantly, the regulations foresee the possibility of revising existing cybersecurity controls in response to emerging threats. However, they do not currently impose prescriptive technical requirements that would inhibit the integration of post-quantum cryptographic solutions.

2.4 E-governance Sector

In this context, it is important to examine the **eIDAS Regulation (Regulation (EU) 910/2014)[65] which is being updated by the EU Digital Identity Framework Regulation (known as EUDI Regulation)**[66] and its full implementation is expected by 2026. An innovative solution, the European Digital Identity Wallet (EUDI Wallet), will be introduced and made available by each Member State to its residents, citizens, and businesses. This new wallet aims to replace and enhance existing national identity schemes, enabling individuals and legal entities to officially identify themselves online, share legally valid documents, digitally sign and seal, and access both public and private services. However, the current technological landscape presents a significant challenge: the public key cryptographic systems (PKI) widely used today—including those implemented in EUDI Wallet prototypes, such as RSA and Elliptic-Curve Cryptography (ECC)—are vulnerable to the advent of quantum computing. It is suggested that the **European Digital Identity Wallet (EUDI Wallet)** could serve as an ideal starting point for the effective introduction of **quantum-resistant hybrid cryptographic tools** (PQC) to align Member States in the transition. The **flexibility and technological neutrality** of the **eIDAS2** language allow for the **timely implementation of new secure cryptographic methods**, making the Wallet an **exemplary model for large enterprises, app developers, and SMEs**, which will also need to undergo this transition. Given the anticipated broad and rapid adoption, the EUDI Wallet approach could become a reference point for the shift toward post-quantum capabilities, serving as a metaphorical “ark” to guide all stakeholders from the pre-quantum to the post-quantum era[67].

eIDas Regulation aims to enhance trust in electronic transactions within the internal market by providing a common framework for secure electronic interactions between citizens, businesses, and public authorities. To this end, it sets out the conditions under which Member States recognize electronic identification means issued in another Member State under a notified scheme. In its Recitals, the Regulation seeks to adapt to new technologies without requiring fundamental changes to the legal text. It emphasizes the importance of the security of electronic services[68] (such as electronic signatures) and the need to establish obligations for the recognition of such electronic identification means that provide specific levels of assurance, based on standards, procedures, and technical requirements that should be technologically neutral. The Regulation aims to be open to innovation and technologically neutral, so that its legal effects can be achieved through any technical means, provided the requirements are met[69].

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

The Regulation provides that a notified electronic identification scheme must specify the levels of assurance (low, substantial, and high) for the electronic identification means issued under that scheme, in order to define the degree of confidence with which the electronic identification means establish a person's identity. Article 8, paragraph 3, of the eIDAS Regulation empowers the Commission to define, by means of implementing acts, the minimum technical specifications, standards, and procedures in reference to which the levels of assurance are specified[70].

The European Commission, through Implementing Regulation 2015/1502, defined the essential minimum technical specifications and procedures to ensure a common understanding of the details of the levels of assurance and to guarantee interoperability between the notified national schemes[71]. The Annex to the Implementing Regulation provides the technical and procedural details for each of the elements necessary to determine the reliability and quality of the identification means (enrolment, management of the means, authentication, and management and organization), specifying the requirements for each level of assurance. The requirements maintain a fairly technology-neutral approach, as they define characteristics that can be adapted to future technological innovations: for example, with regard to the features of electronic identification means required during the registration process[72], or the requirements set for each level of assurance in relation to authentication mechanisms[73], or with regard to information security management, policies, and risk management approaches adopted by electronic identification service providers in a cross-border context[74].

As mentioned, eIDAS2 introduces the EUDI Wallet, which is built upon the principle of **security-by-design**, requiring the highest level of data protection and security for electronic identification and authentication—whether data is stored locally or in the cloud. Wallets must incorporate advanced security features to protect against identity and data theft, denial-of-service attacks, and other cyber threats. This includes state-of-the-art encryption and storage methods that are accessible and decryptable **only by the user**, along with **end-to-end encrypted communications**. Moreover, all operations must require **explicit, secure, and active user confirmation**[75]. In parallel, the Wallet adheres to the principles of privacy-by-design and data minimization. It supports the "una tantum" principle, aiming to reduce administrative burdens and facilitate cross-border mobility[76]. Users can selectively disclose only the data strictly necessary to access a given service. Wallet providers are prohibited from collecting data unrelated to the provision of the service or combining Wallet data with other personal information—unless explicitly requested by the user and in full compliance with the GDPR[77].

The user control and transparency of the EUDI Wallet is ensured through a built-in, unified management interface, allowing individuals to view relying parties they have interacted with, the data exchanged, and to monitor all transactions. Users also have the right to request the deletion of personal data and report suspicious data requests[78]. Additionally, the Wallet includes functionality for pseudonym generation, allowing users to authenticate online using pseudonyms they create and manage, in cases where legal identity is not required[79]. The Wallet also enables users to create and use **qualified electronic signatures and seals**, which are recognized across the EU. Individuals will be able **to sign using qualified electronic signatures free of charge for non-professional purposes**. To ensure security and compliance, all EUDI Wallets must undergo **certification by accredited bodies**. These certifications are valid for a maximum of five years, provided vulnerability assessments are conducted at least every two years[80].

In line with the methodology adopted for the current risk assessment, the European e-governance sector can be classified as a low-risk context with respect to the impact of quantum threats. While the underlying cryptographic infrastructure of current identity systems—including PKI protocols such as RSA and ECC—remains vulnerable to future quantum computing threats, the regulatory approach adopted in eIDAS and the EUDI Regulations remains technology-neutral. Rather than imposing rigid cryptographic standards, the framework emphasizes security- and privacy-by-design, proportional risk management, and adaptability to future technological developments. The flexibility afforded by this approach allows for the timely integration of PQC solutions, without requiring fundamental changes to the legal texts.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2.5 Transportation Sector

On March 21, 2023, the ENISA published a report analysing the cyber threat landscape of the transport sector in the EU. Covering the period from January 2021 to October 2022, the report is based on an analysis of cyberattacks targeting the aviation, maritime, rail, and road sectors, which fall under the scope of the NIS Directive. The methodology involved analysing 98 publicly reported incidents. For the aviation sector, this data was supplemented with incidents reported to the European Union Aviation Safety Agency (EASA) and the European Centre for Cybersecurity in Aviation (ECCSA), as well as those provided by Eurocontrol's EATM-CERT.

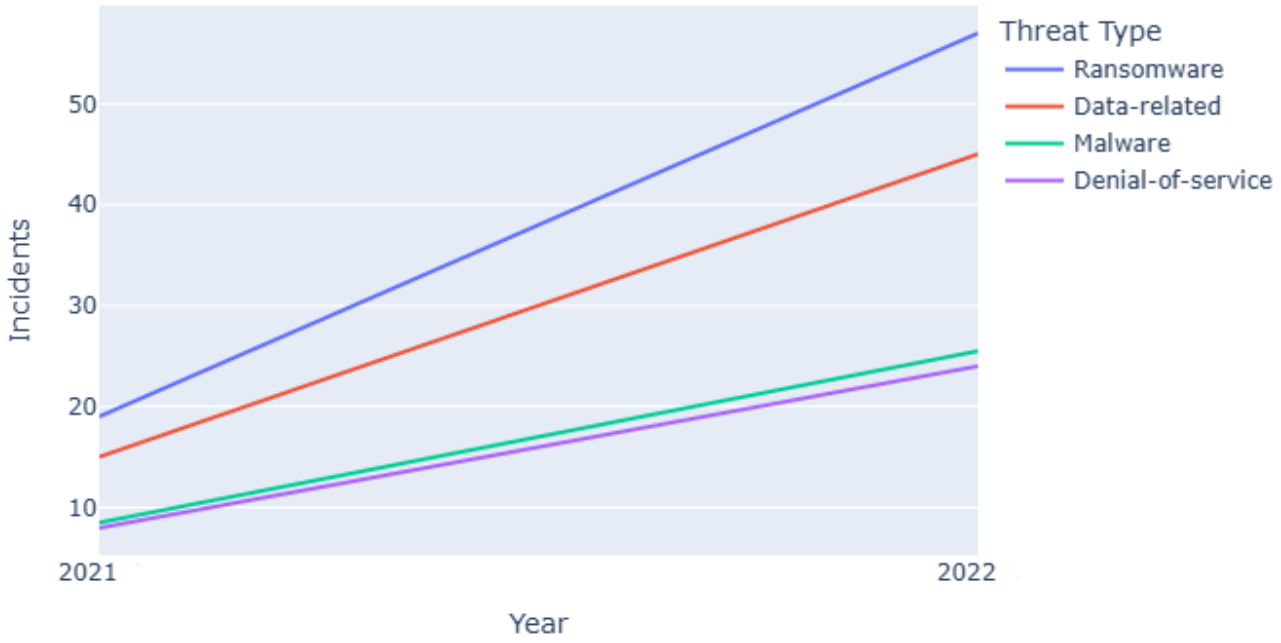


Figure 2.3: Cyber Incidents in the EU Transport Sector (by Attack Type).

The report (see the above table, extracted from the report) acknowledged a 25% increase in the average number of reported incidents per month between 2021 and 2022, with a significant rise in incidents within the EU borders and in geographical areas close to EU borders in 2022, due to the geopolitical situation during the reporting period. One of the most frequent threats observed was ransomware, accounting for 38% of all reported incidents. Ransomware became the dominant cyber threat in 2022, with a noticeable increase in the number of reported cases compared to 2021. The second most common category involved data-related threats (e.g. unauthorized access, disclosure, data breaches and data leaks) making up 30% of incidents. Malware was involved in 17% of the incidents, showing a decrease in 2022 and denial-of-service attacks were responsible for 16% of the incidents. The latter increased in 2022, largely due to hacktivist activity linked to the Russian invasion of Ukraine.

The main targets included airports, railways, and European transport authorities — and this trend is expected to continue. Regarding the findings for each transport sector, in the aviation sector, the most common threats were data related (45%), ransomware (36%) and malware (23%). In most ransomware cases, the attack was followed by data exfiltration or leakages, meaning these two threat categories often overlap. Customer data remains a primary target, followed by proprietary information from Original Equipment Manufacturers (OEMs). In 2022, ransomware attacks on airports increased, primarily targeting airport operators. Airlines and passengers were also affected by other types of incidents that compromised personal and operational data. A significant threat reported by Eurocontrol's EATM-CERT was the rise in

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

fraudulent websites impersonating airlines — targeting both the companies and their customers. Other threats reported in 2022 included web application attacks (22%), DDoS attacks (13%) — mainly hacktivist-driven and directed at airports and aviation authorities — phishing (12%), ransomware (6%), and malware (1%). In the maritime sector, cybercriminals and individual attackers mainly launched ransomware, malware, and phishing or spear-phishing campaigns. These attacks typically targeted port authorities, port operators, and manufacturers, particularly in the supply chain. Many of these attacks appear to be politically motivated and carried out by state-sponsored actors.

Between 2021 and 2022, several notable incidents linked to nation-state activities were reported. These operations suggest that disrupting port operations or vessel activity is a growing interest for hostile governments. Another emerging threat is the spoofing of the Automatic Identification System (AIS) used by ships. Although rare, this type of attack — possibly orchestrated by a hostile state — could become a serious concern. In the rail sector, ransomware and data-related threats were the most common, representing 45% and 25% of incidents, respectively. These are often linked, as ransomware attacks frequently result in data leakage or exfiltration. DDoS attacks also increased significantly in 2022, making up 20% of rail-related incidents — again, largely attributed to hacktivist activity tied to the war in Ukraine. Most attacks targeted railway IT systems, including passenger services, ticketing platforms, mobile apps, and display boards, leading to service disruptions caused by system outages. Ransomware was also the leading threat in the road transport sector, accounting for 43% of incidents, followed by data-related threats (26%) and malware (17%). The automotive industry was heavily targeted. In some cases, ransomware attacks forced companies to halt the production of vehicles or parts.

Data-related threats in this sector mainly focused on IT systems and aimed to obtain customer or employee data, as well as confidential business information. There were also a number of cyber incidents that did not fall neatly into a specific transport subsector. These include large-scale campaigns targeting the entire transport sector within certain countries. Such campaigns are often attributed to hacktivists or state-sponsored actors and are typically linked to geopolitical tensions. Some incidents directly targeted national or regional transport authorities.

2.5.1 Analysis of the main regulations in the transportation sectors

Regulation (EU) 2018/1139 sets common rules in the field of civil aviation, with the main objective of ensuring a high and uniform level of safety across the EU[81]. The regulation acknowledges the increasing reliance of civil aviation on modern information and communication technologies, and it establishes essential requirements to ensure the security of the information used in the aviation sector[82]. The principles guiding the adoption of safety and security measures include: reflecting the current state of the art; being based on data and analysis; enabling rapid responses to safety issues; taking into account the interdependencies between different areas of aviation safety, and between aviation safety, cybersecurity, and other technical aspects of aviation regulation; and being proportionate to the nature and risk of the activity involved[83].

The Regulation sets out the essential airworthiness requirements for aircraft (other than unmanned aircraft) and their components, as well as the essential environmental compatibility requirements[84]. Annex II outlines the essential airworthiness requirements, covering the integrity of the product. It states that integrity must be ensured, including protection against information security threats, under all intended flight conditions [85]. Systems and equipment must be designed to minimize risks arising from reasonably foreseeable threats, including both internal and external information security threats, as well as from failures or significant disruptions of non-installed equipment[86] Essential requirements are also established for the operation of aircraft (other than unmanned aircraft)[87]..

Annex V sets out the essential requirements related to flight operations, stating that the data, documents, and records needed to demonstrate compliance with the conditions set out in point 5.3[88] must be retained and protected against unauthorized modifications[89]. Organizations responsible for operations must de-

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

velop and maintain security programs that include the protection of electronic and IT systems, in order to prevent both intentional and unintentional interference or tampering[90]. The Regulation lays down the essential requirements for airports, safety-related airport equipment, airport management, and the provision of ground handling and Apron Management Services (AMS)[91].

Annex VII, which details these requirements, also refers to airport data: such data must be accurate, complete, unambiguous, and possess integrity and authenticity. It must be made available to relevant users and Air Navigation Service (ANS)[92] providers through a communication method that is sufficiently secure and fast[93]. The Regulation sets out the essential requirements for air traffic controllers and the individuals, organizations, and devices involved in their training, testing, and medical fitness assessment. These requirements are described in Annex VIII, which establishes that aeronautical and meteorological information must be accurate, complete, up to date, unambiguous, originate from a legitimate source, have the required level of integrity, and be presented in a format suitable for users. Their transmission must take place through communication means that are sufficiently reliable and fast, and protected against interference and tampering[94]. ATM/ANS systems and components must be properly designed, manufactured, installed, maintained, protected from unauthorized interference, and used in a manner that ensures their fitness for purpose[95]. The integrity and security performance of systems and components must be appropriate for their intended use. The EATMN, along with its systems and components, must support the timely exchange of accurate and consistent information between civil and military parties, without prejudice to security or defence interests, including information confidentiality requirements. Systems and components must be designed to meet applicable security requirements and to ensure their protection—as well as the protection of the data they carry—against harmful interactions from both internal and external sources[96].

With regard to unmanned aircraft (drones), their design, production, maintenance, and operation, as well as the personnel (including remote pilots) and organizations involved, Annex IX describes the essential requirements for design, production, maintenance, and operation (including knowledge of regulations, fitness for purpose, safety/privacy/security features, and information provided by the manufacturer). Unmanned aircraft must have specific features and functionalities to mitigate risks related to privacy protection, personal data protection, security, or the environment arising from their operation, taking into account the principles of privacy and data protection by design and by default[97]. The design of unmanned aircraft must include precautions to minimize risks, including protection against interference caused by electronic devices[98]. Unmanned aircraft operators must be registered if the use of drones poses risks to privacy, personal data protection, security, or the environment[99].

Delegated Regulation (EU) 2022/1645, which applies from 16 October 2025, lays down rules (Information Security Management System or ISMS and related requirements) to specify the technical and security measures for managing information security risks that could impact aviation safety[100]. It legally enforces the application of these measures on specific civil aviation entities—namely, aircraft design and production organisations, airport operators, and apron management service providers—already subject to Regulations (EU) No 748/2012 and (EU) No 139/2014, by amending those regulations to explicitly include the obligation to implement an ISMS. The detailed technical and security measures set out in the delegated regulation—such as risk assessment, detection and response processes, and specific reporting requirements—thus become an integral part of the aviation safety regulatory framework established by Regulation (EU) 2018/1139 for the areas it covers.

This delegated regulation was adopted by the European Commission based, among other things, on Article 19(1)(g) and Article 39(1)(b) of Regulation (EU) 2018/1139[101]. Requirements for the relevant organisations (i.e., design and production organisations under Regulation (EU) No 748/2012, and airport operators and apron management service providers under Regulation (EU) No 139/2014) are contained in Annex entitled “INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR]”. The latter provides that organisations must establish, implement, and maintain an ISMS to manage information security risks with a potential impact on aviation safety[102].

The ISMS must ensure that the organisation: (i) Establishes an information security policy that defines

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

the organisation's general principles regarding the potential impact of information security risks on aviation safety; (ii) Assesses the elements exposed to information security risks (such as activities, facilities, resources, services, equipment, systems, data) and identifies the interfaces with other organisations based on the potential threat and severity of consequences for aviation safety, taking into account the likelihood of the threat scenario and the severity of its consequences[103]; (iii) Defines and implements measures to treat information security risks[104]; (iv) Implements an internal reporting system to collect and internally analyse events related to information security[105]; (v) Defines and implements measures to detect information security events, identify incidents and vulnerabilities with a potential impact on aviation safety, respond to such events, and restore safe conditions[106]; (vi) Takes appropriate action in response to non-compliance notified by the competent authority (by identifying root causes, defining a corrective action plan, and demonstrating its implementation to the competent authority)[107]; (vii) Implements an external reporting system to enable the competent authority to take appropriate action[108].

Regarding the maritime sector, for ships flying the flag of EU Member States and for port facilities, security (including cybersecurity) is addressed at the European level by **Regulation (EC) No 725/2004**[109]. The Regulation primarily establishes **physical security measures**: for example, Rule 6 of Annex I[110] requires the installation of a **ship security alert system** on certain categories of ships (e.g., passenger vessels). This system must transmit a **ship-to-shore security alert** to a competent authority, indicating the ship's identification, its position, and that the ship's security is under threat or has been compromised. Nevertheless, the Regulation—through the incorporation of provisions from the SOLAS Convention and the ISPS Code—also includes cybersecurity-related measures. These measures, in addition to physical ones, can be found in Part A and in the binding provisions of Part B of the ISPS Code, which the Regulation makes applicable.

For both ships and port facilities, the **security assessment** (the **Ship Security Assessment** for ships and the **Port Facility Security Assessment** for ports) must take into account the protection of **radio and telecommunication systems, including networks and computer systems**, as these are inherently vulnerable to cyber threats. As a result, both the Ship Security Plan (SSP) and the Port Facility Security Plan must include procedures and practices aimed at protecting security-sensitive **information, whether stored in paper or electronic format**[111]. The **SSP may be stored in electronic format**, but in such cases, **it must be protected through procedures designed to prevent its deletion, destruction, or unauthorized modification**[112]. The same principle applies to documentation stored on board[113] and to the port facility security plan[114]. These provisions are intended to ensure the integrity and confidentiality of digital information.

In this context, **Directive 2005/65/EC**[115], which aims to enhance port security more broadly, reinforces and expands upon the measures established by the Regulation previously discussed, applying them to the **entire port area**. The Directive generally requires the adoption of **appropriate measures to protect information subject to confidentiality obligations**[116], thereby implying the need for **information security systems**. With regard to the measures and procedures to be implemented in **port security plans, Annex II** outlines the requirements for **access control and identity, baggage, and cargo verification**, including:

- the explicit mention of the use of "specific identification cards for port security purposes," with clear procedures for their issuance, use, control, and return. This necessitates the implementation of identity and credential management systems;
- the connection with authorities responsible for controlling cargo, baggage, and passengers, including potential information and authorization systems and "pre-arrival authorization systems." This indicates a reliance on IT and network infrastructure for data exchange and authorization processes;
- monitoring requirements for specific areas or activities conducted within them, referring to the use of video surveillance systems, sensors, and other monitoring technologies;
- communication and security authorizations, including the need to communicate security information

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

appropriately and to protect "sensitive information from unauthorized disclosure"[117].

Recently, **Regulation (EU) 2019/1239**[118] was adopted on 25 July 2019, establishing a European Maritime Single Window environment (EMSWe). The EMSWe consists of a decentralized network of **Maritime National Single Windows (MNSW)**, which serves as the single-entry point for information exchange in each maritime Member State. These national interfaces are harmonized through the use of a common software module developed by the European Commission, ensuring technical consistency and continuous updates[119]. It is important to highlight that the EMSWe is designed as a **technologically neutral system**, based on the existing national infrastructure, with the aim of enabling an efficient, transparent, and interoperable flow of information among Member States[120].

Additionally, the Regulation acknowledges the potential of emerging digital technologies to enhance the efficiency of the sector and empowers the Commission to adopt implementing acts to amend technical specifications, standards, and procedures, ensuring that the harmonized declaration interfaces remain "open to future technologies" [121] [122]. In this context, on 28 October 2023, **Implementing Regulation (EU) 2023/204**[123] was adopted, setting out the technical specifications, standards, and procedures for the EMSWe. Alongside the technical requirements for the development and operation of the system, the regulation defines a series of security measures for various common databases (the EMSWe ship database[124], the common site database[125], and the common Hazmat database[126]), including:

1. Identification: implementation of a reliable mechanism for uniquely identifying database users through a unique user ID;
2. Authentication: for system-to-system interfaces, authentication must rely on recognized methods using two-way Secure Socket Layer (SSL) protocols. For web user interfaces, users must authenticate via credentials;
3. Authorization: access to the database interfaces must be controlled through access management measures, with all accesses logged and authorizations regularly reviewed;
4. Traceability and accountability: the databases must ensure non-repudiation of user actions, tracking every access, event, and data modification. Each event must log the user's identity, timestamp, and the action performed;
5. Integrity: integrity checks must be in place to prevent harmful events that could compromise the functionality of the system[127].

To enable access to the national maritime single window interface, the European Commission has established a **common system for managing the registration and access of declarants** and data service providers using that interface. This system ensures a **single user registration** recognised throughout the Union, a consolidated user management process, and EU-level monitoring, with the goal of ensuring the integrity and security of authentication and access procedures[128].

On 14 December 2023, the Commission adopted **Implementing Regulation (EU) 2023/2790**[129], establishing the technical and functional specifications of the **Reporting Interface Module (RIM)** for the national maritime single windows (MNSW), as well as for the **User Registration and Access Management system (URAM)**[130].

Key technical and security measures set out in the Regulation include:

1. The RIM must ensure the **confidentiality of information** and the **protection of personal data** exchanged by encrypting data between the sender's access point and the RIM. The RIM is responsible for decrypting messages and making them available to the MNSW core.
2. To ensure secure message exchange, the **Web Service Security (WSS)** standard is applied. **Sender authentication is mandatory** and must be initiated by the RIM through a central or national authentication service. Senders must obtain a **qualified electronic seal certificate** in accordance with Regulation (EU) No 910/2014 (eIDAS).
3. The **central authentication service** (part of URAM) verifies the certificate's validity, the sender's

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

EORI number, and the association between the certificate and the EORI number, by querying the central or, if available, the national register of the sender's country.

4. Communication and message validation via the RIM must include security measures to **ensure message authenticity** and **prevent repudiation**. Technical measures must also be in place to guarantee the **integrity of exchanged data**.
5. Within the URAM system, the use of **Transport Layer Security (TLS)** ensures encryption at the network level and safeguards data integrity during transmission.
6. Finally, the RIM must implement mechanisms to ensure **message preservation and recovery** in the event of service unavailability, avoiding data loss.

Furthermore, it is worth noting that **Regulation (EU) 2019/1239 builds upon Regulation (EU) 910/2014 (eIDAS)**[131], and the processing of personal data, including data related to authentication, must comply with **Regulation (EU) 2016/679 (GDPR)**. Member States and the Commission are required to take all necessary measures to ensure the **confidentiality of commercial and other sensitive information** exchanged through the system[132].

According to the risk assessment framework adopted in this analysis, the transport sector can be classified as a **medium-risk** context with respect to quantum threats. The regulations examined adopt technologically neutral approaches based on general principles of information security, encryption, integrity, and risk management, without imposing prescriptive cryptographic standards that would hinder the adoption of post-quantum solutions. However, while the existing cybersecurity requirements are robust, they do not yet include explicit quantum-safe provisions, leaving room for the gradual introduction of hybrid or post-quantum cryptographic technologies.

2.6 Telecommunication Sector

The telecommunications sector represents one of Europe's most critical infrastructures, serving as the backbone for digital communications, economic activities, and public services. The **European Electronic Communications Code (EECC)**, established by **Directive (EU) 2018/1972**, serves as the primary regulatory framework for electronic communications networks and services within the European Union. It consolidates and replaces earlier directives to address new market realities, technological advancements such as 5G, and the rise of internet-based communication services.

The European telecommunications sector is governed by several regulations spanning network operations, net neutrality[133], infrastructure deployment, consumer protection, and market competition. In the context of cybersecurity, the focus of this document, some relevant ones are:

- Network and Information Security Directive (**NIS2**) directive explicitly designates telecommunications as critical infrastructure and establishes the requirement to implement robust measures for cyber risk management and to notify authorities about significant security incidents.
- General Data Protection Regulation (**GDPR**) is the reference in Europe's privacy and data protection law. It applies to all network operators, mandating strict controls over the processing of personal data, user privacy, and the confidentiality of communications.

Additionally, network operators in Europe are subject to several specific regulations, particularly complex concerning data retention and lawful interception. This latest development is a complex set of national regulations based on the Council Resolution of 17 January 1995 on the lawful interception of telecommunications and is strongly dependent on ETSI technical specifications and standardization, which will need to address the quantum-safe transition.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2.6.1 Analysis of the main regulations in the telecommunication sector

The telecommunications sector exhibits several characteristics that make it particularly vulnerable to quantum threats:

- **High ICT dependency**: Telecommunications networks are entirely dependent on information and communication technologies. This complete reliance on digital systems amplifies the potential impact of quantum attacks. For example, the lack of availability of quantum-safe communication infrastructure supply chain can limit the capability to address quantum attacks.
- **Interconnected infrastructure**: The sector's highly interconnected nature creates systemic risks where a quantum attack on one component could cascade throughout the entire network domain.
- **Critical services provision**: Telecommunications infrastructure supports other critical sectors, including healthcare, military, government, finance, or energy, making it a high-value target for quantum-capable adversaries.
- **Multiple actors**: The telecommunications sector's own nature requires transmitting sensitive and long-term valuable information over a complex and extensive number of networks and nodes with different administrative domains, which increases the risk of capturing traffic by adversaries, to apply the attack of the 'store now, decrypt later' when quantum computers are available.

Also, adopting quantum-safe technologies brings relevant implementation challenges:

- **Network Complexity**: Modern telecommunications networks exhibit extraordinary complexity, with multiple generations of technology operating simultaneously.
- **Performance Requirements**: Telecommunications networks must maintain high performance and low latency, which may limit some quantum-safe implementations.
- **Interoperability**: Ensuring interoperability between quantum-safe and legacy systems during transition periods presents significant technical challenges.

Despite the comprehensive nature of existing regulations identified, several gaps exist in addressing quantum threats to telecommunications:

- **Lack of sector-specific requirements**: Current regulations do not provide telecommunications-specific guidance on quantum threat mitigation, unlike more prescriptive requirements in sectors such as finance, or health.
- **Technology implementation guidance**: While regulations promote quantum-safe approaches, they lack detailed implementation guidance for telecommunications operators.
- **Certifications**: The absence of harmonized certification schemes for quantum-safe telecommunications equipment creates uncertainty for operators. This will need operators' work on standards.

The European Commission's **Recommendation 2024/1101**[134] on post-quantum cryptography, issued in April 2024, provides the first regulatory guidance on quantum threats, where some dates are provided, and where operators are considered relevant actors[135]. The recommendation has been transformed in a clear strategy defined by the NIS Cooperation Group[136], which establishes a coordinated implementation roadmap with specific timelines:

- **By the end of 2026**: All EU Member States must develop national PQC transition roadmaps and begin pilots for high- and medium-risk use cases.
- **By the end of 2030**: Transition of high-risk use cases should be complete, with quantum-safe upgrades becoming standard in critical systems.
- **By the end of 2035**: PQC should be implemented across most medium- and low-risk systems

In parallel, a work is in progress for a European Quantum Act[137] to position quantum technologies as a relevant activity, and where the quantum threat is identified and some of the technologies, such as PQC or QKD, are identified to address this threat.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Some of the potential recommendations associated with the Telecom sector for regulators are:

- **Industry-Government Partnerships**: partnerships between telecommunications operators and regulatory authorities should be established to facilitate information sharing and coordinated response to quantum threats.
- **Certification development**: Active participation in international standardisation efforts and certification programs should be promoted to ensure European influence in quantum-safe telecommunications standards. Examples such as ETSI ISG QKD or ETSI CYBER QSC are clear actions in this direction. Additionally, other example is the recent (May 2025) European Cybersecurity Certification (**EUCC**) group scheme's inclusion of PQC algorithms[138].
- **Increase Research Investment**: Expand funding for quantum-safe research and development, particularly in telecommunications applications, as a substrate with impact in several critical sectors.

According to the risk assessment framework adopted in this analysis, the telecommunications sector can be classified as **medium/high risk** context with respect to quantum threats. This classification reflects the high criticality of the sector, combined with a regulatory environment that is predominantly principles-based, emphasizing general objectives such as resilience, integrity, and encryption, while also incorporating specific policy instruments that directly address quantum computing issues. In particular, the Recommendation 2024/1101 encourages a coordinated and proactive transition toward post-quantum cryptography in public infrastructures and critical services: it advocates for the assessment and selection of PQC algorithms, the deployment of hybrid cryptographic models, and the active engagement of cybersecurity authorities and standards organizations. However, despite its strategic importance and comprehensive guidance, the Recommendation remains at an early, non-binding stage and does not impose mandatory cryptographic standards, thereby contributing to a regulatory context where preparedness levels may vary significantly across Member States and sectors.

2.7 Analysis of cross-sector data protection and cybersecurity regulations

Current regulatory frameworks on data protection and cybersecurity still rely on assumptions rooted in classical cryptography. They are built on the premise that existing encryption techniques are secure against the computational power of traditional, non-quantum systems and they offer limited – if any – guidance on how to mitigate the emerging challenges posed by quantum computing. A clear example is the **Regulation (EU) 2016/679** (hereinafter, "**GDPR**") which remains the key legal reference for personal data protection in Europe. Its strong emphasis on data integrity and security has the potential to foster the adoption of more robust and future-proof technologies, including those resilient to quantum threats. It becomes crucial to question whether the GDPR, in its current form, provides a truly dynamic framework—one that can adapt to and addressing future threats arising from technological innovations such as quantum computing. One possible answer lies in the principle of **privacy-by-design**, enshrined in Article 25 of the Regulation, which requires data controllers to implement appropriate technical and organizational measures—such as pseudonymization—to effectively apply data protection principles and incorporate the necessary safeguards into the processing. This principle establishes that systems intended for the processing of personal data must be designed from the outset to ensure privacy protection, promoting a proactive and preventive approach to identifying data protection needs. However, the current implementation of the privacy by design principle tends to favour a vertical dimension—focused on the internal architecture of individual systems—rather than a horizontal one, which would entail a cross-cutting and systemic view of threats. Such an approach would be better suited to anticipating and addressing emerging risks, including those posed by quantum computing.

Article 32 of the GDPR is also particularly relevant in this context, as it requires both data controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These measures must take into account the state of the art and the costs of

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

implementation. Among the measures listed are the pseudonymization and encryption of personal data. Data controllers and processors are expected to assess the specific risks associated with their processing activities and to implement appropriate safeguards—such as encryption—to mitigate those risks and prevent violations of the Regulation. If not properly and promptly addressed, such violations could result in significant harm, including, for example, the unauthorized decryption of pseudonymized data.

Alongside the GDPR, **Regulation (EU) 2023/2854** (also known as "**Data Act**")[139] sets out various rules and principles related to technical security measures, particularly concerning data access, use, and sharing. The Data Act explicitly preserves the GDPR and Directive 2002/58/EC as foundational frameworks for sustainable and responsible data processing of both personal and non-personal data, integrating their provisions without prejudice[140]. In line with the principles of minimization and privacy by design and by default, where data processing entails significant risks to fundamental rights, all parties involved in data sharing must implement appropriate technical and organizational safeguards, including **pseudonymization** and **encryption**. Moreover, the Data Act emphasizes the protection of trade secrets. Data holders are required to identify trade secrets prior to disclosure and agree with users or third parties on proportionate technical and organizational measures to maintain confidentiality, such as standard contractual clauses, non-disclosure agreements, strict access protocols, and technical standards[141].

Data holders may also apply technical protections, including **smart contracts** and **encryption**, to prevent unlawful disclosure or unauthorized access, ensuring compliance with the Regulation. Application vendors using smart contracts must ensure these contracts meet essential requirements related to robustness, access control (to prevent errors and tampering), secure termination, data archiving for verifiability, and strict access management. In cases of abusive practices by third parties—such as false information, deceptive methods, exploiting technical gaps, unauthorized use for competitive advantage, illicit disclosure, or failure to maintain agreed-upon safeguards—corrective measures including data deletion, cessation of product or service production, and compensation for damages may be required. The Data Act also mandates maintaining high security throughout the entire data processing service transition, including during data transfer and retention, to ensure continuity of protection[142].

Also, **Regulation (EU) 2022/868** (also known as the **Data Governance Act**[143]), establishes a governance framework aimed at creating a human-centric, trustworthy, and secure European data market. It underscores the importance of ensuring high cybersecurity standards in common European data spaces. The Regulation addresses security measures in various contexts, especially concerning the reuse of protected data held by public bodies, data intermediary services, and data altruism activities. All actors involved in managing non-personal data—including public bodies, authorized reusers, data intermediaries, and recognized data altruism organizations—must adopt all reasonable measures to prevent unauthorized system access, such as **data encryption** and organizational policies[144]. Data intermediaries must ensure adequate security for storing, processing, and transmitting non-personal data and guarantee maximum protection for competition-sensitive information[145]. They must also promptly notify data holders of any unauthorized data transfer, access, or use.

Recognized data altruism organizations are required to ensure adequate security in data storage and processing[146]. Public bodies authorizing data reuse must implement safeguards such as anonymization to prevent the identification of data subjects. **Pseudonymization** is recognized as an appropriate solution for data reuse in secure environments[147]. Reidentification from anonymized data sets is prohibited, and reusers must take **technical and operational measures** to prevent it, as well as notify any breaches involving reidentification[148]. Competent authorities designated in each Member State may provide technical assistance for pseudonymization and ensure data processing protects privacy, confidentiality, integrity, and availability[149]. Data intermediary service providers may also offer anonymization and pseudonymization services as additional tools to facilitate data exchange[150].

Lastly, if we look at security measures established by the **Regulation (EU) 2024/1689**, commonly referred to as the "**AI Act**" [151] , AI systems must be developed and used in a manner that ensures robustness in the face of failures and resilience against attempts to manipulate their use or performance for unlawful

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

purposes[152]. Article 15 mandates that high-risk AI systems be designed and developed to achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they function consistently throughout their lifecycle. High-risk AI systems must **support automatic logging** and maintain a post-market monitoring system to promptly detect and respond to emerging risks[153]. The AI Act explicitly acknowledges AI-specific attack vectors, including data poisoning, adversarial attacks, model poisoning, membership inference, and model evasion. Providers of general-purpose AI models with systemic risk must implement robust protection for the model and its physical infrastructure, guarding against accidental leaks, unauthorized releases, and model theft[154].

Recital 81 introduces a presumption of compliance with the AI Act's cybersecurity requirements if the system also meets the cybersecurity standards of the Cyber Resilience Act—provided it considers AI-specific vulnerabilities[155]. The regulation reinforces that privacy and personal data protection must be maintained throughout the AI system's lifecycle. It applies principles such as **data minimization, privacy-by-design, and privacy-by-default**. **Encryption and anonymization** are among the measures encouraged[156]. AI providers generating synthetic content must ensure outputs are clearly marked as artificially created or modified, using machine-readable and reliable techniques such as watermarking, metadata tagging, cryptographic methods, or digital fingerprints[157]. Compliance requirements rely heavily on the concept of "**state of the art**," allowing adaptation to technological progress through harmonized standards and delegated acts[158].

It is essential to note that the GDPR, the Data Act, the Data Governance Act, and the AI Act establish broad security obligations, but do not specifically address the advent of quantum computing within their core text. Consequently, any regulatory response to quantum threats would likely come in the form of secondary legislation (for example, by implementing acts or delegated regulations) rather than fundamental legislative amendments.

The EU's cybersecurity strategy encompasses the Cybersecurity Act and the NIS2 Directive, both of which establish robust standards for protecting digital infrastructure. These frameworks are gradually building quantum readiness. Nevertheless, harmonizing implementation across Member States remains a persistent challenge.

Directive (EU) 2022/2555 (also known as **NIS2 Directive**[159]) features comprehensive provisions aimed at ensuring a high level of cybersecurity throughout the Union. It mandates that entities adapt to emerging technologies and evolving threats, implicitly including the future challenges posed by quantum computing. The Directive encourages the use of innovative technologies—such as artificial intelligence—for detecting and preventing cyberattacks, while stressing compliance with EU data protection laws and the adoption of the **state-of-the-art encryption**[160]. The Directive underlines multi-risk management approaches that cover data security, availability, authenticity, integrity, and confidentiality[161]. Recital 98, which promotes encryption—particularly end-to-end encryption—and recommends making it mandatory for public electronic communications providers, aligned with "**security-by-design and by-default**". It requires integrating encryption and cybersecurity certification requirements into public procurement and promoting advanced technologies to manage cybersecurity risks[162]. Article 21 mandates that essential and important entities adopt up-to-date, proportionate technical, organizational, and operational measures, including explicit encryption policies, and continually update defences based on evolving threats. The Directive empowers Member States to require certified products or services and allows the Commission to update certification rules[163].

Regulation (EU) 2019/881 (also known as the **Cybersecurity Act**)[164] similarly seeks a common level of cybersecurity and resilience across the EU. Recognizing ICT systems as economic and societal cornerstones, it encourages:

- Security-by-design and security-by-default, requiring manufacturers to embed protective measures from the early stages of development and throughout the entire lifecycle of the ICT products and services, with the most secure settings pre-configured for the initial user[165].

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

- A certification framework protecting data confidentiality, integrity, and availability throughout the product lifecycle, including cybersecurity vulnerability management. Specific security objectives include protecting data from accidental or unauthorized access or disclosure, from accidental or unauthorized destruction, loss, or alteration, or lack of availability, and ensuring that only authorized individuals, programs, or machines can access data, services, or functions[166].
- NISA's role in issuing guidance on encryption and anonymization, based on the analysis of current and emerging risks. The Cybersecurity Act states that ENISA should promote basic advice on "encryption" and "anonymization" (which may include pseudonymization) among citizens, organizations, and businesses. This indirectly links the regulation to Regulation (EU) 2016/679 (GDPR), which is cited in Recital 15 as another legal instrument contributing to a high level of cybersecurity.
- Assurance levels established by the certification framework: basic, substantial and high. These levels must correspond to the degree of risk associated with the intended use of the ICT product, service, or process. The "high" assurance level requires effectiveness testing (including a penetration test) to verify the robustness of security functionalities against sophisticated cyberattacks carried out by attackers with significant skills and resources[167].

Also, **Regulation (EU) 2024/2847** (also known as the **Cyber Resilience Act**[168]) sets a horizontal regulatory framework for essential cybersecurity requirements for all products with digital elements placed on the EU market starting from 11.12.2027, explicitly designed to adapt to emerging threats. The regulation aims to ensure that hardware and software products enter the market with fewer vulnerabilities, and that manufacturers seriously incorporate security considerations throughout the product lifecycle. This "**secure-by-design**" approach is fundamental, as it implies that future design must also account for emerging threats[169]. Key provisions mandate essential cybersecurity requirements for the design, development, and manufacture of products with digital elements, obliging manufacturers to embed security measures from the outset, including awareness of potential future threats. Digital products meet the essential cybersecurity requirements detailed in Annex I, Part I, provided they are correctly installed, maintained, used, and updated with necessary security patches – mandating ongoing post-sale security vigilance[170].

Pursuant to Annex I Part I, digital products must be designed, developed, and manufactured to ensure a level of cybersecurity appropriate to the risks involved; products must protect the confidentiality of personal or other data at rest and in transit using state-of-the-art encryption and other technical measures; they must protect the integrity of data, commands, software, and configurations from unauthorized manipulation and must detect and signal corruption. The Regulation requires manufacturers to effectively manage vulnerabilities in their products and components, in line with essential cybersecurity requirements in Annex I, Part II, for at least five years or the product's expected useful life. Product vulnerabilities have to be promptly addressed and remediated via security updates. Manufacturers have to identify and document vulnerabilities and product components, including a machine-readable Software Bill of Materials[171].

Overall, the EU cybersecurity framework outlines general security requirements but does not directly address the implications of quantum computing within its main legal text. Therefore, any adaptation to emerging quantum threats would most likely be addressed through supplementary legal instruments (for example, delegated acts or implementing measures) rather than through a major revision of the primary legislation.

2.8 A roadmap for quantum computing regulation

This Policy Brief has provided an overview of the current situation in six key industry sectors (finance, healthcare, energy, e-government, transport, and telecommunications) and in relation to the main EU cross-sectoral regulations. This was achieved by analyzing the vulnerabilities and inherent gaps in the European Union's current regulatory framework. The main findings reveal a scenario that does not focus specifically on quantum computing, with a few exceptions. This is critical in terms of the readiness

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

of existing regulations and the provision of specific guidance to operators in various EU industry sectors. Nevertheless, the existing regulatory framework is flexible enough to permit the development of quantum-oriented solutions. The most common scenario involves principles-based legal frameworks. These can be combined with more detailed technical provisions that contextualize these principles to address the issues relating to quantum computing specifically. This applies to both sector-specific and cross-sectoral regulations, such as the GDPR and the AI Act. In light of this overall trend, the detailed, sector-specific analysis presented in this report provides the EU legislator with a roadmap for intervention when revising existing regulations. However, given the similarities that emerged in the findings, this roadmap should be developed in parallel for all the examined sectors, prioritising the telecommunications sector, where the regulatory risk is comparatively higher. This regulatory risk analysis, which focuses on the obligations set out in EU law, therefore reveals the need to address the gap in the existing framework, which largely ignores quantum technologies due to their recent development, by adopting complementary provisions. When implementing a roadmap to address this gap, it is important to define the most appropriate instruments to align the examined scenario with the emerging issues related to the transition to quantum computing technologies. In this regard, the most suitable solution is to build on the EU's co-regulatory approach, which is frequently employed in technology regulation. This would enable the principles-based provisions in existing EU laws to be complemented with specific guidelines or other technical input for operators. This will address the emerging issues relating to quantum computing while providing flexibility in this innovative and evolving sector. To achieve this regulatory objective, it is crucial to conduct a sectoral analysis to identify existing best practices and design specific policies that will bridge the gaps in the current legislation. This will be the focus of the next policy brief in 2026.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Notes

[1] See, e.g., NIS Cooperation Group, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography Part 1, Version: 1.1, EU PQC Workstream,2025, available online at: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography. This document is based on the Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography published by the European Commission on 11 April 2024. The report highlights two principal threat scenarios posed by the quantum transition that require immediate policy attention: (i) the 'store now, decrypt later', in which malicious actors intercept and store encrypted data with the intention of decrypting it once cryptographically relevant quantum computers become operational; and (ii) long transition periods relating to certain systems, such as public key infrastructures (PKIs) and embedded devices with long life cycles, that may require an extended timeline to achieve full transition.

[2] This phase is characterized by the risk that quantum-resistant solutions may not be consistently implemented across sectors or stakeholders, leaving certain entities and infrastructures exposed and vulnerable. See also QUBIP; 2024. "Policy Brief No. 1. Regulating Quantum Computing. Deliverable number: D4.7".

[3] ENISA, Threat Landscape: Finance Sector. February 21, 2025. Available online at https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector.

[4] Ibid.

[5] 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 (NIS 2 Directive), available online at https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng.

[6] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), available online at https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

[7] Jančiūtė, L. Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework. Int. Cybersecur. Law Rev. (2025). https://doi.org/10.1365/s43439-025-00135-7.

[8] Paragraph 1 of this Article stipulates that "financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures". Paragraph 2 prescribes that "Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity, and confidentiality of data, whether at rest, in use, or in transit."

[9] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework, available online at https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj/eng.

[10] According to Article 6(3), such policy should include "criteria for the selection of cryptographic techniques and use practices, taking into account leading practices" and international, European or national standards. Furthermore, according to Article 6(4), such policy should include "provisions for updating or changing, where necessary, the cryptographic technology on the basis of developments in cryptanalysis. Those updates or changes shall ensure that the cryptographic technology remains resilient against cyber threats". Financial entities that are not able to adhere to the above requirements "shall adopt mitigation and monitoring measures that ensure resilience against cyber threats".

[11] Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. There does not seem to be a need to guarantee the same level of protection to payment transactions initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders, or telephone orders. A solid growth of internet payments and mobile payments should be accompanied by a generalised enhancement of security measures. Payment services offered via internet or via other at-distance channels, the functioning of which does not depend on where the device used to initiate the payment transaction or the payment instrument used are physically located, should therefore include the authentication of transactions through dynamic codes, in order to make the user aware, at all times, of the amount and the payee of the transaction that the user is authorising.

[12] Article 97 Authentication 1. Member States shall ensure that a payment service provider applies strong customer authentication where the payer: (a) accesses its payment account online; (b) initiates an electronic payment transaction; (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. 2. With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

link the transaction to a specific amount and a specific payee. 3. With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials. 4. Paragraphs 2 and 3 shall also apply where payments are initiated through a payment initiation service provider. Paragraphs 1 and 3 shall also apply when the information is requested through an account information service provider. 5. Member States shall ensure that the account servicing payment service provider allows the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with paragraphs 1 and 3 and, where the payment initiation service provider is involved, in accordance with paragraphs 1, 2 and 3.

[13]Article 98: Article 98 Regulatory technical standards on authentication and communication 1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying: (a) the requirements of the strong customer authentication referred to in Article 97(1) and (2); (b) the exemptions from the application of Article 97(1), (2) and (3), based on the criteria established in paragraph 3 of this Article; (c) the requirements with which security measures have to comply, in accordance with Article 97(3) in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials; and (d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers. 2. The draft regulatory technical standards referred to in paragraph 1 shall be developed by EBA in order to: (a) ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements; EN 23.12.2015 Official Journal of the European Union L 337/107 (b) ensure the safety of payment service users' funds and personal data; (c) secure and maintain fair competition among all payment service providers; (d) ensure technology and business-model neutrality; (e) allow for the development of user-friendly, accessible and innovative means of payment. 3. The exemptions referred to in point (b) of paragraph 1 shall be based on the following criteria: (a) the level of risk involved in the service provided; (b) the amount, the recurrence of the transaction, or both; (c) the payment channel used for the execution of the transaction. 4. EBA shall submit the draft regulatory technical standards referred to in paragraph 1 to the Commission by 13 January 2017. Power is delegated to the Commission to adopt those regulatory technical standards in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010. 5. In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments.

[14]European Commission, Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, 2018, available online at https://eur-lex.europa.eu/eli/reg_del/2018/389/oj/eng.

[15]Article 2 of the Regulation (EU) 2018/389.

[16]See Chapter IV (UE) 2018/389 in this regard.

[17]Article 4 of the Regulation (EU) 2018/389.

[18]Article 6-7-8 of the Regulation (EU) 2018/389.

[19]Article 9 of the Regulation (EU) 2018/389.

[20]Article 30 of the Regulation (EU) 2018/389.

[21]Article 10 of the Regulation (EU) 2018/389.

[22]Article 35 of the Regulation (EU) 2018/389.

[23]European Banking Authority, EBA publishes final Report on the amendment of its technical standards on the exemption to strong customer authentication for account access, 2022, available online at https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-final-report-amendment-its-technical-standards; European Commission, Commission Delegated Regulation (EU) 2022/2360 of 3 August 2022 amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 as regards the 90-day exemption for account access, 2022, available online at https://eur-lex.europa.eu/eli/reg_del/2022/2360/oj/eng.

[24]Article 10-bis of the Regulation (EU) 2022/2360.

[25]Article 10 of the Regulation (EU) 2022/2360.

[26]Article 95 (3) By 13 July 2017, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant. EBA shall, in close cooperation with the ECB, review the guidelines referred to in the first subparagraph on a regular basis and in any event at least every 2 years.

[27]https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measure

[28]Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets,

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114

[29]ENISA, Health Threat Landscape, July 5, 2023 https://www.enisa.europa.eu/publications/health-threat-landscape

[30]ENISA NIS Investments 2022. https://www.enisa.europa.eu/publications/nis-investments-2022

[31]ENISA Foresight Cybersecurity Threats for 2030, March 2023, https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030.

[32]Several examples are highlighted in the report, including the data tampering in infusion pumps (such as insulin pumps) components due to wireless communication flaws, and the targeting of servers managing autonomous hospital robots, which could result in DDoS conditions and data exposure.

[33]European Parliament and Council of the European Union, Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, available online at https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng.

[34]European Parliament and Council of the European Union, Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU, available online at https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng.

[35]European Parliament and Council of the European Union, 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, 2025, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202500327.

[36]Annex II, point 5 MDR and IVDR.

[37]Annex II, point 4 MDR and IVDR.

[38]Recital 29 EHDS.

[39]Recital 77 EHDS.

[40]"In particular, the secure processing environment shall comply with the following security measures: (a) the restriction of access to the secure processing environment to authorised natural persons listed in the data permit issued pursuant to Article 68; (b) the minimisation of the risk of the unauthorised reading, copying, modification or removal of electronic health data hosted in the secure processing environment through state-of-the-art technical and organisational measures; (c) the limitation of the input of electronic health data and the inspection, modification or deletion of electronic health data hosted in the secure processing environment to a limited number of authorised identifiable individuals; (d) ensuring that health data users have access only to the electronic health data covered by their data permit, by means of individual and unique user identities and confidential access modes only; (e) the keeping of identifiable logs of access to and activities in the secure processing environment for the period necessary to verify and audit all processing operations in that environment; logs of access shall be kept for at least one year; (f) ensuring compliance and monitoring the security measures referred to in this paragraph to mitigate potential security threats".

[41]Recital 46, Article 36 (1-6) EHDS.

[42]Annex II (1) EHDS.

[43]Annex II (3) EHDS: "3.2. The European logging software component of an EHR system designed to enable access by healthcare providers or other individuals to personal electronic health data shall provide sufficient logging mechanisms that record at least the following information on every access event or group of events: (a) identification of the healthcare provider or other individuals having accessed the personal electronic health data; (b) identification of the specific natural person or persons having accessed the personal electronic health data; (c) the categories of data accessed; (d) the time and date of access; (e) the origin or origins of data."

[44]Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast) (Text with EEA relevance.), available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0943.

[45]"2. The Commission is empowered to adopt delegated acts in accordance with Article 68 supplementing this Regulation with regard to the establishment of network codes in the following areas: ... (e) sector-specific rules for cyber security aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management".

[46]COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Digitalising the energy system - EU action plan COM/2022/552 final, p. 13, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0552&qid=1666369684560.

[47]Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401366.

[48]Recital 4 EU network code on cybersecurity for the electricity sector.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

[49]Recitals 18-19 EU network code on cybersecurity for the electricity sector.

[50]Article 12 e 17 EU network code on cybersecurity for the electricity sector.

[51]Article 23 EU network code on cybersecurity for the electricity sector.

[52]Article 26 EU network code on cybersecurity for the electricity sector.

[53]Article 28 EU network code on cybersecurity for the electricity sector.

[54]Article 19 and 21 EU network code on cybersecurity for the electricity sector.

[55]Article 29 EU network code on cybersecurity for the electricity sector.

[56]Article 46 EU network code on cybersecurity for the electricity sector.

[57]Article 48 EU network code on cybersecurity for the electricity sector.

[58]Regulation (EU) 2024/1789 of the European Parliament and of the Council of 13 June 2024 on the internal markets for renewable gas, natural gas and hydrogen, amending Regulations (EU) No 1227/2011, (EU) 2017/1938, (EU) 2019/942 and (EU) 2022/869 and Decision (EU) 2017/684 and repealing Regulation (EC) No 715/2009 (recast) (Text with EEA relevance), available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401789.

[59]Article 71(f) Regolamento (UE) 2024/1789.

[60]Article 72(i) Regolamento (UE) 2024/1789.

[61]Commission Regulation (EU) 2015/703 of 30 April 2015 establishing a network code on interoperability and data exchange rules (Text with EEA relevance), available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1430734293842&uri=OJ:JOL_2015_113_R_0003.

[62]Commission Regulation (EU) No 312/2014 of 26 March 2014 establishing a Network Code on Gas Balancing of Transmission Networks Text with EEA relevance, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.091.01.0015.01.ENG.

[63]Commission Regulation (EU) 2017/459 of 16 March 2017 establishing a network code on capacity allocation mechanisms in gas transmission systems and repealing Regulation (EU) No 984/2013 (Text with EEA relevance), available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1503060564207&uri=CELEX:32017R0459.

[64]Commission Regulation (EU) 2017/460 of 16 March 2017 establishing a network code on harmonised transmission tariff structures for gas (Text with EEA relevance.), available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0460.

[65]European Commission, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 28 August 2014, available online at https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng.

[66]European Parliament and the Council of the European Union, Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, 2024, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183&qid=1716986198888.

[67]G.Comandé and M.M.Varilek,"The Many Features Which Make the eIDAS 2 Digital Wallet Either Risky or the Ideal Vehicle for the Transition to Post-Quantum Encryption", available at https://doi.org/10.2139/ssrn.4848669.

[68]Recital 6-7-11 of the eIDAS.

[69]Recital 16-26-27 of the eIDAS.

[70]Article 8 par. 3 of the eIDAS: "3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1. Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements: (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means; (b) the procedure for the issuance of the requested electronic identification means; (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party; (d) the entity issuing the electronic identification means; (e) any other body involved in the application for the issuance of the electronic identification means; and (f) the technical and security specifications of the issued electronic identification means. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2)."

[71]To establish these specifications and procedures, consideration was given, among other things, to the international standard ISO/IEC 29115 and the large-scale pilot project STORK. However, the content of the eIDAS Regulation differs from ISO/IEC 29115, particularly regarding the requirements for identity control and verification. Therefore, the Annex to the Implementing Regulation is based on this international standard but does not reference specific content from ISO/IEC 29115.

[72]To comply with the substantial and high levels of assurance, the electronic identification means must respectively use at least two authentication factors from different categories and be designed in such a way that exclusive use by the holder or use

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

under the holder's control can be assumed. In addition to these elements, the identification means must be protected against duplication, tampering, and attackers with high attack potential. It must also be reliably protected by the holder to prevent use by others.

[73]The authentication mechanism verifies the electronic identification means by implementing security controls that make it highly unlikely for the mechanism to be compromised by activities such as guessing attacks, interception, replay attacks, or the manipulation of communication by an attacker with an enhanced-basic, moderate, or high attack potential.

[74]With regard to information security management, in order to achieve a substantial or high level of assurance, an effective information security management system is required, which adheres to established standards or proven principles for risk management or control. Appropriate technical controls are also foreseen for managing security risks to the services, in order to protect the confidentiality, integrity, and availability of the information processed. For compliance with a low level of assurance, 'access to sensitive cryptographic material used for issuing electronic identification means is restricted to roles and applications for which it is strictly required. It is ensured that such material is never stored in plain text permanently. Procedures are in place to ensure ongoing security and the ability to respond to changes in risk levels, incidents, and security breaches over time. All media containing personal, cryptographic, or other sensitive information are stored, transported, and disposed of securely and safely.' To meet the substantial level of assurance, in addition to the elements mentioned above, the sensitive cryptographic material used for issuing electronic identification means and for providing authentication must be protected against tampering.

[75]Recital 31 of the EUDI Regulation.

[76]Recital 11 of the EUDI Regulation.

[77]Recital 32 and Article 5-bis (14) of the EUDI Regulation.

[78]Article 5-bis (4) (d) of the EUDI Regulation.

[79]Recital 22 and Article 5-ter of the EUDI Regulation.

[80]Article 5-quater of the EUDI Regulation.

[81]European Parliament and Council of European Union, Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91, 22 August 2018, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1139.

[82]Article 1(f) Regulation (EU) 2018/1139.

[83]Article 4 Regulation (EU) 2018/1139.

[84]Articles 9-19 Regulation (EU) 2018/1139.

[85][. . .] "1. PRODUCT INTEGRITY Product integrity, including protection against information security threats, must be assured for all anticipated flight conditions for the operational life of the aircraft. Compliance with all requirements must be shown by assessment or analysis, supported, where necessary, by tests."

[86][. . .] "1.3.5. Design precautions must be taken to minimise the hazards to the aircraft and occupants from reasonably probable threats, including information security threats, both inside and external to the aircraft, including protecting against the possibility of a significant failure in, or disruption of, any non-installed equipment".

[87]Articles 29-32 Regulation (EU) 2018/1139.

[88]"5.3. All data necessary for the execution of the flight by the crew must be updated and available on board the aircraft taking account of applicable air traffic regulations, rules of the air, flight altitudes and areas of operation."

[89]Annex V point 1.5. Regulation (EU) 2018/1139. '

[90]'8.4. The aircraft operator must develop and maintain security programmes adapted to the aircraft and the type of operation including particularly: (a) security of the flight crew compartment; (b) aircraft search procedure checklist; (c) training programmes; and (d) protection of electronic and computer systems to prevent intentional and non-intentional system interference and corruption."

[91]Articles 33-39 Regulation (EU) 2018/1139; Article 3 (19) Regulation 2018/1139: "(19) 'Apron Management Service (AMS)' means a service provided to regulate the activities and the movement of aircraft and vehicles on an apron;"

[92]Article 3 (5) Regulation (EU) 2018/1139: "(5) 'ATM/ANS' means air traffic management and air navigation services and covers all of the following: the air traffic management functions and services as defined in point (10) of Article 2 of Regulation (EC) No 549/2004; the air navigation services as defined in point (4) of Article 2 of that Regulation, including the network management functions and services referred to in Article 6 of Regulation (EC) No 551/2004, as well as services which augment signals emitted by satellites of core constellations of GNSS for the purpose of air navigation; flight procedures design; and services consisting in the origination and processing of data and the formatting and delivering of data to general air traffic for the purpose of air navigation;"

[93]Annex VII point 1.4.3. Regulation (EU) 2018/1139.

[94]Annex VIII point 2.1.2. Regulation (EU) 2018/1139.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

[95]Annex VIII point 3.1. Regulation (EU) 2018/1139.

[96]Annex VIII point 3.3. Regulation (EU) 2018/1139.

[97]1.4. The organisation responsible for the production or for the marketing of the unmanned aircraft must provide information to the operator of an unmanned aircraft and, where relevant, to the maintenance organisation on the kind of operations for which the unmanned aircraft is designed together with the limitations and information necessary for its safe operation, including operational and environmental performance, airworthiness limitations and emergency procedures. This information shall be given in a clear, consistent and unambiguous manner. The operational capabilities of unmanned aircraft that can be used in operations that do not require a certificate or declaration must allow the possibility to introduce limitations which meet airspace rules applicable to such operations.

[98]Annex IX point 2.1.8. Regulation (EU) 2018/1139.

[99]Annex IX point 2.1.8. Regulation (EU) 2018/1139.

[100]Recital 6 Regulation 2022/1645.

[101]These articles of Regulation (EU) 2018/1139 grant the Commission the power to adopt delegated acts to establish detailed rules on airworthiness (including the approval of design and production organisations) as well as on airport management and the provision of ground handling and apron management services (AMS).

[102]Annex INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR 200] of Delegated Regulation 2022/1645.

[103]Annex INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR 205] of Delegated Regulation 2022/1645.

[104]Annex INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR 210] of Delegated Regulation 2022/1645.

[105]Annex INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR 215] of Delegated Regulation 2022/1645.

[106]Annex INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR 220] of Delegated Regulation 2022/1645.

[107]Annex INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR 225] of Delegated Regulation 2022/1645.

[108]Annex INFORMATION SECURITY — REQUIREMENTS FOR THE ORGANISATION [PART-IS.D.OR 230] of Delegated Regulation 2022/1645.

[109]European Parliament and the Council of European Union, Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, 2004, available online at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32004R0725.

[110]Chapter XI-2 of the SOLAS Convention, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02004R0725-20090420.

[111]Annex II, Part A and Annex III, Part B, par. 16.8.6 Regulation (CE) 725/2004.

[112]Annex II, Part A, par. 9.6 Regulation (CE) 725/2004.

[113]Annex III, Part A, par. 10.3 Regulation (CE) 725/2004.

[114]Annex III, Part A, par. 10.3 Regulation (CE) 725/2004.

[115]European Parliament and Council of Europe, Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security, 2005, available online at https://eur-lex.europa.eu/eli/dir/2005/65/oj/eng.

[116]Article 16 Directive 2005/65/CE.

[117]Annex II of the Directive 2005/65/CE.

[118]European Parliament and the Council of the European Union, Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU, 2019, available online at https://eur-lex.europa.eu/eli/reg/2019/1239/oj/eng. The Regulation will apply from 15 August 2025.

[119]Recitals 4,7 and Article 6 of the Regulation (EU) 2019/1239.

[120]Recital 5 of the Regulation (EU) 2019/1239.

[121]Recital 11 and Article 6 par. 4 and 5 of the Regulation (EU) 2019/1239.

[122]In this regard, see also Article 22 of Regulation (EU) 2019/1239, which states the following: “By 15 August 2027, the Commission shall review the application of this Regulation and submit an evaluation report, which shall include, where necessary, an assessment of emerging technologies that may lead to amendments or the replacement of the harmonised reporting interface module”.

[123]European Commission, Commission Implementing Regulation (EU) 2023/204 of 28 October 2022 laying down technical specifications, standards and procedures for the European Maritime Single Window environment pursuant to Regulation (EU)

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2019/1239 of the European Parliament and of the Council, 2022, available online at https://eur-lex.europa.eu/eli/reg_impl/2023/204/oj/eng. The Implementing Regulation will take effect on 15 August 2025.

[124]See Annex V of Implementing Regulation (EU) 2023/204 and Article 14 of the Regulation (EU) 2019/1239.

[125]See Annex VI of the Implementing Regulation (EU) 2023/204 and Article 15 of the Regulation (EU) 2019/1239.

[126]See Annex VII of the Implementing Regulation (EU) 2023/204 and Article 16 of the Regulation (EU) 2019/1239.

[127]See Annexes V, VI, and VII of the Implementing Regulation (EU) 2023/204.

[128]See Article 12 of the Regulation (EU) 2019/1239.

[129]European Commission, Commission Implementing Regulation (EU) 2023/2790 of 14 December 2023 laying down functional and technical specifications for the reporting interface module of the Maritime National Single Windows, 2023, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2790. The Implementing Regulation will take effect on 15 August 2025.

[130]Article 1 of the Implementing Regulation (EU) 2023/2790.

[131]See Recital 30 of the Regulation (EU) 2019/1239.

[132]Recital 24 and Article 10 of the Regulation (EU) 2019/1239.

[133]BEREC guidelines for Open Internet Regulation (EU 2015/2120).

[134]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AL_202401101

[135]The sub-group may invite representatives of relevant stakeholders to participate in its work, such as those of advisory bodies of public organisations, industry, service providers, and operators.

[136]https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

[137]https://www.european-quantum-act.com/

[138]https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

[139]European Parliament and the Council of European Union, Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 2023, available online at https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng.

[140]Article 1 par. 6 of the Data Act

[141]Articles 4(6) and 5(9) of the Data Act.

[142]Article 25(2)(iv) of the Data Act.

[143]European Parliament and the Council of European Union, Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), 2022, available online at https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng.

[144]Recital 23) of the Data Governance Act.

[145]Article 12(1) (l) of the Data Governance Act.

[146]Article 21 of the Data Governance Act.

[147]Recital 30 of the Data Governance Act.

[148]Article 5 (5) of the Data Governance Act.

[149]Article 7(4) (c) of the Data Governance Act.

[150]Article 12 (e) of the Data Governance Act.

[151]European Commission and the Council of the European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024, available online at https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

[152]Recital 24 of the AI Act.

[153]Recitals 75, 128, 146, and Articles 12 and 72 of the AI Act.

[154]Article 15 (1) of the AI Act.

[155]Recital 81 of the AI Act.

[156]Recitals 69 and 73 of the AI Act.

[157]Recital 129 and Article 50 (2) of the AI Act.

[158]Recitals 66, 78 and Articles 8, 15, 40 and 41 of the AI Act.

[159]European Parliament and the Council of European Union, 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).

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

[160]Recitals 51 and 89 of the NIS2 Directive.

[161]Recitals 78 and 79 of the NIS2 Directive.

[162]Article 7 of the NIS2 Directive.

[163]Article 24 of the NIS2 Directive.

[164]European Parliament and the Council of the European Union, 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, available online at https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

[165]Recitals 12 and 13 of the Cybersecurity Act.

[166]Recital 96 of the Cybersecurity Act.

[167]Article 52 of the Cybersecurity Act.

[168]European Parliament and the Council of the European Union, 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), available online at https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

[169]Recital 32 of the Cyber Resilience Act.

[170]Articles 1 (b) and 6(a) of the Cyber Resilience Act.

[171]Annex I Part. I and II Cyber Resilience Act.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

3 Bibliography

ENISA, Threat Landscape: Finance Sector. February 21, 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector

ENISA, Health Threat Landscape, July 5, 2023. https://www.enisa.europa.eu/publications/health-threat-landscape

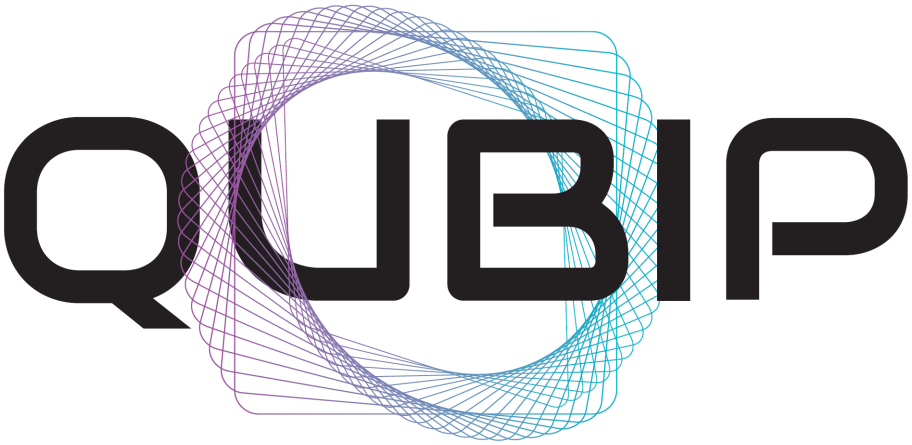
ENISA NIS Investments 2022. https://www.enisa.europa.eu/publications/nis-investments-2022

ENISA Foresight Cybersecurity Threats for 2030, March 2023. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030. Several examples are highlighted in this report, including the data tampering in infusion pumps (such as insulin pumps) components due to wireless communication flaws, and the targeting of servers managing autonomous hospital robots, which could result in DDoS conditions and data exposure.

G. Comandé and M. M. Varilek, "The Many Features Which Make the eIDAS 2 Digital Wallet Either Risky or the Ideal Vehicle for the Transition to Post-Quantum Encryption," May 2024, https://doi.org/10.2139/ssrn.4848669

L. Jančiūtė, "Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework," Int. Cybersecur. Law Rev. (2025). https://doi.org/10.1365/s43439-025-00135-7

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].



Quantum-oriented Update to Browsers and Infrastructures for the PQ transition (QUBIP)

https://www.qubip.eu

D4.8 – Policy Brief No. 2 Regulating Quantum Computing

Version 1.0

Horizon Europe