Leiden University

ICT in Business and the Public Sector

Leveraging Financial Sector Cyber Maturity to Strengthen Critical Infrastructure Resilience under EU Cyber Regulations

Name:	Onno van Limburg Stirum
Student ID:	s3750043
Date:	03/31/2026
1st supervisor:	Prof.dr.ir. J.M.W. Visser
2nd supervisor:	Dr. O. Gadyatskaya

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Einsteinweg 55
2333 CC Leiden
The Netherlands

Abstract

Background: As a prime target for cyberattacks, the financial sector has developed resilient cybersecurity practices, guided by regulations such as the Digital Operational Resilience Act (DORA). Meanwhile, other sectors of critical infrastructure face emerging cybersecurity challenges as they prepare for the implementation of the Network and Information Systems Directive (NIS2). NIS2 aims to enhance cybersecurity across these sectors and does so by introducing extensive regulatory requirements that pose significant compliance challenges, especially for sectors with low cybersecurity maturity.

Aim: We investigate the transferability of mature cybersecurity practices from the financial sector, guided by DORA, to improve cybersecurity practices, maturity, and compliance within critical infrastructure sectors under the upcoming NIS2 directive.

Method: The study involves a review of existing literature, regulatory frameworks, and industry reports to identify key regulatory requirements and perceived cybersecurity maturity differences across critical infrastructure sectors. Interviews with industry experts provide insights into best practices and challenges in both the financial sector and broader critical infrastructure. In addition to the interviews, we made a structured comparative analysis on ten key dimensions between DORA and NIS2, which was validated by experts. Based on this, we identify concrete areas where DORA-inspired practices can be adapted to support NIS2 implementation and we offer guidance to improve cybersecurity maturity and regulatory alignment across critical infrastructure sectors.

Results: Insights from nine expert interviews, combined with the structured comparison, show that there is a high degree of overlap between NIS2 and DORA. However, DORA provides significantly more prescriptive and operationalized requirements. The findings indicate that practices from DORA cannot be directly transferred to NIS2-regulated sectors due to differences in cybersecurity maturity, sector-specific constraints, and the more flexible nature of NIS2. Instead, successful transfer requires adaptation into sector-appropriate guidance, supported by practical implementation approaches and increased cross-sector knowledge sharing.

Conclusion: By bridging the regulatory and strategic implementation gaps, this study offers valuable insights into improving cybersecurity resilience across critical infrastructure sectors, as well as potentially easing the transition to NIS2 compliance.

Conclusion: This study finds that cybersecurity practices developed under DORA can be leveraged to support NIS2 implementation, but these practices cannot be directly transferred due to differences in regulatory structure, sector-specific constraints, and varying levels of cybersecurity maturity. Instead, their value lies in serving as a structured reference for implementation, requiring translation into sector-appropriate and scalable approaches. By identifying where practices align, where they diverge, and how they can be adapted, this study contributes to improving cybersecurity resilience across critical infrastructure sectors and supports a more effective transition towards NIS2 compliance.

Acknowledgements

I would like to express my sincere gratitude to my primary supervisor, Prof. dr. ir. Joost Visser, for his guidance, critical feedback, and support throughout this research. His insights and involvement were instrumental in shaping the direction and quality of this thesis.

I would also like to thank Dr. Olga Gadyatskaya for her valuable feedback and support during the course of this project, which helped to further strengthen this work.

I am also grateful to the industry professionals who supported this research. In particular, I would like to thank Carlien Groenewegen and Valeria van de Logt for their practical insights, supervision, and support during this project. Their experience and feedback provided an important bridge between academic research and real-world application. Additionally, I would like to thank Hamish Wishart for his valuable contributions and expertise related to NIS2, which significantly strengthened the depth and practical relevance of this research.

Finally, I would like to thank everyone who contributed their time and insights through interviews, as well as those who supported me throughout the process of completing this thesis.

Contents

List of Figures

List of Tables

Glossary and Acronyms

AI Artificial Intelligence. 14, 16, 20

CIFI Critically Important Financial Institutions. 39

CISO Chief Information Security Officer. 34, 46

CSF Cybersecurity Framework - typically referring to the NIST Cybersecurity Framework, a voluntary guidance based on existing standards, guidelines, and practices for organizations to manage cybersecurity risk. 19, 20

CSIRT Computer Security Incident Response Team - a group responsible for receiving, analyzing, and responding to cybersecurity incidents within an organization or sector. 12, 13, 18, 20, 30, 39, 58

DORA The Digital Operational Resilience Act (EU) 2022/2554, applicable to financial entities and ICT third-party service providers. 1, 4, 7–11, 14, 17–25, 27, 29–50, 56–60, 62

DPO Data Protection Officer. An organizational role responsible for overseeing data protection strategy, compliance, and implementation to ensure that an organization processes personal data in accordance with applicable laws. 18

EBA European Banking Authority. 20, 45

EIOPA European Insurance and Occupational Pensions Authority. 20

ESA European Supervisory Authority. 20, 30, 31, 41, 46, 56, 58–60

ESMA European Securities and Markets Authority. 20

EU European Union - a political and economic union of 27 member states primarily located in Europe. 7, 8, 10–12, 14, 15, 17, 19–21, 30, 31, 33, 43, 45, 46, 56, 59

EU-CyCLONe European Cyber Crisis Liaison Organisation Network - facilitates coordinated response to large-scale cross-border cybersecurity incidents. 13, 31, 59

GDPR General Data Protection Regulation. 14, 17, 18, 45, 47

IAM Identity and Access Management. A set of policies, processes, and technologies used to manage digital identities and control user access to systems and data. 14

ICT Information and Communications Technology. 8, 10, 11, 13, 14, 19–21, 25–32, 38, 40–42, 48, 49, 56–58, 60

IEC International Electrotechnical Commission - an international standards organization that prepares and publishes standards for electrical, electronic, and related technologies. 11, 19, 21, 35

ISAC Information Sharing and Analysis Center. 36, 46, 47

ISO International Organization for Standardization. 11, 19, 21, 35, 40

IT Information Technology. 14, 20, 34, 35, 39, 43, 46

NIS The original Network and Information Systems Directive (EU) 2016/1148, predecessor to NIS2. 12, 13, 17, 45

NIS2 The Network and Information Systems Directive (EU) 2022/2555, which establishes baseline cybersecurity requirements for critical infrastructure sectors. 1, 4, 7–10, 12, 13, 15–24, 27, 29–50, 56–60, 62

NIST National Institute of Standards and Technology. 19–21, 35

OLIR Online Informative References - a NIST mechanism for mapping cybersecurity frameworks to external standards, guidelines, and practices. 19

OT Operational Technology. 15, 32, 34–36, 39, 43, 46, 47

PCI-DSS Payment Card Industry Data Security Standard. 14

SME Small and Medium-sized Enterprise. 36

TLPT Threat-Led Penetration Testing. 11, 20, 30, 39, 57

TPRM Third-Party Risk Management - the process of identifying, assessing, and managing risks posed by external suppliers, service providers, or ICT partners that support organizational operations. 24, 40, 42

Chapter 1

Introduction

In recent decades, imagining a world without technology interwoven into our daily lives has become increasingly difficult. Technology and digitalization have made us more productive, efficient, and connected, fundamentally transforming how we work, communicate, and manage essential services. Critical infrastructure sectors, from banking and finance to energy and healthcare, now heavily rely on complex information systems and digital technologies to operate smoothly and effectively.

While information technology has significantly improved our lives, it also comes with certain costs. Never before have malicious actors had such a vast attack surface targeting the most important parts of our infrastructure. Should our critical infrastructures suffer from digital attacks, the consequences could be dire. Disruptions to essential services, such as energy grids or telecommunications, would result in severe economic losses and potentially threaten national security. Incidents such as the 2017 NotPetya malware attack on Maersk, which disrupted global shipping and supply chains with an estimated 300 million dollars in damage [47], the 2021 Colonial Pipeline ransomware attack, which halted fuel distribution across the U.S. East Coast and exposed vulnerabilities in energy infrastructure [43], and the 2022 Viasat satellite hack, which disrupted European communications during the onset of the war in Ukraine [12], demonstrate how digital disruptions can cascade across sectors. Such events show that attacks on energy, logistics, or communication systems can rapidly escalate into national or even international crises.

Among the sectors classified as "critical", the financial sector has arguably led the way in developing and implementing robust cybersecurity measures [20]. Due to the high value of its data and the financial transactions it processes, the financial sector has long been a prime target for cyber threats. These efforts have been further reinforced by the Digital Operational Resilience Act (DORA), which mandates cybersecurity requirements to ensure the financial sector's ability to withstand, respond to, and recover from cyber incidents [29].

However, critical infrastructure is not limited to the financial sector. Other sectors, such as energy, healthcare, transportation, water supply, and telecommunications, also face distinct cybersecurity challenges. Each of these sectors plays a crucial role in our daily lives but is often less mature in terms of cybersecurity readiness. In 2024, the European Union implemented the Network and Information Systems Directive 2 (NIS2), which aims to enhance cybersecurity and resilience across critical infrastructure. NIS2 establishes baseline security measures, promotes cross-sector collaboration, and improves incident response capabilities. However, many companies in these sectors have not previously faced such stringent cybersecurity legislation, and with generally low levels of cybersecurity maturity in these industries [13], challenges emerge that many companies are not yet prepared for.

Given the disparities in cybersecurity maturity across critical infrastructure sectors, we aim to investigate the transferability of practices from the financial sector to other sectors. Leveraging the financial sector's experience can provide valuable insights, helping other industries not only comply with EU cyber regulations but also strengthen their overall cybersecurity resilience.

1.1 Problem Statement

The financial sector, regulated under the Digital Operational Resilience Act (DORA), has developed relatively mature cybersecurity practices due to its long-standing exposure to regulatory pressure. These practices include structured approaches to ICT risk management, incident reporting, and oversight of third-party providers. In contrast, many other critical infrastructure sectors are still developing their cybersecurity posture and are only now facing comparable obligations under the Network and Information Systems Directive 2 (NIS2).

NIS2 introduces broad requirements for cybersecurity and resilience across sectors such as energy, healthcare, transport, and water. However, its less prescriptive nature compared to DORA, combined with differing national implementations and generally lower cybersecurity maturity in these sectors, raises challenges in interpretation and execution.

Now more than ever, issues arise that need to be covered to ensure a secure and robust infrastructure:

1. **Rising cyber threats and sector vulnerabilities**
   Critical infrastructure sectors are increasingly targeted by sophisticated cyberattacks, including from state-sponsored actors. Without robust cybersecurity and risk management practices, disruptions can cascade across sectors and borders, impacting economic stability and public safety.
2. **NIS2 demands but doesn't prescribe**
   While NIS2 significantly raises expectations for cybersecurity in critical sectors, its flexible and high-level nature may limit its real-world impact unless organizations adopt structured implementation strategies. Many of these strategies already exist in more mature sectors like finance.
3. **Bridging regulatory and practical gaps**
   Organizations often struggle to interpret and apply regulatory requirements without clear guidance or experience. By examining expert perspectives and regulatory documents, this research provides practical insights into how implementation can be improved by leveraging cross-sector knowledge.

We address the problem of how mature cybersecurity practices shaped by DORA in the financial sector can inform or support improved implementation of NIS2 in other critical infrastructure domains. Rather than developing new frameworks, the study evaluates perceived overlaps, gaps, and transferability of practices between these two regulatory environments.

This research highlights the gap between regulatory mandates and their real-world application, providing insight into how sector-specific characteristics shape compliance strategies. It contributes to the growing body of knowledge on cybersecurity governance by showing how perceived maturity and regulatory structure influence implementation outcomes. Furthermore, by examining how practices from a highly regulated sector might be transferred to others with lower cybersecurity maturity, this thesis adds to the discussion on cross-sector knowledge transfer and regulatory design in the context of EU cybersecurity policy.

1.2 Research Questions

This research investigates how cybersecurity practices developed in the financial sector and under DORA are perceived in terms of their applicability and usefulness for improving cybersecurity maturity in other critical infrastructure sectors affected by NIS2. The study combines a comparative analysis of regulatory texts with expert interviews to explore perceived challenges, gaps, and the transferability of sector-specific practices.

This research answers the main question:

RQ.1 *How can cybersecurity practices developed under DORA in the financial sector be leveraged to improve cybersecurity maturity and regulatory compliance in other critical infrastructure sectors subject to NIS2?*

To answer this, we have formulated the following sub-questions:

RQ.2 *What are the key similarities and differences between DORA and NIS2 across core regulatory dimensions?*

RQ.3 *How do organizations across different sectors interpret and implement these requirements, and what challenges do they encounter in doing so?*

RQ.4 *Which DORA practices are seen as most useful or transferable to less mature sectors under NIS2, and why?*

RQ.5 *How do differences in regulatory structure, sector maturity, and national implementation influence the effectiveness and transferability of cybersecurity practices across sectors?*

1.3 Overview of the thesis

The remainder of this thesis is structured as follows. Chapter 2 provides the background and related work, introducing the Digital Operational Resilience Act (DORA) and the Network and Information Systems Directive 2 (NIS2), and examining differences in cybersecurity maturity between the financial sector and other critical infrastructure sectors. It further reviews academic and policy literature on regulatory implementation, sectoral challenges, and the transferability of cybersecurity practices across domains.

Chapter 3 outlines the research methodology. It describes the qualitative research design, including regulatory document analysis and the development of a structured comparative framework consisting of ten key dimensions. These dimensions are used to systematically map and compare DORA and NIS2, and to guide the design and analysis of semi-structured expert interviews.

Chapter 4 presents the findings of the study. It first provides a structured comparative analysis of DORA and NIS2 across the ten relevant dimensions, followed by the results of the expert interviews, which offer insights into practical implementation challenges, sectoral differences, and opportunities for cross-sector learning.

Chapter 5 interprets these findings in the broader context of EU cybersecurity governance, with particular focus on the transferability of financial-sector practices and their implications for strengthening third-party risk management under NIS2.

Finally, Chapter 6 summarizes the main findings, answers the research questions, reflects on the contributions and limitations of the study, and outlines directions for future research.

Chapter 2

Background and Related Work

This chapter provides background and a review of existing research relevant to the adoption of cybersecurity practices across critical infrastructure sectors in the European Union. As DORA introduces one of the most detailed and prescriptive regulatory regimes in the EU's cybersecurity landscape, scholars and regulators have begun exploring its interplay with broader frameworks like NIS2 [18], including the potential for cross-sector alignment. This chapter explores the content and objectives of both regulatory frameworks, reviews current implementation practices, and discusses academic and industry perspectives on their effectiveness, limitations, and potential for cross-sector application.

The goal is to establish a clear understanding of both the technical and strategic context of these regulations, while identifying gaps in current literature that this research aims to address. In particular, this study focuses on the practical transfer of regulatory practices from the financial sector to other domains of critical infrastructure.

2.1 Digital Operations Resilience Act (DORA)

In this section we focus on the Digital Operational Resilience Act (DORA), the European Union's dedicated regulatory framework for strengthening the cybersecurity and operational resilience of the financial sector. We first outline its background and policy objectives, after which we examine the regulation's five core pillars that establish a baseline for digital resilience across EU financial entities. Finally, we discuss how DORAis being implemented in practice and the challenges financial institutions face in translating legal requirements into operational processes.

2.1.1 Background and Objectives

In 2023, the three European Supervisory Authorities: the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA), began preparing a set of policy products to enable the application of the Digital Operational Resilience Act (DORA) [23, 25]. DORA applies to a broad set of financial entities, including credit institutions, payment institutions, investment firms, credit rating agencies, statutory auditors, crowdfunding service providers, and ICT third-party service providers [26]. These entities are subject to harmonized digital resilience requirements, with full application of the regulation being in effect as of January 2025 [33].

The regulation was introduced in response to growing concerns about systemic risk and the potential for single points of failure in the highly interconnected financial sector [8, 61]. By subjecting all regulated financial entities to a unified framework, DORA aims to raise the overall cybersecurity maturity of the sector and reduce inconsistencies in how institutions manage digital operational risks [9, 27]. It also represents a broader shift in the EU's cybersecurity strategy: from soft coordination mechanisms to enforceable legal obligations [61, 17].

2.1.2 DORA Pillars

The regulation is structured around five key pillars [17], each addressing a core component of digital operational resilience. These pillars and their legal basis are summarized below:

ICT Risk Management (Chapter II, Articles 5–16) Financial entities must establish, implement, and maintain ICT risk management frameworks that cover the full lifecycle of ICT risk, including identification, protection, detection, response, and recovery. These frameworks must be reviewed and updated regularly to stay aligned with the evolving threat landscape.

ICT Incident Classification and Reporting (Chapter III, Articles 17–23) Entities are required to classify and report ICT-related incidents in a timely manner, using standardized formats. Significant incidents must be reported to competent authorities, and post-incident reviews are mandated to improve future resilience.

Digital Operational Resilience Testing (Chapter IV, Articles 24–27) DORA introduces rigorous testing obligations, including regular vulnerability assessments and advanced TLPT for systemically important entities. These tests simulate real-world attack scenarios to expose potential weaknesses.

ICT Third-Party Risk Management (Chapter V, Articles 28–44) Entities must perform due diligence when contracting ICT third-party providers, particularly those supporting critical functions. Contracts must contain specific clauses on security, continuity, and incident reporting, with ongoing oversight throughout the provider relationship.

Information Sharing (Chapter VI, Article 45) DORA encourages financial entities to participate in trusted information-sharing arrangements on cyber threats, vulnerabilities, and incidents. This supports sector-wide situational awareness and proactive threat response.

In addition to these pillars, DORA introduces a Union-level oversight framework for critical ICT third-party providers, enabling European Supervisory Authorities to supervise providers whose services are essential to financial stability. These measures reflect a transition from fragmented national practices to a coherent, EU-wide digital resilience regime for the financial sector.

2.1.3 DORA in Practice

DORA is part of a broader EU regulatory trend toward "resilience through regulation," in which digital stability is no longer treated as just an IT issue but as a central pillar of financial supervision [17]. This aligns with the EU's ongoing effort to embed cybersecurity mandates across critical sectors and ensure systemic robustness in the face of increasingly complex digital threats.

While the financial services industry is widely regarded as the most mature in terms of cybersecurity infrastructure [11], many institutions are still working to fully align with DORA. Since the regulation's adoption, firms have been compelled to overhaul large portions of their ICT risk management systems. With limited lead time and evolving technical guidance, many institutions have relied on existing frameworks such as ISO/IEC 27001 to establish a baseline for compliance.

ISO/IEC 27001, a globally recognized standard for information security management systems, provides a structured foundation for managing sensitive company and customer data, ensuring confidentiality, integrity, and availability. However, DORA goes beyond ISO 27001, demanding more dynamic, resilience-focused capabilities such as real-time incident response, sector-wide information sharing, and regulatory oversight of ICT third-party providers [52]. These differences underscore DORA's ambition to embed cybersecurity into the operational and supervisory core of financial regulation.

Recent industry data further illustrate the scale of this transition. A 2025 survey of European financial institutions [44] found that a majority still face significant challenges in meeting DORA's requirements, particularly in areas such as incident reporting, ICT third-party risk management, and operational resilience testing. While 94% of survey respondents report to have elevated DORA's importance within the company, 96% believe their data does not meet DORAstandards. Limited lead time, evolving technical guidance, and the complexity of aligning DORAwith existing frameworks were cited as key obstacles, highlighting the gap between regulatory intent and practical implementation.

2.2 The Network and Information Systems Directive 2 (NIS2)

This section focuses on the Network and Information Systems Directive 2 (NIS2), the EU directive that sets baseline cybersecurity requirements for a wide range of critical infrastructure sectors. We first outline its background and objectives, then review its key components and obligations for essential entities. Finally, we discuss the expected impact of NIS2on critical sectors and the challenges organizations face in meeting its requirements.

2.2.1 Background and Objectives of NIS2

In 2016, the European Union adopted the first Network and Information Systems Directive (NIS), aimed at improving cybersecurity across Member States by establishing a common framework for network and information systems security [28]. Its structure rested on three pillars: (1) implementation of cybersecurity measures in seven initial sectors, (2) national-level preparedness through the creation of strategies and Computer Security Incident Response Teams (CSIRTs), and (3) establishment of the NIS Cooperation Group to enable cross-border collaboration.

However, the evolving threat landscape and uneven implementation across Member States soon revealed limitations. The EU identified several key shortcomings in the original directive: inconsistent national resilience capabilities, diverging interpretations of what constitutes an "essential service," limited joint crisis response capacity, and an overall lack of shared understanding of cyber threats [32].

To address these issues, the EU adopted the revised Network and Information Systems Directive 2 (NIS2) in 2022 [30]. Its objectives are to enhance cybersecurity resilience across the Union, broaden sectoral coverage, harmonize requirements, and improve coordination and threat intelligence sharing across public and private actors. Additionally, the term "critical infrastructure" was defined more clearly. The term officially refers to sectors, systems, and assets that are essential for the functioning of society and the economy, such that their disruption would have significant negative consequences for security, public safety, or economic stability. Within the EU legal framework, NIS2(Directive (EU) 2022/2555), annexes 1 and 2 [30] designate these as "essential" and "important" entities, covering organizations that provide vital services in sectors such as energy, transport, banking, financial market infrastructures, healthcare, drinking water, digital infrastructure, public administration, and space.

2.2.2 Key Components and Requirements of NIS2

NIS2 builds on the foundation of its predecessor but introduces several notable enhancements, as set out in Directive (EU) 2022/2555 [53]. These include:

Expanded Scope NIS2 extends its coverage to additional sectors such as energy, water, waste management, transportation, banking, public administration, digital infrastructure, and space. The directive also applies to all medium and large enterprises within these sectors, unless exempted due to their non-critical nature. Small and micro-enterprises are generally excluded unless explicitly designated as essential service providers.

Enhanced Security Requirements Covered entities must implement comprehensive cybersecurity risk management measures, including policies for incident prevention, detection, response, and recovery. These measures must also address supply chain risks, vulnerability management, and business continuity planning.

Incident Reporting and Management Organizations are required to report significant incidents that impact service provision to their national CSIRT or competent authority within specified timelines. The directive also mandates post-incident response and recovery planning to minimize disruption and prevent recurrence.

Supply Chain Security Given the increasing reliance on third-party services, NIS2 places particular emphasis on managing risks throughout the supply chain. This includes conducting due diligence on suppliers, defining cybersecurity obligations in contracts, and performing ongoing security assessments.

Supervision and Enforcement NIS2 strengthens the enforcement capacity of national authorities. Member States must designate competent authorities and single points of contact to oversee implementation. The directive also introduces a regime of administrative sanctions, including significant fines, for non-compliance.

Cooperation and Information Sharing To foster a more unified response to cyber threats, NIS2 reinforces collaboration between Member States. It establishes the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) for coordinated incident response and encourages information exchange between public and private sectors.

2.2.3 Critical Obligations for Essential Entities

Articles 20 to 24 of the directive are particularly relevant to critical infrastructure entities [30]:

Governance (Article 20) Management bodies must approve and oversee the cybersecurity measures adopted by their organizations and may be held liable for non-compliance. Furthermore, they are required to undergo cybersecurity training and to promote training initiatives within their organizations.

Cybersecurity Risk Management Measures (Article 21) Entities must take proportionate technical, operational, and organizational steps to mitigate risks to their network and information systems. This includes adopting an "all-hazards" approach that covers both cyber threats and broader operational disruptions.

Incident Notification (Article 23) Entities must notify the competent authority or CSIRT in the event of significant incidents. They may also be required to inform service recipients about mitigation actions or, where appropriate, the threat itself.

Use of European Cybersecurity Certification Schemes (Article 24) Member States may require entities to use ICT products and services that comply with European cybersecurity certification schemes. Trust services and qualified ICT providers are also encouraged.

2.2.4 Expected Impact on Critical Infrastructure Sectors

The broader scope and stricter requirements introduced by NIS2 are expected to significantly affect critical infrastructure sectors. Sectors such as energy, healthcare, and water services, many of which were either previously excluded or less regulated under the original NIS [31], are now required to adopt more mature cybersecurity frameworks. This includes further developed systematic risk assessments, incident response protocols, and more secure third-party relationships.

For sectors with low baseline maturity, compliance demands substantial investment in cybersecurity tooling, personnel, and training [53]. Organizations may also need to bring in external expertise to meet requirements. These obligations may be especially burdensome for smaller operators with limited resources [34].

NIS2 also introduced heightened regulatory scrutiny. Management-level accountability and the possibility of administrative sanctions create strong incentives for organizations to prioritize cybersecurity [58]. While this may enhance oversight and governance, it also places pressure on sectors that historically underinvested in digital resilience.

At the same time, NIS2 encourages horizontal learning and intersectoral collaboration. By enabling information sharing between sectors with different levels of maturity, it provides an opportunity to raise overall cyber readiness. However, achieving this will depend on overcoming challenges such as fragmented national implementations, trust barriers, and incompatible regulatory interpretations [32].

Finally, implementation varies depending on each sector's maturity level. For instance, energy infrastructure may face stricter supervision due to national security relevance. Healthcare may struggle to upgrade legacy systems within tight budgets, while sectors such as waste and water may require structural transformation to meet basic resilience thresholds [35]. Despite these challenges, NIS2 presents a strategic opportunity to modernize outdated systems and improve resilience across the board.

2.3 Cybersecurity in the Financial Sector

This section examines the financial sector's cybersecurity landscape. We outline the drivers of its relative maturity, review strategic and operational practices that define its approach, and lastly explain how DORAreinforces these practices and extends their influence beyond finance into other critical sectors.

2.3.1 Overview and Maturity Drivers

The financial sector has long been a prime target for cyberattacks due to the high value of its digital assets and the broader systemic importance of its services [66]. As a result, financial institutions have developed some of the most mature cybersecurity practices across all industries, often setting the benchmark for others [21]. This maturity is driven by a combination of stringent regulatory obligations, substantialITsecurity budgets, and the necessity of maintaining consumer trust. Regulatory frameworks such as the GDPR, PCI-DSS, and DORA require institutions to demonstrate resilience against disruptions and ensure rapid recovery from cyber incidents. Routine audits and supervisory oversight further reinforce this accountability. Financial institutions typically allocate a significantly larger share, estimated at around 7.8%, of theirITbudgets to cybersecurity compared to other parts of critical infrastructure, [71, 15].

2.3.2 Strategic and Operational Cybersecurity Practices

Cybersecurity strategies in the financial sector are increasingly proactive and risk-based. Leading institutions treat cyber risk as a core business risk, integrating it into overall enterprise risk management. This includes:

- **Comprehensive Risk Management Frameworks:** Institutions implement end-to-end frameworks covering data protection, fraud prevention, and regulatory compliance [4].
- **Penetration Testing and Vulnerability Assessments:** Regular red-teaming and vulnerability scanning help identify weak points before they can be exploited [4].
- **Incident Response and Business Continuity:** Well-developed incident response protocols and recovery planning ensure minimal disruption during attacks [41].
- **Cultural Integration and Awareness:** Sector-wide, there's a growing emphasis on embedding cyber awareness into company culture. Employees receive regular training and undergo phishing simulations. [21].

In addition, the financial sector also leads in adopting advanced cybersecurity technologies such as Threat Detection programs and AI Integration, stricter Identity and Access Management (IAM), and more developed Cloud and Third-Party Risk Management [55].

2.3.3 DORA's Influence

The introduction of DORA reinforces and formalizes many of the financial sector's existing practices. As an already mature sector, DORA serves as a codifier and unifier of best practices. It sets detailed requirements for ICT risk management, incident reporting, third-party oversight, and digital operational resilience, aligning regulatory expectations across the EU financial ecosystem [41].

Importantly, DORA's influence is not limited to finance. Its structured approach provides a roadmap for other critical sectors [41]. Industries such as energy, healthcare, and telecommunications, which are heavily reliant on digital infrastructure, can adopt similar due diligence protocols, testing requirements, and governance structures. The directive's emphasis on continuous monitoring of third-party ICT providers and systemic risk management is particularly relevant for sectors with expanding digital supply chains.

Moreover, DORA promotes internal and sector-wide information sharing on cyber threats. This practice, while common in finance, is still emerging in many other industries. Cross-sector adoption of these models could significantly improve Europe's collective cyber resilience. Finally, as ICT providers work to meet DORA's demands, their improved security posture will benefit not only financial clients but also entities in other regulated domains [65]. Through both its internal maturity and external regulatory influence, the financial sector continues to shape the broader cybersecurity landscape in the EU.

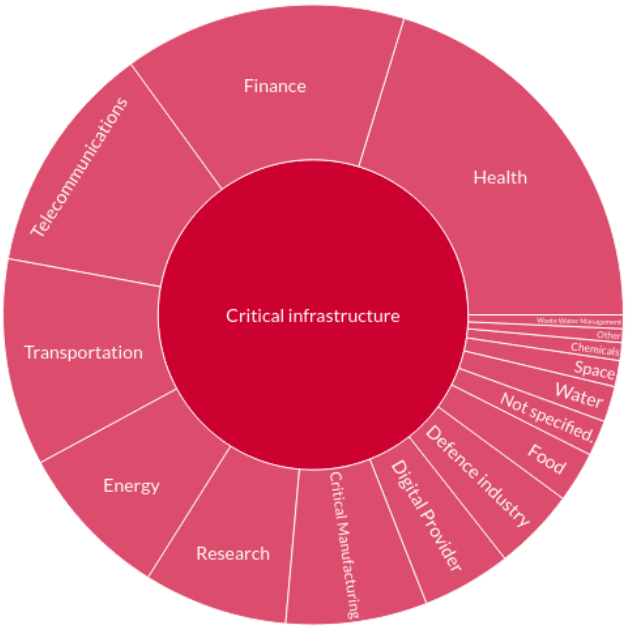

Figure 2.1: Top sectors targeted by cyber incidents between 01-01-2020 and 31-12-2024 [22]

2.4 Cybersecurity Challenges in Other Critical Infrastructure Sectors

This section examines the cybersecurity challenges facing critical infrastructure sectors outside finance. We outline the current state of cybersecurity, and discuss key challenges most prevalent across the different sectors which fall under "critical infrastructure".

2.4.1 Current State of Cybersecurity Across Different Sectors

As digitalization accelerates across all sectors, critical infrastructure has become increasingly reliant on interconnected systems. While this transformation improves efficiency and service delivery, it also exposes these systems to significant cyber risks. According to EuRepoC data, over 54% of cyberattacks since 2022 have targeted critical infrastructure, as shown in Figure 2.1 [22] . These attacks are primarily used for extortion, espionage, and system disruption, with direct implications for public safety, economic stability, and national security. Sectors such as energy, transportation, and healthcare are particularly vulnerable due to their operational dependency on digital infrastructure [38].

The consequences of a successful cyberattack on these sectors could be catastrophic, ranging from power outages and transportation gridlocks to compromised patient safety in hospitals [38]. Despite the rising threat level, many critical infrastructure sectors remain underprepared. They often rely on outdated systems that were never designed with cybersecurity in mind [36], making them attractive targets for attackers. A lack of specialized cybersecurity expertise, limited financial resources, and fragmented regulatory environments cause these vulnerabilities to be even more prominent [37, 50].

As the EU implements the NIS2 Directive, these sectors face increased pressure to enhance their cyber resilience. Yet, preparedness levels differ significantly. Some sectors, particularly those with historically lower digital maturity, such as healthcare or transport, are struggling to meet NIS2 requirements [13]. Understanding these challenges is essential to closing the security gap in Europe's critical infrastructure.

2.4.2 Challenges of Critical Infrastructure Cybersecurity

Increasing Cyberattack Frequency and Sophistication Critical infrastructure sectors are increasingly at risk from cyberattacks. As an example, digital transformation continues to integrate more operational technologies (OT) with IT systems, the attack surface for cyber threats expands, creating significant vulnerabilities across these sectors. Critical infrastructure sectors have seen a sharp rise in

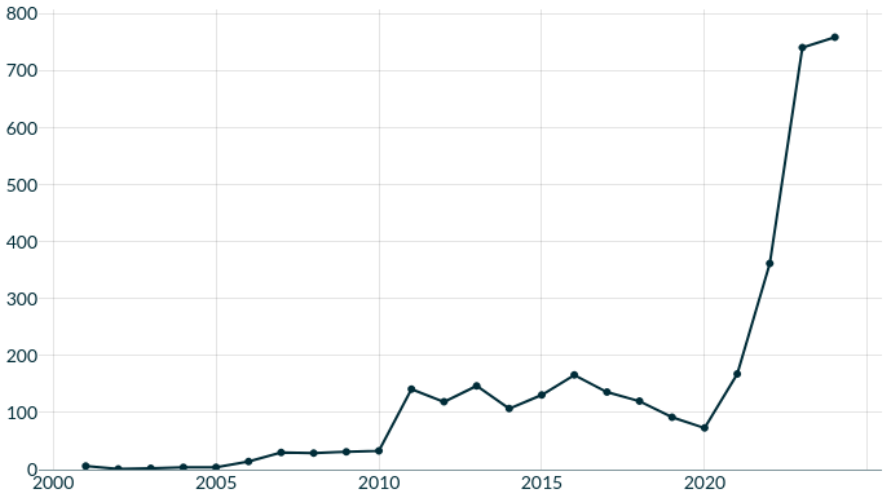

Figure 2.2: Number of cyber incidents across all countries between 01-01-2001 and 31-12-2024 [22]

the sophistication [40] and frequency (See Figure 2.2 [22]) of cyberattacks. These attacks often target the underlying systems that support essential services, such as power grids, communication networks, and water supply systems. Additionally, the criminal use of AI, including the exploitation of deepfakes, is expected to increase in the future [40]. The incorporation of AI into existing techniques may further widen the scope and scale of cyberattacks.

Usage of Legacy Systems and Outdated Technology One of the primary challenges facing critical infrastructure sectors is the reliance on legacy systems that were not designed with cybersecurity in mind. These systems often lack both basic and modern security features such as encryption, access control, or zero trust, making them vulnerable to cyberattacks [36]. The WannaCry ransomware attack in 2017 offers a strong example. Exploiting a vulnerability in older versions of Microsoft Windows, the ransomware affected over 200,000 computers across 150 countries [67]. Many of these systems were legacy computers still running outdated versions of Windows, which were particularly susceptible to the attack.

The integration of legacy systems with newer technologies complicates cybersecurity efforts, as it introduces additional vulnerabilities that are difficult to manage. Legacy systems might lack the necessary functionalities to accommodate advanced security measures, leaving gaps in the defense framework. Replacing legacy systems requires not only hardware and software upgrades, but also investments in training, integration, and downtime management. Despite the risks, legacy systems are deeply rooted in some industries, especially those with long-established infrastructures like energy, transportation, and healthcare. For these organizations, the trade-off between maintaining legacy systems and transitioning to modern technologies remains a persistent challenge.

Low Level of Expertise and Resources Another significant challenge is the shortage of skilled cybersecurity professionals. Many critical infrastructure organizations struggle to attract and retain the necessary talent to protect their systems effectively, due to the high demand for these skills across industries [37]. This shortage is compounded by the increasing sophistication of cyberattacks, which require advanced skills to defend against.

Additionally, limited budgets often prevent these sectors from investing in the advanced cybersecurity tools and training needed to defend against modern cyber threats. 16% of companies in the U.S. have experienced cyber incidents due to insufficient cybersecurity investment in the last two years. Alarmingly, critical infrastructure, energy, oil, and gas organizations suffered the biggest number of cyber incidents due to improper budget allocation (43%) [50].

Fragmented Regulatory Landscape The cybersecurity regulatory landscape for critical infrastructure in the European Union is marked by fragmentation, creating challenges for consistent implementation and enforcement across member states [63]. While efforts like the NIS2 Directive aim to standardize

cybersecurity practices, the collection of diverse national regulations, the inconsistent implementation of regulations across different member states [46], and sector-specific rules continue to pose significant hurdles. The original NISDirective left much of the interpretation and enforcement to individual countries, leading to variations in how cybersecurity measures were adopted. This resulted in a patchwork of regulations with various levels of enforcement and accuracy, creating challenges for organizations operating in multiple EU countries [48].

Organizations operating across multiple EU member states face additional challenges due to the varying regulatory requirements in each country. The lack of harmonization means that these organizations must navigate different sets of rules, which can be both costly and complex. This regulatory fragmentation not only increases the administrative burden but also creates potential security gaps, as companies may struggle to maintain consistent cybersecurity practices across all jurisdictions. In addition, different critical infrastructure sectors are governed by sector-specific regulations within each country that may not always align with broader cybersecurity mandates [69]. This sectoral approach often results in even further fragmented regulatory frameworks, where some sectors might be subject to stricter cybersecurity requirements than others.

Dependence on Third-Parties Critical infrastructure sectors often rely on third-party vendors for essential services, such as cloud computing or the maintenance of operational systems. This dependence introduces additional risks, as the cybersecurity practices of third-party vendors directly impact the security of the critical infrastructure they support [1]. The involvement of third-party vendors in critical infrastructure operations significantly increases the attack surface. If these third parties are not adequately secured, they can become entry points for cyberattacks. Supply chain attacks have been on the rise, where attackers compromise a vendor to gain access to the infrastructure of multiple clients, as seen in incidents like the SolarWinds hack [68].

Managing the cybersecurity risks associated with third-party vendors is a complex task. Many organizations struggle with conducting thorough due diligence, ongoing monitoring, and ensuring that third parties comply with their security standards. ENISA reports that in 2025, cybercriminals are increasingly targeting third-party providers, likely as an opportunity to optimize the efficiency of their attacks [39]. ENISA highlights that many critical infrastructure providers still lack formalized third-party risk management programs, leaving them vulnerable.

Sector Preparedness As stated before, the preparedness of critical infrastructure sectors to handle cybersecurity threats varies widely. Sectors such as finance and telecommunications are generally more advanced in their cybersecurity measures, while sectors like healthcare, water supply, and transportation often lag behind [13]. Each sector faces unique challenges, such as reliance on legacy systems, limited cybersecurity budgets, and a lack of specialized cybersecurity expertise. As a result, some are less prepared to respond to cyber incidents and may struggle to meet the requirements set by the NIS2 Directive.

2.5 Broader Literature on Implementing Security-Related Regulations

Beyond DORA and NIS2, a substantial body of research examines how organizations adopt security- and privacy-related regulations, which provides useful analogies for understanding current implementation dynamics and motivating cross-regulatory learning. This section aims to give an insight into the available literature.

2.5.1 Lessons from GDPR Adoption Studies

A systematic mapping study by Machado et al. (2023) [54] surveyed the academic and practitioner literature to identify which organizational areas are most affected by GDPR compliance, the main challenges encountered, and the methods, technologies, and practices used to address them. Across the reviewed works, budget constraints emerged as the most frequently cited challenge, alongside difficulties in drafting clear communications, managing international data sharing, and the anonymization of data. Cryptography, pseudonymization, anonymization, in-house software development, and staff training were among the most common practices adopted to achieve compliance. The mapping also highlighted thematic areas

such as privacy policy management, social companies, mobile banking, and backup systems, where challenges were identified but no specific mitigating practices were reported. This suggests a need for targeted solutions. By linking specific challenges to practical responses, the study offers a preliminary guide for organizations still adapting to GDPR, enabling them to anticipate common obstacles and adopt proven approaches. These findings also illustrate how regulatory impact is shaped not only by legal requirements but by the availability of resources, technical capabilities, and sector-specific conditions.

Management research on GDPR compliance treats regulatory implementation as an organizational-change process and identifies barriers and enablers that shape outcomes [3]. Reported barriers include the complexity and subjectivity of the regulation, the extensive and resource-intensive nature of compliance, lack of privacy expertise, absence of practical implementation guides or standard procedures, and difficulty meeting specific requirements such as the right to erasure, maintaining processing records, embedding data protection by design and by default, and appointing a data protection officer. Enablers include designing an implementation roadmap, performing a GDPR gap analysis, identifying and managing privacy risks, documenting processing operations, applying robust data governance practices, implementing appropriate security measures, conducting staff training, designating a DPO, and carrying out data protection impact assessments. These findings reinforce that the effectiveness of regulatory frameworks depends not only on statutory text but also on the organizational capabilities and incentives that mediate their implementation, an insight equally relevant to NIS2 entities with lower baseline maturity.

2.5.2 NIS to NIS2 iteration

Related analysis of incident-reporting obligations under the NIS and NIS2Directives shows how vague definitions of a "significant" incident in the original NIS framework made consistent compliance difficult and contributed to low reporting volumes across the EU [62]. NIS2addresses these shortcomings by extending the reporting obligation to incidents that are capable of causing substantial or considerable harm, removing the need to prove materialized damage before reporting. The new tiered reporting process introduces an early warning followed by a full notification, encouraging earlier engagement with competent authorities and CSIRTs. Feedback provisions are intended to incentivize reporting and enhance incident-handling capacity, while the broadened threshold aims to improve cyber situational awareness and promote a culture of proactive information sharing.

This shift is consistent with broader academic evaluations of the directive's evolution. Vandezande (2024) [70], for example, emphasizes that one of the central aims of NIS2is to remedy the uneven and often inconsistent implementation of NIS across Member States. By clarifying definitions such as "significant incident" and harmonizing reporting timelines, NIS2seeks to reduce fragmentation and ensure a more uniform baseline of cyber resilience across the Union. In this way, NIS2reflects a process of regulatory learning, where the practical difficulties of the first NIS Directive made for a more prescriptive and preventive framework in its successor. These insights underline the importance of comparing NIS2with other regulatory frameworks, as such comparative perspectives can reveal whether similarly prescriptive elements, such as those found in DORA, could help address persistent challenges like incident reporting and third-party oversight in less mature sectors.

2.5.3 Research on DORA readiness

Other empirical work explores how DORA is being operationalized in practice, with a particular focus on the readiness of service providers to support regulated financial entities. A qualitative study of Dutch consulting and legal firms (Kos, 2024) [51] found that in 2024, with the compliance deadline approaching at the start of 2025, many financial organizations faced resource constraints, skills shortages, and the complexity of translating DORA's prescriptive requirements into practical business processes. As a result, external service providers played a central role in gap assessment, readiness validation, and implementation support. The study identifies multidisciplinary expertise, combining technical, legal, and operational resilience competencies as a critical success factor, alongside structured go-to-market strategies and sector-specific knowledge. To support consistent service quality, the authors propose a practical readiness checklist covering service proposition design, client engagement, and compliance validation. While the study's national focus and pre-implementation timing limit how it can be generalized, it underscores the reliance on external actors in meeting DORA obligations. An observation that holds lessons for NIS2-covered sectors facing similar maturity and capacity constraints.

2.5.4 Research on interplay between NIS2 and the Cyber Resilience Act

Eckhardt and Kotovskaia (2023) [16] provide a systematic comparison, focusing on the interplay between NIS2 and the proposed Cyber Resilience Act (CRA). Their analysis shows how the CRA's product-oriented obligations (e.g. secure-by-design requirements for ICTproducts and services) complement the organizational and sectoral obligations imposed by NIS2, together forming a more coherent EU-wide cybersecurity framework. This demonstrates that NIS2does not operate in isolation but interacts with other regulatory instruments that target different layers of the digital ecosystem. For this thesis, the study is particularly relevant because it illustrates how cross-regulatory comparisons can highlight both overlaps and gaps. Whereas their focus lies on NIS2 and the CRA, this research extends the comparative approach to DORA, a regulation with a narrower financial-sector scope but a much more prescriptive set of rules for ICTand third-party risk management. Drawing on the methodological insights from such comparative studies, this thesis contributes to the broader discussion on how different EU cybersecurity frameworks can be leveraged to raise resilience across critical infrastructure sectors.

2.6 Transferability of Financial Sector Practices to Other Sectors

As discussed, the financial sector's relatively high cybersecurity maturity, driven by stringent regulation, substantial budgets, and sector-wide coordination, makes it a logical candidate for benchmarking other critical infrastructure sectors (See section 2.3, "Cybersecurity in the Financial Sector"). As sectors affected by the NIS2 Directive work toward compliance, a growing body of literature looks to the financial domain to learn from it. The EU already explicitly acknowledges the complementary nature of DORA and NIS2. Recital 13 of the NIS2 Directive recognizes DORA as *lex specialis*, meaning that where both frameworks apply, DORA takes precedence as the more specific regulation [30]. This legal distinction reinforces DORA's role as a more detailed model compared to NIS2, and allows it to be used as such when needed.

2.6.1 Cross-Domain Standards Adaptation

The idea of adapting standards across domains is not new. In both academia and industry, methods such as manual mapping are frequently used to align frameworks and assess compatibility. Mussmann et al. argue that manual mapping remains the most transparent and effective method for cross-framework analysis, especially when comparing standards in sectors with differing levels of cybersecurity maturity [56]. This method allows evaluators to assess the purpose and implementation of controls, even when terminology or structural layout diverges.

More formalized tools also exist. The U.S. NIST OLIR program offers informative references that map frameworks like ISO/IEC 27001 to NIST CSF [57]. Similarly, the Secure Controls Framework (SCF) compiles controls from dozens of global standards, enabling crosswalks between models and highlighting control coverage gaps [10]. These tools are particularly relevant for organizations that operate in multi-regulatory environments and need to streamline compliance efforts.

2.6.2 DORA to NIS2 Transferability

DORA and NIS2 address similar themes, but NIS2 often does so in broader and more flexible terms. For example, NIS2 requires risk management but leaves implementation details to the entities and Member States, whereas DORA sets concrete standards and enforces them through European financial regulators.

The academic literature on this topic is still limited but growing. Ruohonen (2024) provides a systematic literature review on NIS2 and identifies significant research gaps regarding its interaction with parallel regulations such as DORA [60]. However, this does not cover much regarding whether, and how the stricter requirements of DORA can be adapted to sectors with differing cybersecurity capabilities and regulatory cultures. Seeba et al. (2025) offer a promising path forward by evaluating NIS2 through organization-level use cases, showing how abstract requirements can be interpreted through practical implementations [64].

Fysarakis et al. (2023) contribute from a resilience engineering perspective. Their PHOENI2X framework bridges multiple EU resilience initiatives and demonstrates how principles central to DORA such as structured testing, threat modeling, and third-party governance, can inform broader cross-border cyber resilience models that also support NIS2 goals [42].

From a legal and policy standpoint, the transferability of DORA practices seems clear. Recital 13 of the NIS2 As mentioned before in chapter 2.6, the directive explicitly designates DORA as "lex specialis", confirming that DORA takes precedence where both regulations apply. A 2024 article by BDO emphasizes this legal interplay and explores how entities operating under both regimes must reconcile their obligations, highlighting how financial sector mechanisms can shape NIS2 implementation [5]. Another article by ActiveMind Legal (2024) also notes that the structured supervisory and reporting mechanisms under DORA offer a degree of operational maturity that NIS2 could benefit from, especially in areas like third-party oversight and incident reporting [2].

2.7 Regulatory and Strategic Implementation Gaps

Although both aim to enhance cybersecurity resilience within the EU, DORA and NIS2 differ significantly in structure, scope, and enforcement mechanisms. DORA is an EU regulation focused on financial entities with binding rules and centralized oversight by institutions such as ESMA, EBA, and EIOPA. In contrast, NIS2 is a directive that applies broadly across critical sectors and relies on national transposition and supervision by member state authorities, resulting in varied application and enforcement across the EU.

Ruohonen (2024) highlights the risk of regulatory incoherence and institutional fragmentation when multiple cybersecurity policies, such as NIS2, DORA, and AI Act, intersect without joint strategic oversight [59]. Additionally, while both include stiff penalties for non-compliance and management liability, DORA stipulates fine structures and timelines specific to ICT providers, whereas NIS2 leaves sanction levels up to national implementation [2]. There are further gaps in incident reporting thresholds, testing mandates, and third-party oversight: DORA's strict TLPT regime and detailed reporting timelines are more demanding than the broader risk-based mandates under NIS2. This divergence creates strategic challenges for entities subject to both frameworks or those that operate in multiple sectors or countries. The fragmented transposition of NIS2, with guidelines unevenly implemented across member states, complicates compliance strategies for cross-jurisdictional firms [19]. Similarly, organizations face considerable operational burdens when aligning dual compliance regimes that differ in specificity, supervisory regime, and maturity requirements.

Several options exist to overcome the inconsistencies and fragmentation between NIS2 and DORA. Cross-directive supervisory coordination for one, is seen as essential. Currently, DORA is supervised by ESAs, while NIS2 enforcement depends on national cybersecurity authorities. This can lead to misaligned expectations and fragmented compliance strategies, especially for multinational organizations operating across regulated sectors. ECSO (2025) recommends formalizing cooperation between ESAs, national CSIRTs, and competent authorities to ensure aligned interpretations, enforcement expectations, and information sharing across the EU [19]. In addition to this, adopting unified risk management frameworks might offer a promising way to bridge the implementation divide. Tools such as NIST CSF 2.0 and the PHOENI2X model promote a harmonized control language and resilience architecture across sectors. These frameworks are designed to be flexible enough for cross-sector adoption while retaining rigor through tiered maturity models. Fysarakis et al. (2023) argue that applying such frameworks facilitates better alignment of DORA-style resilience mechanisms within broader infrastructure landscapes governed by NIS2 [42].

2.8 Conclusion

This literature review has examined the evolution, structure, and implementation of two major EU cybersecurity regulations and their relevance for enhancing digital resilience across critical infrastructure sectors. The review identified several key findings. First, the financial sector stands out in terms of cybersecurity maturity, driven by strict regulatory oversight, sector-specific best practices, and high investment levels. DORA further introduces sector-wide obligations that go beyond traditionalITsecurity, extending into systemic risk management and third-party oversight.

NIS2 broadens the scope of EU cybersecurity legislation by encompassing a wide range of critical infrastructure sectors. However, its high-level and flexible nature creates challenges in implementation, especially for less mature sectors. Compared to DORA, NIS2 lacks prescriptive clarity in areas such as operational testing, third-party risk governance, and supervisory mechanisms.

Although DORA and NIS2 differ in regulatory design and enforcement mechanisms, there is growing

academic and policy support for cross-sector learning. DORA's structured requirements in areas like ICT risk management, incident reporting, and third-party oversight offer practical models that can help inform implementation efforts in NIS2-covered sectors. Rather than serving as a universal template, DORA provides a benchmark that can be adapted to different sectoral contexts. Widely adopted frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework are proven to enable this kind of cross-regulatory alignment, offering organizations a common reference point for translating high-level regulatory obligations into actionable controls.

Our review also highlighted several strategic challenges in harmonizing DORA and NIS2. These include inconsistent national implementations, fragmented oversight, and regulatory overlap. Scholars and institutions suggest that bridging these gaps will require greater supervisory coordination, shared technical guidance, and the adaptation of financial sector practices into other domains. From a research perspective, further empirical work is needed to examine how DORA-style controls can be operationalized in non-financial contexts, as most existing studies focus on financial sector compliance or high-level policy analysis. Future studies could explore implementation case studies, cost-benefit analyses of cross-sector controls, or the role of sector-specific constraints in shaping resilience strategies.

From a practical standpoint, the findings underscore the importance of tailored implementation strategies. While DORA provides a robust model, its practices must be contextualized for sectors with different risk profiles, resource levels, and operational realities. Still, the direction is clear: enhancing cybersecurity resilience across the EU will require borrowing from the structured and enforceable practices pioneered in finance, while ensuring they are meaningfully adapted for other critical domains.

Chapter 3

Method

This chapter outlines the research approach and the steps taken to address the research questions. The methodology combines qualitative document analysis, structured comparative mapping, and semi-structured expert interviews. These methods were selected because they allow for both a systematic examination of the regulatory texts (DORAand NIS2) and an exploration of practical insights from professionals directly involved in cybersecurity and compliance. The regulatory document analysis follows the approach described by Bowen [6], who highlights document analysis as a systematic method for extracting and interpreting meaning from textual sources. In the subsequent comparative mapping, this study follows the design-science approach described by Hevner et al. [45], where knowledge is produced through the building and evaluation of an artifact. In this research, the artifact consists of a structured comparative framework that models the overlap between DORAand NIS2across ten key regulatory dimensions. The framework functions as a conceptual model that supports analysis and practical understanding [45]. The expert interviews are conducted in a semi-structured format, well suited for combining comparability with in-depth exploration, as described by Kallio et al. [49]. The mapping artifact is used again during the interviews as a discussion guide, consistent with the notion of Hevner et al. [45] of evaluating an artifact in practice. The analysis is informed by principles of thematic analysis Braun and Clarke [7], particularly the identification of recurring patterns within the data. However, rather than conducting an open inductive coding process, interview data were structured according to the predefined comparative dimensions developed during the document analysis phase. Together, these methods provide a balanced foundation for assessing the transferability of financial-sector practices to other critical infrastructure sectors.

3.1 Regulatory Document Analysis

The first step of the research consists of a qualitative analysis of the regulatory texts. This method is selected because it is widely used to systematically extract and interpret meaning from textual sources. Among the specific uses of documents outlined by Bowen [6], this study applies document analysis primarily as a main data source for qualitative interpretation, and secondarily as a means of corroborating and contextualizing findings derived from later expert interviews.

Following Bowen's process of skimming, reading, and interpreting, the analysis includes the full texts of both DORA and NIS2, but particular attention is directed to the parts most closely connected to the research focus: cybersecurity risk management, incident reporting, operational resilience testing, governance and accountability, third-party and supply-chain risk management, information sharing, supervision, and enforcement. Based on those areas, certain chapters and articles of both frameworks can be identified as the primary focus, which forms the foundation for the comparative mapping in the next stage of the research. Similar to the thematic analysis method described by Bowen, the selected articles are examined in detail, and their main focus is noted, indicating which areas they cover. After identifying the main areas of each article, these provisions are compared and iteratively grouped into broader thematic clusters. The clusters and the contents of these clusters are then arranged and re-arranged into categories until the contents each fit into a proper dimension. These are labeled as specific analytical dimensions that capture the core regulatory themes of both frameworks. These dimensions are introduced and explained in Chapter 4, while their methodological role is outlined in the following section.

3.2 Comparative Analysis and Mapping

Having established the material to be analyzed, the second step is a structured comparative analysis across the core regulatory dimensions that emerge from the thematic analysis presented in Section 3.1. Since this step involves the construction of the comparative framework to evaluate the degree of alignment between DORA and NIS2, we identify it as a mapping activity and the creation of a research artifact as outlined by Hevner et al. [45].

Analysis Levels

To find the overlap between each dimension, the comparative analysis is broken down into three levels: objectives, requirements, and implementation. Examining both frameworks across these levels allows for a systematic and nuanced comparison. These levels are chosen because they cover the written rule, aim, and real-world application of each article of both regulations. Objectives capture the intended purpose of the law, requirements define the concrete rules to be followed, and implementation shows how these rules are operationalized and enforced in practice. Using these three levels ensures that the comparison captures not only similarities in wording but also differences in depth, specificity, and practical applicability:

1. **Objectives**
   Definition: Objectives are the high-level goals or intended outcomes of a regulatory framework. They explain **why** a regulation exists and what it seeks to achieve.
   Purpose: Objectives provide the overarching mission that guides the entire framework, such as ensuring sector resilience, protecting public safety, or maintaining market stability.

2. **Requirements**
   Definition: Requirements are the specific rules, guidelines, or standards that entities must follow to comply with the framework. They represent **what** regulated entities are required to do to meet the objectives.
   Purpose: Requirements translate the high-level objectives into actionable obligations, such as mandating incident reporting, conducting risk assessments, or ensuring data protection.

3. **Implementation**
   Definition: Implementation refers to the practical application and enforcement of requirements by entities and regulatory bodies. It addresses **how** the requirements are put into practice, including procedures, oversight mechanisms, and any flexibility provided.
   Purpose: Implementation details show how the requirements are operationalized in real-world contexts, which can vary based on the framework's structure, sectoral focus, or geographic reach.

Overlap Degrees

Using the aforementioned analytic dimensions we determine the extent to which NIS2 and DORA align within each of these levels. We developed five-point overlap scale, which can be found in Table 3.1, for this reason. Our overlap scale ranges from complete absence of similarity to practically identical objectives, requirements, and implementation. We have chosen five degrees of overlap because it provides a balance between nuance and clarity: the scale is detailed enough to capture meaningful distinctions between regulatory objectives, requirements, and implementation, while remaining simple and transparent enough to apply consistently across dimensions. This scoring system provides a structured way to evaluate convergence and divergence across the frameworks and serves as the basis for the comparative framework presented in the following chapter.

3.3 Expert Interviews

In this section, we discuss the collection of data through the interviews and the subsequent analysis we conducted on said data.

3.3.1 Data Collection

To complement the document-based comparison of NIS2 and DORA, we conduct semi-structured expert interviews with practitioners involved in cybersecurity governance, risk and compliance, third-party

Table 3.1: Degrees of Overlap

Degree of overlap	Criteria
0 - No overlap	No similarity in objectives, requirements, or implementation. The frameworks address entirely different topics or needs with no alignment in purpose or practice.
1 - Minimal Overlap	Mention of similar objectives but with very different requirements and implementation. Minimal common ground in terms of intent, with vastly different specifics and practical applications.
2 - Low Overlap	Shared objective or dimension, but significant differences in requirements and implementation. The frameworks align on the overarching goal but diverge substantially in the specifics and methods of application.
3 - Moderate Overlap	Common objective with similar requirements, though with some distinctions in implementation. Comparable goals and main requirements, with some variations in enforcement, depth, or specific sectoral applications.
4 - High Overlap	Nearly identical objectives and requirements, with minor distinctions in implementation. Strong alignment across goals and requirements, with only slight differences in practical application.
5 - Full Overlap	Identical objectives, requirements, and implementation. Complete alignment in terms of purpose, specifics, and application, making the frameworks indistinguishable in this dimension.

ICT-risk management, as well as offensive and defensive digital security professionals. Participants were recruited through professional networks and contacts at KPMG the Netherlands. This provided access to practitioners with direct experience of NIS2 and DORA. We used a purposive sampling of different profiles to reach a wider variety of knowledge. Roles include senior and junior consultants, managers, partner-level employees, TPRM experts, and compliance officers, whose daily work is directly connected or closely related to NIS2 and/or DORA. Participation is voluntary, and responses are reported anonymously. We decided to conduct semi-structured interviews, because they balance systematic coverage of key topics with the flexibility to adapt questions to each participant's expertise [49].

Interview Structure

The interviews are organized into two main phases: an exploratory part (Phase A) and a confirmatory part (Phase B). The exploratory part is intended to gather broad insights and uncover themes, challenges, and perceived overlaps between the two regulatory frameworks. The confirmatory part subsequently focuses on validating and refining the comparative framework developed from the document analysis.

Phase A – Interview Questions (Exploratory)

1. **Background/setup:** role, responsibilities, familiarity, and daily exposure to NIS2/DORA.
2. **Exploration:** how organizations manage NIS2/DORA compliance; major challenges or gaps; whether current practices meet critical-infrastructure needs.
3. **Reflective close:** transfer potential from DORAto NIS2, recommendations for cross-sector knowledge transfer, and perspectives on regulation's role in resilience.

During the explorative part of phase A, we present the interviewees with the following exploratory questions:

Q1: How do organizations manage NIS2 and DORA compliance?

Q2: What are the most significant challenges or gaps when implementing standards?

Q3: Do the standards effectively address the cybersecurity needs of critical infrastructure?

Q4: Can DORA best practices be effectively adapted to enhance NIS2 implementation?

Q5: What recommendations would you give for improving cross-sector knowledge transfer of cybersecurity practices?

Q6: What is your general perspective on protecting critical infrastructure and the role of regulation in enhancing resilience?

Phase B – Framework Appraisal (Confirmatory)

4. **Dimension review:** experts reviewed the proposed overlap framework (objectives, requirements, and implementation with 0–5 overlap levels) and provided confirmations, corrections, or nuance per dimension they selected.

For Phase B, instead of asking interviewees to cover all ten dimensions, participants are invited to select the dimensions they feel most qualified to discuss. This prioritization allows more in-depth responses and reduces speculative answers on unfamiliar topics.

The interviews are conducted either in-person or remotely, each lasting approximately one hour. Sessions are held in English or Dutch, depending on participant preference. All interviews are audio-recorded with permission; Dutch excerpts used in the research are translated into English for consistency in coding and reporting.

Participant Selection Participants were selected using purposive sampling, with the objective of recruiting individuals possessing expertise in cybersecurity governance,ICTrisk management, and regulatory compliance within sectors affected by DORAand/or NIS2. To ensure suitability, potential participants were assessed against the following criteria:

- Professional involvement with DORAand/or NIS2, including implementation, advisory, supervisory, or compliance responsibilities;
- Operational responsibility in areas such asICTrisk management, cybersecurity strategy, third-party risk management, incident response, or regulatory reporting;
- Direct exposure to regulatory interpretation or implementation challenges.

Sectoral Distribution The final sample included experts from:

- Financial institutions subject to DORA;
- Critical infrastructure sectors covered by NIS2;
- Advisory and consulting roles working across both regulatory environments.

This cross-sector representation enabled comparative insights into differences in maturity, interpretation, and implementation strategies.

The detailed demographic overview of participants, including sector affiliation and professional roles, is presented in Section 4.2.1.

Ethical Considerations Our study adheres to standard ethical research practices for qualitative research involving human participants. The interviews focused exclusively on participants' professional experiences, interpretations, and practices related to DORA, NIS2, cybersecurity governance, and regulatory compliance. No sensitive personal data or confidential organizational data were requested or collected. Participants were not asked to disclose proprietary information, classified material, or commercially sensitive operational details.

Prior to participation, all interviewees were informed about the purpose of the study, the nature of the data being collected, and how the data would be used in the thesis. They were explicitly informed that participation was voluntary and that they could withdraw from the study at any time without consequences. Informed consent was obtained before conducting each interview.

To protect participant privacy, all interview transcripts were anonymized prior to analysis by removing names, company identifiers, and any potentially identifiable details. Audio recordings and original transcripts were stored securely and were accessible only to the researcher. In the reporting of results, participants are referenced in a non-identifiable manner to ensure confidentiality.

3.3.2 Data Analysis

The analysis reflects the interview structure.

Analytical Procedure Our analysis proceeded as follows:

1. **Transcription and familiarization** All interviews were transcribed and reviewed in full to gain a comprehensive understanding of each participant's perspective.
2. **Dimension-based categorization** Interview content was examined and grouped according to the predefined regulatory dimensions (e.g.,ICTrisk management, incident reporting, third-party risk management, etc.). Statements relevant to each dimension were extracted and organized accordingly.
3. **Identification of patterns within dimensions** Within each dimension, recurring themes, shared concerns, implementation challenges, and sector-specific observations were identified.
4. **Identification of divergences and unique insights** Particular attention was paid to contrasting views or insights that appeared only once but were analytically relevant.
5. **Cross-sector comparison and synthesis** Findings were compared across financial and non-financial sectors to evaluate perceived overlap, maturity differences, and transferability of practices.

This procedure loosely follows the principles of thematic analysis, which uses systematic theme development while allowing for researcher interpretation and contextualization [7]. However, our research diverges slightly from the thematic analysis principles. Our research did start with a familiarization of the data, but not precisely follow the six phases of thematic analysis as described by Braun and Clarke. Instead of generating initial codes and themes (steps 2 and 3 from Braun and Clarke), the analysis was guided by the ten comparative dimensions identified during the regulatory document analysis phase (Table 4.1). These dimensions functioned as analytical categories for organizing and interpreting interview data, and is what we used to review and define (steps 3 and 4 from Braun and Clarke) the interview results.

Framework appraisal (dimensions). For the confirmatory part, the predefined dimensions (D1–D10) and their corresponding overlap criteria (0–5) are mapped into a similar matrix. Expert statements are systematically labeled to:

- **Confirm** the preliminary overlap assessment,
- **Adjust** it where substantiated counter-evidence or relevant nuance is provided, or
- **Flag** uncertainty or gaps (e.g., "insufficient evidence" or "implementation varies by jurisdiction").

For each of the ten dimensions, interview excerpts are reviewed and manually assigned to the corresponding dimension-response matrix. The resulting dimension table allows recurring confirmations, nuanced adjustments, and diverging perspectives to be identified. The analysis helps to refine and contextualize the comparative framework and provides insight into implementation realities and expert perspectives. The integration of expert validation alongside document-based comparison reflects the design science principle of combining artifact construction with iterative stakeholder evaluation [45].

Integration of Document and Interview Phases The ten comparative dimensions identified during the regulatory document analysis served as the conceptual bridge between the two phases of the study. The dimensions informed the development of the semi-structured interview guide and provided the primary structure for organizing interview findings. This sequential design ensured coherence between the textual regulatory comparison and the empirical validation phase. While the regulatory analysis focused on formal legal requirements, the interviews provided practical insight into how these dimensions are interpreted and implemented in real-world organizational contexts.

Chapter 4

Results

This chapter reports the empirical outputs of the study in two complementary parts: a structured comparative analysis of DORAand NIS2, and an interview-based assessment of the ten comparative dimensions with domain experts.

4.1 Comparative Analysis

This section presents the comparative analysis of DORA and NIS2. As described in Section 3.2, the goal is to systematically examine how both frameworks address core regulatory dimensions relevant to cybersecurity and operational resilience. By mapping their objectives, requirements, and implementation mechanisms, we can identify areas of convergence, divergence, and potential transferability of practices between the financial sector and other parts of critical infrastructure. Below, we present the concrete outcomes of applying the method that was described in Section 3.2.

The analysis proceeds in three steps. First, the key dimensions used for comparison are introduced and briefly illustrated to clarify how they are defined in each framework. Second, a structured overview table summarizes where these dimensions appear in DORAand NIS2, alongside the assessed level of overlap. Finally, a textual analysis (provided in detail in Appendix A) unpacks each dimension across objectives, requirements, and implementation, forming the foundation for the interview-based insights presented later in this chapter.

4.1.1 General Dimension Overview

While reviewing the regulatory documents, we established a set of ten analytical dimensions that capture core aspects of cybersecurity governance, risk management, and operational resilience relevant to critical infrastructure sectors. These dimensions serve as an abstracted analytical framework, allowing findings from regulatory analysis and expert interviews to be organized in a consistent and comparable manner. The most prevalent dimensions we found in Table 4.1 and are further elaborated on outside the context of NIS2 and DORA below that. The dimensions are defined independently of any specific regulatory framework. They represent functional areas of cybersecurity practice that recur across sectors and regulatory environments, rather than direct translations of legal articles or obligations. This abstraction enables the analysis to focus on underlying practices, maturity differences, and perceived overlaps, rather than on formal compliance language.

D1: Cybersecurity Risk Management and ICT Risk Management This dimension captures how organizations identify, assess, and manage risks related to information and communication technologies. It includes the existence of structured risk management frameworks, risk ownership, continuous monitoring, and the integration ofICTrisks into broader enterprise risk management processes.

D2: Incident Reporting Incident reporting refers to the mechanisms and processes through which cybersecurity incidents are identified, classified, escalated, and communicated to relevant internal and external stakeholders. This dimension focuses on timeliness, thresholds, and procedural clarity, rather than on specific reporting obligations.

D1:	Cybersecurity Risk Management and ICT Risk Management
D2:	Incident Reporting
D3:	Operational Resilience Testing
D4:	Third-Party Risk Management
D5:	Governance and Accountability
D6:	Information Sharing
D7:	Supervision and Enforcement
D8:	Penalties
D9:	Crisis Management
D10:	Oversight of ICT Providers

Table 4.1: Dimension Overview

D3: Operational Resilience Testing This dimension covers the extent to which organizations test their ability to withstand, respond to, and recover from disruptive events. It includes activities such as vulnerability assessments, scenario-based testing, penetration testing, and resilience exercises aimed at validating preparedness under adverse conditions.

D4: Third-Party Risk Management Third-party risk management addresses how organizations manage cybersecurity risks arising from external suppliers, service providers, and partners. This includes due diligence, contractual safeguards, ongoing monitoring, and the treatment of supply-chain dependencies as part of the overall risk posture.

D5: Governance and Accountability This dimension reflects the role of organizational leadership and governance structures in cybersecurity. It includes management oversight, allocation of responsibilities, decision-making authority, and accountability mechanisms that ensure cybersecurity is addressed at the appropriate organizational level.

D6: Information Sharing Information sharing captures the extent to which organizations exchange cybersecurity-related information with peers, sectoral bodies, or authorities. This includes sharing threat intelligence, vulnerabilities, and lessons learned, as well as participation in trusted collaboration mechanisms.

D7: Supervision and Enforcement This dimension focuses on external oversight mechanisms that monitor compliance and cybersecurity maturity. It encompasses supervisory approaches, audit activities, corrective measures, and the presence of authorities responsible for assessing and enforcing cybersecurity requirements.

D8: Penalties Penalties refer to the existence and perceived role of sanctions or consequences for non-compliance. This dimension does not assess penalty amounts, but rather considers how enforcement mechanisms are structured to incentivize compliance and accountability.

D9: Crisis Management Crisis management addresses organizational preparedness for large-scale or systemic incidents that exceed routine incident handling. It includes escalation structures, coordination mechanisms, decision-making under crisis conditions, and alignment between technical response and strategic management.

D10: Oversight of ICT Providers This dimension captures mechanisms for overseeing criticalICTservice providers whose failure could have systemic impact. It focuses on monitoring, assessment, and control of providers that play a central role in supporting essential services, particularly where dependencies are concentrated. While similar to D4: Third-Party Risk Management, this dimension focusses on regulatory supervision of critical providers whose services support multiple organizations and whose disruption could have systemic consequences, compared to how D4 looks at how individual organizations assess and manage risks arising from their own suppliers and service providers.

4.1.2 Detailed Dimension Overlap Analysis

To support the comparative findings, a full analysis per dimension is included in Appendix A. As an example, the detailed analysis for one dimension is provided in Table 4.2. The full analysis provides a detailed breakdown of each regulatory dimension, structured by three aspects: objectives, requirements, and implementation. These form the basis for our overlap scores. The assessment in Table 4.2 is also used in the interview analysis and cross-sector insights discussed in the following sections.

Dimension	Cybersecurity- and ICT-Risk management
Overlap Level	Moderate (3)
Objectives	Both frameworks aim to manage and improve cybersecurity and ICT risk management to ensure the security of ICT systems and operational stability.
Requirements	NIS2 mandates a range of general cybersecurity measures across sectors, including continuous risk assessments, protection against cyber threats, and business continuity planning. Member States are permitted to adapt these requirements to their unique national risks. DORA's approach, however, is more prescriptive for ICT risk management in the financial sector, outlining specific protocols for protecting ICT infrastructure, continuity planning, and advanced resilience testing. Both frameworks emphasize cybersecurity, but DORA includes stricter measures and testing protocols in its documentation.
Implementation	NIS2 allows each member state flexibility to adapt cybersecurity measures according to local risks and critical infrastructure needs, whereas DORA requires specific cybersecurity protocols across the financial sector such as mandatory resilience testing.

Table 4.2: Detailed Dimension Analysis Example

4.1.3 Dimension Comparison

In Table 4.3 the main regulatory dimensions used in this comparative analysis are listed, outlining where each is addressed under NIS2 and DORA, and assigning a corresponding overlap score ranging from 1 (minimal) to 5 (full alignment), as described in Section 3.2. In Section 4.1.3, a summary for each dimension shows the analysis that supports the assigned overlap level.

Table 4.3: Overview of Key Comparative Dimensions between NIS2 and DORA

D#	Dimension Name	Chapter and Article in NIS2	Chapter and Article in DORA	Perceived Overlap
D1	Cybersecurity and ICT Risk Management	Ch. IV, Art. 18–21	Ch. II, Art. 5–16	3 (Moderate)
D2	Incident Reporting	Ch. IV, Art. 23	Ch. II, Art. 17	4 (High)
D3	Operational Resilience Testing	Ch. IV, Art. 20	Ch. II, Art. 21–22	3 (Moderate)
D4	Third-Party Risk Management	Ch. IV, Art. 21–22	Ch. III, Art. 28–31	3 (Moderate)
D5	Governance and Accountability	Ch. IV, Art. 20–21	Ch. II, Art. 5	5 (Full)
D6	Information Sharing	Ch. II–III, V, Art. 26	Ch. III, Art. 40	3 (Moderate)
D7	Supervision and Enforcement	Ch. II–III, VII, Art. 29–32	Ch. IV, Art. 42–48	2 (Low)
D8	Penalties	Ch. VII, Art. 31	Ch. IV, Art. 45	2 (Low)
D9	Crisis Management	Ch. V, Art. 25	Ch. II, Art. 15	2 (Low)
D10	Oversight of ICT Providers	Not explicitly covered	Ch. II, Art. 31–35	1 (Minimal)

Dimension Analysis Summaries

1. Cybersecurity and ICT Risk Management NIS2 mandates a range of general cybersecurity measures across sectors, including continuous risk assessments, protection against cyber threats, and business continuity planning. Member States are permitted to adapt these requirements to their unique national risks. DORA's approach, however, is more prescriptive for ICT risk management in the financial sector, outlining specific protocols for protecting ICT infrastructure, continuity planning, and advanced resilience testing. Both frameworks emphasize cybersecurity, but DORA includes stricter measures and testing protocols in its documentation.

2. Incident Reporting Requirements NIS2 applies broadly across critical infrastructure, emphasizing criteria such as the number of users affected, incident duration, geographical spread, and overall service disruption, with a goal of maintaining operational continuity in essential services across multiple sectors. In contrast, DORA focuses specifically on the financial sector, prioritizing factors that directly impact financial stability and market integrity, including the effect on critical financial functions, economic loss, reputational damage, and data confidentiality. NIS2 requires entities to report significant cybersecurity incidents within 24-72 hours to national authorities. The timeline and level of detail allow for flexibility across the varied sectors it covers. DORA mandates an initial report to financial regulators within 24 hours of an ICT incident, with detailed follow-up based on incident severity.

3. Operational Resilience Testing NIS2 mandates general testing of security measures and infrastructure resilience, providing entities across sectors with guidelines for regular assessments and audits. DORA goes further, requiring specific testing protocols such as TLPT for high-risk financial entities. This advanced testing simulates real-world cyber threats to identify vulnerabilities proactively, making DORA's approach far more rigorous in operational testing. NIS2's testing requirements are practical for its broader scope, while DORA's specialized protocols address the unique risks within financial markets. However, this might have to do with NIS2 being a broader directive which can be tightened by the affected Member States.

4. Third-Party Risk Management and Supply Chain Risk Management NIS2 requires entities to manage supply chain risks by assessing and securing their network systems against vulnerabilities from third-party providers, as well as having a deep understanding of their providers' supply chain and the risks that come with it. However, oversight of these providers remains with the entities themselves. DORA, in contrast, gives ESAs direct regulatory oversight of critical ICT service providers, such as cloud providers, when they are deemed essential to financial stability. The comparative benefit of DORA's approach is its ability to monitor and enforce resilience at the ICT provider level in finance, where disruptions could have cascading effects.

5. Governance and Accountability NIS2 mandates senior management and board-level accountability, requiring executives to prioritize cybersecurity within their organization's strategic planning. The aim is to ensure cybersecurity is an integral component of overall governance. DORA similarly requires senior management to be actively responsible for ICT resilience in financial institutions, with specific roles in overseeing risk management strategies and reporting incidents. Both frameworks foster a culture of accountability, but DORA's provisions are more prescriptive, emphasizing the importance of executive involvement in financial ICT security.

6. Information Sharing NIS2 encourages cross-sector information sharing through national coordination centers and cooperation with industry peers, with the goal of strengthening resilience across sectors. This promotes knowledge exchange and quick adaptation to emerging threats. DORA encourages information sharing within the financial sector specifically, creating networks where financial institutions share insights on cyber threats and vulnerabilities with each other and regulators. The scope of information sharing under NIS2 supports EU-wide resilience, while DORA's sector-specific sharing fosters quick adaptation to financial-sector threats.

7. Supervision and Enforcement Under NIS2, national competent authorities, most often CSIRTs, are responsible for supervision and enforcement, including audits, compliance checks, and, where necessary, penalties for non-compliance. DORA is enforced through ESAs, who ensure compliance across financial entities and impose penalties for non-compliance specific to the financial sector. This allows DORA to leverage sector expertise through ESAs, while NIS2's national-level supervision ensures enforcement is adapted to each member state's context

8. Penalties NIS2 allows for administrative fines up to €10 million or 2% of global turnover, enforced

by national authorities. This flexibility accommodates the wide variety of sectors under NIS2. DORA specifies penalties within the financial sector based on the severity of non-compliance, with ESAs empowered to impose targeted fines. While both frameworks include penalties for non-compliance, DORA's sector-specific penalties reflect the higher risk and interconnected nature of financial markets, where non-compliance could lead to systemic impacts.

9. Crisis Management and Coordination NIS2 includes crisis management provisions, including the EU-CyCLONe network for cross-border coordination during cyber incidents. This framework aims to ensure a cohesive EU response to significant threats across sectors. DORA's crisis management provisions focus on the continuity of financial market operations, with protocols designed to maintain stability and mitigate systemic risks. NIS2's EU-wide coordination is valuable for managing large-scale incidents, while DORA's crisis management structure supports stability in financial markets, where disruptions can have far-reaching effects.

10. Oversight of ICT Providers NIS2 does not provide direct oversight for third-party ICT providers; rather, it places the responsibility of managing third-party risk on the entities themselves. DORA, on the other hand, establishes direct oversight by ESAs for critical ICT providers within the financial sector. This allows ESAs to ensure that providers essential to financial resilience, such as cloud services, meet stringent security and operational standards. The oversight distinction is significant, as DORA's approach enables tighter control of critical service providers in finance, addressing the sector's unique vulnerability to ICT disruptions.

4.2 Interview results

The interviews of this research consist of two distinct parts. The first part is exploratory and aims to identify general challenges, implementation gaps, and perceptions regarding the effectiveness of DORA and NIS2 across their appointed sectors. Interview participants were invited to reflect on their experiences with regulatory compliance, cybersecurity risks, and sectoral preparedness and maturity. These insights helped contextualize the regulatory comparison and highlighted practical issues.

For the second part of the interview, we focus on validating a structured comparative analysis between DORA and NIS2. Participants were presented with the ten key analytical dimensions (as described earlier in this chapter, see table 4.3) and asked to provide feedback on the degree of overlap between the regulations, including commentary on requirements, implementation realities, and practical alignment. This validation helped refine the overlap assessments and allowed for the identification of areas of divergence, consensus, and interpretive ambiguity.

The interview results are presented in three subsections. Section 4.2.1 provides an overview of the interviewees and the structure of the data collected. Section 4.2.2 discusses the thematic findings from the exploratory phase of the interviews. Section 4.2.3 presents the validation of the dimension-based comparative analysis through expert feedback.

4.2.1 Overview

To support the comparative analysis of DORA and NIS2, a total of 9 expert interviews were conducted. A list with interviewee information can be found in Table 4.4. The interviewees came from different levels of expertise and backgrounds within the field of cybersecurity, including technical and non-technical consultants, managers, project leads, and partners. Their roles spanned both financial-sector organizations subject to DORA and broader critical infrastructure entities affected by NIS2. Participants were selected based on their practical experience with cybersecurity regulation and their involvement in implementing, advising on, or interpreting the requirements of DORA and/or NIS2. This provided a varied sample, capturing perspectives from both strategic and operational levels of regulatory engagement.

All interviews were transcribed and reviewed using the original audio recordings. The analysis focused on extracting responses to specific, predefined interview questions. Interviewee input was systematically organized under per question to allow for direct comparison, identification of recurring patterns, and observation of sector-specific differences.

As mentioned in section 3.3, interviewees were presented with six interview questions. All nine interviewees responded to each of the questions. In addition to the interview questions, participants were also asked to comment on the ten predefined dimensions that compare NIS2 and DORA. As described in

Interviewee	Role	Summary	Responded to Dimensions
R1	Consultant	Project management officer: reporting and team management	D1, D2, D5, D9
R2	Manager	Requirement manager for cyberdefence and incident response teams	D2, D3, D4, D5
R3	Consultant	Consultant in cyber strategy and risk.	D2, D4, D5
R4	Technical Consultant	OT cybersecurity consultant; works with cyber operations teams	D1, D3, D4, D9
R5	Sr. Technical Manager	Offensive security team lead. Focused on penetration testing	D3
R6	Sr. Manager	Senior manager in the cybersecurity team, works directly with clients	D2, D4, D6
R7	Sr. Consultant	Operational lead and manager of NIS2 programs	D3, D4, D5, D9, D10
R8	Partner	Partner level expertise. Works on stategic and governance aspects	D1, D3, D4
R9	Technical Partner	Technical lead for most NIS2 engagements. Manages large compliance programs	D2, D3, D4

Table 4.4: Interviewee roles, summaries, and response index

section 3.3, interviewees were asked to comment on the dimensions on which they felt most qualified to provide input. For each chosen dimension, they were invited to reflect on its formulation, the perceived overlap between the two frameworks, and any relevant observations or disagreements based on their experience.

4.2.2 Exploratory Interview Findings

This section presents the thematic findings from the exploratory part of the interviews. We analyzed recurring patterns, key observations, and divergent perspectives among the interviewees, and responses are grouped by interview question.

Compliance Management Approaches

Q1: *How do organizations manage NIS2 and DORA compliance?*

Interviewees described multiple approaches to managing compliance with NIS2 and DORA, largely dependent on sector, organizational maturity, and regulatory familiarity. In more mature organizations, compliance is typically managed through centralized governance structures and embedded within broader cybersecurity or enterprise risk management functions, particularly those under DORA. These entities often have dedicated compliance teams and formal programs, with support from cross-functional collaboration between legal, IT, and security departments.

According to the interviewees, a key distinction between organizations subject to DORA and those covered by NIS2 is that financial-sector entities are generally further along in formalizing compliance processes, often due to pre-existing obligations under frameworks such as the European Banking Authority [24] Guidelines on ICT and Security Risk Management or the De Nederlandsche Bank [14] Good Practice Guidelines. One interviewee noted that compliance with DORA is typically treated like any other regulatory program in finance: centralized, cross-domain, and well-resourced.

In contrast, many NIS2-covered entities are still in earlier stages. These organizations are often focused on interpreting the directive, conducting readiness or gap assessments, and determining whether they fall within scope. As R4 noted, "Many are still unsure if they are in scope for NIS2," which results in organizations prioritizing scoping analyses and readiness assessments before implementing structural governance changes. This is especially true for entities that were not previously covered under the 2016 NIS1 directive. Compliance obligations under NIS2 vary by sector and designation: some organizations can operate reactively using annual control cycles, while others must proactively demonstrate continuous

governance. Although all interviewees agreed on the importance of building structured compliance evidence early, most organizations seem to underestimate the effort and coordination required.

Several interviewees also highlighted the risk of fragmented approaches, especially in sectors where cybersecurity has not yet been integrated into the business strategy. In such organizations, compliance efforts often rely on individual initiative or ad hoc projects rather than systematic programs with sustained executive backing. This challenge was observed mostly in smaller financial organizations, and in the broader "non-finance" critical infrastructure landscape.

Consulting support plays a significant role across sectors. Most interviewees emphasized that many organizations actively seek external guidance not just for implementation but also to determine whether they are in scope of NIS2 or DORA. Uncertainty around which types of organizations the rules apply to, and how the regulations are being implemented in different countries was cited as one of the main reasons companies engage consultants. Regulatory pressure, combined with a lack of internal legal or cybersecurity expertise, often leads organizations to outsource gap assessments, scoping analyses, and the operational translation of regulatory texts into internal controls and procedures. Consultants seem to be vital in shaping the overall compliance strategy, especially in sectors where dedicated compliance capabilities are limited or absent.

Overall, the interviews indicate that while structured compliance management is emerging across both DORA and NIS2 contexts, significant variation remains. Financial institutions typically benefit from clearer governance models, established regulatory routines, and the dedication of additional resources. NIS2-covered entities, by contrast, are often still working toward building the foundational structures necessary to sustain long-term compliance, frequently with the help of external consultants.

DORA and NIS2 Implementation Challenges and Gaps

Q2: *What are the most significant challenges or gaps when implementing standards?*

The following challenges and gaps have been identified:

1. Scope Issues
2. International Unclarity
3. Complexity Challenges
4. Internal Obligations
5. Low Third Party Risk Management Oversight
6. Lack of Documentation
7. OT-Specific Challenges

Scope Issues Uncertainty on whether and how regulations apply is consistently described as one of the most disruptive challenges during implementation. For many organizations, particularly those under NIS2, it is unclear not only if they fall under the regulation but also to what degree different parts of their operations are affected. One interviewee highlighted how this ambiguity plays out in practice: a company producing both livestock feed and birdseed might find only the former classified as critical infrastructure, despite identical production processes. This kind of scope confusion where parts of a business may be in scope while others are not, raises complex legal and operational questions for which most organizations are currently ill-equipped. While still an issue, scoping criteria like this are less prevalent under DORA, where the cutoffs for which companies fall under the regulation are much more precise and refined.

International Unclarity The previously mentioned confusion is amplified for organizations operating across borders. Several interviewees noted that different interpretations of the regulation across EU Member States, combined with delayed or vague national implementations, make it difficult for companies to understand which standards apply to them and how. As a result, many organizations spend a long time in the scoping phase and take few concrete steps while waiting for clarity from their host countries that has yet to arrive. In turn, these countries deal with the diversity of businesses operating within a single country. Heavy industry to digital startups, each business has specific, complex, and varying operations. This makes it difficult to create rules that are both specific and widely applicable,

which further delays national implementation efforts and adds to the regulatory uncertainty felt by organizations. Some interviewees linked this directly to the political sensitivity of NIS2, which has led to lobbying and hesitation in finalizing guidance at the national level.

Complexity Challenges When organizations do recognize that they are likely in scope, many underestimate the depth and complexity of what is required. Several interviewees described how clients assumed that minor updates to existing policies would be sufficient to achieve compliance. In reality, both NIS2 and DORA demand broad improvements in areas such as documentation, supplier risk management, governance, and incident handling, to name a few. Many entities are not prepared for this scale of change, particularly those outside the financial sector or in OT-heavy environments where basic cybersecurity measures are not in place. A recurring theme is that organizations often fail to see themselves as "critical" and therefore delay taking ownership of regulatory obligations until forced by external parties or geopolitical events.

Internal Obligations Many organizations have not defined who is responsible for regulatory implementation, and in cases where responsibility is assigned, the role itself is often not well understood. CISOs are sometimes tasked with overseeing compliance in addition to their operational duties, but without executive-level support or formal governance processes, they may lack the mandate or resources to implement structural change. One interviewee mentioned that board members often remain disengaged, while CISOs become "trapped" by previous assurances of compliance made under outdated assumptions. Even in organizations that are aware of their obligations, misunderstanding the depth and nature of the required changes is common. Both DORA and NIS2 are frequently misread as "checklist" regulations, leading to superficial efforts that fail to address underlying security gaps. In practice, implementing these standards requires broad improvements in cybersecurity posture, and in many cases even the organization as a whole.

Low Third Party Risk Management Oversight Third-party risk management in particular is shown to be one of the most persistent and underdeveloped areas covered by NIS2 and DORA. Organizations routinely lack insight into their supplier ecosystems, particularly in terms of indirect or shared dependencies. As R2 explained, "Many organisations do not have a clear view of their own vendors or third-party dependencies," making it difficult to assess systemic exposure. Many struggle to define which vendors are critical, how to assess their security controls, or how to build audit mechanisms. This issue is mentioned in nearly every interview and is seen as especially problematic in NIS2-regulated sectors, where visibility into vendor networks is often low and oversight mechanisms are lacking, while being crucial to maintaining a robust and protected (digital) infrastructure.

Lack of Documentation While some companies have implemented security measures, many fail to formally document these practices, making it difficult to monitor, assess, or demonstrate compliance. On the one hand, DORA explicitly requires approved and traceable policies and procedures not just in practice, but on paper too. By contrast, NIS2's requirements are often too vague for organizations to know what is relevant to document. Interviewees noted that many organizations believe they are compliant because certain processes are being followed operationally, yet there is no structured evidence to prove this during audits or supervisory reviews. Common issues include undocumented risk assessments, missing mappings between policies and regulatory requirements, and a general lack of version-controlled documentation. One interviewee mentioned that even where testing or controls are in place, insufficient reporting and traceability undermine their effectiveness in a compliance context.

OT-Specific Challenges Challenges are even more pronounced in OT-heavy sectors, such as energy or manufacturing. These environments often operate with legacy systems, minimal cyber-hygiene, and rigid operational constraints that make the implementation of standard IT-based controls more difficult. For example, patching systems or deploying endpoint detection tools may not be possible due to continuous up-time requirements, proprietary hardware, or unsupported vendor platforms. Network segmentation is often lacking, and visibility into which assets are even connected to the environment is limited. This is further complicated by the sheer diversity of OT systems: a water treatment facility, an industrial bakery, and a gas distribution network may all fall under NIS2, yet their architectures, operational risks, and security needs are fundamentally different. Unlike in the financial sector where DORA can build on a relatively standardized landscape of transactions, data flows, andITsystems, cybersecurity in OT must

be tailored to highly specific technical and operational realities. In many cases, processes are governed more by safety and continuity concerns than by security principles. As a result, cybersecurity is often not embedded into broader business processes, and implementation efforts are either improvised or heavily reliant on external consultancy.

The Effectiveness of DORA and NIS2

Q3: *Do the standards effectively address the cybersecurity needs of critical infrastructure?*

Most interviewees agreed that DORA and NIS2 play a crucial role in raising cybersecurity standards across critical infrastructure sectors, but their actual effectiveness depends heavily on implementation. Both regulations were seen as necessary triggers that force organizations to take actions that they might not otherwise prioritize. As R2 noted, "The directive itself doesn't directly improve cybersecurity, it forces organizations to start thinking seriously about resilience, but effectiveness depends on moving from paper compliance to actual implementation." \gls{dora}'s requirements for formal documentation, traceability, and oversight were said to have driven visible improvements in cybersecurity maturity, especially in organizations that previously lacked structured policies or executive support.

While both NIS2 and DORA raise cybersecurity standards, NIS2's broad scope brings cybersecurity into sectors that have historically operated with minimal regulatory oversight, prompting organizations to systematically assess their risk posture for the first time. However, many interviewees also stressed that NIS2's language is vague and offers little practical guidance on implementation. Without further interpretation from national authorities or external consultants, organizations often struggle to translate its obligations into concrete controls and processes. This vagueness was seen both as a weakness and a potential strength: it allows Member States and organizations to adapt implementation to their sector-specific contexts, which may be necessary given the directive's cross-sector reach and to their national and cultural themes.

As stated earlier in this chapter (Section 4.2.2, page 33), the broad applicability of NIS2 creates challenges. In sectors unfamiliar with cybersecurity regulation, baseline maturity remains low. Several interviewees observed that many organizations only recently began to recognize their designation as "critical infrastructure." Third-party risk management and supply chain security continue to be major gaps, as does the protection of legacy or complex OT systems. Despite these weaknesses, the overall impact of both standards is framed positively. Interviewees consistently noted that without DORA or NIS2, many organizations would remain disengaged or under-invested in cybersecurity. Even partial compliance efforts, or initial steps such as scoping and documentation, were seen as significant improvements compared to prior inaction. Alignment with existing frameworks such as ISO 27001, NIST, and IEC 62443 was also highlighted as a strength, making the regulations more actionable for organizations that already follow international best practices.

Ultimately, the consensus was that the following of either regulation can not guarantee security outcomes, but both serve as effective levers to elevate cybersecurity on the organizational agenda. The key variable is whether companies move beyond formal compliance and commit to actual implementation, continuous testing, and risk-informed governance.

The Adaption of DORA Best Practices for enhancing NIS2 Implementation

Q4: *Can DORA best practices be effectively adapted to enhance NIS2 implementation?*

Most interviewees agreed that the best practices embedded in DORA, such as structured documentation, formalized testing, third-party risk oversight, and incident response procedures, offer valuable input for improving NIS2 implementation. These practices are not inherently tied to the financial sector and were often described as general cybersecurity principles that could benefit any organization usingITsystems. Activities such as logging, network segmentation, encryption, supply chain monitoring, and policy documentation are seen as widely applicable and beneficial across sectors.

However, nearly all respondents emphasized that a direct transfer of DORA requirements into NIS2 environments would be impractical. While DORA provides a highly structured compliance framework tailored to financial institutions, NIS2 covers a much broader and more diverse set of sectors, including many with OT-heavy environments such as manufacturing, water, energy, and food production. The operational constraints, system architectures, and baseline cybersecurity maturity in these sectors differ substantially from the financial sector. As R9 noted, "You can't apply financial-sector rules to a

power plant or a food processing company without completely rethinking the implementation for each organization individually." In the OT environments under NIS2 especially, prescriptive rules can be counterproductive. Systems are often highly specialized, subject to up-time constraints, and maintained by staff with little cybersecurity training. Several interviewees cautioned that while DORA's specificity is valuable in high-regulation, IT-dominant environments, it could be too rigid for OT contexts. In contrast, NIS2's vagueness was seen by some as a deliberate and necessary design choice, allowing Member States and organizations to adapt their implementation to sector-specific conditions. Yet, this flexibility also comes with a risk: without additional guidance or sector-specific translation, many NIS2-covered entities lack the tools to act on the regulation effectively.

The general consensus was that DORA best practices should be translated into sector-appropriate formats for NIS2. Rather than adopting strict rules, interviewees advocated for scalable expectations, lightweight templates, and maturity-based baselines. For example, simplified versions of DORA's incident classification logic, third-party oversight models, or accountability structures could help sectors unfamiliar with cybersecurity regulation take the first meaningful steps. This approach was seen as important for both smaller or less regulated industries, where formal governance and compliance cultures are not yet established, as well as for bigger and more mature companies that would fall under such a regulation's scope for the first time.

Crucial to this is that several interviewees also pointed out that failing to build on DORA's lessons would be a missed opportunity. The financial sector has already invested in processes and frameworks that could accelerate NIS2 readiness if adapted thoughtfully. From a policy perspective, this offers a more efficient path forward than building entirely new approaches from scratch.

Overall, DORA provides a strong foundation for cybersecurity best practices that can and should inform NIS2 implementation. However, effective use of this foundation depends on thoughtful adaptation. Without sector-specific tailoring, cultural awareness, and practical guidance, the benefits of cross-regulatory alignment risk being lost.

Recommendations for Improving Cross-Sector Knowledge Transfer of Cybersecurity Practices

Q5: *What recommendations do you have for enabling better transfer of cybersecurity best practices between sectors?*

As mentioned before, interviewees broadly agreed that regulations such as DORA and NIS2 have been crucial in initiating cybersecurity efforts across sectors, particularly where prior investment or urgency was lacking. However, while these frameworks elevate the topic to a strategic level, their actual implementation across diverse sectors remains uneven. A key takeaway was that transferring cybersecurity best practices, especially those developed in the financial sector, requires careful adaptation rather than direct replication.

Several participants stressed that many DORA-aligned practices, such as structured documentation, third-party risk assessments, and incident response planning, represent general cybersecurity maturity rather than finance-specific processes. These should be made available to other sectors through clear, step-by-step guidance. Recommendations included developing "playbooks" or implementation libraries that offer scalable templates, baseline expectations, and concrete examples. This applies especially to supplier analysis, contract language, testing programs, and escalation procedures. Such resources should account for varying levels of cybersecurity maturity, allowing sectors such as manufacturing, logistics, and healthcare to gradually adopt stronger practices without being overwhelmed by complexity or cost, and allowing them to implement practices where possible, depending on their sector.

Some interviewees also pointed to the need for cultural translation. Financial institutions operate within established compliance cultures, whereas many NIS2-covered organizations, particularly SME's or OT-heavy sectors, lack similar structures or experience. Simply importing DORA's structure may be ineffective unless its core principles are rephrased in sector-relevant language and supported by accessible training and awareness programs. The key is not just to share content but to ensure it is realistically implementable in their respective environments.

Suggestions also included expanding sector-specific working groups or ISACs (Information Sharing and Analysis Centers), which could act as platforms for cross-sector knowledge exchange. Interviewees suggested support from national authorities or regulators and have them serve as conduits for practical

information, such as real-life case studies, incident handling approaches, or lessons-learned from testing programs. One interviewee even proposed that regulators explicitly encourage organizations under NIS2 to study how financial-sector institutions manage third-party risks, crisis exercises, and resilience planning.

Finally, respondents emphasized the importance of standardizing and maintaining knowledge libraries that document successful practices from regulated sectors like finance. These libraries could be curated by experts familiar with both DORA and NIS2 and adapted into usable guidance for other sectors. While full alignment is neither expected nor desirable, structured knowledge transfer from high-maturity sectors was seen as a practical and efficient path toward national cybersecurity resilience. As R6 noted, "It would not be that hard to translate the DORAbest-practice library into NIS2, especially for someone who understands both frameworks," emphasizing that failing to build on financial-sector lessons would be inefficient.

The role of DORA and NIS2 in the protection of Critical Infrastructure

Q6: *What is your general perspective on protecting CI and the role of regulations in enhancing resilience?*

Answers to this question closely resembles those given in response to Q3, which focused on the effectiveness of DORAand NIS2. However, several nuances emerged here. While Q3 responses centered more on practical implementation and regulatory precision, interviewees addressing Q6 emphasized the broader role of regulation in driving strategic change, board-level engagement, and long-term resilience. The discussion shifted slightly from evaluating effectiveness towards recognizing regulation as an enabler of change of the organizational and societal views on cybersecurity, especially in sectors where the level of action has historically been lower.

Interviewees consistently emphasized that regulations such as NIS2 and DORA are essential to improving cybersecurity across Europe's critical infrastructure. While awareness of cyber threats has grown over the past decade, most participants observed that actual investments and changes tend to occur only when regulations demand them. Both DORA and NIS2 were seen as necessary triggers for action, providing the leverage cybersecurity professionals need to elevate the issue to the board level. Several respondents specifically noted that regulatory pressure has increased executive involvement, with board members now taking active responsibility for cybersecurity agendas.

Beyond awareness and accountability, the real value of regulation lies in converting intent into structured improvement. Interviewees stressed that resilience requires more than just policy creation: it depends on operational readiness, structured testing, and the formalization of processes such as incident handling, third-party oversight, and documentation. DORA was viewed as more effective in this respect, due to its specificity and stricter compliance culture. NIS2, in contrast, was seen as an important step forward in extending regulation to previously uncovered sectors, but was again criticized for being too vague. Several interviewees pointed out that the absence of a concrete scope list leaves organizations unsure whether and how the directive applies to them, which hinders confident implementation.

Despite these shortcomings, interviewees broadly agreed that regulation is the only viable path toward societal-scale cybersecurity resilience. Voluntary action remains limited and inconsistent, particularly in sectors with low baseline maturity or competing operational priorities. As R8 stated, "Many organizations would not have acted without regulatory pressure," underscoring the view that legal obligations are often the primary driver of meaningful cybersecurity investment. Although a few organizations do act proactively, most only begin to implement necessary improvements once compelled by legal obligations. For many, cybersecurity has shifted from being an optional technical concern to a matter of national and economic security, especially given recent geopolitical developments.

Some participants also cautioned that cyber regulation is still an immature legal domain, especially when compared to more established regulatory areas. The complexity and diversity of critical infrastructure sectors make it difficult to formulate rigid rules that apply equally across all environments. As such, the combination of regulation with adaptable guidance, sector-specific interpretation, and shared best practices was seen as the most realistic way to drive resilience without undermining flexibility.

While cost was raised as a barrier, the general consensus was that investment in cybersecurity should be treated as essential infrastructure spending. NIS2 and DORA may introduce short-term burdens, but they are widely seen as investments in long-term societal safety, continuity, and competitiveness.

4.2.3 Confirmatory Interview Results

This section presents the analysis of the second part of the interview, in which we asked participants to reflect on the comparative framework developed earlier in the study (see Table 4.3). Each of the ten regulatory dimensions were discussed with interviewees to validate, refine, or challenge the initial analysis of overlap and differences between DORA and NIS2. The responses provide insight into how practitioners perceive the relevance, clarity, and applicability of each dimension, as well as how the two regulatory frameworks may be leveraged in practice. Where appropriate, the results also highlight areas of divergence or ambiguity that require further attention in policy or implementation.

Because interviewees were asked to answer according to their expertise, some dimensions received more attention than others during the confirmatory interviews. The following table shows the number of interviewees who responded to each dimension-specific question:

Table 4.5: Interviewee Response per Dimension

#	**Dimension**	**Responses**
D1	Cybersecurity Risk Management and ICT Risk Management	3
D2	Incident Reporting	5
D3	Operational Resilience Testing	6
D4	Third-Party Risk Management	7
D5	Governance and Accountability	4
D6	Information Sharing	1
D7	Supervision and Enforcement	0
D8	Penalties	0
D9	Crisis Management	3
D10	Oversight of ICT Providers	1

Legend: 0 1 3 4 5 6 7 = number of interviewees who commented on that dimension.

As shown in the response overview above, no interview responses were recorded for Dimensions D7 (Supervision and Enforcement) and D8 (Penalties). This reflects a conscious trade-off made during the interview design phase: by focusing on the dimensions most relevant to the daily practices of interviewees, more time was spent on topics that took priority over others. This absence of responses does not necessarily indicate a lack of relevance but rather highlights the relatively higher level of interest in other dimensions in both the regulations themselves and expert reflections. Because of this, these two dimensions are excluded from the analysis section below.

D1. Cybersecurity Risk Management and ICT Risk Management

When discussing the first dimension, DORA was described as more prescriptive and structured, requiring detailed documentation of procedures, controls, and responsibilities, particularly tailored to financial-sector ICT environments. In contrast, NIS2 was seen as broader in scope and less specific in its requirements, which allows it to be interpreted differently on national and sector-level when needed. This flexibility, while useful in adapting to local contexts, was also described as a source of fragmentation and complexity, particularly for organizations operating across multiple jurisdictions.

Every interviewee emphasized the importance of cybersecurity risk management as a regulatory dimension, noting that fundamental controls such as backups, user access management, and multi-factor authentication are still missing in many critical infrastructure sectors. One participant noted that "cyber hygiene" is often lacking outside the financial sector, not due to unwillingness but due to gaps in awareness, maturity, and regulatory pressure. The discrepancy between DORA's structured approach and NIS2's interpretive model was seen as a reflection of these broader maturity differences across sectors.

Several interviewees pointed out that even within NIS2 implementation, regulatory language varies substantially between Member States, complicating risk management for cross-border entities. While many core risk management principles are reusable across borders, one interviewee estimated that while a large portion of an 'average' risk management framework can be reused across borders, around 20% of controls or processes still require adaptation to local regulatory expectations.

Overall, the responses supported the idea that DORA's risk management provisions can serve as a

baseline of best practices, though their direct application under NIS2 requires sector- and jurisdiction-specific translation.

D2. Incident Reporting

Similar to D1, practitioners emphasized a contrast between DORA's structured incident reporting regime and NIS2's more flexible, interpretive approach. DORA was described as significantly more prescriptive, requiring strict timelines, structured templates, and formal procedures. Interviewees again noted that this level of precision allows for more consistent implementation, clearer benchmarking of maturity, and better auditability. By contrast, NIS2 was seen as more flexible but also more ambiguous. While it does require phased reporting, (initial notification within 24 hours, a follow-up within 72 hours, and a final report within one month) several respondents observed that these stages are often not clearly understood or uniformly applied across Member States.

Multiple participants emphasized that incident reporting serves a broader purpose than regulatory compliance. It is intended to support coordination between organizations and CSIRTs, facilitate cross-sector information sharing, and enable faster mitigation of systemic risk. Some interviewees felt that this enabling function was underemphasized in both practice and policy discussions. They also suggested the comparison report they were presented could better reflect this goal.

A key refinement emerged regarding NIS2's scope. One interviewee stressed that NIS2 reporting is not limited to cybersecurity breaches but includes any digital incident that disrupts the delivery of critical services. This broader framing requires more emphasis, especially given the directive's applicability beyond traditional cyber events. As such, definitions of "critical" services and appropriate reporting thresholds were viewed as essential to the succes of NIS2, but still inconsistently implemented.

Overall, the interview results support the comparative analysis while suggesting greater clarity is needed in articulating NIS2's phased structure, its broader scope beyond cyber incidents, and the operational purpose behind reporting requirements. Respondents generally agreed that DORA represents a more mature and structured model, though several noted that its rigor may not be appropriate for all sectors when it comes to incident reporting.

D3. Operational Resilience Testing

Interviewees unanimously emphasized that DORA provides a significantly stronger and more actionable foundation for operational resilience testing compared to NIS2. DORA's requirements were described as formalized, prescriptive, and well-structured: particularly through its testing model which allows tests to be proportional to each institution (smaller, lessITheavy institutions might not require the same level of testing as larger, moreITheavy ones). Several interviewees highlighted how this model avoids a one-size-fits-all approach by classifying entities such as Critically Important Financial Institutions (CIFIs), and tailoring obligations accordingly.

While NIS2 nominally calls for testing through Article 21, respondents noted that it lacks both concrete criteria and enforcement mechanisms. This vagueness was not seen as neutral. Several interviewees argued that it allows for superficial testing or procedural checklists that do little to build genuine resilience. Some interviewees framed this as a missed opportunity, especially since real-world, scenario-based testing such as OT penetration tests or red-teaming is essential for uncovering hidden or easy to miss vulnerabilities. Without structured requirements, many organizations might conduct low-value exercises that create the appearance of compliance without actually improving preparedness. In contrast, some interviewees argued that NIS2's flexibility could be useful. A few respondents acknowledged that flexible interpretation allows for sector-specific adaptation, particularly in operational technology environments. However, even these interviewees stressed that flexibility should not preclude accountability or quality standards. One participant noted that while technical contexts may differ between IT and OT, the underlying principles of structured testing, scenario planning, and measurable outcomes remain broadly applicable.

One interviewee specifically pointed out that Threat-Led Penetration Testing (TLPT) under DORA applies only to a subset of entities classified as critical or systemically important. This testing requirement is not imposed on all financial sector organizations by default. Instead, TLPT obligations are determined by the competent supervisory authorities based on several criteria, such as the entity's size, complexity, and the potential impact on financial stability in the event of a disruption.

Overall, the responses confirmed that DORA sets a much clearer standard for operational resilience testing. Interviewees strongly recommended that NIS2 draw from this model to develop principle-based, enforceable testing requirements, particularly given the growing threat landscape and the risk posed by critical infrastructure vulnerabilities.

D4. Third-Party Risk Management

Interviewees were again in strong agreement that DORA offers a much more prescriptive and enforceable approach to third-party risk management (TPRM) than NIS2. DORA requires financial entities to maintain detailed registers of third-party ICT service providers, implement oversight mechanisms, classify providers by criticality, and share this information with supervisory authorities. This structured approach was consistently praised for not only requiring action but also ensuring follow-up through regulatory scrutiny. Supervisors such as De Nederlandsche Bank (DNB) were mentioned as actively reviewing TPRM documentation, turning the obligation into a concrete, monitored process.

By contrast, NIS2 was described as vague and high-level, leaving organizations responsible for defining their own supplier scope, risk classification, and contractual safeguards. Several interviewees stressed that this lack of specificity makes effective implementation challenging, particularly in sectors without prior regulatory exposure. While NIS2 includes the expectation that critical entities manage supply chain risks, it does not outline how this should be done. As a result, many organizations default to assessments such as ISO certifications, without deeper analysis or meaningful supplier engagement.

A recurring theme was the risk of shared dependencies. For both NIS2 and DORA, interviewees noted that critical entities across different sectors often rely on the same cloud, telecommunication, or software providers. DORA attempts to address this through coordinated supervisory assessments of concentration risk, whereas NIS2 leaves such systemic issues largely unaddressed. One interviewee warned that this represents a significant gap in national cyber resilience, particularly in the face of state-level threats or targeted supply chain attacks.

Some respondents questioned how NIS2's third-party reporting obligations will function in practice, given the absence of enforcement mechanisms or uniform guidance. While the intent is widely supported, interviewees were skeptical on wether organizations would implement robust controls without clearer expectations or supervisory follow-up.

Overall, the feedback strongly confirmed the presented comparative analysis. Several interviewees recommended clarifying that many of the mechanisms described under NIS2 reflect best practices rather than formal requirements. DORA's supervisory enforcement and detailed expectations were seen not just as more mature but as essential for managing the real-world complexity of modern supply chains. Many agreed that NIS2 would benefit from adopting more structured and enforceable practices based on the DORA model, particularly as cross-sector dependencies and geopolitical risks continue to grow.

D5. Governance and Accountability

Interviewees strongly agreed that both NIS2 and DORA elevate cybersecurity from a technical matter to a strategic board-level responsibility. This dimension was described as one of the most aligned between the two frameworks, with both mandating active involvement from senior management and clearly defining roles, responsibilities, and oversight functions. The analysis was broadly validated, with no major points of divergence reported.

One area of emphasis was the mandatory training obligation for management under NIS2, particularly as implemented in the Netherlands. Interviewees noted that management-level staff must complete cybersecurity training: a compliance requirement that was seen as especially relevant in demonstrating sustained board engagement. While DORA does not explicitly mandate training, it was acknowledged to embed governance more structurally through instruments like the Operational Resilience Strategy, which lays out formal responsibilities, accountability lines, and escalation procedures.

Respondents described NIS2 as promoting a "culture of accountability" through high-level requirements and broader applicability across sectors, while DORA achieves a similar outcome via prescriptive internal frameworks and regulatory supervision. The presence of penalties tied to senior management failure was cited as further evidence that DORA treats governance as a critical issue.

Overall, the responses confirmed that this dimension is one of clear overlap. Both frameworks send a strong signal that cybersecurity must be integrated into enterprise risk management, with visible, accountable leadership and documented governance practices. The distinction lies more in structure and enforceability than in objective, with DORA offering greater procedural formalization and NIS2 relying more on sectoral implementation and national adaptation.

D6. Information Sharing

Interview feedback on information sharing was limited, but the responses received support the original analysis. Both DORA and NIS2 promote the exchange of threat intelligence and cybersecurity information, yet interviewees saw DORA's model as more mature and structured, particularly due to its integration with the ESAs and established networks within the financial sector. In contrast, NIS2's reliance on national coordination centers was seen as less clearly defined and more variable across Member States.

Sectoral culture was noted as a critical factor. Financial institutions, shaped by longstanding regulatory cooperation, were described as being more accustomed to structured collaboration. In comparison, NIS2-covered sectors such as energy, healthcare, and manufacturing may hesitate to share information due to liability concerns, reputational risks, or perceived competitive disadvantages. These cultural and institutional differences were said to significantly influence how information sharing is implemented in practice.

The limited number of responses was also telling. Information sharing remains a "soft" obligation, especially under NIS2, where enforcement and practical mechanisms are still emerging. Compared to areas such as third-party risk management or incident reporting, information sharing might be less defined, less prioritized, and harder to operationalize, contributing to its relatively low visibility in implementation discussions.

D9. Crisis Management

Interviewees generally agreed that while both DORA and NIS2 address crisis management, they do so in distinct ways. Their goals, such as resilience, continuity, and recovery, are largely aligned, but the underlying mechanisms and implementation strategies differ significantly.

Under NIS2, crisis management is primarily internal and entity-specific. It focuses on preparedness through business continuity plans, disaster recovery measures, and crisis response protocols, interviewees specifically pointed at requirements like Article 21, which states that: *"Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems [...] including at least: [...] (c) business continuity, such as backup management and disaster recovery, and crisis management;"* This structure emphasizes the individual organization's ability to remain operational and recover independently following a disruption.

In contrast, DORA frames crisis management in terms of sector-wide coordination, especially within the financial system. It prioritizes collective resilience through cross-entity response strategies, information sharing, and coordinated supervisory oversight. The goal is not just to safeguard individual institutions but to preserve overall financial stability in the face of systemic risks.

While the goals of both frameworks align, interviewees hesitated to describe their implementation as directly overlapping. The entity-level approach in NIS2 makes it highly dependent on an organization's internal maturity and risk posture. DORA, by comparison, leverages a governance infrastructure that enables harmonized response across the sector, reducing fragmentation during crisis events.

One interviewee summarized this distinction by noting that "NIS2 tells each company to be ready for a crisis, while DORA sets rules for how the sector as a whole responds." The result is a shared direction but different pathways: a high-level alignment in intent, but divergent tools and scopes in practice.

D10. Oversight of ICT Providers

Dimension 10 received only one response. The response received for this dimension supports the distinction between DORA and NIS2 in their treatment of ICT provider oversight. The interviewee confirmed that DORA establishes far stronger and more explicit obligations, particularly through its emphasis on

contractual accountability and regulatory scrutiny of critical third-party ICT service providers. DORA enables financial supervisors to maintain visibility into key outsourced functions and requires firms to assess, manage, and formally report on their reliance on these providers.

In contrast, NIS2 does not offer equivalent supervisory mechanisms. While it acknowledges the importance of supply chain risk and calls for coordinated assessments, the directive leaves oversight and enforcement largely to the entities themselves. The interviewee suggested that NIS2's treatment of ICT provider risk is indirect, placing responsibility on organizations without embedding it into a structured regulatory framework. As a result, DORA was seen as more demanding and enforceable in this domain, despite some thematic overlap.

This dimension is closely related to the broader topic of third-party risk management, and the limited response may reflect this overlap. Many of the core issues such as supplier classification, risk concentration, and regulatory involvement are already covered under TPRM, possibly leading interviewees to prioritize their input there. This topic was retained as a separate dimension in the analysis due to its distinct regulatory framing, especially under DORA. The regulation treats ICT provider oversight as a standalone issue with specific provisions for supervisory engagement, including the potential for direct oversight of critical ICT third-party providers.

Chapter 5

Discussion

In this chapter, we contextualize the results of the research, connect them to one another, and relate them to the literature. Following this, we provide an interpretation and appreciation of the relevance and impact of the results. Lastly, we discuss the limitations of our research.

5.1 Interpretation and Synthesis

In this section, we summarize how our findings relate to each other and their practical applications. We answer the research questions and present our interpretation of the collected data.

5.1.1 Interview findings and results

Overall, our results confirm the central propositions we formulated at the beginning of this research (Ch. 1.1, 1.2, 2). Our study hypothesized that the financial sector, with its long-standing regulatory exposure and the prescriptive nature of DORA, possesses a relatively high level of cybersecurity maturity. Certain practices developed under this way of operation can be meaningfully adapted to strengthen the implementation of NIS2 in other critical infrastructure sectors. Both the comparative analysis and the interviews support this assumption with different explanations.

First, the comparative mapping across the ten regulatory dimensions, as described in Chapter 4 and Table 4.3, revealed that NIS2 and DORA share a high degree of alignment in their overall objectives and structural themes. While differing per dimension, this overlap supports the original idea that the practices resulting from the usage of DORA can serve as an interpretive and operational model for NIS2 entities. The practices bound to DORA can help translate NIS2's broader principles into more concrete implementation steps. At the same time, the results from the analysis confirm that DORAremains more specific in its requirements and oversight mechanisms. The findings reinforce the expectation that DORAprovides a "maturity benchmark" rather than a directly transferable blueprint.

Second, the expert interviews revealed broad agreement that the financial sector's structured approach to IT risk management, resilience testing, and third party oversight provides valuable lessons for less mature sectors. Interviewees consistently emphasized that adaptations of practices such as continuous testing, predefined reporting structures and rules, and supervisory accountability could accelerate NIS2 readiness for companies that are new to its scope if adapted in proportion and to the context in which they are used. However, they also highlighted contextual constraints for companies in critical infrastructure that limit one-to-one transferability, such as resource imbalance, OT dependencies, and different (supervisory) cultures. These nuances reinforce the idea that the real value of cross-sector learning lies less in replicating the rules from DORA's regulatory text and the exact practices that companies in the financial sector apply, and more in applying its principles with nuance.

The results indicate that while the maturity of the financial sector can help strengthen broader EU cyber resilience policy, a transfer of practices would require sector-specific tailoring. DORA's strength mostly lies in its oversight, enforcement, and clear description of its requirements. Combine this with the inherent cyber maturity of the financial sector, and the result could prove to be very strong in practice. In contrast, NIS2is deliberately flexible and leaves many parts to the interpretation of EU

member states and individual sectors. The findings confirm that cross-sector learning is feasible, but effective adaptation depends on translating the prescriptive financial-sector models and best practices into proportionate, context-aware guidance for the other domains.

5.1.2 Dimension Overlap Interpretation

The comparative analysis across the ten dimensions from Section 4.1.1 shows that DORA and NIS2 are conceptually aligned but differ noticeably in their levels of specificity, enforcement structures, and intended maturity levels. This distinction lies at the heart of how the overlap should be interpreted. High overlap does not imply that DORA can simply be copied into NIS2 environments, but rather that both frameworks share common objectives that can be approached through different regulatory methods. The overlap analysis provides insight into where cross-sector learning is feasible, where it requires more sector-specific adaptation, and what forms of maturity transfer are realistic.

Across most dimensions, the analysis revealed a strong conceptual alignment but partial implementation overlap. Particularly, D1: ICT Risk Management, D2: Incident Reporting, D4: Third Party Risk Management, and D5: Governance and Accountability stood out as dimensions that align in the goals they pursue but differ in their methods. We believe this reflects the intended design of both frameworks: NIS2 establishes broad, outcome oriented obligations, while DORA translates similar objectives into prescriptive, supervised operational requirements. In other words, the overlap is strongest in "what" the regulations want to achieve, and weakest in the "how" they are expected to achieve it. This seems to confirm the interpretation that DORA offers a more structured operational pathway for implementing NIS2's broader requirements rather than functioning as a competing or contradictory framework.

The interviews reinforce this view. Interviewees consistently recognized the similarity in regulatory intent and noted that DORA's detailed requirements provide a level of clarity that many NIS2-covered sectors currently lack. Interviewees described DORA as a source of knowledge that can be useful for sectors that currently have a lower cybersecurity maturity level. This sentiment is particularly applicable to dimensions where there was a high overlap in intent, such as D2: Incident Handling, D4: ICT Risk Management, and D5: Governance. In these sectors, the approach that the financial sector maintains towards cybersecurity is seen as directly useful for translating NIS2's general mandates into more concrete processes.

At the same time, the dimensions with lower overlap such as D7: Supervision & Enforcement, D8: Penalties and certain aspects of D10: Oversight of ICT Providers highlight the regulatory and structural boundaries of cross-sector transferability. These differences are not maturity gaps but they are different by design. DORA's enforcement is centralized through European Supervisory Authorities, while NIS2 relies on national implementation and decentralized competent authorities. The interview results support this: they show that NIS2 enforcement diversity complicates the adoption of more "DORA-esque" supervisory mechanisms, particularly for sectors heavily dependent on OT or characterized by fragmented ownership structures. In addition, certain parts of NIS2 seem to have been left vague on purpose so that countries can fill in the requirements as they see fit, and in a way that best fits each individual, complicated landscape of companies, culture, and geopolitical standing.

Taken together, the dimension overlap analysis shows that the value of DORA related practices from the financial sector for NIS2 implementation lies primarily in the operationalization of cybersecurity practices. High-overlap dimensions signal where structural practices such as continuous resilience testing, more standardized incident handling methods, or third-party oversight with additional detail may be effectively adapted by entities which are subject to NIS2. Low-overlap dimensions indicate where cross-sector transfer options reach their limit, and where NIS2's inherit "vagueness" intentionally diverges from DORA's financial-sector specificity.

Overall, the overlap interpretation seems to confirm that cross-sector learning between entities subject to DORA and NIS2 is not only possible, but beneficial. However, it also clarifies that effective transfer requires proportionality and contextualization of practices, not replication. The formulated and reviewed dimensions can therefore serve as a map of alignment, and as a guide to show where adaptation is possible or beneficial.

5.2 Relevance

In this section, we discuss the ways in which our study contributes to the regulatory learning body and to the existing literature.

5.2.1 Academic Contribution

The study contributes to the academic discourse on EU cybersecurity regulation by addressing the relationship of sector-specific and cross-sector regulatory frameworks. While other literature has examined DORA and NIS2 individually, the interaction between the two has received limited attention, particularly regarding the transferability and maturity of practices across different sectors. Ruohonen [59] explicitly identifies the interplay between DORA and NIS2 as an underdeveloped research area, both conceptually and empirically [59] [60]. Existing studies typically examine these frameworks in isolation or compare them horizontally with other instruments at the same regulatory layer (e.g., NIS2 and the Cyber Resilience Act as shown by Eckhardt and Kotovskaia [18]). We provide a systematic analysis of vertical regulatory transferability: how a more prescriptive and sector-specific regulation such as DORA and the practices related to it can inform the implementation of a broader, cross-sector directive like NIS2 and the entities affected by it.

Our findings support and extend several themes from prior research. They reinforce observations from the GDPR adoption literature such as Machado et al. [54] and Almeida Teixeira et al. [3], which highlight that regulatory effectiveness depends not merely on legal requirements but on organizational capacity, available expertise, and the maturity of underlying processes. Interviewees in our study also noted these patterns: the challenges seen at organizations outside the financial sector are not because of the lack of clarity in NIS2, but because the baseline cybersecurity and governance structures in these organizations are less mature. This similarly suggests that lessons from privacy regulation adoption translate into cybersecurity governance more broadly.

The analysis also connects with research on NIS to NIS2 evolution. Studies such as those by Vandezande [70] and Schmitz-Berndt [62] show how ambiguity, inconsistent national interpretations, and low reporting volumes, led the EU to draft a more prescriptive framework. This thesis builds on that narrative by showing that NIS2's improved structure still leaves operational ambiguity for less mature sectors, which is where DORA's prescriptive approach may provide value. The findings suggest that NIS2's evolution mirrors earlier regulatory learning, and that cross-sector learning from DORA could act as the net iteration of that learning process.

Additionally, the results resonate with empirical work on DORA readiness, particularly Kos [51], who found that even well-resourced financial institutions struggle to translate DORA requirements into operational practice without external expertise and structured frameworks. Our study extends those insights by demonstrating that such implementation challenges are magnified in non-financial critical infrastructure sectors.

Finally, our work applies a dimension-based manual mapping approach, as advocated by Mussmann et al. [56], to compare cybersecurity frameworks that differ in both structure and maturity level. By validating the mapping with expert interviews, our study illustrates how manual mapping, when combined with expert perspectives, reveals differences and similarities that are not visible from the regulatory text alone.

5.2.2 Practical Contribution

This study offers several insights for organizations, consultants and regulators involved in implementing NIS2 and DORA, particularly in secors with lower baseline security maturity. Our findings translate the high-level objective of "leveraging financial-sector maturity" into specific observations, pitfalls and patterns that can inform framework or best-practice implementation efforts in the rest of our critical infrastructure.

The results from our interviews results provide a clear picture of how compliance management currently differs between DORA-regulated entities and those covered by NIS2. Financial institutions tend to manage DORA compliance through more centralized, better-resourced governance structures that are generally more integrated into broader risk and security functions. They are often able to build on pre-existing frameworks such as EBA guidelines or existing best practices. By contrast, many entities which fall under NIS2 are still trying to understand the exact requirements to being "NIS2 ready". They are in

the early stages of scoping, interpretation, and basic readiness assessments. They frequently lack defined responsibility rules or compliance routines. This contrast could offer practitioners a maturity benchmark: let entities which are less mature and are inexperienced with falling under scope of a regulation like NIS2 learn from companies which, while dealing with some of the same clarity problems with DORA, have proven to be more experienced with being "cybersecurity-regulation-ready". The financial sector's style of compliancy can serve as a reference model for entities which are trying to move away from fragmented, ad-hoc approaches.

Our study also finds a set of recurring implementation challenges for organizations and advisors. Scope uncertainty, underestimation of regulatory complexity, unclear internal responsibilities, weak third-party risk management, poor documentation, and OT-specific constraints emerged as consistent pain points across our interviews. Our results show how these points manifest in practice. For example, entities stuck in prolonged scoping phases, CISO's carrying responsibilties without mandate, or OT-environments where standardITcontrols are not realistic. These examples makes our findings directly usable as a tool where other organizations can see which areas they are most likely to be facing challenges, or where they might have to invest first to reach compliance.

In addition to showing differences and challenges, our study also clarifies how DORA-aligned practices can practically support NIS2 implementation efforts, without suggesting what we have found to be an unrealistic one-to-one transfer. The results from the interviews found that many DORA practices such as structured documentation, formalized testing, third-party oversight and incident response procedures, embody general cybersecurity maturity that would benefit any critical infrastructure provider. At the same time, interviewees warned that directly imposing DORA's specificity on certain sectors, specifically those with OT-heavy or resource-constrained sectors would be counterproductive. The practical takeaway is that the practices used by the financial sector under DORA should be used as a source of information, not as a template. Scaled-down incident classification schemes, simplified supplier oversight models and lightweight governance structures could be derived from financial–sector practice and adapted to the sector specific constraints and differing maturity level of other critical entities. Concrete mechanisms include sector-tailored playbooks and implementation libraries, scalable templates for supplier analysis and testing programs, culturally adapted training and awareness materials, and the expansion of ISAC's or similar structures as platforms for sharing case studies and lessons learned.

5.2.3 Policy Implications

While both DORAand NIS2aim to raise the cybersecurity baseline across critical infrastructure, the results show that the gap between regulatory intent and practical implementation remains substantial. The interviews highlight that without clearer guidance, sector-specific interpretation, and more consistent supervisory approaches, many NIS2-covered entities struggle to operationalize the directive. This suggests that regulators may need to adopt more active, structured support mechanisms to ensure the directive's goals translate into real improvements in resilience. Our findings carry several implications for policymakers, regulators, and national authorities responsible for the implementation and enforcement of NIS2.

While NIS2's flexibility is intentionally designed to accommodate sector diversity, it also creates ambiguity that slows implementation. This seems to have to do mostly with scoping, documentation expectations and governance responsibilities. Several interviewees stressed that DORA's prescriptiveness in for example incident classification, documentation requirements and third-party oversight provides a certain clarity that is currently missing for many new NIS2 entities. Regulators could consider introducing additional and optional but detailed reference guidance, mirroring DORA's structured approach for sectors or organization types that benefit from clearer expectations. In relation to this, the findings point to a need for greater supervisory consistency across EU member states. differences in national timelines and different interpretations of NIS2create uncertainty. This delays compliance and undermines the directive's objective of reducing fragmentation. Regulators should consider adapting more centralized oversight options, similar to how DORA uses their ESAs for guidance. The adoption of more harmonized supervisory playbooks or coordinated guidelines through the NIS Cooperation Group or EU-CyCLONe, for example, could help narrow the interpretive gap between member states.

Another smaller, but prevalent finding is that sector-specific support for OT environments could hold value. OT-heavy environments face fundamentally different constraints than IT-dominated sectors. Directly transplanting DORA-like controls into OT-heavy sectors such as energy, water, manufacturing,

would be both unrealistic and disruptive. Instead, regulators could prioritize developing OT-focused interpretations of NIS2 requirements. While specific solutions lie outside the scope of this research, a starting point could be guidance on compensating controls, uptime-constrained environments, and legacy systems.

Finally, the interviews indicate that regulation alone is insufficient to ensure meaningful progress. Several participants argued that shared knowledge infrastructures (sector ISACs, public-private working groups, curated best-practice libraries, and regulator-led training) play a crucial role. Policymakers could consider formalizing such mechanisms as part of national NIS2 implementation strategies, particularly for smaller organizations or sectors with low cybersecurity maturity. These collaborative structures can accelerate learning, reduce duplication of effort, and support organizations in interpreting regulatory expectations in a practical, context-appropriate way.

5.3 Limitations

Methodological and Data Collection There are methodological constraints inherent in the study design and data collection. Allowing interviewees to select the regulatory dimensions they wished to discuss offered depth but led to imbalanced coverage, with dimensions D7: Supervision and Enforcement, and D8: Penalties, receiving no input. In addition, presenting the comparative overlap framework during the interviews may have shaped respondents' interpretations, because of the formatting of the framework and its contents. The interviews were conducted in different languages, which introduces a risk of different meaning or interpretation. The manual mapping of regulatory dimensions was transparent and validated by experts but remains partly subjective, and the fact that the study was conducted by a single researcher means a certain level of bias exists. Finally, expert perceptions may over- or understate organizational maturity levels, challenges, or timelines, which is inherent to the subjectivity of interview-based research.

Sampling and Participants The participant sample introduces limitations. Many interviewees were associated with the same organization or consulting environment, which may over-represent certain interpretations or perspectives. Respondents were already familiar with NIS2 and DORA, meaning the sample may skew toward more mature or aware organizations, and thus may not fully represent entities with lower baseline compliance readiness. The number of participants (N=9) supports analytical but not statistical generalization. The study's geographic and cultural scope is largely limited to the EU, which is to be expected when focusing on EU regulations, with a concentration in Western Europe. This may reduce the transferability of findings to Member States with different supervisory cultures or resource constraints, or for countries outside of the EU which deal with different regulations.

Regulatory and Temporal Context Both NIS2 and DORA were still undergoing implementation and refinement during the research period, with technical standards, national transpositions, and supervisory expectations still changing. As a result, some perceived "gaps" or ambiguities identified by interviewees may already have been clarified by updated versions or by Member State updates. The findings reflect a pre-enforcement snapshot of regulatory understanding, which may differ from how the frameworks are used once supervisory mechanisms and sector-specific interpretations mature.

Scope and Analytical Boundaries Lastly, the study's analytical scope has some boundaries on the conclusions that can be drawn. The findings primarily reflect Dutch and EU practice and may not map directly to all Member States. The analysis focuses specifically on NIS2 and DORA and does not examine the interplay with adjacent frameworks such as the Cyber Resilience Act, GDPR, or national sector-specific regimes.

Chapter 6

Conclusions

We conclude our research with a summary of the main findings and their implications for both research and practice. This chapter revisits the central objective of the thesis, provides direct answers to the research questions, and reflects on the broader relevance of the results. It further outlines practical recommendations for organizations and policymakers involved in NIS2 implementation and identifies avenues for future research, building on the limitations and insights of this study.

6.1 Summary

We investigated whether and how cybersecurity practices developed under the Digital Operational Resilience Act (DORA) in the financial sector can inform and support the implementation of the Network and Information Systems Directive 2 (NIS2) in other critical infrastructure sectors. The study combined a structured comparative analysis of both regulatory frameworks across ten key dimensions with expert interviews involving professionals from financial and non-financial critical infrastructure sectors.

The results show that while DORA and NIS2 differ in scope, prescriptiveness, and supervisory structure, there is substantial thematic overlap between the two. Financial-sector practices shaped by DORA demonstrate a higher level of operational maturity, particularly in areas such as ICT risk management, operational resilience testing, and third-party risk management. At the same time, the findings indicate that these practices cannot be transferred one-to-one to NIS2-regulated sectors, due to differences in sector maturity, organizational context, and national implementation.

Rather than proposing new regulatory frameworks, this study contributes by identifying where structured practices from the financial sector can be adapted to support NIS2 implementation, and by clarifying the conditions under which such transfer is considered feasible and useful.

6.2 Answers to the research questions

RQ.1 *How can cybersecurity practices developed under DORA in the financial sector be leveraged to improve cybersecurity maturity and regulatory compliance in other critical infrastructure sectors subject to NIS2?*

The results from our research indicate that cybersecurity practices developed under DORAcan be leveraged as implementation reference points rather than as direct compliance templates for NIS2. When translated into sector-appropriate and proportional formats, specific practices found in DORAcan help NIS2-regulated organizations interpret high-level obligations, prioritize investments, and structure their internal governance. We conclude that DORAserves best as a maturity benchmark and implementation guide, not as a one-to-one compliance model.

RQ.2 *What are the key similarities and differences between DORA and NIS2 across core regulatory dimensions?*

Through our comparative analysis we found that DORA and NIS2 address largely overlapping themes. Across the analyzed dimensions, a high degree of conceptual alignment was observed. The primary

differences lie in regulatory structure and level of prescriptiveness. DORA provides clearer operational guidance, while NIS2offers greater flexibility but also leaves more room for interpretation.

RQ.3 *How do organizations across different sectors interpret and implement these requirements, and what challenges do they encounter in doing so?*

Our interview results show that organizations interpret and implement cybersecurity requirements through the lens of existing maturity, resources, and regulatory experience. Financial institutions generally approach DORA as a formalization and extension of established practices, while many NIS2-regulated organizations face a steeper learning curve.

Key challenges include ambiguity in regulatory interpretation, limited cybersecurity expertise, legacy systems, and difficulties in managing third-party dependencies. In sectors with lower baseline maturity, compliance efforts are often driven by external consultants and framed as transformation projects rather than incremental improvements. These findings highlight a recurring gap between regulatory intent and operational execution, particularly outside the financial sector.

RQ.4 *Which DORA practices are seen as most useful or transferable to less mature sectors under NIS2, and why?*

Interviewees identified several DORA-aligned practices as particularly useful for enhancing NIS2 implementation:

1. Structured documentation and policy formalization because of DORA's emphasis on clearly documented processes, defined responsibilities, and audit-ready governance structures.
2. Given the shared dependency on external ICT providers across critical infrastructure sectors, interviewees viewed formalized third-party risk management, including supplier due diligence procedures, contractual security clauses, ongoing monitoring, and escalation mechanisms as directly applicable beyond finance.
3. Simplified versions of DORA's incident categorization and escalation procedures could help NIS2-covered entities operationalize reporting obligations more effectively.
4. Structured resilience testing and exercise programs were seen as important maturity drivers. While advanced testing regimes may not be proportionate for all sectors, the principle of regular scenario-based exercises and validation of response capabilities was widely regarded as transferable.

RQ.5 *How do differences in regulatory structure, sector maturity, and national implementation influence the effectiveness and transferability of cybersecurity practices across sectors?*

They strongly influence how cybersecurity practices are perceived and adopted. DORA's centralized supervision and detailed requirements support consistent implementation within the financial sector, while NIS2's decentralized enforcement leads to greater variability across sectors and Member States. Lower sector maturity increases reliance on external guidance and limits the immediate applicability of complex practices. National implementation choices further shape compliance strategies, particularly for multinational organizations. These factors do not prevent cross-sector learning but constrain how directly practices can be transferred.

6.3 Recommendations

Based on the findings, the following recommendations are proposed for organizations and policymakers involved in the implementation of NIS2:

1. Translate DORA-inspired practices into sector-appropriate guidance, focusing on intent and structure rather than strict replication. Results from our interviews show that while DORA's structured governance and documentation models are valuable, direct replication is often impractical.
2. Prioritize third-party risk management and ICT governance as early focus areas for improving cybersecurity maturity under NIS2. Interviewees repeatedly noted limited visibility into supplier ecosystems, unclear accountability, and fragmented oversight mechanisms.
3. Support NIS2-regulated organizations with practical implementation examples, templates, and maturity benchmarks to reduce interpretation uncertainty. A recurring theme in the interviews

was that NIS2's broad and flexible language creates uncertainty about what constitutes sufficient compliance.

4. Encourage cross-sector knowledge sharing, particularly between financial institutions and less mature critical infrastructure sectors. Interviewees emphasized that failing to leverage this accumulated experience would be inefficient.

6.4 Future work

This study focused on perceived transferability and implementation challenges rather than on measuring the effectiveness of transferred practices. Future research could empirically evaluate whether the adoption of DORA-inspired practices leads to measurable improvements in cybersecurity outcomes within NIS2-regulated sectors.

Additional research could also examine national NIS2 implementations in greater detail to assess how differences in enforcement influence organizational behavior. Finally, longitudinal studies following organizations through their NIS2 compliance journey could provide deeper insight into how cybersecurity maturity evolves over time and whether cross-sector learning results in sustained resilience improvements.

Bibliography

[1] Abnormal Security. Connected third-party applications widen the attack surface area, 2023. URL https://abnormalsecurity.com/blog/connected-third-party-applications-widen-attack-surface-area.

[2] ActiveMind Legal. Nis2 vs dora: A comparison, 2024. URL https://www.activemind.legal/guides/nis2-dora/.

[3] Gonçalo Almeida Teixeira, Miguel Mira da Silva, and Ruben Pereira. The critical success factors of gdpr implementation: a systematic literature review. *Digital Policy, Regulation and Governance*, 21(4):402–418, 06 2019. ISSN 2398-5038. doi: 10.1108/DPRG-01-2019-0007. URL https://doi.org/10.1108/DPRG-01-2019-0007.

[4] Bank for International Settlements, Financial Stability Board. Cyber resilience practices - executive summary, 2020. URL https://www.bis.org/fsi/fsisummaries/cyber_resilience.htm.

[5] BDO Malta. The relationship between nis2 directive & dora, 2024. URL https://www.bdo.com.mt/en-gb/insights/the-relationship-between-nis-2-directive-and-dora.

[6] Glenn A. Bowen. Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2):27–40, 2009. doi: 10.3316/QRJ0902027.

[7] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006. doi: 10.1191/1478088706qp063oa.

[8] CiTiP KU Leuven. From operational risk to systemic risk? dora and the oversight of critical ict third-party providers, 2022. URL https://www.law.kuleuven.be/citip/blog/from-operational-risk-to-systemic-risk/. Blog post.

[9] Commission de Surveillance du Secteur Financier. Digital operational resilience act (dora), 2023. URL https://www.cssf.lu/en/digital-operational-resilience-act-dora/.

[10] ComplianceForge. Secure controls framework (scf): A unified metaframework for cybersecurity standards, 2024. URL https://complianceforge.com/grc/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf.

[11] Consultancy.uk. Financial services most mature in cybersecurity, 2023. URL https://www.consultancy.uk/news/37801/financial-services-most-mature-in-cybersecurity.

[12] CyberPeace Institute. Case study: Viasat, 2023. URL https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat.

[13] CYE. Cybersecurity maturity report 2023, 2023. URL https://www.cyesec.com/reports/cybersecurity-maturity-report-2023.

[14] De Nederlandsche Bank. Good practice information security risk analysis (sira). https://www.dnb.nl/media/aeudln5i/dnb-sira-gp-2025-en.pdf, 2025.

[15] Deloitte. Cybersecurity insights, budgets & benchmarks for financial services institutions, 2023. URL https://www.deloitte.com/global/en/services/risk-advisory/perspectives/cybersecurity-insights-budgets-benchmarks-financial-services-institutions.html.

[16] Patrick Eckhardt and Anastasiia Kotovskaia. The eu's cybersecurity framework: the interplay between the cyber resilience act and the nis 2 directive. *International Cybersecurity Law Review*, 4 (1):147–164, 2023. doi: 10.1365/s43439-023-00084-z.

[17] Philipp Eckhardt. The cybersecurity policy of the european union: Resilience through regulation? *International Cybersecurity Law Review*, 3:23–35, 2022. doi: 10.1365/s43439-022-00076-5. URL https://link.springer.com/article/10.1365/s43439-022-00076-5.

[18] Philipp Eckhardt and Alena Kotovskaia. The eu's cybersecurity framework: the interplay between the cyber resilience act and the nis 2 directive. *International Cybersecurity Law Review*, 4:147–164, 2023. doi: 10.1365/s43439-023-00084-z. URL https://link.springer.com/article/10.1365/s43439-023-00084-z.

[19] ECSO. Nis2 implementation: Challenges & priorities, 2025. URL https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf.

[20] Kevin Eiden, James Kaplan, Bartlomiej Kazimierski, Charlie Lewis, and Kevin Telford. Organizational cyber maturity: A survey of industries, 2021. URL https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries.

[21] Kevin Eiden, James Kaplan, Bartlomiej Kazimierski, Charlie Lewis, and Kevin Telford. Organizational cyber maturity: A survey of industries, 2021. URL https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/organizational-cyber-maturity-a-survey-of-industries. McKinsey & Company.

[22] EuRepoC. European repository of cyber incidents – dashboard, 2024. URL https://eurepoc.eu/dashboard/.

[23] European Banking Authority. Esas launch consultation on first batch of dora policy products, 2023. URL https://www.eba.europa.eu/esas-launch-consultation-first-batch-dora-policy-products.

[24] European Banking Authority. Guidelines on ict and security risk management. https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-ict-and-security-risk-management, 2025.

[25] European Insurance and Occupational Pensions Authority. Esas consult on digital operational resilience act (dora), 2023. URL https://www.eiopa.europa.eu/media/news/esas-consult-digital-operational-resilience-act-dora.

[26] European Insurance and Occupational Pensions Authority. Digital operational resilience act (dora) overview, 2023. URL https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[27] European Insurance and Occupational Pensions Authority. Why is dora needed?, 2023. URL https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en#why-is-dora-needed.

[28] European Parliament and Council of the European Union. Directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union, 2016. URL https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148.

[29] European Parliament and Council of the European Union. Regulation (eu) 2022/2554 of the european parliament and of the council of 14 december 2022 on digital operational resilience for the financial sector and amending regulations (ec) no 1060/2009, (eu) no 648/2012, (eu) no 600/2014, (eu) no 909/2014 and (eu) 2016/1011, 2022. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554.

[30] European Parliament and Council of the 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, repealing directive (eu) 2016/1148, 2022. URL https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

[31] European Parliament Research Service. Cybersecurity in the eu common security and defence policy: Challenges and risks for the eu, 2020. URL https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf.

[32] European Parliament Research Service. The nis2 directive: A high common level of cybersecurity in the eu, 2021. URL https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.

[33] European Securities and Markets Authority. Digital operational resilience act (dora), 2023. URL https://www.esma.europa.eu/regulation/digital-operational-resilience-act-dora.

[34] European Union Agency for Cybersecurity (ENISA). Cybersecurity for smes: Challenges and recommendations, 2021. URL https://www.enisa.europa.eu/publications/cybersecurity-for-smes.

[35] European Union Agency for Cybersecurity (ENISA). Enisa threat landscape for critical sectors, 2022. URL https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-critical-sectors.

[36] European Union Agency for Cybersecurity (ENISA). Legacy systems and cybersecurity risk in critical sectors, 2023. URL https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[37] European Union Agency for Cybersecurity (ENISA). Skills shortage and cybersecurity workforce challenges in the eu, 2023. URL https://www.enisa.europa.eu/news/skills-shortage-and-unpatched-systems-soar-to-high-ranking-2030-cyber-threats.

[38] European Union Agency for Cybersecurity (ENISA). Enisa threat landscape 2023, 2023. URL https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[39] European Union Agency for Cybersecurity (ENISA). Enisa threat landscape 2025. Technical report, European Union Agency for Cybersecurity, October 2025. URL https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf. European Union Agency for Cybersecurity (ENISA) annual threat assessment report.

[40] Europol. Internet organised crime threat assessment (iocta), 2021. URL https://securitydelta.nl/media/com_hsd/report/378/document/socta2021-2.pdf.

[41] Financial Stability Board. Effective practices for cyber incident response and recovery, 2018. URL https://www.fsb.org/wp-content/uploads/P191020-1.pdf.

[42] Konstantinos Fysarakis, Alexios Lekidis, Vasileios Mavroeidis, Konstantinos Lampropoulos, George Lyberopoulos, Ignasi Garcia-Milà Vidal, José Carles Terés i Casals, Eva Rodriguez Luna, Alejandro Antonio Moreno Sancho, Antonios Mavrelos, Marinos Tsantekidis, Sebastian Pape, Argyro Chatzopoulou, Christina Nanou, George Drivas, Vangelis Photiou, George Spanoudakis, and Odysseas Koufopavlou. Phoeni2x – a european cyber resilience framework with artificial-intelligence-assisted orchestration, automation & response capabilities for business continuity and recovery, incident response, and information exchange. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, page 538–545. IEEE, July 2023. doi: 10.1109/csr57506.2023.10224995. URL http://dx.doi.org/10.1109/CSR57506.2023.10224995.

[43] Thomas Harrison, Emily Johnson, and Wei Lin. Analyzing the colonial pipeline ransomware attack: Implications for critical infrastructure protection. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2023. doi: 10.1109/CSR57506.2023.10181159.

[44] Help Net Security. Six months into dora, most financial firms are still not ready. Technical report, Helpnet Security, 2025. URL https://www.helpnetsecurity.com/2025/07/25/dora-compliance-challenges-financial-firms/.

[45] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Quarterly*, 28(1):75–105, 2004. doi: 10.2307/25148625.

[46] Industrial Cyber. Securing europe's critical infrastructure: A year in review and strategies for cyber resilience, 2023. URL https://industrialcyber.co/features/securing-europes-critical-infrastructure-a-year-in-review-and-strategies-for-cyber-resilience/.

[47] SOS Intelligence. Maersk's response to notpetya: How cybersecurity best practices mitigated a major cyberattack, 2023. URL https://sosintel.co.uk/case-study-maersks-response-to-notpetya-how-cybersecurity-best-practices-mitigated-a-major-cybe Accessed: 2025-10-21.

[48] Ivanti. International inconsistencies: How cybersecurity preparedness varies across countries, 2023. URL https://www.ivanti.com/blog/international-inconsistencies-how-cybersecurity-preparedness-varies-across-countries.

[49] Hanna Kallio, Anna-Maija Pietilä, Marja Johnson, and Mari Kangasniemi. Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72(12):2954–2965, 2016. doi: 10.1111/jan.13031.

[50] Kaspersky. Critical infrastructure: Energy, oil, and gas see the most cyber incidents due to lack of budget, 2023. URL https://usa.kaspersky.com/about/press-releases/critical-infrastructure-energy-oil-and-gas-see-the-most-cyber-incidents-due-to-lack-of-budget-i

[51] Nicky Kos. Navigating the DORA landscape: A study of service provider readiness. Master's thesis, Leiden University, Leiden Institute of Advanced Computer Science (LIACS), 2024.

[52] Savvas Kourmpetis. Management of ict third party risk under the digital operational resilience act. In *Digitalisation, Sustainability, and the Banking and Capital Markets Union*, pages 753–765. Springer, 2023. doi: 10.1007/978-3-031-30694-5_40. URL https://link.springer.com/chapter/10.1007/978-3-031-30694-5_40.

[53] KPMG The Netherlands. Network and information security directive (nis2), 2023. URL https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2023/10/kpmg-network-and-information-security-directive-nis2.pdf.

[54] Pedro Machado, Jéssyka Vilela, Mariana Peixoto, and Carla Silva. A systematic study on the impact of GDPR compliance on organizations. In *Proceedings of the 25th International Conference on Enterprise Information Systems*, page 8, Maceió, Brazil, 2023. Association for Computing Machinery. doi: 10.1145/3592813.3592935.

[55] MorganFranklin Consulting. 2023 cybersecurity predictions: Financial services, 2023. URL https://www.morganfranklin.com/insights/2023-cybersecurity-predictions-financial-services/.

[56] Dominik Mussmann, Jens Schröder, and Stephan Tiemeyer. Mapping the state of security standards mappings, 2021. URL https://library.gito.de/wp-content/uploads/2021/08/L4_Mussmann-Mapping_the_State_of_Security_Standards_Mappings-305_c.pdf.

[57] NIST OLIR Program. Informative reference mappings—iso/iec 27001 to nist cybersecurity framework, 2025. URL https://csrc.nist.gov/projects/olir/informative-reference-catalog.

[58] Alexander Nohre. Nis2 – europe's strengthened cybersecurity regime. *Science and Technology Law Review*, 2023. URL https://journals.library.columbia.edu/index.php/stlr/blog/view/577.

[59] Jukka Ruohonen. The incoherency risk in the eu's new cyber security policies. *arXiv preprint arXiv:2405.12043*, 2024.

[60] Jukka Ruohonen. A systematic literature review on the nis2 directive. *arXiv*, 2024. URL https://arxiv.org/abs/2412.08084.

[61] Julian Schmidt. Cybersecurity in the eu: The example of the financial sector—a legal perspective. *German Law Journal*, 24(4):689–708, 2023. doi: 10.1017/glj.2023.50. URL https://www.cambridge.org/core/journals/german-law-journal/article/cybersecurity-in-the-eu-the-example-of-the-financial-sector-a-legal-perspective/E74D7AB0D2FDF2B0017BD93BD324267C.

[62] Sandra Schmitz-Berndt. Defining the reporting threshold for a cybersecurity incident under the nis directive and the nis 2 directive. *Journal of Cybersecurity*, 9(1), 2023. doi: 10.1093/cybsec/tyad009. URL https://doi.org/10.1093/cybsec/tyad009.

[63] ScienceDirect. Fragmented cybersecurity regulatory landscape in the eu, 2024. URL https://www.sciencedirect.com/science/article/pii/S0267364924000980.

[64] Mari Seeba et al. Evaluating organization security: User stories of european union nis2 directive. *arXiv preprint arXiv:2504.19222*, 2025. URL https://arxiv.org/abs/2504.19222.

[65] Skadden, Arps, Slate, Meagher & Flom LLP. The eu's digital operational resilience act (dora), 2024. URL https://www.skadden.com/insights/publications/2024/07/the-eus-digital-operational-resilience-act.

[66] Stiftung Wissenschaft und Politik (SWP). European repository of cyber incidents (eurepoc), 2023. URL https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc.

[67] TechCrunch. Wannacry ransomware attack, two years on, 2019. URL https://techcrunch.com/2019/05/12/wannacry-two-years-on/.

[68] TechTarget. Solarwinds hack explained: Everything you need to know, 2023. URL https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[69] UpGuard. Cybersecurity regulations by industry, 2023. URL https://www.upguard.com/blog/cybersecurity-regulations-by-industry.

[70] Nicolas Vandezande. Cybersecurity in the eu: How the nis2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52:105890, 2024. doi: 10.1016/j.clsr.2023.105890.

[71] Wavestone. Cyber benchmark 2024: Progress in cyber maturity continues yet pace is slow, 2024. URL https://www.wavestone.com/en/insight/cyber-benchmark-2024-progress-in-cyber-maturity-continues-yet-pace-is-slow.

Appendix A

Dimension Comparison and Overlap Analysis

The following tables show the comparative analysis between NIS2 and DORA. It elaborates on each of the ten regulatory dimensions introduced in Chapter 4. Each entry follows a standardized structure assessing objectives, requirements, and implementation, concluding with an assessed level of overlap between NIS2 and DORA, and a general summary of the dimension. One extra dimensions (D0) has been added to give context to the scope and coverage of NIS2 and DORA

D0: Sectoral Scope and Coverage
NIS2's wide scope is intended to secure services foundational to EU societal stability and economic resilience, while DORA focusses on the financial sector. Although both seek to protect critical services, they apply their protections in vastly different contexts. NIS2 applies broadly across essential and important entities within critical sectors such as energy, transport, healthcare, and public administration. In contrast, DORA targets the financial sector specifically, covering entities like banks, insurers, and investment firms. NIS2's wide application means implementation is adapted by each EU member state, while DORA applies uniformly across the financial sector with centralized oversight from ESAs. NIS2 and DORA have fundamentally different scopes: NIS2 applies across a wide range of critical infrastructure sectors, while DORA is limited to financial entities. Both aim to secure essential services, but operate in separate domains with distinct regulatory ecosystems.

D1: Cybersecurity and ICT Risk Management
Overlap Level: Moderate (3) **Objectives**: Both frameworks aim to manage and improve cybersecurity and ICT risk management to ensure the security of ICT systems and operational stability. **Requirements**: NIS2 mandates a range of general cybersecurity measures across sectors, including continuous risk assessments, protection against cyber threats, and business continuity planning. Member States are permitted to adapt these requirements to their unique national risks. DORA's approach, however, is more prescriptive for ICT risk management in the financial sector, outlining specific protocols for protecting ICT infrastructure, continuity planning, and advanced resilience testing. Both frameworks emphasize cybersecurity, but DORA includes stricter measures and testing protocols in its documentation. **Implementation**: NIS2 allows each member state flexibility to adapt cybersecurity measures according to local risks and critical infrastructure needs, whereas DORA requires specific cybersecurity protocols across the financial sector such as mandatory resilience testing.

Summary: Both frameworks promote cybersecurity resilience, but DORA offers far more prescriptive and sector-specific ICT controls. NIS2 leaves room for national interpretation, while DORA mandates uniform implementation across the financial sector. The difference reflects sectoral maturity and regulatory strictness.

D2: Incident Reporting Requirements

Overlap Level: High (4)
Objectives: Both frameworks emphasize prompt incident reporting to facilitate timely response, with similar reporting timelines. Reporting serves as a critical tool to ensure operational continuity and minimize broader impacts.
Requirements: NIS2 applies broadly across critical infrastructure, emphasizing criteria such as the number of users affected, incident duration, geographical spread, and overall service disruption, with a goal of maintaining operational continuity in essential services across multiple sectors. DORA, meanwhile, focuses specifically on incidents impacting financial stability and market integrity, such as disruptions to critical financial functions, economic loss, reputational damage, and data confidentiality breaches.
Implementation: NIS2 requires entities to report significant cybersecurity incidents to national authorities within 24-72 hours. DORA mandates an initial report to financial regulators within 24 hours of an ICT incident, with stricter follow-up reporting requirements based on incident severity.
Summary: NIS2 and DORA both require timely incident reporting, though with different scopes and technical criteria. DORA mandates stricter timelines and structured formats for financial regulators. NIS2 provides more flexible thresholds based on service disruption and criticality. The mechanisms differ, but the intent closely aligns.

D3: Operational Resilience Testing

Overlap Level: Moderate (3)
Objectives: Both frameworks require operational resilience testing to identify vulnerabilities and strengthen systems, but DORA's protocols are more rigorous, especially with TLPT for high-risk financial entities.
Requirements: NIS2 mandates general testing of security measures and infrastructure resilience, providing entities across sectors with guidelines for regular assessments and audits. DORA goes further, requiring specific testing protocols such as TLPT for high-risk financial entities.
Implementation: DORA mandates regular, rigorous resilience testing, particularly for systemically important financial institutions. NIS2's testing requirements are practical for its broader scope, and much less detailed than DORA's. However, this might have to do with NIS2 being a broader directive which can be tightened by the affected Member States.
Summary: DORA includes detailed resilience testing obligations, such as TLPT for high-risk financial entities. NIS2 requires testing in broader terms without prescriptive detail. While both promote testing, DORA's implementation is much more specific and enforceable.

D4: Third-Party and Supply Chain Risk Management

Overlap Level: Moderate (3)
Objectives: Both frameworks seek to mitigate risks associated with third-party dependencies.
Requirements: NIS2 requires entities to manage supply chain risks by assessing and securing their network systems against vulnerabilities from third-party providers, as well as having a deep understanding of their providers' supply chain and the risks that come with it. However, oversight of these providers remains with the entities themselves. DORA, in contrast, gives ESAs direct regulatory oversight of critical ICT service providers, such as cloud providers, when they are deemed essential to financial stability. The comparative benefit of DORA's approach is its ability to monitor and enforce resilience at the ICT provider level in finance, where disruptions could have cascading effects.

Implementation: NIS2 requires entities to manage their own third-party risks without external regulatory involvement. DORA enables ESAs to oversee critical third-party ICT providers, imposing compliance obligations directly on these providers.
Summary: Both frameworks address third-party risk, but DORA includes explicit regulatory oversight of ICT providers, while NIS2 places responsibility on entities themselves. Overlap exists in intent, but diverges strongly in supervisory mechanisms and enforcement.

D5: Governance and Accountability

Overlap Level: Full (5)
Objectives: Both frameworks mandate senior management accountability for resilience and cybersecurity, underscoring the importance of executive involvement across all sectors.
Requirements: NIS2 mandates senior management and board-level accountability, requiring executives to prioritize cybersecurity within their organization's strategic planning. The aim is to ensure cybersecurity is an integral component of overall governance. DORA similarly requires senior management to be actively responsible for ICT resilience in financial institutions, with specific roles in overseeing risk management strategies and reporting incidents. Both frameworks foster a culture of accountability, but DORA's provisions are more prescriptive, emphasizing the importance of executive involvement in financial ICT security.
Implementation: Both NIS2 and DORA emphasize executive accountability and assign clear roles for senior leadership to report incidents and oversee cybersecurity strategies.
Summary: This is one of the most aligned dimensions. Both NIS2 and DORA assign cybersecurity accountability to senior management and require board-level engagement. While DORA offers more structured governance documentation, the frameworks share strong alignment in overall intent and requirements.

D6: Information Sharing

Overlap Level: Moderate (3)
Objectives: Both frameworks promote information sharing with the goal of strengthening resilience across sectors, though NIS2's cross-sectoral focus contrasts with DORA's sector-specific approach.
Requirements: NIS2 encourages collaboration across critical infrastructure sectors to share insights and threat intelligence in general, but has requirements for information sharing in some cases. DORA encourages information sharing within the financial sector specifically, creating networks where financial institutions share insights on cyber threats and vulnerabilities with each other and regulators.
Implementation: NIS2 relies on national coordination centers for cross-sectoral information exchange, while DORA enables financial institutions to share information directly with each other and financial regulators.
Summary: Both frameworks encourage threat intelligence exchange, but implementation differs. DORA leverages existing networks within the financial sector; NIS2 promotes national coordination across sectors. Cultural and regulatory differences affect how sharing is implemented in practice.

D7: Supervision and Enforcement

Overlap Level: Low (2)
Objectives: Both frameworks aim to ensure compliance through supervision, but DORA centralizes oversight at the ESA level, while NIS2 relies on decentralized national authorities.
Requirements: Under NIS2, national competent authorities (E.g. CSIRTs) are responsible for supervision and enforcement, including audits, compliance checks, and, where necessary, penalties for non-compliance. DORA is enforced through ESAs, who ensure compliance across financial entities and impose penalties for non-compliance specific to the financial sector. This allows DORA to leverage sector expertise through ESAs, while NIS2's national-level supervision ensures enforcement is adapted to each member state's context.

Implementation: NIS2's decentralized supervision allows member states to tailor enforcement approaches to local contexts, while DORA's centralized ESA enforcement ensures consistency across the financial sector.
Summary: DORA centralizes enforcement via European Supervisory Authorities, ensuring harmonized implementation across financial entities. NIS2 relies on national authorities and varies by member state. This results in diverging supervision styles, with DORA offering more consistency.

D8: Penalties

Overlap Level: Low (2)
Objectives: Both frameworks aim to penalize non-compliance to deter regulatory violations, though their approaches are tailored to their respective scopes.
Requirements: NIS2 allows member states flexibility in determining penalties, while DORA imposes harmonized EU-wide penalties based on the severity of non-compliance in the financial sector.
Implementation: NIS2's penalties are variable and determined at the national level, allowing for administrative fines up to €10 million or 2% of global turnover, enforced by national authorities. This flexibility accommodates the wide variety of sectors under NIS2. DORA specifies penalties within the financial sector based on the severity of non-compliance, with ESAs empowered to impose targeted fines.
Summary: Both frameworks use penalties as a tool to enforce compliance, but DORA sets out EU-wide harmonized rules, while NIS2 allows national discretion. NIS2's penalties may vary widely, whereas DORA's are tightly linked to regulatory breaches within the financial sector.

D9: Crisis Management and Coordination

Overlap Level: Moderate (3)
Objectives: Both frameworks include crisis management provisions, but NIS2 coordinates EU-wide cross-sectoral responses, whereas DORA's crisis management is specifically focused on financial market continuity.
Requirements: NIS2 establishes cross-border coordination through mechanisms like EU-CyCLONe, addressing crises affecting multiple sectors. DORA focuses on financial-sector-specific protocols.
Implementation: NIS2 includes crisis management provisions, including the EU-CyCLONe network for cross-border coordination during cyber incidents. This framework aims to ensure a cohesive EU response to significant threats across sectors. DORA's crisis management provisions focus on the continuity of financial market operations, with protocols designed to maintain stability and mitigate systemic risks.
Summary: Both frameworks include crisis management, but DORA focuses on financial market stability while NIS2 covers cross-sector coordination. DORA's mechanisms are tailored to systemically important entities; NIS2 builds EU-wide cooperation structures like EU-CyCLONe.

D10: Oversight of ICT Providers

Overlap Level: Minimal (1)
Objectives: DORA allows direct ESA oversight of critical ICT providers, whereas NIS2 leaves third-party oversight to the entities themselves.
Requirements: NIS2 does not provide direct oversight for third-party ICT providers; rather, it places the responsibility of managing third-party risk on the entities themselves. DORA, on the other hand, establishes direct oversight by ESAs for critical ICT providers within the financial sector.
Implementation: DORA enables ESAs to directly supervise ICT providers critical to financial stability, while NIS2 assigns third-party risk management responsibilities to entities without regulatory oversight.

Summary: DORA gives ESAs direct authority to oversee critical ICT providers, enabling supervisory intervention at the provider level. NIS2 has no equivalent mechanism: oversight is left to the regulated entities themselves, creating a major difference in regulatory reach.

Appendix B

Comparative Analysis Table

Comparative Dimension	NIS2 Article	DORA Article	Comments/Overlap	Overlap Level 1-5
Sectoral Focus	Ch. I, Art. 2 (Scope of Application for Essential & Important Entities)	Ch. I, Art. 2 (Scope for financial entities)	NIS2 applies to multiple critical infrastructure sectors, while DORA focuses specifically on financial entities.	2 (Low Overlap)
Cybersecurity- and ICT Risk Management	Ch. IV, Art. 18-21 (Cybersecurity Risk Management Measures)	Ch. II, Art. 5-16 (ICT Risk Management)	Both mandate risk management, but DORA's requirements are tailored to financial ICT resilience.	3 (Moderate Overlap)
Incident Reporting	Ch. IV, Art. 23 (Incident Reporting Obligations)	Ch. II, Art. 17 (Incident Reporting for ICT-related Events)	Both require timely incident reporting, with different timelines, reporting criteria and targeted authorities.	4 (High Overlap)
Operational Resilience Testing	Ch. IV, Art. 20 (Security and Resilience Testing Requirements)	Ch. II, Art. 21-22 (Operational Resilience Testing, incl. TLPT)	DORA mandates Threat-Led Penetration Testing (TLPT) for some specific financial institutions, while NIS2 has more general testing requirements	3 (Moderate Overlap)
Third-Party Risk Management	Ch. IV, Art. 21-22 (Cybersecurity Risk management Measures & Critical Supply Chains)	Ch. III, Art. 28-31 (ICT Third-Party Risk Management)	Both address third-party risk, with DORA overseeing critical ICT providers and NIS2 requiring a deep understanding of third party entities	3 (Moderate Overlap)
Governance and Accountability	Ch. IV, Art. 20-21 (Governance and Accountability at Management Level)	Ch. II, Art. 5 (Governance Framework and Accountability)	Both frameworks emphasize high-level governance, requiring involvement from senior management.	5 (Full Overlap)
Information Sharing	Ch. II-III & V, Art. 26 (Coordination and Information Sharing)	Ch. III, Art. 40 (Information Sharing Arrangements)	Both enforce certain levels of information sharing, but NIS2 is cross-sector, while DORA focuses on financial sector sharing.	3 (Moderate Overlap)
Supervision and Enforcement	Ch. II-III & VII, Art. 29-32 (Supervision and Enforcement)	Ch. IV, Art. 42-48 (Supervision, Enforcement, and Sanctions)	Both have penalties for non-compliance, though enforcement mechanisms differ.	2 (Low Overlap)
Penalties	Ch. VII, Art. 31 (Penalties and Administrative Fines)	Ch. IV, Art. 45 (Administrative Penalties Specific to DORA)	NIS2 penalties are managed by national bodies, while DORA's penalties are overseen by financial regulators like ESAs and NCAs.	2 (Low Overlap)
Crisis Management	Ch. V, Art. 25 (EU-CyCLONe for Cross-Border Crisis Coordination)	Ch. II, Art. 15 (Financial Market Crisis Continuity)	Both address crisis management, with DORA tailored to financial stability, and NIS2 focusing on cross-sector crises.	2 (Low Overlap)
Oversight of ICT Providers	Not directly covered	Ch. II, Art. 15 (Financial Market Crisis Continuity)	DORA includes provisions for ESAs to oversee critical ICT providers.	1 (Minimal Overlap)

Table B.1: Key Dimension Overview