CRISP

- Cybersecurity Regulation Impact Study on Practices -

Master's Thesis

Jacob Sylvest Krab-Johansen

Joar Belsnes

Alejandro Lozano Rebollo

Aalborg University
Cybersecurity

AALBORG UNIVERSITET

Cybersecurity
Aalborg University
http://www.aau.dk

Title:
Cybersecurity Regulation Impact Study on Practices

Theme:
Cyber Security

Project Period:
February 2025 - June 2025

Participant(s):
Joar Belsnes
Alejandro Lozano Rebollo
Jacob Sylvest Krab-Johansen

Supervisor(s):
Lene Tolstrup Sørensen

Page Numbers: 82

Date of Completion:
June 3, 2025

Keywords:

Cybersecurity,
NIS2 Directive,
EU Cybersecurity Policy,
Security Governance,
Risk Management,
Risk-Based Governance,
Compliance Minimalism,
Regulatory Fragmentation,
Cross-Border Transposition,
Incident Reporting,
Board Accountability,
SME Capacity Constraints

Abstract

This Master's thesis investigates the real-world consequences of the European Union's cybersecurity regulation, with a focus on the NIS2 Directive. The study examines whether such legislation drives meaningful improvements in organizational security practices or unintentionally promotes superficial, compliance-oriented behavior.

Findings indicate that while the directive aims to establish a high common level of cybersecurity, its legal ambiguity, uneven national implementation, and reliance on consultancy-driven interpretation risk undermining those objectives. The study identifies recurring issues such as compliance fatigue, disproportionate burdens on small and medium-sized businesses (SMBs), and fragmented enforcement landscapes.

This thesis provides a grounded perspective on how cybersecurity regulation is interpreted and applied in practice. It reveals a significant gap between the directive's intended goals and the outcomes observed. The study concludes that clearer expectations, harmonized enforcement, and stronger support mechanisms are essential to achieving meaningful improvements in cyber resilience.

The research is exploratory and employs a mixed-methods approach. Semi-structured interviews with leading cybersecurity consultants form the core of the qualitative analysis, complemented by a targeted survey and review of related literature. This design enables the study to capture insights and behavioral dynamics that are often overlooked in existing academic discourse.

Contents

Preface

Aalborg University June 3, 2025

This Master's thesis was prepared by Joar Belsnes, Jacob Sylvest Krab-Johansen, and Alejandro Lozano Rebollo and submitted on 4th June as part of the Cybersecurity Master's program at Aalborg University. The project was conducted independently by the student team, under the guidance of supervisor Lene Tolstrup Sørensen.

The use of generative AI in this thesis was limited to language refinement and search assistance. All use was conducted in full compliance with Aalborg University's official guidelines on generative AI in academic work [1].

The authors would like to thank their supervisor for her guidance throughout the project, as well as all participants in the qualitative study for generously sharing their insights. Special thanks also go to the professionals and peers who contributed with perspectives, feedback, or informal support during the course of this research.

Abbreviations

A list of the abbreviations used in this report, sorted in alphabetical order:

Abbreviations		
1.	AI	Artificial Intelligence
2.	CCPA	California Consumer Privacy Act
3.	CIS	Center for Internet Security
4.	CISO	Chief Information Security Officer
5.	CRA	Cyber Resilience Act
6.	CSF	Cybersecurity Framework (NIST CSF)
7.	CSIRT	Computer Security Incident Response Team
8.	DORA	Digital Operational Resilience Act
9.	DPA	Data Processing Agreement
10.	DPO	Data Protection Officer
11.	EDPB	European Data Protection Board
12.	EEA	European Economic Area
13.	ENISA	European Union Agency for Cybersecurity
14.	EU	European Union
15.	GDPR	General Data Protection Regulation
16.	IAPP	International Association of Privacy Professionals
17.	ICT	Information and Communication Technology
18.	ISO	International Organization for Standardization
19.	ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
20.	IT	Information Technology
21.	KPI	Key Performance Indicator
22.	LGPD	Lei Geral de Proteção de Dados
23.	NCA	National Competent Authority
24.	NIS1	Network and Information Security Directive (2016)
25.	NIS2	Network and Information Security Directive (2022)
26.	NIST	National Institute of Standards and Technology
27.	NGO	Non-Governmental Organization
28.	PCI DSS	Payment Card Industry Data Security Standard
29.	SaaS	Software as a Service
30.	SIEM	Security Information and Event Management
31.	SMB	Small and Medium-sized Business
32.	SME	Subject Matter Expert *or* Small and Medium-sized Enterprise
33.	SOC	Security Operations Center

Chapter 1

Introduction

The digital transformation has woven information and communication technology (ICT) into every layer of contemporary society. Critical energy grids rely on industrial control systems that are increasingly Internet-connected; financial markets transact in microseconds over globally distributed networks; public administrations deliver citizen services almost exclusively through digital channels. While this hyper-connectivity delivers unprecedented efficiency and innovation, it also expands the attack surface for malicious actors. According to ENISA *Threat Landscape 2023* [2], ransomware attacks on European entities rose by 45 % year-on-year, with 38 % of victims falling within the category of "essential service". Against this backdrop, policymakers and industry leaders increasingly view baseline cyber resilience as a prerequisite for economic stability and public safety.

1.1 The Regulatory Turn in European Cybersecurity

During the last decade, the European Union has pursued a regulatory strategy to raise the collective security posture of Member States. Milestones include the Network and Information Security Directive (**NIS1**) in 2016 [3], the General Data Protection Regulation (**GDPR**) in 2018 [4], the EU Cybersecurity Act in 2019 [5], and most recently the Digital Operational Resilience Act (**DORA**) [6] for the financial sector. The adoption of the **NIS2 Directive** in December 2022 represents the EU's most ambitious horizontal intervention by the EU to date, expanding the sectoral scope, tightening incident reporting timelines and introducing harmonized enforcement provisions [7]. By setting a statutory "floor" of cyber hygiene, legislators aim to reduce systemic risk and improve collective incident response across the Single Market.

1.2 Complementarity and Tension with Industry Frameworks

Historically, organizations have relied on *industry-driven* frameworks such as ISO/IEC 27001, NIST's Cybersecurity Framework (CSF), and the CIS Controls to structure their security programs [8]. These standards are voluntary, risk-based, and continuously updated through practitioner feedback, enabling firms to tailor controls according to threat exposure and business context. Regulatory instruments, in contrast, are legally binding and often prescriptive. While regulations like NIS2 can accelerate the diffusion of best practices, they also risk creating a "compliance mindset" in which organizations focus on meeting the narrow letter of the law rather than pursuing holistic risk reduction. Whether regula-

tion and voluntary frameworks act as *complements* or *substitutes* remains an open empirical question.

1.3 Problem Statement and Research Focus

Despite widespread consensus that NIS2 will raise Europe's cyber baseline, evidence on its practical efficacy is scarce. Early industry surveys suggest that many companies view the directive primarily as a legal hurdle, budgeting for audits and documentation rather than for transformative security controls [8]. Academic literature on GDPR shows a similar pattern: major compliance investments did not always translate into better privacy outcomes [4]. The present study therefore investigates whether NIS2 is perceived and implemented as (i) a *strategic security enhancer* or (ii) merely a *minimum-viable compliance obligation*. These patterns and their implications will be explored in detail in the literature review 2.2 and further discussed in comparison with NIS2 in Chapter 5

1.4 Research Aim and Questions

The overarching aim is to conduct a *gap analysis* between the directive's security intent and its organizational reality. The thesis addresses the following research question:

> **RQ:** To what extent does the NIS2 Directive lead to substantive improvements in organizational cybersecurity practices, and to what extent does it merely drive minimal, compliance-oriented implementation?

This primary question is operationalized through four sub-questions that examine observable implementation patterns, the drivers of compliance minimalism, the short- and long-term security value, and expert assessments of the directive's clarity and practicality. These are:

> **RQ1:** What are the Observable Patterns Among Organizations Implementing NIS2?
>
> **RQ2:** What Organizational or Regulatory Factors Contribute to a Compliance-driven Approach?
>
> **RQ3:** Does NIS2 Provide Tangible Security Improvements, and is the Value of Implementation Present Short/Long-term?
>
> **RQ4:** How do Industry Experts Interpret the NIS2 Directive in terms of its Completeness, Clarity or Practicality?

1.5 Contribution

By triangulating semi-structured interviews, a supportive survey methods elaborated in Chapter 3, and comparative insights from earlier frameworks such as GDPR and ISO/IEC 27001, the study delivers three contributions:

1. *Empirical evidence* on how NIS2 is interpreted and operationalized across sectors not governed by parallel statutes such as DORA or the Energy Security Package.
2. *Insight into drivers of compliance minimalism*, clarifying whether resource constraints, enforcement ambiguity, or directive vagueness dominate decision-making.
3. *Policy recommendations* for regulators and industry bodies on aligning legal mandates with risk-based best practices, thereby maximizing security benefit while minimizing administrative overhead.

1.6 Supplemental Exploration

During the progression of the study, recurring references to challenges in interpretation and implementation of the NIS2 Directive necessitated an additional research initiative. An initiative which sought to explore the absence of national guidance. To empirically examine the extent and implications of these challenges, a structured investigation was conducted to assess how Member States are transposing the directive into national law, as seen in results 4.3.
This exploration was designed to complement the primary data collection by providing a view of how regulatory divergence is displayed across the EU. While the interview and survey data reflects perceptions of ambiguity, delay, and fragmentation, the supplemental investigation seeks to verify whether these concerns are corroborated by observable differences in legislative progress, and interpretation of the regulatory scope, that goes beyond the organizations affected by the implementation requirements of NIS2.
The findings are integrated in the results chapter 4 and discussion chapter 5 and hopes to offer a more comprehensive view of the conditions under which organizations must operate and illustrates how formal regulatory architecture may influence compliance behavior across jurisdictions.

1.7 Thesis Structure

The remainder of the thesis is organized as follows. Chapter 2 reviews related work on regulatory efficacy and industry frameworks. Chapter 3 details the mixed-methods research design, including sampling, data collection instruments, and ethical safeguards.

Chapter 4 presents the empirical results aligned with each sub-question. Chapter 5 discusses the findings in light of existing literature and policy debates. Chapter 6 concludes with practical recommendations and suggestions for future research.

Chapter 2

Literature Review

This chapter will review existing literature relevant to the practical implementation of cybersecurity regulation on the European Union, hereunder with a primary focus on the NIS2 Directive. It will start by outlining the regulatory intent, expanded scope, and risk management provisions under NIS2. The chapter will further examine how organizations have historically responded to similar regulatory efforts, particularly the General Data Protection Regulation (GDPR), identifying patterns that may foreshadow the implementation dynamics of NIS2. Attention is given to the contrast between risk-based and compliance-based approaches, and the organizational challenges associated with translating regulatory requirements into practice. Finally, the chapter draws on lessons from GDPR implementation to guide the interview design and frame key areas where NIS2 may produce similar operational and compliance challenges.

2.1 Impact of NIS2 on Security Practices

This section outlines the key elements of the NIS2 Directive that are most relevant to organizational security practices. It focuses on how the directive extends its scope compared to NIS1, introduces mandatory incident reporting, and requires risk-based governance and supply chain oversight. Rather than analyzing the legal structure in isolation, the section highlights those provisions most likely to shape implementation behavior in practice.

2.1.1 Regulatory Intent and Scope of NIS2

The NIS2 Directive of the European Union (Directive (EU) 2022/2555) was enacted at the end of 2022 as the cornerstone of the new cybersecurity regulatory framework of the EU [9]. It builds upon the original 2016 NIS Directive by substantially expanding the scope of covered entities and sectors [10]. The directive's intent is to strengthen cyber resilience in essential and important organizations that support critical social or economic activities, from energy and transportation to health care, banking, public administration, and digital services. Furthermore, the directive is set out to enhance the overall cybersecurity posture of all member states of the European Union.

In contrast to its predecessor, which consisted of 7 sectors, NIS2 categorizes entities by criticality, size, and significantly expands on the scope of involved sectors to cover 18 sectors as seen in figure 2.2 and 2.1. It now applies to a larger group of entities, which has resulted in an expansion of the applied scope to include thousands of additional organi-

zations across the EU. This broad reach is the result of the recognition that cyber threats have intensified since the birth of NIS1 in conjunction with a rapid digitization, and as well as the geopolitical tensions [2]. These factors have necessitated an uplift in security and defense practices across the internal market.

Crucially, the regulatory intent of NIS2 is not merely punitive compliance but to drive a risk-based approach to cybersecurity. Article 21 [10] requires that organizations implement "appropriate and proportionate technical, operational and organizational measures" to manage the risks posed to their networks and information systems. These measures must align with the evolving state of the art and be commensurate with the entity's risk exposure, size, and the potential impact of incidents.

The directive embeds risk management into its core by mandating an "all-hazards" risk approach across ten key domains: from risk analysis, incident handling, and business continuity, to supply chain security and vulnerability disclosure. While these define a baseline, NIS2 allows flexibility in implementation to promote effectiveness over formality.

Notably, NIS2 also introduces explicit top management accountability for cybersecurity. Senior executives are expected to oversee cyber risk governance, signaling a strategic shift in how security is managed at the board level. This reflects the EU's broader vision, expressed in the 2020 Cybersecurity Strategy, that cybersecurity should be an enabler of innovation and trust, not a cost to be minimized[11].

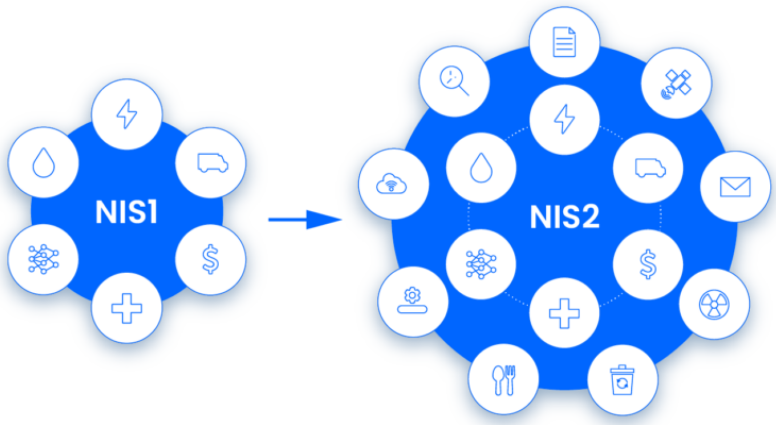


Figure 2.1: Scope of NIS1 and NIS2 [12]

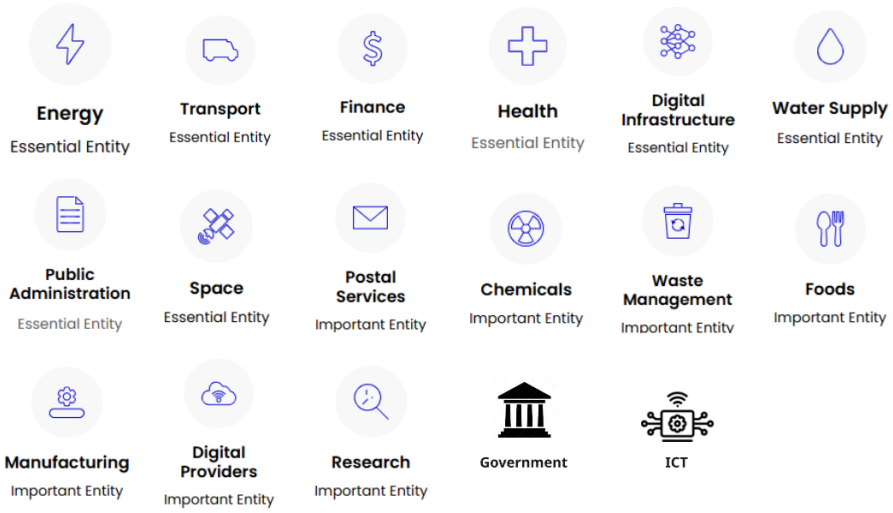


Figure 2.2: NIS1 and NIS2 scope of sectors

2.1.2 Compliance Behavior under Cybersecurity Regulations

Although NIS2 promotes risk-based security improvements, earlier responses to comparable EU regulations - most notably the General Data Protection Regulation (GDPR) [13]- highlight a tendency among organizations to adopt a compliance-first mindset. Despite GDPR's intent to embed privacy-by-design principles, its 2018 rollout was characterized by fast, surface-level adaptions, particularly among SMBs, who experienced ambiguity in the regulation's wording and struggled with limited internal resources. Research by Sirur et al. (2018) [14] and Teixeira et al. (2019) [15] illustrates how compliance efforts often resulted in little more than policy updates and documentation exercises, with minimal operational impact. These behavioral patterns raise questions whether NIS2 may trigger similar outcomes. While GDPR and NIS2 address distinct domains, privacy, and cybersecurity, respectively, the structural parallels between the two provide a useful basis for comparative analysis, which will be explored later in this thesis.

The behavior regarding surface-level adaption suggests a risk for NIS2: heavy penalties could motivate organizations to focus on avoiding sanctions, rather than proactively enhancing their cybersecurity posture. Research confirms that such negative enforcement dynamics can drive "check-box" compliance cultures, particularly in resource-constrained environments such as the ones often times seen in SMBs.

2.1.3 Risk-Based Security vs. Compliance-Based Approaches

The tension between risk-based and compliance-based approaches is longstanding. A risk-based approach focuses on identifying and mitigating threats relevant to a specific context, while compliance-based models ensure all mandated controls are formally in place.

Literature from Lin & Saebeler (2019) [16] cautions against treating these approaches as opposites. Instead, a hybrid strategy, where compliance frameworks provide a baseline and risk-based methods address evolving threats, is more effective. Cybersecurity frameworks like ISO/IEC 27001 and NIST CSF reflect this integrated vision by combining control structures with continuous risk assessment and improvement cycles.

Wang et al. (2024) [17] argue that true cybersecurity efficacy lies in going beyond compliance, embedding risk thinking into security operations. Yet they also note that overlapping standards (GDPR, ISO 27001, CRA, etc.) can increase complexity and detract from real security gains.

2.1.4 NIS2's Risk Management Provisions and Expectations

NIS2 attempts to balance compliance mandates with a flexible risk-based ethos. Article 21 [10] outlines key domains where measures must be taken, yet leaves implementation details to the organization. For example, while vulnerability disclosure is required, the process itself is not rigidly defined, allowing entities to align it with their governance systems.

Continuous improvement is also mandated: organizations must assess and test the effectiveness of their measures over time. State-of-the-art technologies are cited as a benchmark, implying a moving target that evolves with the threat landscape. Incident reporting timelines (Article 23) and enforcement mechanisms ensure these provisions are not optional, while national CSIRTs and EU cooperation structures encourage shared risk management across sectors.

2.1.5 Implementation Challenges and Organizational Responses

Implementation will pose hurdles, especially for *medium-sized* organizations that have newly fallen under the directive's scope. Practitioner guides aimed at SMBs flag limited budgets, skills shortages and uncertainty about what constitutes "proportionate" controls as the most common pain-points [18, 19, 20]. Survey data collected by the European Cyber Security Organization (ECSO) show that nearly three-quarters of entities lack a dedi-

cated NIS2 budget and one-third report *no* top-management involvement; medium-sized companies are the most affected [21]. These observations echo the GDPR rollout, where ambiguous wording and compliance costs weighed the heaviest on small businesses [14, 15, 22].

The broader regulatory environment further complicates matters. NIS2 co-exists with sector-specific regimes such as the **Digital Operational Resilience Act (DORA)**, which from 17 January 2025 supersedes NIS2 for financial entities and introduces parallel ICT-risk and incident-reporting duties [23, 24]. In the product domain, the **Cyber Resilience Act (CRA)** (Regulation (EU) 2024/2847)imposes mandatory vulnerability-handling and disclosure obligations for digital products, risking dual-reporting when service providers are already subject to NIS2 timelines [25, 26, 27].

Divergent national transposition amplifies the burden. An ECSO white paper catalogs differing classification thresholds, reporting templates and supervisory models, noting that only four Member States had fully transposed the directive by December 2024 [21]. Consultancy analyses reach similar conclusions, warning that multinationals may need to parallel compliance tracks until harmonization improves [28]. Such fragmentation encourages "lowest-common-denominator" compliance among cross-border firms.

Finally, early industry messaging reveals a pronounced *checklist mindset*. Vendor checklists and gap-assessment playbooks dominate the public discourse, emphasizing documentation over substantive risk reduction [19, 29, 20]. Interviewees in the present study caution that genuine risk-based programs emerge only when executive leadership allocates recurring resources *and* sector authorities issue clear, interoperable guidance.

2.1.6 Towards Risk-Based Improvement or Mere Compliance?

The central question remains: will NIS2 catalyze genuine security improvement, or merely expand regulatory formality? The literature paints two potential trajectories. In the best case, NIS2 encourages strategic, risk-driven practices across Europe. In the worst case, it produces surface-level compliance that fails to elevate actual cyber resilience.

Several enablers could help tip the balance toward meaningful change: active sectoral regulators, EU support for SMB capacity-building (e.g., through the Digital Europe Program), and a strong culture of information-sharing. Ruohonen & Timmers [30] argue that these support structures are essential to help organizations move beyond legal checklists.

Ultimately, the success of NIS2 will depend on how its principles are translated into organizational behavior. Real-world adoption of risk-based security (as opposed to form-only

compliance) requires more than regulation: it demands resources, leadership, and shared understanding across sectors. As empirical studies emerge over the next years, they will determine whether the directive's promise of cyber resilience has been fulfilled.

2.2 GDPR Implementation: Insights and Impact

This section provides a brief overview of the GDPR's implementation experience to offer relevant points of comparison with NIS2. It highlights how organizations approached compliance and how this can be compared to a risk-based approach, the role of external consultants, and the emergence of audit-oriented behavior. These insights serve as a foundation for identifying recurring patterns that may also appear under NIS2, particularly in relation to documentation practices and enforcement-driven strategies.

2.2.1 Policy Implementation Across EU Nations

The GDPR, as a regulation, applied directly across EU Member States from May 2018. However, national legal landscapes still influenced implementation. Countries introduced national Exemptions allowed under GDPR, leading to divergence. For example, the minimum age for consent was set at 16 in the GDPR, but many countries lowered it to 13, resulting in a patchwork of consent ages across Europe [31].

Germany went further on Data Protection Officer (DPO) requirements, mandating DPOs for firms with just ten employees processing personal data, surpassing GDPR's own threshold [31]. Other states allowed broader exemptions: the Netherlands permitted biometric data processing for security without consent, and many allowed health data to be processed without consent when necessary for medical treatment [31].

Additionally, enforcement strategies varied: Austria and Hungary's early laws recommended warnings before fines, creating an informal grace period [31]. On collective redress, some Member States enabled NGOs to file GDPR complaints, though implementation was uneven [31].

2.2.2 Economic Impact on Businesses

Compliance costs. GDPR implementation imposed high direct costs, especially for smaller businesses. A 2017 PriceWaterhouseCoopers (PWC) survey found over 40 % of companies expected to spend more than $10 million on compliance [32]. Follow-up work by Ernest

& Young (EY) and the International Association of Privacy Professionals (IAPP) estimated organizations were already spending an average of €1.3 million per year by 2018, mostly on legal advice, data-mapping tools, and staff training [33]. Cisco's 2023 *Data Privacy Benchmark* suggests that ongoing privacy budgets now average $2.7 million for mid-size firms and $4.4 million for large enterprises, with staffing (especially Data-Protection Officers (DPOs)) representing the single largest line-item [34]. While blue-chip companies can absorb these figures, SMBs face proportionally higher burdens: a 2020 European SME (Small and Medium Enterprises, Not Subject-Matter Experts) panel showed that 62 % spent at least €10 000 in their first year of GDPR compliance, and nearly one-third had to defer other IT projects to fund privacy controls [35].

Productivity and operational drag. Beyond budget outlays, firms cite slower product release cycles and protracted vendor onboarding as indirect costs. A joint IAPP-EY governance study found that median review-and-approval time for new data-processing projects more than doubled (from 4 weeks to 9 weeks) after GDPR came into force [36]. Interviewees in that study noted a "red-tape effect," whereby even low-risk internal analytics required multi-layer privacy impact assessments, delaying time-to-market.

Innovation and market effects. Venture-capital flows into EU tech declined markedly in the first 18 months post-GDPR. Jia, Jin Wagman (NBER) document a 26 % drop in deal count and roughly $3.4 million in lost investment per week, attributing the decline to heightened uncertainty around data-driven business models [37]. Smaller ad-tech firms were hit particularly hard as advertisers consolidated spend with "privacy-ready" platforms such as Google and Facebook, thereby increasing market concentration [38]. Some U.S. publishers chose to geo-block EU traffic; American Action Forum identified more than 1 000 U.S. websites that became inaccessible to European users within weeks of GDPR day-one, a tactic aimed at avoiding extraterritorial compliance risk [38].

Ongoing effects and emerging benefits. Although compliance remains expensive, firms are beginning to report positive returns. Cisco's latest benchmark shows that 94 % of respondents believe their privacy investments now deliver net benefits, citing shorter sales delays and faster incident recovery [34]. Consumer trust appears to have improved as well: Eurobarometer polling shows two-thirds of EU citizens are now aware of their data-protection rights, and businesses with visible GDPR credentials report higher customer-retention rates [31]. Nonetheless, costs persist: an SME (Small and Medium Enterprise, Not Subject-Matter Expert) survey in 2020 found that most firms still spend between €1 000 and €50 000 annually on GDPR upkeep, with 57 % doubting full compliance [35]. Taken together, the evidence points to a mixed legacy: GDPR raised the privacy baseline and stimulated trust, but it also imposed material financial and operational drag, outcomes that may foreshadow the implementation dynamics of NIS2.

2.2.3 Enforcement Mechanisms and Oversight

DPAs and Enforcement. Enforcement is handled by national Data Processing Agreements (DPAs), with the European Data Protection Board (EDPB) coordinating cross-border issues [31]. In the first year, only 15 EU countries issued fines, totaling 91 in all. Germany alone issued nearly half of those [31].
By 2021, over 800 fines had been issued. Major actions included Google (€50M), H&M (€35.3M), Telecom Italia, and British Airways [31]. Spain became a leading enforcer by number of cases, though fine sizes varied.

Company-Level Impact. Enforcement prompted companies to revise practices. H&M's profiling of staff led to both a fine and remedial action. Thousands of smaller firms faced corrective orders or warnings [31]. Common infractions included weak security and consent mechanisms.

Resourcing Issues. Many DPAs remain underfunded, prioritizing complaint handling over proactive guidance [31]. EU reports urge more resources and IT expertise to sustain enforcement levels.

2.2.4 Legal and Regulatory Perspectives

GDPR required states to align national laws, leading to reforms in employment, media, and research regulations. Initial delays in legislative alignment caused rollout confusion [31].
The EDPB has since issued interpretive guidance to promote harmonization, although national differences persist [31]. Globally, GDPR has inspired laws like Brazil's LGPD and California's CCPA, reinforcing its influence [39].

2.2.5 Sector-Specific Implementation

Technology. Online platforms underwent massive changes: explicit cookie consent, privacy dashboards, and frequent DPA investigations [39].

Finance. Financial institutions largely adapted smoothly, but tensions remain between GDPR and anti-fraud retention requirements [39].

Healthcare. Healthcare faced challenges balancing data sharing and privacy. Projects were delayed due to uncertainty in handling sensitive data [39].

Public Sector. Governments implemented GDPR with varying success. Public awareness

improved, but legacy systems and legal exceptions created friction [31].

2.2.6 Corporate and Public Response

Public Reaction. GDPR raised awareness; over two-thirds of Europeans knew their rights within a year [39]. Consent fatigue was common, but complaints and requests surged.

Corporate Shift. Initial fear gave way to strategic compliance. GDPR is now a reputational matter, with companies marketing their privacy stance [39].

2.2.7 Academic and Policy Insights

Scholars praise GDPR for empowering individuals [31], but studies note high compliance costs and increased market consolidation [39].

Economists debate short-term economic impacts versus long-term trust benefits [39]. Legal researchers analyze DPA case law and call for stronger EU-level enforcement [31].

Behavioral research questions whether consent mechanisms truly empower users, and policy studies call for SMB guidance and privacy-by-design tech development [39].

In sum, GDPR has shaped global data governance, but its implementation reveals enduring challenges in balancing privacy, economic growth, and regulatory clarity.

2.3 GDPR Implementation as a Precedent

The implementation of the General Data Protection Regulation (GDPR) over the past several years serves as a valuable precedent, and numerous studies have dissected the challenges organizations have faced [40, 41, 42], many of which are instructive for the Network and Information Security Directive (NIS2). Sirur, Nurse, and Webb [14] provide an early empirical look at the GDPR rollout, documenting significant costs and resource demands. Their study reported that companies "had to allocate extended budgets for GDPR compliance" and often needed to hire new professionals and invest in new systems and processes [14]. This directly informed our interview questions about compliance costs under NIS2: we asked experts whether their organizations have devoted additional budget or personnel to meet NIS2 obligations, anticipating similar financial strain.

Sirur, Nurse, and Webb [14] also found that smaller enterprises felt "unequipped" and

lacked dedicated data-protection focus, partly owing to delayed official guidance. We reflected this finding in questions about guidance and support, probing whether interviewees felt sufficient direction from regulators or whether, as with the GDPR, clarity came only after initial struggles. Freitas and Silva [43] likewise, noted that small and medium-sized businesses (SMBs) faced acute constraints in "human and financial resources, making it challenging to undertake required measures for compliance".

Another recurrent theme is internal resistance and organizational change. Teixeira, Ferreira, and Liu [15] observed that GDPR compliance often required cultural shifts and that "a significant challenge lies in overcoming resistance to change ... at various organizational levels".

Importantly, the GDPR literature also sheds light on implementation outcomes and longer-term effects once initial hurdles are overcome. In a systematic review, Smirnova and Travieso-Morales [22] it found that, while organizations struggled with compliance, those efforts increasingly became tied to broader organizational objectives. They note that the GDPR's influence extended beyond mere legal compliance to aspects such as competitive positioning, customer trust and "aligning privacy with organizational goals". This perspective influenced our interviews to go beyond challenges and ask about the perceived benefits or strategic value of compliance. For instance, we queried whether experts see NIS2 bringing competitive advantage (e.g., as a credential of good security) or improved incident resilience, not just penalties for non-compliance. The idea, drawn from Smirnova and Travieso-Morales [22] and others, is that effective implementation might be leveraged to build trust or streamline security practices, much as some firms eventually integrated the GDPR into their business strategy rather than treating it as a check-box exercise. Additionally, the literature emphasizes ongoing difficulties with regulatory complexity, ambiguity in legal texts and lack of practical guidelines were recurring problems for GDPR implementers [22]. We therefore asked experts whether NIS2's requirements are clear or whether interpretation is challenging, to capture whether NIS2 is following the same pattern of initial legal ambiguity that needs iterative clarification.

In summary, lessons from the GDPR's implementation heavily informed our expert-interview design for NIS2. Early studies such as Sirur, Nurse, and Webb [14] and Freitas and Silva [43] alerted us to ask about compliance costs and resource allocation, as these were major pain points in 2018. Work by Teixeira, Ferreira, and Liu [15] put internal resistance and change management on our radar, leading us to include questions on how NIS2-related changes are communicated and accepted internally. Finally, the comprehensive review by Smirnova and Travieso-Morales [22] encouraged us to examine both challenges and positive outcomes, prompting interview questions on whether organizations are using NIS2 as an opportunity to improve security posture or achieve other benefits. By directly linking these GDPR implementation insights to analogous aspects of NIS2, our literature review ensured that the interview guide was grounded in known real-world issues and that we

probed the most pertinent areas of concern and opportunity as identified by prior scholarship.

Chapter 3

Methodology

This chapter presents the methodological approach of the study. It begins by detailing the research design and its rationale, followed by a description of the qualitative and quantitative methods used for data collection. The chapter then outlines the development of the interview guide, including ethical considerations, pilot testing, and the reasoning behind participant selection. Sampling strategies for both the interviews and the survey distribution are addressed to ensure transparency regarding participant inclusion and exclusion. The methods for analyzing qualitative data are presented, which covers the coding process and the analytical approach.
A final section includes the supplementary research done, examining Member State transpositions of the NIS2 Directive, which complements the primary findings. The chapter concludes by addressing the study's limitations.

3.1 Research Design

This study adopts a mixed-methods research design, combining qualitative and quantitative elements to examine the organizational impact of cybersecurity regulation; Specifically, the NIS2 Directive, in line with the research questions outlined in section 1.4. The primary focus is on qualitative insights gathered through semi-structured interviews which is supported by a supplementary survey to test whether the patterns observed through interviews also comes to show more broadly across a larger respondent base, without aiming for statistical generalization. This will, in theory, highlight recurring patterns across the interview-, and survey-respondent base.

The research design has been selected to enable an in-depth understanding of how organizations interpret, implement, and respond to regulatory demands, especially in the context of complex, non-prescriptive legislation. This section outlines the methodological structure of the study, including the type of study conducted, the rationale behind the chosen approach, as well as the (philosophical stance supporting this research.

3.1.1 Methodological Development and Decision Rationale

The methodology used in this study is the product of a deliberate and iterative development process, which has been shaped by both theoretical interests and practical constraints encountered during the early stages of the project.
The initial research idea emerged from a noticeable gap in the current academic and industry discourse: While much attention has been paid to the benefits of cybersecurity regulation, little has been written about the potential unintended consequences. This absence sparked a critical interest in exploring how the transition from industry-driven standards to state-imposed regulation may influence organizational cybersecurity practices. Not only in terms of compliance, but also in relation to strategic depth, risk awareness, and security investment behaviors.

To examine this question, the NIS2 Directive was selected as a concrete legislative anchor point. As a newly adopted and still-unfolding directive within the EU, NIS2 offers a timely opportunity to assess how organizations interpret and respond to its requirements. it allowed the study to be grounded in a contemporary regulatory context while simultaneously addressing broader questions about the nature and effectiveness of cybersecurity legislation. The directive's relatively young position in the cybersecurity-related legislative landscape, and the lack of critical analysis surrounding its implementation, created the opportunity for this to be a suitable candidate through which the underlying hypothesis of the study could be explored.

Early conceptual discussions with experienced practitioners helped refine the direction of the study. One particularly influential input came from a regulatory consultant who suggested avoiding sectors previously known for operating in strictly regulated domains, such as Finance, Energy, Health, or digital infrastructure. Due to their longstanding familiarity with compliance demands, these sectors were less likely to exhibit the behavioral dynamics that the project set out to explore. As a result, the study chose to focus on the organizations and experts connected to sectors that have historically been less regulated. Here, the introduction of NIS2 might bring more disruptive of unfiltered reflections.

Following the decision to exclude certain heavily regulated sectors from the study, it was also considered whether organizational size should influence the selection of interview participants. While no strict thresholds were set, size was treated as an indicative factor during the interviewee search. This was primarily done to avoid extreme outliers that could distort the analysis. In early conversations with professionals, it became clear that both very large and very small organizations tend to follow distinct implementation paths that may not reflect the broader group. The study has drawn on the size classifications outlined in the NIS2 Directive to establish a loosely defined range. These indicators closely mirror the European Commission's Small and Medium Business (SMB) definitions [44] as depicted in figure 3.1. These classifiers were used not as hard inclusion criteria, but as

a practical reference for identifying organizations likely to show early and observable patterns in their response to NIS2. The aim is not to categorize organizations strictly by size, but rather to note how organizational scale might influence the level of preparedness, internal capacity, and strategic response to regulatory pressure.

SMB Definition				
Company category	**Staff headcount**	**Turnover**	**Or**	**Balance sheet total**
Large-scale	> 250	> € 50 m		> € 43 m
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

Figure 3.1: SMB definition

The data collection strategy also evolved significantly throughout the project. The initial plan was to conduct interviews directly with affected organizations. However, after several unsuccessful outreach attempts and one early interview that provided little insight, the approach was reassessed. It became clear that many organizations were either unwilling to speak openly about their implementation efforts or were still in too early stage of engagement with the directive to provide meaningful reflections.
This led to a strategic pivot in the data gathering phase. Rather than attempting to extract fragmented insights from individual companies, the study turned to consultants and advisors who work across multiple organizations. These professionals offered broader and more informed perspectives on how the directive is being interpreted and operationalized in practice. Consultants and advisors were also more willing to participate in interviews and could share anonymized observations across industries, which provided the type of comparative insight that would have been difficult to gather from single organizations. This shift in the approach not only improved access but also aligned more closely with the study's focus of exploring structural and behavioral patterns and outliers rather than isolated case studies.

Ultimately, the research approach evolved through a process of critical reflection, environmental scanning, and practical testing. The final methodology has emerged as a direct response to both the subject and the limitations of the research context. This methodological development further reflects the adaptive, exploratory nature of the study itself, where data collection strategies could remain aligned with the core research objectives.

3.1.2 Type of Study

This study applies a predominantly qualitative mixed-method design which centers around semi-structured expert interviews as the primary data source. This approach is selected to capture the nuanced perspectives of individuals directly involved in the implementation, or interpretation, of the NIS2 Directive, including those in regulatory compliance, Cybersecurity leadership, and consulting/advisory roles. The interview is designed to explore how organizations or consultants experience regulatory demands, how they interpret risk versus compliance, what impacts the decision path of organizations, and whether NIS2 leads to meaningful changes in security posture.

To support, supplement, and expand on the scope of these insights, the study includes a quantitative component in the form of a structured survey. The survey is intended to identify whether themes coming from the interviews are observable across a broader group of organizations which may lay outside the scope of the study criteria, as further detailed in Section 3.5.4. While the survey does not aim to produce generalizable statistics, it can serve as a supporting tool to reinforce or nuance the qualitative findings.
The qualitative track is prioritized due to the nature of the research questions that may not be evident through quantitative measures alone.

3.1.3 Approach Justification

The decision to adopt a qualitative and exploratory approach is grounded in the nature of the research questions posed in this study. The overall aim is not to test a predefined hypothesis, but rather to investigate how organizations respond to a "newly" introduced regulatory framework (NIS2) whose implementation is still in progress and whose effects remain largely undocumented. The study focuses specifically on uncovering the perceptions, strategic adaptions, and unintended consequences that may emerge as organizations attempt to align with the directive. These are the dimensions of organizational behavior that are unlikely to be otherwise meaningfully captured through solely quantitative measures.

The qualitative approach is particularly applicable when exploring how regulation is interpreted and operationalized within organizations. It allows for flexibility in capturing complex reasoning, varying levels of maturity, and potentially highlighting tensions between compliance obligations and security priorities. By conducting the semi-structured interviews, the wanted outcome is that the study gains access to the perspectives of those directly involved in regulatory implementation or advisory roles, enabling the identification of patterns, concerns, and decisions that are otherwise left unseen which are context-dependent and often shaped by informal, non-public processes.

The exploratory nature of the research is equally important. As NIS2 is still in its early stages of implementation across the EU, the amount of academic literature and formal evaluations remain somewhat limited. This creates an opportunity, and in conjunction with this a need, for an approach that is open-minded, adaptive to a degree, and capable of identifying rising themes. Instead of attempting to assess the effectiveness through predefined metrics or outcome indicators, the study aims to understand how organizations experience the directive and what consequences may come to show in the journey towards compliance.

The combination of the qualitative approach and the exploratory angle makes it possible to identify not only how organizations interpret regulatory demands, but also what consequences - short-term and long-term -, compromises and strategic adjustments may occur along the path towards compliance. The study is particularly interested in whether the compliance process leads to meaningful improvements in security, or whether it instead results in resource misallocation, a reduction in security ambition, or other potential unintended effects. With this approach, the study aims to understand how cybersecurity regulation influences decision-making, resource-allocation, and strategic direction as a broader organizational response rather than the step-by-step implementation process.

3.1.4 Philosophical Grounding

This study adopts a pragmatic philosophical stance which his grounded in the belief that knowledge is best generated through engagement with real-world practices and experiences. Rather than starting with a predefined and fixed hypothesis or attempting to test predefined variables, this study takes an exploratory approach focusing on how organizations and consultants interpret and implement the NIS2 Directive in practice.

The decision on choosing a mixed-methods design reflects this orientation. Qualitative interviews were conducted to assess nuanced insights based on experience, while the supporting quantitative survey provided complementary data to broaden the scope and strengthen the empirical ground.

The study does not aim to produce or claim a singular and objective account of NIS2 implementation. instead, the study focuses on capturing patterns, interpretations, and recurring challenges expressed by those closest to the directive itself. This approach aligns with the study's core objective, which is to critically assess whether the NIS2 Directive fosters substantial improvements in cybersecurity practices or encourages superficial compliance.

3.2 Data Collection Methods

This section outlines the data collection methods used in the study, as further entailed in 3.4. The objective is to gather insight on how organizations respond to cybersecurity regulation in practice, with an emphasis on how the NIS2 Directive is perceived and acted upon by professionals with direct exposure to the implementation. The following subsections will detail the primary and secondary methods used, including interview structure, participation selection, survey purpose, and how the data is interpreted to support the overall research objectives.

3.2.1 Primary Method

The primary method of data collection is a series of semi-structured interviews that were conducted with subject-matter experts (SMEs) that engage in the interpretation as well as the operationalization of the NIS2 Directive. The candidates include Cybersecurity consultants, compliance professionals, advisors, and top management individuals; People who work close with organizations affected by the directive. In total, eight structured interviews were completed: six with Danish consultants and compliance professionals, one with a Spanish consultant, and lastly one with a Norwegian consultant. The study notes that while Norway is situated geographically within Europe, they are not a Direct member of the European Union. Therefore, their contribution and adherence to directives and other EU-demanded legislation happens on the obligations under the European Economic Area (EEA) requirements, which outlines a different set of adherence requirements. Therefore, the NIS2 Directive, while serving as a positive cybersecurity foundation, is not mandated for the country. The interviewee was still chosen because of relevance in implementing NIS2.
The approach of semi-structured interviews were chosen to allow for consistency across various themes while leaving room for flexibility and to follow up on interesting or unexpected responses. The method provide a much-needed balance between structure and the option to go off track. This deemed itself valuable in the context of exploring complex topics such as regulatory pressure, resource trade-offs, or strategic decision-making under uncertainty. The interview guide was constructed around a handful of thematic areas which were identified during the early stages of the project. These themes include:

- Organizational context and sector.
- Level of awareness and interpretation of NIS2.
- Perceived strategic impact of the directive.

- Resource allocation and internal prioritization.
- Experiences with compliance planning and implementation.
- Observed consequences, both intended and unintended.

The interviews were conducted both physically and online and lasted somewhere between 30–60 minutes. All participants were informed about the full anonymity, which not only served as a strategic decision to gather more insightful responses, but also ensured the interviewees responses were masked to an extent that even partially identifiable information could not be attributed to the individual. The result of this created a space for discussions wherein sensitive organizational considerations were no issue. Interview responses were transcribed and prepared for thematic analysis from section 3.5.1 in accordance with ethical handling procedures described later in the section 3.4.

3.2.2 Secondary Method

To complement the data of the interviews, an optional online survey was developed and distributed to a broader group of professionals within the cybersecurity-related domain. The survey was initially designed to validate or contrast certain themes from the interviews, and to provide an indication of how widespread certain patterns might be across different sectors or organization sizes.
The survey content was derived directly from the interview guide with minor adjustments, to focus on aspects such as:

- Compliance status and perceived impact.
- Budgetary and resource shifts attributed to NIS2.
- Strategic motivations behind compliance efforts.
- Minimum viable compliance goals.
- Organizational readiness and internal engagement.

The survey was further distributed through LinkedIn, and responses were collected anonymously. The questions consisted primarily of closed questions using Likert scales or predefined multiple-choice formats. This made the aggregation of the data collection for trend analysis much more efficient.
While the survey was not designed to deliver generalizable results, it supports the primary data collection method by providing insights that either reinforce or challenge the qualitative findings. Therefore, the survey finds its place in the study by offering a broader perspective of the detailed viewpoints from the interviews.

3.3 Interview Design

This section outlines the design and rationale of the interviews conducted for this study. It explains the ethical considerations, interview structure, question development, and pilot process that shaped the final data collection. The goal was to ensure methodological rigor and relevance in capturing expert perspectives on the NIS2 Directive.

3.3.1 Ethical Questions used to Shape the Approach

Before developing the interview structure and guide, the topic of ethical considerations were carefully reviewed and implemented in accordance with the book "Interviews–learning the craft of qualitative research interviewing" [45]. These principles informed all stages of the interview process, from participant recruitment to data handling. The ethical guidelines outline four key areas of focus: informed consent, confidentiality, consequences, and the role of the researcher.

Informed consent was obtained through a formal agreement shared with participants prior to each interview in the form of a contract in appendix A. Since the interviews sought participants' general professional knowledge, individuals were considered capable of making informed decisions about their involvement. Participants were also provided with a copy of their interview transcripts to review and revise if necessary, which in essence supports transparency. This raises the question of how much information should be shared with participants. In this study, the decision was made to provide them with as much information as possible. To support informed and meaningful contributions from industry experts, participants were given access to the interview questions, a description of the project scope, and a clear explanation of the study's objectives. The rationale for this level of transparency was to ensure participants had a solid foundation for responding to the questions, while also understanding the overarching goals of the project. Given the neutral nature of the study's aim, this approach was intended to foster clarity and minimize bias.

Confidentiality was maintained throughout the research process, starting with interview planning and continuing through data storage and analysis. All data was securely stored using the university's OneDrive system. When AI tools such as Microsoft Copilot were used, they operated exclusively within the same secure environment, and in accordance with their principles under consent to manage data securely and to not be used as training data [46]. Interview data was reviewed to remove any sensitive-, identifiable-, or partially identifiable information about the participant(s) or any third parties mentioned during. Additionally, all interviews were coded and abstracted so that original sources and phrasing could not be traced back to individuals.

Consequences in this context primarily involve the potential identification of business partners mentioned by participating consultants or the participants themselves. However, because the project focused on generalized knowledge and incorporated appropriate safeguards, the risk of harm was minimal. Another potential consequence is the possibility that readers might misuse the findings, particularly if they apply insights from the study without fully understanding the NIS2 Directive. This scenario is unlikely, and responsibility for such interpretation rests with the reader.

Regarding the **role of the researcher**, it is recognized that the research was conducted by a team of students rather than industry professionals. While this may introduce certain biases, such as a limited understanding of insider organizational dynamics, it also brings an independent perspective. This position was considered throughout the study, though it did not require changes to the interview guide or the way interviews were conducted.

3.3.2 Interview Structure

The structure of the interviews was designed based on several key factors: the type of interview, organization and flow of questions, time allocation, mode of delivery, and the role of the interviewer.
Given the novelty of the NIS2 Directive and the limited number of real-world implementations and available experts, a qualitative, semi-structured interview format was chosen. This approach allowed for both consistency across interviews and flexibility to adapt to each participant's expertise and insights. The semi-structured format was particularly suited to exploring a topic still in development, where rigid questioning would risk overlooking valuable contextual knowledge.

Each interview was scheduled to last approximately 40 to 50 minutes, which provided participants with sufficient time to elaborate on their perspectives while respecting the time constraints of busy professionals. Although longer interviews could have yielded even richer data, this time frame represented a practical balance between depth, feasibility, and respect towards the participants' time.

The interview flow was designed to begin with general questions to establish context and rapport, followed by more abstract and targeted questions aligned with the research objectives. This progression helped ease participants into the discussion and facilitated more thoughtful responses on complex issues. While a guiding structure was in place, the interviewer maintained the flexibility to adjust the order of questions as needed to preserve the flow of conversation and allow participants to develop their ideas naturally.

Most interviews were conducted online via Microsoft Teams, with a few conducted in person. The remote format did not negatively impact the quality of the interviews and

was found to be equally effective. Each interview was conducted by one interviewer and accompanied by at least one note-taker. In one specific case, the interview was recorded due to scheduling constraints; transcription was completed afterward, and the video was permanently deleted to comply with ethical data handling procedures.

3.3.3 Interview Guide

Developing an interview guide for a project focused on the NIS2 Directive presented a unique challenge, especially when determining what constitutes a sufficient foundation for drafting meaningful questions. The process began with the creation of a shared working document in which the team outlined the overall goals of the project and how the study would be conducted. Based on this framework, each team member independently drafted a preliminary version of the interview guide, including references to sources that inspired their proposed questions.

The interview guide was primarily shaped through internal team discussions and expert conversations, guided loosely by themes present in emerging literature on NIS2 and broader regulatory compliance frameworks like GDPR. While existing literature offered useful context, the interview questions were not drawn directly from specific academic studies. Instead, the guide reflected the team's shared curiosity and the exploratory nature of the project, with a focus on real-world interpretations and applications of the directive. During the research phase, it became clear that there was a lack of credible, targeted literature addressing the efficacy of cybersecurity directives like NIS2. Much of the available material focused on the speculative societal impact of the directive or the practical challenges of implementation within organizations. A partial gap was observed in the GDPR literature with respect to cybersecurity-specific regulatory dynamics. While GDPR implementation studies offer valuable insight into compliance behavior and organizational adaptation, their primary focus remains on privacy outcomes. This thematic emphasis limits direct transferability to the cybersecurity-oriented scope of NIS2. Nonetheless, the structural and behavioral challenges in GDPR studies remain highly relevant and were used to guide interview design and comparative framing throughout this study.

As a result, the development of the interview guide required a synthesis of fragmented sources, combined with a more open-ended approach aimed at uncovering practitioners' real-world interpretations and strategic responses. The goal was not just to validate known implementation issues, but to explore how effective NIS2 is perceived to be in practice. This is a topic that existing research has largely overlooked.

The final draft of the interview guide consisted of 10 questions and one bonus question, designed to fit within the 40–50-minute timeframe. Each question was aligned with one or more of the research questions guiding this study, as shown in table 3.1. While the

questions were grouped thematically, it is important to note that due to the semi-structured and exploratory nature of the interviews, most questions had the potential to generate insights relevant to multiple research questions. And all was generated first to encompass implementers as seen in appendix B, but was later changed to be for consultants as shown in the final draft of table 3.2.

Table 3.1: Mapping of Interview Questions to Research Questions

Interview Question(s)	**Associated Research Question(s)**
Questions 1–6	focused on gathering organizational background and identifying patterns of NIS2 implementation. Primarily addresses RQ1: "What are the observable patterns among organizations implementing NIS2?"
Question 7	Explores whether compliance efforts lead to tangible security improvements. Primarily addresses RQ3: "Does NIS2 provide tangible security improvements, and is the value of implementation present short/long-term?" and also informs RQ2 by exploring motivations behind implementation approaches.
Question 8	Expands the understanding of implementation challenges and participant perceptions of the directive. Supports both RQ1 and RQ4.
Question 9	Investigates whether NIS2 is viewed as a regulatory burden or a strategic opportunity. Provides insight into RQ2: "What organizational or regulatory factors contribute to a compliance-driven approach?"
Question 10	Invites expert suggestions for improving NIS2, directly addressing RQ4: "How do industry experts interpret the NIS2 Directive in terms of its completeness, clarity or practicality?"
Bonus Question (11)	Explores whether patterns from earlier regulations (such as GDPR) are being mirrored in NIS2 implementation. Provides additional insight into RQ4, particularly regarding expert interpretation of NIS2's direction and purpose.

Table 3.2: Final Interview Guide

Q#	Interview Question
1	Can you briefly introduce yourself, your role, responsibilities, and how long you've been with the company?
2	What industry does your company operate in, and how large is it in terms of employees? What is the main size of companies you work with?
3	What are the main sectors of companies you provide services to in regard to NIS2? How do you assess their cybersecurity strategy (risk-based, compliance-driven, or a mixture)?
4	When do clients first become aware of NIS2, and how does it compare to their initial expectations?
5	What prompts organizations to implement NIS2, and how would you describe their current level of compliance after implementation? (e.g., fully compliant, in progress, not started)
6	What is the point at which clients reach out to you for help? What internal and external resources did they rely on before seeking assistance?
7	In retrospect, does NIS2 affect businesses significantly? Do compliance efforts help them achieve tangible security improvements, or do you see a focus on just meeting the minimum requirements?
8	What are the major challenges they encounter when implementing NIS2 (e.g., financial costs, expertise gaps, operational complexity, internal resistance)?
9	Do you see NIS2 as a growth driver or mainly a regulatory requirement? Have you identified a minimum viable compliance level to balance cost and compliance? How do your clients perceive this?
10	If you could change anything about NIS2, what would it be?
11	**Bonus Question:** Have you observed any patterns in how previous regulations like GDPR were implemented? Do you see NIS2 following a similar trajectory?

3.3.4 Pilot Testing and Revisions

Before conducting the first full interview, the initial version of the interview guide was developed with the intention of interviewing individuals responsible for implementing NIS2 within their own organizations. However, this approach proved difficult after the pilot interview. The participant showed limited understanding of the directive, and more broadly, it became clear that securing interviews with internal implementers would be challenging due to limited awareness of NIS2 and a general lack of willingness to participate.

As a result, the study group made a strategic pivot. Instead of interviewing internal implementers, the study refocused on consultants who had advised multiple organizations on NIS2 implementation. This shift allowed for access to more knowledgeable participants and a broader perspective on the directive's implementation across different industries. It also enabled a more abstracted, comparative view by interviewing individuals who had observed patterns across several companies rather than from within just one.

In addition to this sampling change, a minor adjustment was made to the interview guide following the pilot: one bonus question was added, asking whether consultants saw similarities between NIS2 and earlier regulations such as GDPR. This question was intended to provide comparative insight into how NIS2 fits within the broader landscape of cybersecurity and privacy legislation.

3.4 Sampling Strategy

This section outlines how the interview and survey participants were identified, recruited, and protected.
Our study adopts a purposeful, multistage sampling approach designed to (i) capture the full spectrum of organizational responses to the NIS2 Directive, (ii) maximize analytic depth for the qualitative strand, and (iii) generate a sufficiently heterogeneous survey pool for triangulation. This form of sampling, where the researcher deliberately selects participants who are especially knowledgeable about, or experienced with, the central phenomenon, aligns with established practices in qualitative research [47].
This section further defines how the participant's confidentiality was maintained throughout the sampling process.

3.4.1 Target Population

The study originally aimed to investigate *organizations subject to the NIS2 Directive*, or those with recent experience implementing large-scale IT-related regulation (such as GDPR or PCI DSS). This target group included entities across both *essential* and *important* sectors as defined in the directive, as well as advisory firms that facilitate or audit compliance programs. Specifically, the intended categories were:

- **Operational entities** with direct compliance obligations (for example, cloud providers, financial institutions, energy operators).
- **Supporting actors** such as managed-service providers and SaaS vendors whose offerings support NIS2 compliance for clients.

- **Advisory specialists,** including consultancies and law firms that help design or oversee NIS2 implementation across sectors.

The initial sampling strategy proposed to exclude certain sectors whose cybersecurity responsibilities are already governed by overlapping EU legislation. These included:

- **Telecommunications:** These are covered by the European Electronic Communications Code (EECC) and the 5G Security Toolbox. As a result, NIS2 typically plays a secondary role for these operators.
- **Energy:** Electricity and gas transmission-system operators fall under the Risk-Preparedness Regulation, the Clean Energy Package, and the Critical Entities Resilience (CER) Directive. These frameworks impose sector-specific requirements that could obscure the impact of NIS2.
- **Financial services:** Entities in this sector are now regulated under the Digital Operational Resilience Act (DORA) and PSD2, which introduce more detailed ICT risk management standards that could overshadow the effects of NIS2.

In practice, however, all interviews were conducted with consultants and advisors. This adjustment was made due to challenges in accessing internal implementers, especially those in operational roles. As a result, the intended sectoral exclusions could not be applied consistently. Instead, consultants were selected based on their experience advising a diverse range of client organizations, many of which spanned the originally excluded sectors.

While this adaptation limited direct access to internal decision-makers, it provided a broader, cross-sectoral perspective on NIS2 implementation. The consultants interviewed offered informed views on both strategic and practical challenges observed in the field, thereby preserving the study's relevance to the target population.

3.4.2 Sample Composition

To capture variation across organization sizes, sectors, and maturity levels, the study initially proposed a structured sampling plan. This plan, following the principles of stratified purposive sampling, aimed to ensure representation across key organizational characteristics by selecting participants from defined subgroups [47]. It outlined specific interview targets for micro, small, medium, and large enterprises, as well as advisory professionals as shown in table 3.3.

Stratum	Employee Range	Planned Interviews	Rationale
Micro enterprises	< 10	1	Highly resource-limited; compliance likely minimal or externally supported.
Small businesses	10–49	1	May rely on third-party solutions; often unaware of full compliance scope.
Medium-sized businesses	50–249	2–3	Transitional segment; balancing compliance ambition with budget constraints.
Large-scale organizations	≥ 250	2–3	Subject to full NIS2 obligations; wider variance in maturity, internal capacity, and sectoral exposure.
Advisory / legal specialists	n/a	2–3 professionals	Provide cross-sector insight and meta-perspective on directive interpretation and enforcement.

Table 3.3: Planned sampling structure

This approach originally set a minimum threshold of five interviews to enable the identification of recurring patterns across cases, with an extended target of up to ten to enhance variation. In practice, nine interviews were completed, of which eight involved consultants and advisors who actively support NIS2 implementation across sectors. One interview with a direct implementer was conducted but excluded from analysis due to limited relevance. The final qualitative findings are therefore based exclusively on advisory perspectives. The accompanying survey was distributed opportunistically to supplement the interviews, without a predefined sample size target.

3.4.3 Sampling Method

Sampling Frame and Rationale. The original sampling frame was structured to capture variation in how different types of organizations approach NIS2 implementation. The intended unit of analysis was the **organization**, and the unit of observation was an **individual in a NIS2-relevant decision or advisory role**. This included roles such as CISOs,

compliance officers, program managers, legal counsel, and consultants. The sampling plan aimed to include a variety of organization types that (i) fall under NIS2's scope (essential or important entities), (ii) operate in different sectors, and (iii) vary by size and maturity level.

Purposive Sampling Adaptation. A *purposive* approach was used to identify participants with meaningful insight into the implementation of NIS2.This type of sampling is commonly used in qualitative research to select individuals who can provide rich, relevant, and diverse perspectives on the topic of interest [47]. The original plan was to stratify the sample across three dimensions: sector, size, and implementation maturity. However, during recruitment, it proved difficult to gain access to internal implementers. As a result, the final sample included primarily advisory professionals, such as consultants and legal experts, who work across sectors and support client organizations with NIS2 implementation. Their cross-sector experience allowed them to reflect on challenges faced by different types of entities despite the shift in participant profile.

Recruitment Process. Participants were recruited through a mix of outreach methods: (i) professional networks such as LinkedIn, (ii) introductions from academic and industry contacts, (iii) mailing lists associated with regulatory research, and (iv) industry-specific associations. Each invitation included a study description, confidentiality terms, and a consent form approved by the university's ethics review process.

Access Challenges and Sample Adjustments. The original plan to include direct implementers from sectors like energy, finance, and healthcare was not fully realized due to time constraints and limited contact points. Instead, interviews focused on external advisors who actively support these sectors. This shift still enabled the study to capture implementation trends through second-hand experience and broad sectoral exposure.

Inclusion and Exclusion Criteria. Eligible participants were individuals involved in advising or overseeing NIS2 compliance decisions. Participants had to be based in or work with organizations operating in the EU and be involved in activities such as budgeting, compliance planning, or implementation support. Individuals in purely technical roles or vendors selling NIS2 tools without compliance insight were excluded to avoid bias.

Sample Size Rationale. While the original target was five or more interviews to support pattern recognition, a total of nine interviews were ultimately completed. Eight were with advisory professionals, while one direct implementer interview was excluded due to

limited analytical relevance. Interviews continued until the research team observed that no new insights were emerging, a point commonly referred to as theoretical saturation in qualitative research [47].

Survey Distribution. To supplement the interview data, a brief online survey was shared through LinkedIn groups and professional communities. The survey had no fixed target size and was used primarily to validate themes identified during interviews, rather than for statistical generalization.

3.4.4 Anonymity and Confidentiality

Guiding Principle. All data-handling procedures in this study were designed to ensure that no individual, role, or organization can be re-identified, whether directly or through inference, in the final thesis or any derivative publication. These safeguards combine *data minimization*, *technical protection measures*, and *strict access control*.

Consent and Information Sheet: Each participant received (i) a two-page, plain-language information sheet outlining the study's purpose, data flows, and withdrawal rights, and (ii) a GDPR-compliant consent form. Both documents emphasized that participation was *voluntary* and that all data would be stored and reported exclusively in anonymized form, seen in appendix A.

Interview transcripts were processed and stored within AAU's OneDrive/SharePoint environment, which is subject to Aalborg University's internal IT security controls. While Microsoft Office 365 is not formally approved for the storage of Level 2 confidential data under the university's official data classification and system use model [48], all interview material was anonymized prior to upload. No personal, sensitive, or indirectly identifying information was retained. File access was strictly limited to the research team, and all data remained within the university's protected infrastructure.

Access control: Only the authorized researchers had read/write access to the anonymized data files throughout the study. No external collaborators or third parties were granted access.

Data Masking in Reporting: To preserve participant anonymity, all unique project or product names mentioned during interviews were replaced with generic descriptors such as "payment platform" or "internal tool." In addition, direct quotations included in the

thesis underwent a second anonymization pass to ensure that no phrasing could be traced back to individual participants. Participants were also given the opportunity to review and approve any quotes prior to publication.

These combined measures were implemented to ensure that neither individual identities nor organization-specific details can be inferred from the final thesis.

3.5 Data Analysis

The analysis in this project draws on two primary data sources: semi-structured interviews and a supporting questionnaire. The research strategy prioritized the qualitative material, with the questionnaire used later in the process to contextualize and support the interview findings. Throughout the analysis, the data was examined with the research questions (see section 1.4 as the guiding framework, allowing for both focused and exploratory insights.

3.5.1 Analytical Approach

This study applied Braun and Clarke's six-step approach to thematic analysis [49] to identify patterns of meaning across the interview data in relation to the research questions. Thematic analysis was selected because it offers a structured yet flexible method for organizing qualitative data, especially in exploratory studies where existing theory may not fully capture the complexity of the topic.

The first phase involved familiarization with the data. This was achieved during the transcription and cleanup process, where all notes were reviewed by the coding researcher. During this stage, preliminary observations and impressions were also noted to begin identifying meaningful patterns.

The second phase focused on generating initial codes. Segments of the interview data were manually highlighted using a color-coded system in OneDrive Word documents. Each color was used to represent a provisional category, developed in response to recurring ideas or noteworthy patterns identified during early review. While the coding process was inductive, the research questions served as a general lens, helping to guide attention toward content likely to be analytically relevant.

In the third phase, the initial codes were organized into broader themes. This step involved reviewing and clustering related codes into overarching thematic categories. At this stage, the alignment between codes and specific research questions was made explicit, with each theme being mapped directly to the analytical aims of the study. This structured grouping

helped clarify how different segments of data contributed to answering the central research objectives and allowed for a more focused interpretation moving forward.

The fourth phase involved reviewing themes. The research team collaboratively revisited the initial categorizations to identify redundancy, overlap, or missing dimensions. Through group discussion, the structure of the themes was consolidated, and agreement was reached on the central findings that should be carried forward.

The fifth phase focused on defining and naming themes. Final labels were assigned to each category based on the refined understanding developed through earlier steps, and through internal discussions and debate within the research team. While the themes were shaped during analysis, their formal definitions were finalized later during the results chapter, where they are explicitly presented alongside visual representations. This phase also involved preparing the themes for clearer communication by developing spider graphs and other visual models to support interpretation.

In the sixth and final phase, the themes were integrated into the written analysis. Each theme was linked to one or more research questions and structured into visual models that highlight the main findings. These were then presented in the results and discussion sections. While the analysis focused on synthesizing patterns across interviews, supporting data from the accompanying survey was also used to reinforce or contrast these themes where appropriate. This allowed the study to present a more robust interpretation of the findings, grounded in both qualitative depth and broader indicative trends.

3.5.2 Coding Process

The coding process followed a multi-stage approach to ensure both consistency and analytical depth, as shown in figure 3.2. The first stage involved exploratory manual coding, conducted by a researcher who had attended all interviews and had prior experience with qualitative analysis. All transcripts were collected in a single document hosted on OneDrive, where an open coding method was applied. Different color highlights were used to indicate initial thematic categories, which were generated inductively during the review of the data. The resulting document, used for coding and memoing, reached nearly 14,000 words across 49 pages, reflecting the depth of thematic exploration conducted.

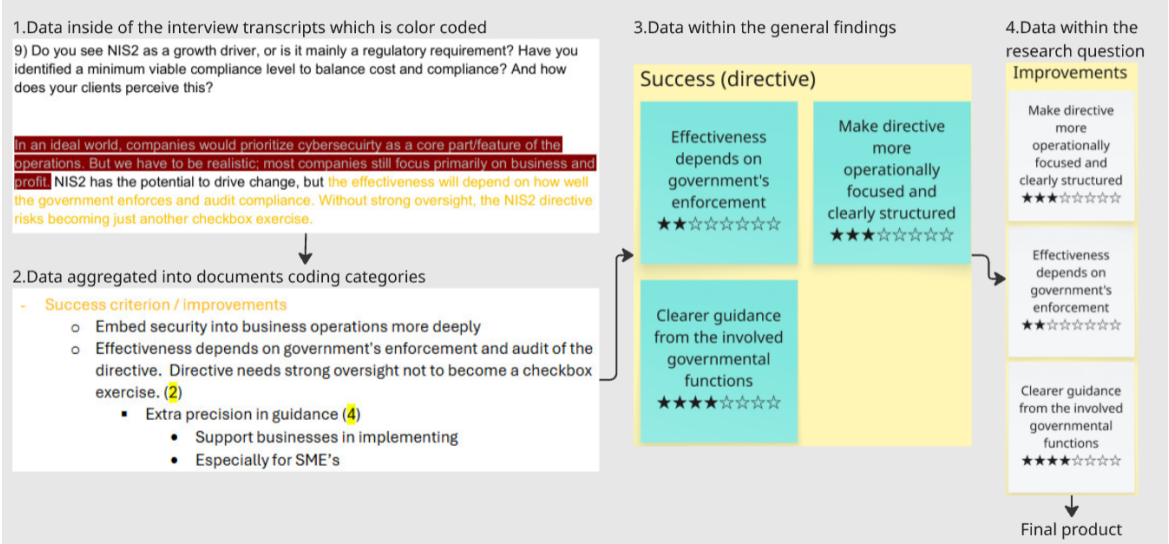


Figure 3.2: This figure shows the internal coding workflow. The final outputs based on this process are presented in chapter 4, particularly in the visualizations under each research question.

In the second stage, the researcher revisited the coded material to identify categories that were mentioned across multiple interviews. Statements were highlighted and annotated with a frequency count to indicate how many participants referenced each theme. This process helped to distinguish between individual observations and more broadly recurring patterns.

The third stage focused on extracting findings that could be considered objective within the context of the study. Specifically, this included themes that were consistently supported by more than one participant. These were anonymized and transferred into Miro, where they were first structured into a general model representing all identified themes. This model was then disaggregated into smaller visual representations organized around each research question. The draft models are included in Appendix C.

During this phase, all project members collaboratively reviewed the categorized findings and discussed how they aligned with the overarching research questions. This group analysis provided an opportunity to cross-validate interpretations and refine thematic groupings.

Finally, the fourth stage involved translating the identified themes and patterns into visual formats, including spider graphs and pie charts. These were developed to improve the clarity and accessibility of the final presentation of interview findings.

3.5.3 Tooling

The coding process was conducted manually using word processing tools available through OneDrive. Although the coding structure followed principles similar to those employed in qualitative data analysis software, the use of dedicated coding platforms was not deemed necessary for this project. The manual approach allowed for full replication of the intended coding framework without compromising quality. Given the learning curve and setup time associated with specialized software, a lightweight manual method was considered more practical and effective within the scope and timeline of the study.

3.5.4 Supporting Survey Content

The survey served as a secondary data source and was used to complement the interview findings with additional context. Given the limited number of full responses, the questionnaire was not treated as a standalone or statistically representative dataset. Instead, it was used to support the interpretation of interview themes in relation to the research questions. The survey responses helped identify patterns that aligned with or contrasted the qualitative findings and were incorporated into the analysis to strengthen the discussion with additional empirical reference points.

3.6 Ethical Considerations

This study has adhered to responsible research practices with respect to data collection, participant interaction, and reporting. As the project involved human participants through expert interviews and a supplementary survey, ethical rigor was maintained even though the study did not fall under categories requiring formal approval by a national ethics committee.

All interview participants were approached directly and informed of the study's academic purpose, their voluntary participation, and their right to withdraw at any point. Participants were not offered compensation, and no identifying personal or organizational details have been disclosed. A deliberate choice was made to anonymize all input to ensure that insights could be shared openly without compromising professional relationships or exposing confidential information. No sensitive personal data, as defined by the GDPR, was collected.

The supplementary survey was constructed to ensure minimal data processing risk. All responses were anonymized at the point of submission, and no IP addresses or track-

ing identifiers were stored. The survey was designed in line with standard practice for academic research, with clear communication of purpose and scope on the landing page.

Particular attention was given to avoiding bias in both qualitative and quantitative tools. Interview prompts were open-ended and aimed at exploring participant perspectives rather than confirming a predefined hypothesis. In reporting, care has been taken to distinguish between subjective perspectives and aggregated trends. Where possible, quotes and interpretations have been verified with participants after the interviews to ensure contextual fidelity.

Although the project did not involve direct ethical dilemmas, the researchers remained aware of their broader responsibility when interpreting and communicating regulatory impact. This includes avoiding the misrepresentation of interviewees' views and acknowledging the limitations of drawing general conclusions from expert-based material. The study's conclusions are intended to support regulatory development and implementation in a constructive way.

Conflict of Interest. The research was conducted independently by the student authors as part of their master's thesis project. No external funding, commercial partnerships, or institutional sponsorships influenced the research. The authors have no financial, professional, or personal affiliations with any organization involved in NIS2 implementation or regulatory lobbying.

3.7 Limitations

While every effort has been to ensure a diligent and relevant research design, some limitations are deep-rooted in the methodological choices made in this study. These limitations do not undermine the value of the findings, but are important to acknowledge in order to frame the scope and validity of the results properly. A more detailed assessment of their implications will be provided in the discussion chapter, specifically in section 5.6

3.7.1 Bias and Subjectivity

As with any qualitative study based on semi-structured interviews, there is a risk of subjective interpretation. This not only comes to show through the contributions from the participants but equally from the researchers. Responses are shaped by the personal experiences, roles, and communication styles of the interviewees, and the thematic analysis involves interpretive judgment by the authors. To mitigate these concerns, interviews were

guided by a structured question set, participants were anonymized to promote openness, and thematic analysis was carried out using a consistent framework in order to reduce an interpretive shift.

3.7.2 Sample Limitations

The study was initially designed to capture insights from organizations directly affected by the NIS2 Directive. However, access to these organizations turned out limited, as many were either early in their implementation journey or unwilling to share internal processes. As a result, this led to a shift in focus toward consultants and advisors with cross-sector experience. This proved to provide broader insight but reduced direct organizational representation.

3.7.3 Generalization Constraints

Due to the qualitative and exploratory nature of the study, the findings are not intended to be overtly generalized to all organizations affected by NIS2. The sample does not represent all sectors, EU member states, or maturity levels of implementation. The survey component is also limited in statistical depth while providing some directional support. Therefore, the results should be interpreted as indicative rather than conclusive, and as a contribution to the broader understanding of early-stage regulatory impact.

3.7.4 Perspective Bias from Advisory-based Insights

A key feature of this study is its reliance on insights from consultants who advise organizations on NIS2 implementation. While this approach enabled access to a wide range of industry cases and cross-sector experiences, it also introduces a specific type of bias. Consultants can only speak to the behaviors, decisions, and challenges of the clients who have actively sought out for advisory support. As such, the data reflects the segment of the market that has already engaged with the directive to some degree.

Organizations that have not yet initiated implementation, are unaware of their obligations, or have chosen to delay compliance are therefore underrepresented or absent throughout. This limits the ability of the study to fully nuance the broader distribution of NIS2 readiness across sectors. The choice to focus on consultants was made in response to limited access to individual organizations, which of many were unwilling to participate. While this decision improved data quality in terms of depth and comparability, it also narrows the scope of perspectives included in the findings.

3.8 Supplementary Transposition Research

A structured desk research exercise was conducted to investigate how EU Member States are transposing the NIS2 Directive into national law, to complement the primary data collection in this study. This supplemental exploration was initiated to examine a recurring concern raised by interview participants, which was that the directive's effectiveness is undermined by inconsistent or delayed national implementation, as seen in results 4.2.4. Initially, the research sought out to investigate these concerns across all Member States, however, through the research it became clear that not all member States have provided publicly available information on this topic, limiting the scope to focus more on certain Countries such as Denmark, Germany, France, Poland, and Croatia to name a few. The most prominent results and observations will be displayed throughout this study, while the research in its entirety can be read in appendix D.

3.8.1 Objective of Research

The purpose of the exploration is to map:

- The current status of transposition across the EU Member States
- Notable differences in legal scope and operational obligations
- The degree of clarity and accessibility of national guidance and implementation resources
- Observable patterns or structural risks that may affect the uniform compliance outcomes of Member States

This sub-study is not intended to conduct a legal analysis as this lies outside the scope of the expertise areas by the group, but to mirror the perspective of organizations attempting to interpret and act upon NIS2 obligations based on publicly available information.

3.8.2 Method and Data Sources

The investigation utilized various search mechanisms to locate the necessary material for this supplementary transposition analysis. This included leveraging the official library database of Aalborg University (Primo), employing targeted Google queries leveraging the now built-in capabilities of Google's LLM 'Google Gemini', and systematically looking up national country-specific public pages. Key search terms included "*NIS2 transposition*",

"*NIS2 delay*", "*Member State implementation*", "*Cybersecurity legislation divergence*", "*infraction proceedings EU NIS2*", and later also "*National Competent Authority*". The investigation relies on material including:

- Official government and parliamentary websites and statements
- Communications from national cybersecurity agencies and ministries
- ENISA updates and European Commission progress trackers
- Reputable secondary sources such as Infosecurity Magazine, academic journals, and policy briefings.

Further, the Member States are categorized by their Transposition status (Fully transposed, partially progressed, or pending), entities' status as either *Essential* or *Important*, the supervisory structure (either centralized, sectoral, or unclear), and finally, the availability to sector-specific guidance (Such as reporting templates, FAQ's, or technical annexes).

3.8.3 Limitations

This sub-study was conducted under time constraints and serves as a "point-in-time" assessment based on publicly accessible documentation. The findings may not fully capture unpolished draft legislation or internal regulatory deliberations. Nonetheless, the analysis is intended to reflect the perspective available to regulated entities who seek to understand their obligations in the current transitional phase.
The result of this transposition exploration are presented in chapter 4, and are referenced in the discussion chapter to support the broader analysis of regulatory fragmentation and compliance behavior.

Chapter 4

Results

This chapter presents the empirical findings of the study; Findings which are drawn from the two main sources: The series of semi-structured expert interviews and the supplementary survey. The following results are organized thematically around the research questions defined in the early stages of the project.
The chapter is divided into three parts. First, insights from the supplementary survey are summarized to provide a broad indication of common perceptions and tendencies. Second, the core findings derived from the interview material are presented, grouped according to the four primary research questions (RQ1-RQ4). Finally, a section will detail the observed differences in NIS2 implementation across Member States, providing important contextual understanding of how the directive is perceived within the affected industries included in the study.

While meticulous care has been taken in order to remain neutral and present the data in an objective manner, further interpretation and critical reflection will follow in the discussion chapter. Here, the findings will be analyzed in light of the literature, regulatory context, and methodological limitations discussed earlier in section 3.7.

4.1 Questionnaire Insights

To supplement the interview findings and to test whether key themes could extend beyond the qualitative sample, the structured questionnaire was utilized. As previously stated in section 3.1.2, the goal was not to generate statistically generalizable data, but rather to capture certain signals which could support or challenge the interview insights of the objective findings 4.2.
The survey received a total of nine fully completed responses from participants, with a total of 39 additional partially completed submissions. The responses represent a mix of sectors and organizational sizes. Respondents were primarily in roles related to cybersecurity leadership, advisory, or technical implementation.

4.1.1 Organizational Size and Sector Representation

Collected responses came from a balanced mix of organization sizes:

- Four respondents from small organizations
- Two respondents from medium-sized organizations
- Three respondents from large organizations

Although the study's interview design deliberately excluded organizations from historically regulation-heavy sectors such as energy, finance, and Healthcare, the survey responses included participants from:

- Energy (3 respondents)
- Finance and banking
- Public administration
- Digital infrastructure
- Education
- Software development for governmental use
- Space services

Interestingly, these sectors did not report definitively clearer interpretations of NIS2, stronger implementation readiness, or improved strategic alignment despite their familiarity to compliance concerns. While these findings are limited in scope, they suggest that prior experience with regulation does not necessarily ease the practical challenges associated with NIS2. This observation will be further revisited in the discussion chapter 5.2.

4.1.2 NIS2 as a Strategic Growth Driver

When asked what extent NIS2 was expected to help their organization grow (rated on a scale of 1 to 10), most participants leaned towards the lower half of the scale:

- Four respondents rated the impact as neutral to low (scores 1-3)
- Two respondents rated NIS2 as neither harmful nor helpful (score 5)

- Two respondents saw it as a potential growth enabler (scores 8 and 10)

This could support the primary data-method in the suggestion that NIS2 is not widely perceived as a driver of strategic advantage, potentially more so among smaller organizations. Instead, the directive is more often viewed as a regulatory necessity; Suggesting that the directive is considered as a checklist task rather than a framework for business value.

4.1.3 Impact on Innovation and Scaling

The question of whether NIS2 has negatively impacted the ability to innovate, scale, or compete revealed a polarized image:

- Three respondents reported no negative impact at all (score 1)
- Three respondents selected a moderate negative impact (score 5)
- The rest spread across the range, with scores from 2 to 7

The spread suggests that NIS2's perceived constraints on innovation are context-dependent, possibly linked to internal resource capacity, sector-specific expectations, or the individual stage of implementation.

4.1.4 Compliance Boundaries

Respondents were asked whether they had identified a point in their NIS2 implementation where they would stop further efforts. This could either be because they believed they had done enough or because continuing would not justify the additional cost:

- Five respondents said yes
- Four respondents said no

This result supports what several interviewees also hinted at. Organizations are beginning to define their own internal threshold for "*good enough*" compliance. Rather than viewing the directive as something to build further improvements on top of, many appear to treat it as a benchmark to reach, followed by a stop. This mirrors similar patterns seen under previous EU regulation like the GDPR, where compliance became the primary objective, which as a result, minimizes broader ambitions once formal requirements were met which is further elaborated in 5.1.2.

4.1.5 Key Challenges in Implementation

respondents were asked to identify their top three implementation challenges. Across all responses, the following issues were highlighted as the most frequently cited:

- Nine mentions of Lack of internal expertise gaps
- Eight mentions of financial costs
- Seven mentions of operational complexity
- Three mentions of internal resistance

These results strongly align with the insights provided by experts and consultants during interviews. Even among organizations with existing compliance infrastructure, expertise gaps were particularly notable, which can point to a structural issue: many organizations are willing to comply, but not equipped to do so.

4.1.6 Partial conclusion

Having presented the majority of the key findings, the survey results reinforce several of the patterns identified in the qualitative interviews. NIS2 is widely seen as a compliance obligation rather than a value-generating initiative. Across both heavily regulated and less mature sectors, organizations face a similar set of challenges: Ambiguous requirements which are yet to be supported by a governmental body, limited guidance, and insufficient internal capabilities.
Moreover, the presence of "compliance ceilings" in multiple organizations suggests that NIS2 may inadvertently incentivize minimal adherence over deeper, risk-based transformation. This raises important questions about the directive's true effectiveness as a tool for improving cybersecurity at scale.

4.2 Objective Findings

The findings presented in this chapter are based on thematic analysis of the coded interview data. To ensure relevance and analytical depth, only themes mentioned by at least two interviewees are included in the core analysis. The results are organized according to the four research questions, with each section outlining the most prominent patterns and insights related to that question. These findings form the basis for the critical reflection and interpretation developed in the discussion chapter.

4.2.1 RQ1 – What are the Observable Patterns Among Organizations Implementing NIS2?

The observable findings for RQ1 are structured into four main categories, as illustrated in Figures: *Positive* 4.2a, *Negative* 4.2b, *Help is needed* 4.3a, and *Reason* 4.3b. Each category reflects patterns identified during interviews and thematic analysis, and you can see the distribution of response types in figure 4.1.

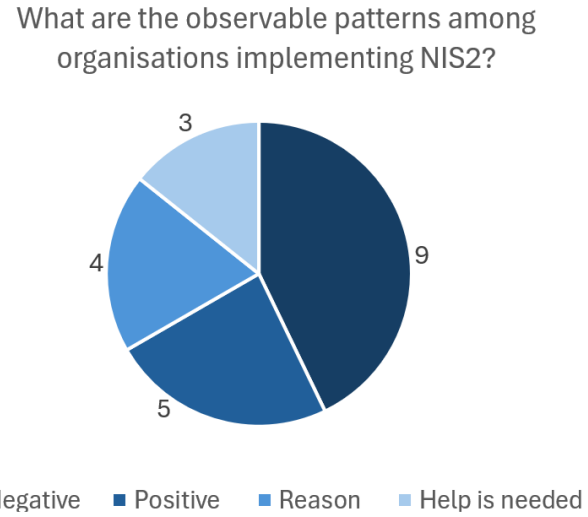
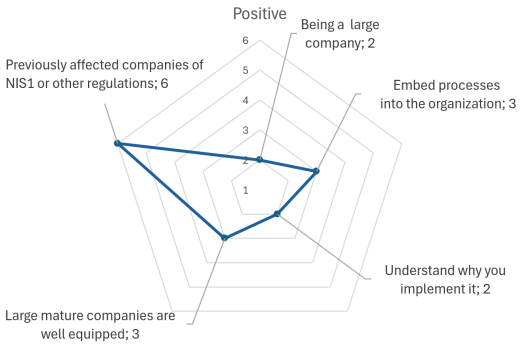
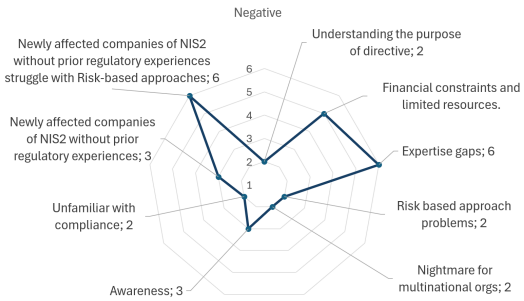


Figure 4.1: Distribution of response types across categories

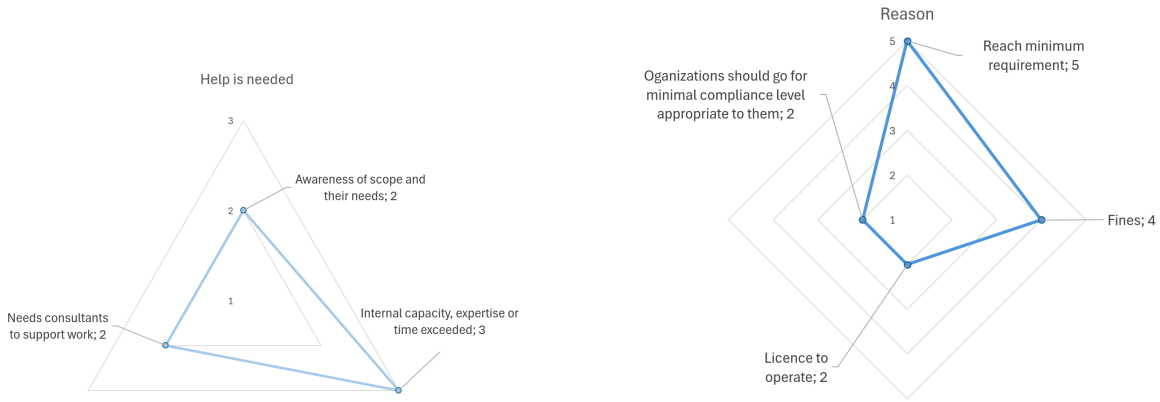


(a) Positive framing



(b) Negative framing

Figure 4.2: Framing responses to RQ1: Positive vs. Negative



(a) Help-seeking framing

(b) Reasoning emphasis

Figure 4.3: Framing responses to RQ1: Help-seeking vs. Reasoned

Accumulated responses are the bundled collection of the answers provided across the four categories further described below. As it is illustrated in 4.1, the majority of collected responses that most interviewees agreed on are situated within the *negative* category.

Positive findings, as depicted in 4.2 - left-hand side, are strongly associated with organizations that have prior experience with regulatory compliance. These entities, typically larger or more mature, are often better equipped to embed NIS2 requirements into their organizational structures. This advantage is not solely tied to company size, but rather to institutional maturity and familiarity with past regulations such as NIS1 or similar frameworks. These organizations tend to treat cybersecurity as a strategic component of operations, rather than a check-box exercise. A key insight for less experienced organizations is the importance of understanding the purpose of NIS2 and embedding it meaningfully into their business practices from the outset.

Negative patterns, as depicted in 4.2 - right-hand side, frequently occurred in organizations with little or no previous exposure to regulatory standards. A recurring issue was the difficulty of understanding and applying NIS2's risk-based approach, which led to uncertainty about what internal changes were necessary. In some cases, this was compounded by limited awareness of the directive itself. Multinational organizations were also highlighted as particularly challenged, due to differences in how NIS2 is interpreted and implemented across jurisdictions. The most consistent barriers cited were financial limitations and resource constraints, which significantly hindered implementation efforts.

Help is needed at three key stages in the implementation process, as depicted in 4.3 - left-hand side. First, during the initial scoping phase, organizations often struggle to identify the scope of their responsibilities under NIS2. Second, during active implementation, external support is frequently brought in to manage technical or procedural gaps. Third,

help is most often required when internal expertise, capacity, or time are exceeded, at which point consultants become essential to moving the process forward. This pattern of escalating support reflects the complexity of the directive and the resource intensity of aligning with its requirements.

Reasons for implementation, as depicted in 4.3 - right-hand side, were often driven by external pressure rather than internal motivation. Many organizations pursued compliance primarily to meet legal requirements, avoid fines, or maintain their ability to operate in regulated markets. Interestingly, several consultants noted that for most organizations, pursuing a minimal, but tailored level of compliance is often the most realistic and appropriate strategy. This perspective reflects a pragmatic approach, where the directive is viewed as something to be managed rather than fully embraced as a catalyst for broader transformation.

4.2.2 RQ2 – What Organizational or Regulatory Factors Contribute to a Compliance-driven Approach?

Figure 4.4 groups the determinants of a compliance-oriented posture into three high-level clusters: *Difficulties (directive) 4.6*, *Reason 4.5a*, and *Low compliance experience / level 4.5b*. Together, they describe why many firms adopt a "minimum-viable" stance rather than pursuing broader security gains.

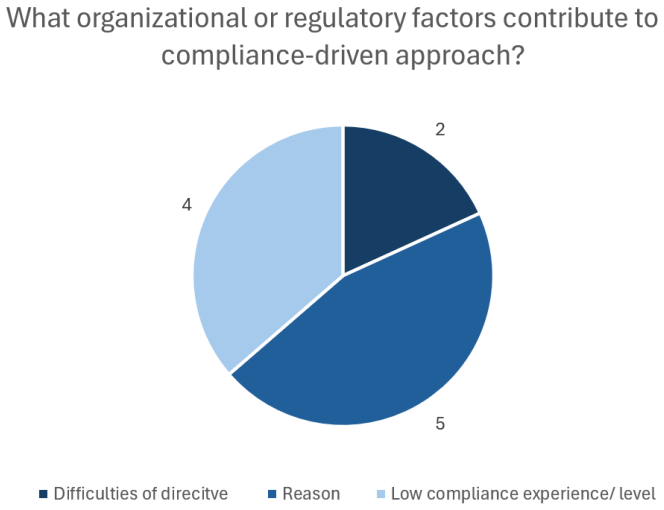
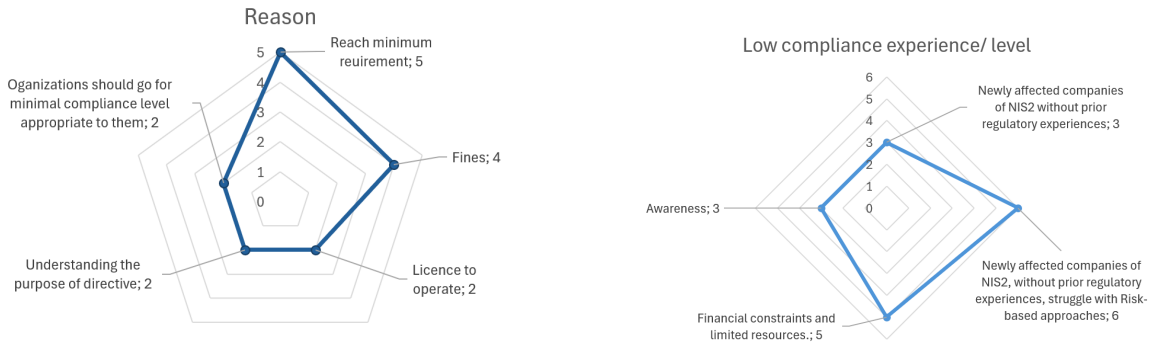


Figure 4.4: Distribution of response types across categories



(a) Reason framing **(b)** Low compliance framing

Figure 4.5: Framing responses to RQ2: Reason vs. Low compliance experience/ level

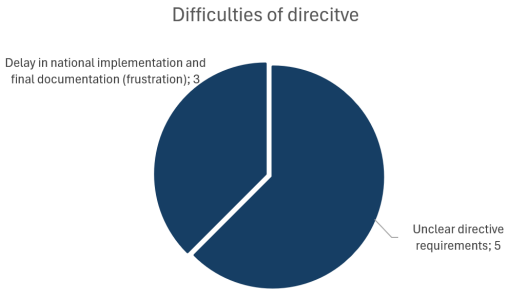


Figure 4.6: Framing of difficulties in directive

Accumulated Responses are the bundled collection of the answers provided across the three categories, further described below. As it is illustrated in 4.4, the majority of collected responses that most interviewees agreed on are situated within the category of motivational drivers, or *reason* as written in the figures.

Directive-specific Difficulties. Interviewees consistently pointed to the regulation itself as a major source of hesitation, as can be seen in Figure 4.6. The figure, even though being on a different format, conveys the same message as for the figures represented as radar charts. The data points, only summarizing to distinct groups, made it impossible to plot as a radar chart. The most frequently cited obstacle was the *ambiguity of NIS2's wording*: key terms such as "appropriate" or "proportionate" controls were viewed as open to interpretation, sparking prolonged internal debate over what level of risk assessment or incident reporting would satisfy a future auditor. That uncertainty is compounded by slow national transposition and the absence of final sector handbooks; several participants said they were "*flying blind*" and therefore defaulted to the safest (yet least ambitious) reading of the directive until official guidance arrives. When requirements remain vague or in flux, risk-averse organizations naturally gravitate toward check-box compliance and postpone

substantive technical upgrades.

Motivational Drivers ("Reason"). As illustrated in Figure 4.5a, four pragmatic incentives dominate implementation strategy. First, firms view NIS2 compliance as basic *license-to-operate hygiene*, seldom as a competitive differentiator. Second, the desire to *avoid fines* looms large, especially among entities still bruised by high-profile GDPR penalties. Third, although most interviewees recognized the directive's broader security purpose, they admitted that *purpose alone rarely unlocks new budget*. Finally, many consultants counsel clients to "*aim for the minimal level you can defend*," reinforcing a norm in which tailored but minimalist compliance is considered both acceptable and cost-efficient. External pressure (legal liability and market access) thus outweighs intrinsic security ambition, nudging organizations toward the smallest set of changes likely to satisfy regulators.

Low Compliance Experience and Resource Constraints. Figure 4.5b highlights the internal capacity limits that cement a compliance-only trajectory. Newly scoped companies (often SMBs) lack legacy governance frameworks and struggle to interpret NIS2's risk-based ethos, defaulting instead to short-term, document-centric fixes. Even when the intent is understood, a missing risk taxonomy or governance forum makes operationalization difficult. Financial constraints further skew priorities: limited budgets are channeled to policies and external audits rather than to new technical controls, a pattern most acute among smaller firms. In many cases, senior leaders are unfamiliar with cyber-regulation; funds are released only when penalties or operational stoppages are explicitly mentioned. Organizational maturity therefore acts as a decisive filter: entities with low compliance experience or tight resources are far more likely to view NIS2 as a legal hurdle than as a platform for genuine security improvement.

As for the implications, organizational maturity acts as a filter: companies with low compliance experience or tight budgets are far more likely to treat NIS2 as a legal hurdle rather than a security program.

4.2.3 RQ3 – Does NIS2 Provide Tangible Security Improvements, and is the Value of Implementation Present Short/Long-term?

Figure 4.7 groups interview insights about RQ3 into two contrasting clusters: positive contributions and negative perceptions. Each of these categories shed light on both the immediate and the enduring value that organizations associate with NIS2 compliance.

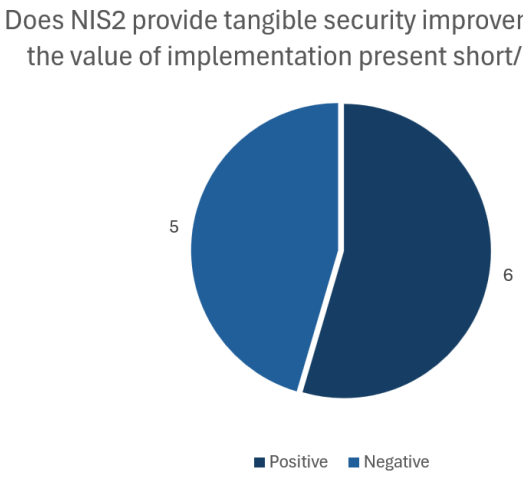
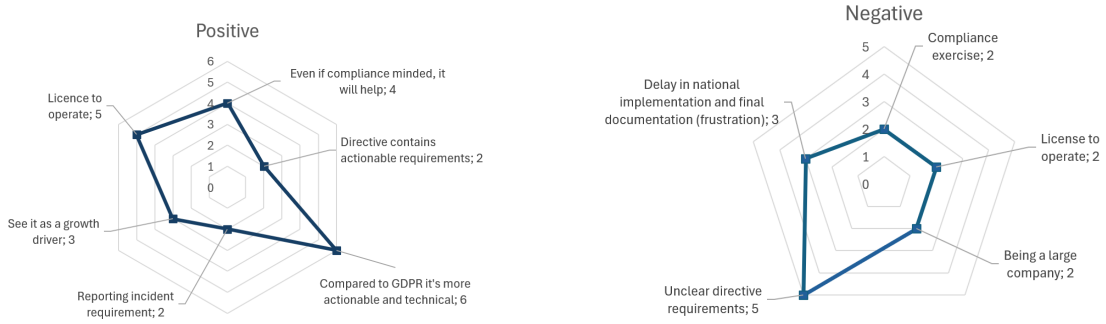


Figure 4.7: Distribution of response types across categories



(a) Positive framing

(b) Negative framing

Figure 4.8: Framing responses to RQ3: Positive vs. Negative

Accumulated responses are the bundled collection of the answers provided across the two categories, further described below. As it is illustrated in 4.7, the majority of collected responses that most interviewees agreed on are situated within the *Positive* category.

Positive contributions, as depicted in 4.8 - left-hand side, Most participants acknowledged that, even when pursued with a narrowly compliance-minded attitude, NIS2 delivers some concrete security gains. Several interviewees stressed that the directive is "more actionable and technical than GDPR", pointing to its explicit incident reporting timelines and governance requirements. Organizations that already had baseline controls in place described NIS2 as a useful "upgrade path" that moves them from ad hoc practices to more systematic monitoring and response. The mandatory incident reporting clause was singled out as an early win: it forces quicker escalation internally and creates a richer feedback loop with national authorities. A minority of respondents, mostly in rapidly growing SaaS firms,

framed NIS2 as a growth driver, arguing that demonstrable compliance helps win larger customers and facilitates cross-border expansion. Even those who admitted to "doing the minimum" conceded that the directive nudges them to document processes, clarify roles, and tighten vendor expectations (incremental but tangible improvements). Lastly, a few participants noted that treating NIS2 as a "license to operate" can in itself hold value. In this context, the directive is not merely a regulatory hurdle, but a signal of trust and credibility that organizations can leverage to demonstrate adherence and market themselves to a broader audience.

Negative Perceptions: Conversely, many participants portrayed NIS2 implementation as a compliance exercise rather than a security transformation, as depicted in 4.8 - right-hand side. The phrase "license to operate" surfaced repeatedly, signaling that the primary objective is to avoid regulatory penalties rather than to strengthen defenses. Two recurrent points explain this stance: First, stakeholders complained about unclear requirements, especially around proportionality and acceptable risk thresholds. Second, the continued delay in national transposition and sector guidance fuels frustration; until concrete templates or audit criteria are issued, companies default to the safest (but often least ambitious interpretation of the rules). Larger enterprises noted an additional drawback: aligning global security frameworks with divergent member-state expectations creates duplication rather than improvement.

Short-term vs Long-term value Across cases, the consensus is that NIS2 offers modest short-term security gains (specially in incident handling and policy documentation) but its long-term impact remains uncertain. Interviewees argued that lasting value will depend on two factors: (i) the clarity and consistency of enforcement once national laws are finalized, and (ii) whether firms move beyond the initial "check-box" phase to integrate lessons learned into their broader risk management cycles. Without sustained enforcement pressure or clear industry benchmarks, several respondents predicted that the directive could plateau at a minimal compliance level, delivering limited strategic benefit. Others were cautiously optimistic, suggesting that the very act of formalizing incident metrics and board-level reporting will, over time, embed a more mature security culture, even if progress is incremental.

4.2.4 RQ4 – How do Industry Experts Interpret the NIS2 Directive in terms of its Completeness, Clarity or Practicality?

Below we see three figures which organizes expert commentary into three thematic bands 4.9: Positive assessments 4.10a, suggestions for improvements 4.11, and persistent criticism 4.10b. All this contributing to a revealing a nuanced but broadly pragmatic reading of the directive.

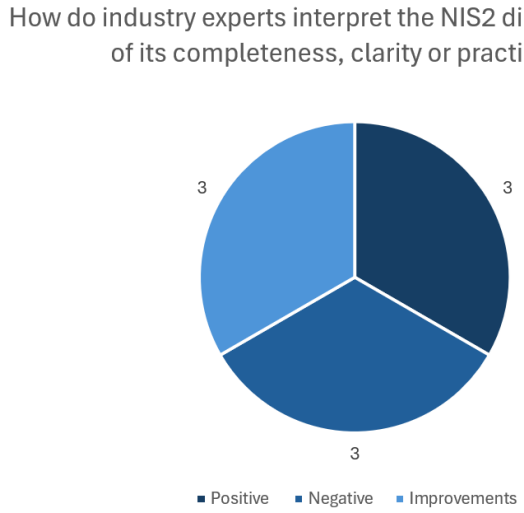


Figure 4.9: Distribution of response types across categories

(a) Positive framing **(b)** Negative framing

Figure 4.10: Framing responses to RQ4: Positive vs. Negative

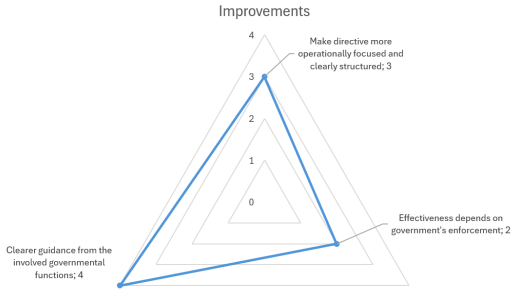


Figure 4.11: Framing responses to RQ4: Improvements

Accumulated responses are the bundled collection of the answers provided across the three categories, further described below. As it is illustrated in 4.9, the collected responses are equally distributed across the three depicted categories.

Positive: Across interviews, subject-matter experts expressed guarded optimism about the practical value of NIS2, as depicted in 4.10 - left-hand side. First, they described the text as "more actionable and technical than GDPR ", noting that its control language (e.g., specific incident reporting timelines) provides clearer operational hooks than the largely principles based on GDPR. Second, several experts argued that even an organization focused only on basic compliance will still raise its security floor: the mandatory incident-notification regime was cited as a concrete mechanism that forces faster internal escalation and forensic readiness. Finally, a subset of security consultants see the directive as a potential growth driver, particularly for SaaS vendors, because demonstrable alignment with NIS2 can differentiate suppliers in tender processes.

Negative: Yet that optimism is tempered by a cluster of recurring frustrations. The first is the complaint of unclear or open requirements; experts pointed to vague phrasing around 'appropriate' risk management and the absence of normative control sets, as depicted in 4.10. They also warned that NIS2 can become a "nightmare for multinational organizations": divergent transposition deadlines, language discrepancies, and country-specific templates create duplication and legal uncertainty. The ongoing delay in national implementation and final guidance was described as a major source of inertia: until ministries publish definitive checklists or supervisory expectations, many firms retain a holding pattern that favors minimum-effort compliance.

Improvements: When asked how NIS2 could be strengthened, three proposals dominated, as depicted in 4.11. First, experts called for the directive to be made "more operationally focused and clearly structured," suggesting annexes that map each article to concrete controls (aligning with ISO 27001's Annex A). Second, they stressed that the directive's real impact will hinge on credible governmental enforcement; without visible supervisory action, organizations may rationally choose the lightest compliance path. Third, respondents urged clearer guidance from national authorities model policies, reporting templates, and sector specific FAQs to reduce interpretive ambiguity and level the playing field across member states.

4.3 Cross-Member State Difference in NIS2 Implementation

While the NIS2 Directive aims to create a harmonized cybersecurity baseline across the EU, the nature of its legal form as a directive allows Member States to determine how its provisions are transposed into national law. This flexibility has resulted in observable

divergences in not only timing, but as well as in sectoral classification, industrial responsibility, and practical guidance [50, 51, 52]. To investigate the extent and the nature of these differences, research across Member States was conducted with the intent of identifying concrete discrepancies and patterns in the transposition.

4.3.1 Transposition Progress and Timelines

As of early 2025, only a minority of Member States have managed to fully transpose the directive, and according to data compiled from national sources and records, most countries remain in various stages of draft legislation, public consultation, or partial transposition [50, 53]. Germany, for instance, has submitted a legislative draft but may face delays linked to their ministerial coordination in the effort to create a coherent yet incomplete framework [51]. Further, has France faced delays in its transposition process due to political instability and was among the Member States that failed to notify full transposition by the deadline. This list additionally includes 18 other countries, hereunder Denmark, Norway and Spain, who have been the focal point of the primary data collection [54]. In Central and Eastern Europe, countries like Poland have progressed more slowly, struggling with institutional fragmentation and unclear enforcement [51]. These widespread delays are consistent with the broader trends in EU law, as the average delay for transposing EU Directives reached an all-time high of 18.3 months in 2023 [50]. An overall summary of transposition statuses across Member States is presented in table 4.2 and further visualized in. This reveals a diverse legal landscape with implications for companies operating cross-border. This type of organizations may face compliance obligations in jurisdictional areas where requirements are still unclear or under development [52].

Member State	Transposition Status (Latest Info)	Notes on Specific Variations/Actions
Austria	Reasoned Opinion Issued (May 2025)	Transposing Directive's text as originally drafted for Article 28.
Belgium	Transposed by Deadline (Dec 2024)	Goes beyond Directive terms for Article 28; closely aligns national law with minor adaptations.
Bulgaria	Reasoned Opinion Issued (May 2025)	Public consultation held.
Croatia	Transposed by Deadline (Dec 2024)	Included additional sectors; detailed entity categorization.
Cyprus	Draft (submitted to the Parliament for voting)	Public consultation held.
Czechia	Reasoned Opinion Issued (May 2025) – Draft law	Goes beyond Directive terms for Article 28; public consultation held.
Denmark	Reasoned Opinion Issued (May 2025) – Draft law	
Estonia	Reasoned Opinion Issued (May 2025) – Draft law	
Finland	Transposed (2025)	Public consultation held.
France	Reasoned Opinion Issued (May 2025) – Draft law	Drafted new law transposing NIS2 and other directives simultaneously; faces delays due to political instability. Public consultation held.
Germany	Reasoned Opinion Issued (May 2025) – Draft law	Drafted new law transposing NIS2 and other directives simultaneously; coherent but incomplete framework. Enforcement expected 2025. Public consultation held.
Greece	Transposed (2024)	Public consultation held.
Hungary	Transposed – in effect (2024)	Public consultation held.
Ireland	Reasoned Opinion Issued (May 2025) – Draft law	
Italy	Transposed by Deadline (Dec 2024)	Transposing Directive's text as originally drafted for Article 28.
Latvia	Transposed (2024)	Public consultation held.
Lithuania	Transposed by Deadline (Dec 2024)	Public consultation held.
Luxembourg	Reasoned Opinion Issued (May 2025) – Draft law	
Malta	Transposed (2025)	Public consultation held.
Netherlands	Reasoned Opinion Issued (May 2025) – Draft law	Transposing Directive's text as originally drafted for Article 28. Public consultation held.
Poland	Reasoned Opinion Issued (May 2025) – Draft law	Revised initial draft; faces challenges with institutional fragmentation and unclear enforcement. Public consultation held.
Portugal	Reasoned Opinion Issued (May 2025) – Draft law	Public consultation held.
Romania	Transposed (2025)	Public consultation held.
Slovakia	Transposed (2025)	Public consultation held.
Slovenia	Reasoned Opinion Issued (May 2025) – Draft law	Public consultation held.
Spain	Reasoned Opinion Issued (May 2025) – Draft law	
Sweden	Reasoned Opinion Issued (May 2025) – Draft law	Public consultation held.

Table 4.2: Transposition statuses across Member States

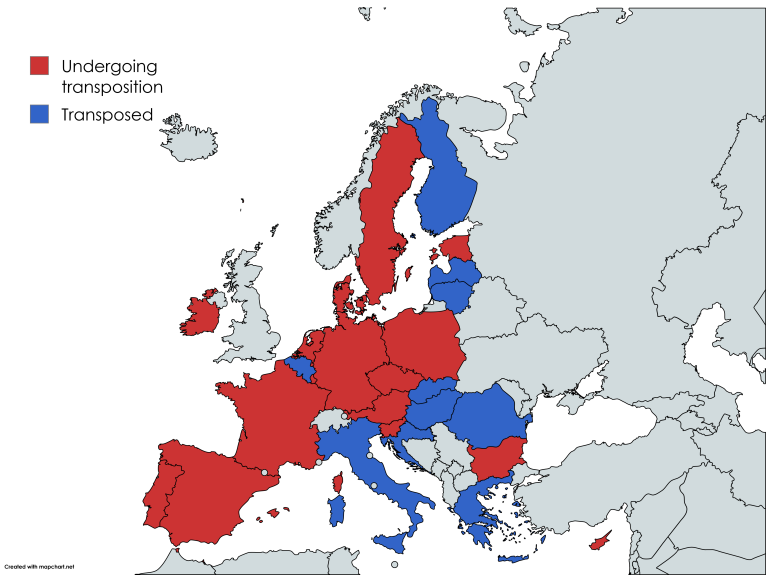


Figure 4.12: The EU transposition status

4.3.2 Divergence in Sector Classification and Scope Interpretation

Member States have the authority to define which entities are classified as *essential* or *important* based on national criteria, which can lead to inconsistent sectoral designations across countries [52]. This is also evident in how specific provisions, such as the Article 28 that revolves around domain name registration data, are being transposed. with this specific article in mind, we see clear variations in national approaches, as mentioned in [50]. For instance, Croatia has chosen to include additional sectors beyond the minimum outlined by NIS2 and has established a more detailed categorization of entities within its national law [55]. These discrepancies raise questions about the directive's harmonization goals. Cross-border entities may find themselves classified differently depending on national criteria, which in turn will complicate strategies and potentially create legal uncertainty.

4.3.3 Structures and Reporting Protocols

Another key area of divergence is the structure and role of supervisory authorities. While each EU Member State must appoint its own National competent Authority (NCA) to supervise and enforce NIS2 locally, national legislation specifies which authorities are responsible for monitoring and whether this oversight is divided by areas of competence [55]. For example, Germany leverages a centralized supervisory body [51].

The absence of uniform incident notification templates or response timelines further worsen the uncertainty of entities. In some Member States, this means that reporting portals and escalation procedures remain unpublished or under development, meaning that organizations could technically be required to comply with incident reporting while having no actionable mechanisms to do so [52]. These gaps are especially problematic for SMBs who often lack the legal or consulting infrastructure to interpret obligations independently which directly align with multiple of the objective findings from the interviews highlighted throughout the sections 4.2.1 –4.2.4 in chapter 4 Results.

4.3.4 Patterns and Strategic Implications

From the comparative assessment, there are two key trends that emerge:

Regulatory fragmentation as the structural risk The divergence across Member States is not merely a matter of timing, but one of structural misalignment. as mentioned, organizations operating in multiple jurisdictions face implementing multiple compliance programs in parallel. Each of which have to align slightly differently to different national versions of NIS2. This risks creating inefficiency, double efforts, and ultimately reducing the directive's effectiveness [21].

Risk of Regulatory Arbitrage The found variations in enforcement maturity and reporting obligations show that companies may be incentivized to establish their NIS2 reporting presence in jurisdictions with lower oversight burdens [50][56]. While this may offer short-term relief for compliance teams, it raises long-term risks for consistency and cyber resilience at the EU-level.

These findings align with the concerns found in the interviews regarding enforcement uncertainty, interpretational ambiguity, and the role of consultancy dependence, which can be derived from the content of the sections and graphs of 4.2.1 –4.2.4 in chapter 4 Results. The transposition exploration reinforces the view that without greater guidance and supervisory alignment, NIS2 may struggle to fulfill its goal of a unified European cybersecurity posture

Chapter 5

Discussion

This chapter outlines the key findings of the study in relation to the research questions defined in chapter 4. Based on insights from the interviews, and the survey results, it explores how organizations and consultants understand and implement the NIS2 Directive in practice. The discussion also considers broader implications for regulatory effectiveness, organizational behavior, and cybersecurity governance. where appropriate, findings are connected to prior literature, as well as the supplementary transposition research, to compare patterns observed under earlier regulations such as the GDPR, or in the transposition delay implications documented. Finally, the chapter outlines potential directions for further research and the limitations met under the scope set for this study.

5.1 Comparison with GDPR and other Regulatory Precedents

The challenges identified in the implementation process of the NIS2 Directive mirror several well-documented difficulties from earlier enforcement of the General Data Protection Regulation (GDPR). While NIS2 introduces a more security-focused framework than GDPR's privacy-oriented scope, early evidence suggests it may replicate many of the regulatory and organizational concerns that characterized the rollout of GDPR. This section will explore both interview findings from chapter 4, and a broader selection of empirical and theoretical research to explore these parallels from section 4.3.

5.1.1 The Compliance Challenges for SMBs under GDPR

As discussed in section 2.2 a consistent theme across GDPR literature is the disproportionate compliance burden experienced by small and medium-sized businesses (SMBs). Several studies reported that GDPR compliance generated high fixed costs that scaled poorly across smaller organizations, which lead to what some authors have characterized as an unintended blocker of innovation and competition [41, 40]. Survey-based work further confirms that SMBs struggled to interpret and operationalize GDPR's qualitative provisions. More precisely, the organizations without pre-existing privacy or security expertise [57, 58]. The impact did extend beyond regulatory effort, which the empirical evidence can

display with a measurable decline in online activity for smaller websites shortly following GDPR's enforcement, suggesting real economic consequences [59].

These dynamics are already somewhat observable in the early NIS2 implementations, as section 4 reflects. As the directive applies to a broader set of entities and introduces stricter obligations, such as the mandatory reporting timelines or the threat of substantial fines, interviewees expressed concern that organizations with limited cybersecurity maturity are unlikely to engage with the directive strategically. Instead, many seek external templates or await national guidance, that, as a result, will lead to delays in implementation and the risk of underdeveloped internal ownership.
The supplementary research further emphasizes this point by highlighting the uneven transposition of the NIS2 Directive across EU Member States. This unevenness in meeting deadlines for national legislation points to more underlying imbalances in national administrative capacity, efficiency, or could even hint a lack of political prioritization of cybersecurity. These delays and inconsistencies further worsen the compliance burden, especially for SMBs, which may lack the resources to navigate the fragmented regulatory landscape and instead default to a "minimalist" approach.

5.1.2 Surface-level Compliance and Interpretational Ambiguity

The enforcement of GDPR was also marked by widespread ambiguity in operational expectations. Studies noted that while GDPR set out overarching principles and legal rights, it provided little guidance on how organizations should technically implement those requirements in practice [60, 14]. This ambiguity has created a "checklist" mentality in which compliance became an exercise in legal defensibility rather than substantive privacy enhancement. Reports from both industry and academic sources warned that organizations often mistake documentation with security, resulting in the perception of procedural compliance for actual resilience [61, 62].

The same dynamic appears to be present under NIS2. While NIS2 is intended to drive real and practical improvements in cybersecurity, interview participants noted a heavy dependence on third-party consultants sector-specific ambiguity, and uncertainty about implementation. As with GDPR, this creates the conditions for surface-level engagement where organizations are likely to satisfy visible requirements to minimize exposure, while more complex controls receive limited attention. The result is a partial implementation that may meet formal compliance thresholds but fail to improve the actual security posture. This concern is shared by experts and is supported by prior regulatory patterns.

The supplementary research in section 4.3 provides clear indications that this issue is affected by the national transposition processes of NIS2. The inherent flexibility of a directive, as seen in contrast to a directly applicable regulation, allows Member States to

interpret and integrate provisions into national law with a degree of variance and precision. This characteristic contributes to the "inconsistency" across Member States in how they scope and classify entities. Terms used, such as "appropriate" or "proportionate", are viewed as open to interpretation, which is directly seen in the notable variance of provisions like Article 28 across nations as previously mentioned in chapter 4. This ambiguity, in conjunction with delays in national transposition as well as the absence of final sector-specific guidance material, forces organizations to "fly blind" and often leads them to prioritize a check-box compliance approach. The result is a "patchwork of local requirements" [52] rather than consistent rules that can lead to shallow adherence over actual resilience.

5.1.3 Regulatory Fragmentation and Hesitation

GDPR's status as a regulation was intended to ensure consistency across EU member states. however, in practice, its rollout revealed significant fragmentation. Supervisory authorities varied in their- enforcement posture, guidance documents, and procedural expectations [60, 14].
This gap created legal uncertainty for organizations operating across borders, which lead many to delay or minimize their compliance investment until local authorities clarified their approach. SMBs lacked the resources to maintain compliance tracks and opted to generic templates as a result. As *Sirur et al.* (2018) observe,
"*SMBs with less focus on data protection struggled to make what they felt was a satisfactory attempt at compliance*",
primarily due to the "*sheer breath of regulation*" and uncertainty in interpreting its qualitative requirements [14]. This supports the conclusion that GDPR's ambiguity did not just result in compliance variation, but also produced an over-reliance on simplified interpretations at the expense of strategic integration.

Early responses to NIS2 suggest a similar trajectory. Interviewees highlighted the uneven national transposition process, reporting that organizations often avoid committing resources until local obligations are formally defined. This waiting period further undermines the directive's ability to drive early and proactive change. The lack of pan-European implementation alignment creates strategic hesitation and continues to impose dependence on interpretive check-points, even for a directive that explicitly aims to harmonize cybersecurity standards.

The fragmentation seen during the rollout of the GDPR is becoming evident in the transposition of NIS2. The Supplementary research suggests that the issue goes beyond delays. There are notable differences in how Member States interpret and apply key elements of the directive. These variations are evident in several areas; For instance, Croatia, who have

extended the scope to include additional sectors not originally covered by NIS2. Further, Enforcement structures also differ. Each Member State continues to rely on its own regulators, reporting platforms, and sector-specific compliance procedures.
This divergence opens the door to regulatory arbitrage. Multinational firms may begin to favor jurisdictions with less comprehensive enforcement or less complex compliance demands. This runs counter to the directive's intended goal of raising cybersecurity standards across the Union. as a result, nations aligning with lighter requirements may offer a more attractive return on equity for organizations; Not due to stronger business fundamentals, but simply sue to lower regulatory costs. For Member States that choose to implement stricter rules will inevitably create a competitive disadvantage for the organizations operating within the given state which could trigger a gradual lowering of standards across the board. Even under the same criteria for fines, the enforcement still varies from Member State to Member State, and therefore the perceived likelihood of inspection may differ from one country to the next.

Adding to the challenge is the need to align NIS2 with pre-existing national law and other EU frameworks, such as the Digital Operational Resilience Act (DORA) or the Cyber Resilience Act (CRA). For companies operating in multiple jurisdictions or across frameworks, the result is a patchwork of overlapping requirements. This "Regulation-stack" complicates risk management or reporting protocols, and can delay incident response efforts. the result is a fragmented cybersecurity landscape that makes it difficult to reach the EU's goals. This is backed by the average timeline of which an EU Directive takes in order to be fully transposed into national law, which reached an all-time high of 18.3 months back in 2023. Going forward, this may prompt the EU to shift more frequently from directives to regulation, where uniformity can be more tightly enforced.

In summary, while NIS2 differs from GDPR in scope and intent, the implementation landscape reveals striking similarities in terms of structure. The literature on GDPR enforcement offers indicative warning signs about regulatory design features that could lead to compliance adherence over strategic adoption, a disproportionate strain on SMBs, higher dependency on external guidance and interpretation, and a potential delayed impact due to regulatory ambiguity and national divergence.

The interviews conducted in this study confirm that these dynamics are not hypothetical under NIS2, there are early signs of the same path.

5.2 RQ1 – What are the Observable Patterns Among Organizations Implementing NIS2?

Positive Patterns: The positive implementation patterns identified in response to the first research question largely point to the critical role of prior experience and internal knowledge when adapting to the NIS2 Directive. These enablers, however, are difficult for many organizations to attain. Successfully integrating NIS2 requires not only a comprehensive understanding of the directive itself, but also the capacity to contextualize its requirements to fit the specific operational and regulatory landscape of the organization. This level of adaptation often depends on several key factors: the availability of substantial internal resources, prior experience with regulatory compliance, the presence of embedded governance processes that can be reused, and an organization's ability to assess its own needs and align its practices accordingly. This suggests that early investments in regulatory literacy and internal governance structures may yield long-term advantages in adapting to evolving security mandates.

These elements, while advantageous, are often inaccessible to less experienced organizations, which makes them significant barriers to effective implementation. For example, one case from the questionnaire, involving a company in the highly regulated energy sector, shows that even organizations familiar with regulatory frameworks may still struggle with NIS2 due to a lack of awareness and internal knowledge. This is consistent with findings from the questionnaire in section 4.1.1, where respondents from sectors like energy and finance, despite being historically regulated, did not report higher readiness or clarity in implementation, suggesting that regulatory maturity alone does not eliminate barriers to NIS2 adoption. This also suggests that meeting only some of the positive implementation criteria, such as having prior experience, is not sufficient on its own. Instead, successful implementation appears to depend on more fundamental capabilities, including the ability to integrate, interpret, and operationalize the directive's requirements. Positive patterns should therefore be viewed not as checklists to be completed, but as strategic tools to guide organizations in defining meaningful implementation goals and identifying areas in need of development.

Negative Patterns: When examining the negative side of the implementation patterns, a clear correlation can be seen with the absence of the factors that support successful adoption. Specifically, a lack of internal knowledge, limited regulatory experience, and financial constraints are major contributors to implementation difficulties. These issues were also among the top challenges identified in the questionnaire, particularly among smaller organizations. These challenges have already been discussed earlier in the thesis. However, one prominent issue that emerges more strongly in this context is the difficulty organizations face with the risk-based approach required by the directive.

This way of thinking is relatively new for many organizations, even for those that have encountered risk-based models in other regulatory contexts such as financial services. Under NIS2, the risk-based approach demands not only technical adjustments but also significant changes in how organizations think about governance, decision-making, and accountability. This shift was consistently highlighted by interviewees as one of the most challenging aspects of the directive.

The reason this challenge is so pronounced may be because the risk-based model sits at the core of the directive. As a result, it represents one of the most substantial areas that organizations need to engage with. For many, this requires a fundamental shift in mindset and internal processes, which can be difficult to achieve without prior experience or dedicated support.

The negative dynamics surrounding NIS2 are further intensified by the fragmented way Member States have approached its transposition, as found in the supplementary research 4.3. As of the October 2024 deadline, only four countries had managed to transpose the directive in time, meaning that the European Commission needed to introduce infraction proceedings against 23 Member States. This widespread delay has created uncertainty, making it troublesome for organizations to understand the directive demands and how to respond. The divergence in national implementation, as seen with the previously mentioned Article 28, have led to a patchwork of local rules. For multinational firms, this means navigating inconsistent national laws rather than working within a unified EU framework. When combined with limited resources and internal expertise, this fragmentation often drives organizations toward surface-level compliance instead of real risk-based improvements.

Help is Needed: The identification of three distinct stages where organizations require external help highlights the critical role that consultants play in supporting effective NIS2 implementation. These stages include the initial scoping phase, the active implementation phase, and the point at which internal capacity is exceeded. Each stage represents a specific area where organizations often struggle. For implementers, understanding these stages can serve as a practical tool to identify their own weaknesses early in the process. This awareness may reduce delays and improve the efficiency of implementation from the start.

For consultants, these patterns present an opportunity to improve the structure of their services. By creating predefined plans and procedures for the most common areas of support, consultants can streamline their response and reduce onboarding time. This approach would also give organizations a clearer understanding of what to expect, which may increase their confidence in seeking external assistance.

At the regulatory level, these findings suggest that clearer official guidance could be orga-

nized around these three stages. Providing tailored recommendations or support materials for each phase would help organizations better understand what is expected of them at different points in the implementation process. The identified need for help is not only a reflection of organizational limitations, but also an opportunity for consultants and regulators to make implementation more accessible and effective.

Reason: When examining the underlying reasons organizations choose to implement the NIS2 Directive, the most commonly cited motivation is the avoidance of financial penalties. This is expected, as enforcement through fines is the directive's primary mechanism for ensuring compliance. However, this also implies that the effectiveness of NIS2 may be significantly influenced by the visibility and frequency of audits. If organizations perceive that enforcement is weak or inconsistent, the incentive to fully implement the directive may diminish. This insight highlights the importance of sustained regulatory oversight in maintaining momentum for implementation.

For consultants, the financial dimension of compliance is a key factor to consider when engaging with decision-makers. Understanding that cost is a central concern allows consultants to frame their recommendations in a way that aligns with the economic priorities of the organization. This approach is particularly useful when communicating with executives or budget holders, and when designing implementation plans that balance compliance requirements with financial constraints.

Another recurring theme is the desire among some organizations to achieve only the minimum level of compliance necessary to meet legal requirements. In these cases, NIS2 is often perceived not as a strategic improvement initiative, but rather as a mandatory hurdle or a "license to operate." This perception was also evident in the questionnaire responses, where several participants rated NIS2's expected contribution to organizational growth as neutral or low. This reinforces the notion that many organizations view the directive more as a burden than as an opportunity for long-term improvement.

Consequently, there is a strong argument for ensuring that the minimum compliance threshold meaningfully addresses core cybersecurity objectives. Without this, the directive risks promoting superficial adherence rather than driving substantial progress. If NIS2 is to avoid being seen purely as a compliance burden, it may be beneficial for future iterations or supporting guidance to align more closely with established certification frameworks. Doing so could provide organizations with a clearer incentive to engage more fully with the directive, as compliance could then contribute toward broader security certifications and strategic positioning.

From the consultant's perspective, recognizing this mindset allows for better alignment with client expectations. Some consultants have already adopted a pragmatic stance by advising clients to meet only the level of compliance required to fulfill legal obligations

and control costs. While this approach may be necessary in some contexts, it reflects the broader challenge that many organizations continue to treat cybersecurity as a cost center rather than a value driver. It is worth noting, however, that consultants still aim to encourage proper implementation by embedding compliance activities into the organization's operations, even if the overall ambition level remains modest.

To partially conclude the first research question regarding observable patterns in NIS2 implementation, it is necessary to reflect across all four analytical categories: positive drivers, negative barriers, support needs, and underlying motivations. The findings suggest that successful implementation is most closely associated with prior regulatory experience, embedded governance structures, and a strategic understanding of cybersecurity. Conversely, organizations lacking internal knowledge and awareness of the directive consistently struggle to interpret and apply its requirements.

A particularly important insight is that knowledge gaps can significantly shape how the directive is perceived. For many organizations, limited familiarity with NIS2 leads to its framing as a burden rather than a security opportunity. These patterns underline the importance of both internal capability-building and external guidance if the directive is to achieve more than surface-level compliance.

5.3 RQ2 – What Organizational or Regulatory Factors Contribute to a Compliance-driven Approach?

The interview and survey data reveal a multi-layered set of reasons why many firms pursue only a minimum-viable implementation of NIS2. These reasons fall into three broad categories: (i) difficulties of directive, (ii) reason, and (iii) low compliance experience or level. Together, they form a feedback loop that encourages check-box compliance behavior even among firms that recognize the strategic value of stronger cyber resilience.

Difficulties of Directive: Although this was the smallest of the three clusters, nearly every interviewee raised at least one obstacle that comes straight from the wording or roll-out of NIS2 (see Figure 4.5). Five respondents said the directive's language is too vague (phrases such as "appropriate" or "proportionate" leave them guessing what an auditor will deem sufficient). Three others highlighted the slow pace of national transposition and the lack of final sector handbooks; until those documents appear, organizations hold back on major security investments because they do not know what will eventually be required. A further complication is timing: many firms are already working on the Digital Operational Resilience Act (DORA) in finance and the Cyber-Resilience Act (CRA) for product security. All three laws demand incident reporting and supplier-risk checks, but each frames those duties slightly differently. As a result, companies often duplicate effort

(maintaining one policy set for NIS2, another for DORA, and a third for CRA) rather than building a single, integrated risk program. Most interviewees described this as a "lowest-effort survival tactic": produce the paperwork each statute asks for, postpone deeper technical fixes, and hope later guidance clarifies how the pieces can be merged.

It seems fair to assume that the vagueness in language of the directive does more than frustrate implementers. It may actively shape behavior. As mentioned, several participants described the terms "Appropriate" or "proportionate" as ways to include too much interpretation, especially in the absence of sector-specific guidance. From a regulatory design perspective, this ambiguity might have been intended to provide organizations room to tailor their approach, but in reality, it appears to do the opposite. Rather than encouraging risk-based adaption, it leads to hesitation and delay. Many organizations would rather do the bare minimum than risk doing the wrong thing. This also reinforces why so many respondents mentioned waiting for national handbooks or more detailed instructions before continuing.
The overlap with existing regulation, such as DORA or the CRA, adds to the complexity. While it makes sense that different regulations address distinctive domains, the practical reality is that many organizations experience them as competing. Rather than aligning on efforts, companies could end up duplicating documentation in order to meet compliance across different regulations. It is not difficult to understand why some organizations adopt a lowest-efforts approach. If even well-resourced companies struggle in interpretation, smaller entities can be considered left paralyzed. The interviews did not lack of interest in improving security, they pointed to structural confusion of where to begin. In this sense, much of the compliance-driven behavior appears to result not from reluctance, but from a lack of clear direction.

Reason: Interviewees and survey data converge on a single behavioral trend: most firms aim first, and sometimes only, at the narrowest set of activities that will survive an audit. Many interviewees went so far as to call NIS2 "just the fee for entry", in other words: a license to operate rather than a lever for competitive advantage. More than two-thirds of the survey respondents indicated that their strategic objective is 'demonstrable compliance' rather than 'risk reduction'. In interviews, this common sentiment among the participants was phrased as "Tell us what the bare minimum to comply is, then we'll think about extras later." This echoes the GDPR experience, where organizations focused on documentation and legal artifacts rather than privacy-by-design controls [14, 43].

This framing of NIS2 as a "license to operate" suggests that organizations often interpret regulatory obligations through a defensive lens rather than strategic. What stands out is not open resistance to regulation, but a rational calculation. Many firms appear to weigh their decisions against expected scrutiny and enforcement likelihood rather than against internal security needs. This approach reflects a tendency to treat compliance as a cost to be minimized, especially when regulation lacks clear incentives for going beyond baseline

requirements.

This behavior is further supported by the questionnaire data, where five out of nine fully responding organizations reported having identified a specific stopping point in their NIS2 implementation efforts, as seen in figure 4.5a. These self-imposed ceilings reflect a common tendency to treat compliance as a fixed target rather than an ongoing improvement process.

The survey responses make it clear that many organizations decide in advance how far they intend to go. Instead of treating implementation as an ongoing process, they define a clear stopping point. This suggests that for some, compliance is seen as something to complete rather than something to improve over time. One possible reason for this is the lack of clear guidance on what a more mature implementation strategy would look like beyond the basic legal requirements.

Consultants play a significant role in shaping these decisions. Most of the advisory specialists interviewed reported that clients routinely open engagements with the question, "What is the minimum we need to stay compliant?" Fixed-price "readiness packages" therefore emphasize policies, risk registers and incident-reporting workflows, deliverables that satisfy auditors but rarely extend to deeper control modernization. Consultants explained that many clients arrive with tight budgets and want a solution that fits the security they can afford, not the security they ideally need. Several consultants admitted that they would prefer to sell more holistic, risk-based programs, but client demand for low-cost, audit-ready artifacts keeps the market anchored at a checklist level. While it is important to note that some consultants advocated for minimum compliance, arguing that it is better for companies to implement what is realistically achievable than to do nothing or fail at more complex requirements, this highlights the challenge consultants face in tailoring implementations. It emphasizes the ongoing effort to assess what organizations actually need and shows that a one-size-fits-all approach does not work.

Low Compliance Experience / Level : As already mentioned, the lack of prior regulatory awareness resulted in the strongest factor of creating a check-box mindset. Cost remains the most frequently cited internal constraint, but it is closely tied to limited awareness and compliance experience. SMBs, in particular, reported diverting funds from planned detection or hardening projects to consultancy fees, staff training and policy generation, replicating the budget-displacement pattern observed during the early GDPR rollout. Even mid-sized firms with prior regulatory experience described NIS2 as "a zero-sum game": new line-items for gap assessments appear, but overall security spend does not grow.

An important observation from the findings is that limited awareness often leads to a check-box mindset. In contrast, companies with more experience and understanding of the directive tend to pursue more holistic and effective implementations. When organi-

zations know what to implement and understand the directive's value, they are better positioned to act strategically rather than superficially. A key factor in moving companies away from a check-box approach is increasing their awareness. This can come through clearer communication in the directive itself, guidance from consultants, or internal implementation efforts. Closing this awareness gap is essential for meaningful adoption. It highlights the importance of implementers having a solid understanding of the directive before making any decisions. The initial stages of implementation require a clear grasp of the available compliance levels and how they align with the organization's specific needs. Without this understanding, implementers may overlook the directive's relevance, resulting in a compliance-driven mindset. This challenge is not limited to smaller organizations; even larger or more mature companies can fall into the same pattern if they lack familiarity with the directive's core risk-based approach. For many, this remains a significant knowledge gap that can undermine the directive's full potential.

These findings are supported by the questionnaire data, where capacity constraints amplify the incentives above, as seen in figure 4.5b. Newly scoped entities without prior regulatory exposure (three references) struggle to interpret NIS2 and, in six instances, admitted difficulty adopting its risk-based mindset. Financial limits (five references) and general awareness gaps (three) push SMBs in particular toward reallocating scarce funds from technical controls to consultant fees, training days, and policy drafting. Even mid-sized companies spoke of a "zero-sum budget," where every euro spent on gap assessments was taken from detection or hardening projects.

To partially conclude, we could agree that taken together, these factors form a reinforcing loop. High marginal costs push organizations toward the smallest defensible scope; ambiguous enforcement removes incentives to exceed that scope; consultants institutionalize a checklist model; and overlapping statutes further entrench artifact production over technical hardening. Unless regulators issue clearer, operationally granular guidance, harmonize supervisory practices, and channel capacity-building funds to SMBs, NIS2 may replicate GDPR's trajectory: substantial expenditure, impressive documentation, and only modest improvement in Europe's practical cyber-resilience.

5.4 RQ3 – Does NIS2 Provide Tangible Security Improvements, and is the Value of Implementation Present Short/Long-term?

Negative: Across our interview set and supporting survey, NIS2 has unquestionably provoked organizational activity, but the bulk of that activity is administrative rather than technical. Smaller and less-mature organizations told us they had to draft these artifacts from scratch, whereas large multinationals mostly reused documents they were already

using under their sector rules. Policies are always increasing, incident-escalation charts are updated, and board briefings now feature "NIS2" on the agenda. Yet only a minority of respondents could point to hard evidence, shorter patch windows, richer telemetry, lower mean-time-to-recover, that the directive has improved real cyber-risk posture. Interviewees from mature firms stressed that the baseline controls from NIS2 were already fulfilled, adding little incremental security value for them. The real improvement is supposed to come from less-mature companies, which is exactly where resources are most lenient.

As illustrated in figure 4.8b, the most frequently coded concerns were *unclear directive requirements* (5 references) and *delays in national implementation* (3 references). Respondents linked these gaps directly to a "compliance exercise" mind-set: documentation grows, but tangible controls lag. Even large firms (which might be expected to lead) admitted they were "waiting for the templates" before funding deeper security upgrades. This combination of vague wording and delayed national templates leave many businesses (especially SMEs) treating NIS2 as nothing more than a license to operate.

These findings also align with the initial scoping decisions made during the research design. Certain sectors, particularly those composed of mature organizations with extensive regulatory exposure, were excluded from the study based on the assumption that they would see limited additional benefit from the NIS2 Directive. As several interviewees confirmed, many of these firms had already implemented comparable controls through prior frameworks, resulting in little added security value from NIS2's baseline requirements.
That said, while the directive may help formalize or reinforce existing governance practices in such organizations, its primary functions is arguably to raise standards among less mature entities, precisely where resource constraints, limited internal expertise, and implementation uncertainty are most present. However, the ambiguity surrounding some of the key provisions, such as scope and interpretation, continues to pose a challenge even for these target groups. This raises a broader concern that whether NIS2 will truly uplift foundational security practices, or whether it will reinforce a compliance-focused mindset with only marginal impact on real-world risk reduction.

Despite the outliers, most organizations remain in a reactive posture. Consultant interviews were unequivocal: new clients typically ask "What do we need to stay compliant?", rarely "How do we reduce risk?" Enforcement ambiguity reinforces this stance; firms are waiting for national guidance before committing to deeper changes, repeating the "checkbox first, optimize later" cycle seen after GDPR [22]. Consequently, NIS2's early dividends are governance-centric and compliance-driven, while tangible security improvements are uneven and contingent.

Positive: As figure 4.8a shows, most of the positive aspects come from pragmatic gains that organizations can realize as soon as they start the project. Interviewees consistently

described NIS2 as more actionable and technical compared to GDPR, resulting in the possibility to leverage it to gain new customers. Unlike high-level frameworks that leave firms wondering how to comply, NIS2 sets out explicit management, technical and reporting obligations. The more actionable nature and it being for cybersecurity as a whole makes consultants more optimistic for its security potential. Some companies actually see the directive as a growth driver, using it as a quasi-"certificate" to win security-sensitive customers (ultimately securing a long-term license to operate and a respected level of trust among their customers). Even with the directive's late transposition and vague requirements, there is a perceived value in having less experienced businesses implement it, as partial implementation is better than no effort at all. For more mature organizations, the directive is often viewed as a growth driver, and they are better positioned to align it with their existing business objectives. This alignment significantly enhances the potential impact and long-term benefits of the directive. All of this provides a positive outlook for the future of NIS2 implementation. It suggests that the directive has the potential to move beyond its current vagueness, particularly for less mature organizations that are expected to benefit the most from its guidance.

Supplementary research viewpoint: However, the uneven transposition of NIS2 across Member States significantly undermines the directive's potential to deliver consistent and long-term improvements in security posture. As outlined in the supplementary research in section 4.3, Member States differ not only in implementation deadlines, but also in sectoral scope, supervisory structures, and enforcement clarity. This divergence creates inconsistencies in how "tangible improvements" are defined and measured. For example, organizations operating in stricter jurisdictions may face higher compliance thresholds that can lead to stronger local security measures. Even though this also can lead to a competitive disadvantage, this imbalance diminishes the comparability of outcomes across the Union, meaning that concerns about improvements observed in some countries may not scale cross-borders.

Moreover, the variation in national enforcement seen from supervisory bodies, introduces ambiguity that limits forward-planning. From a strategic perspective, organizations cannot rely on a stable baseline of regulatory expectations, which inevitably can discourage investment in long-term resilience. instead, some opt to align only with the perceived "minimum viable compliance" level required under local law.

To partially conclude RQ3, early evidence suggests that NIS2's short-term impact is weighted toward compliance paperwork. Where boards view the directive as an opportunity (backed by clear accountability and targeted funding) measurable improvements do follow. Crucially, respondents are optimistic because the directive is viewed as far more actionable than GDPR; organizations with the right level of maturity can already lever-

age that specificity as a growth driver. Still, whether those near-term advantages mature into sustained, measurable risk reduction hinges on consistent national transposition, robust supervision, and a shift from minimum-viable compliance to genuine operational resilience.

Across the sample, the first wave of activity has been overwhelmingly administrative (policy rewrites, incident-notification drills, board briefings). This pattern echoes the GDPR rollout, as discussed in section 2.3 and further explored in section 5.1, where early spending gravitated toward legal artifacts rather than privacy-enhancing technologies [14, 43]. Yet the handful of "positive-outlier" cases demonstrate that NIS2's governance clauses can unlock long-delayed investments when leaders choose to treat the directive as leverage rather than liability.

5.5 RQ4 – How do Industry Experts Interpret the NIS2 Directive in terms of its Completeness, Clarity or Practicality?

Negative: The expert interviews suggest that while the NIS2 Directive introduces a necessary and overdue regulatory improvement, its real-world usability is constrained by interpretational ambiguity, national fragmentation, and a lack of actionable guidance. Respondents consistently emphasized that while the directive represents a step forward compared to previous legislation, its operational effectiveness remains uncertain.

One of the most cited challenges was the vagueness of legal language, particularly around obligations described as "*appropriate*", "*sufficient*", or "*proportionate*". While these classifiers help enable flexibility in theory, they shift interpretational responsibility onto the organizations themselves. This, based on the collection of research material, has created confusion and reliance on external consultants, especially among SMBs. This is represented through the secondary supporting data collection, as well as aligning with figure 4.10, which shows that concerns about ambiguity were among the most frequently cited negative framings of the directive.

Interview responses highlight the persistent uncertainty regarding the directive's practical clarity. This perception aligns with findings from the supplementary research, which documents substantial differences in national interpretations, especially around entity classification, reporting procedures, and supervisory authority mandates. For instance, the term "management body" remains variably defined across Member States, leaving room for interpretation that fragments accountability structures across jurisdictions.

Positive: However, despite these critiques, most experts did not view the directive as fundamentally flawed. Figure 4.9 illustrates that the balance of responses included an

equal amount of positive and negative perspectives, which highlights a pragmatic and conditional optimism. On the positive side, 4.10a shows that several participants valued NIS2's more actionable design compared to GDPR, especially in relation to its incident reporting obligations and top-level accountability requirements.

Improvements: In discussing potential improvements, experts made several concrete proposals, as seen in 4.11. One of the more prominent highlights from this collection included the introduction of operational annexes that translate articles into control sets (e.g., aligned with ISO/IEC 27001 and the subsequent 27002), and the need for sector-specific guidance from national authorities. The distinction of sector-specific guidance has already begun for some of the sectors identified within the *Essential* category; For instance, as seen with the guidance material for the energy sector. Here, the Danish government has published proposals which will guide the organizations with directly applicable paths of implementation [63, 64]. Importantly, many emphasized that the directive's success would depend less on its wording and more on its enforcement architecture. Without credible supervisory follow-up, several experts argued that firms will default to the lightest viable interpretation of the requirements.

From a macro perspective, several experts expressed a preference for a more prescriptive, regulation-style approach rather than the current directive-based model. This viewpoint resonates the broader policy concern identified in the transposition research. Even though the directive's inherent legal flexibility should serve as an enabler, it hinders uniform implementation. So, while NIS2 offers a promising conceptual framework, its effectiveness is constrained due to the observed variations.

To partially conclude, these perspectives portray NIS2 as a directive with clear intent but incomplete delivery infrastructure. Experts do not reject its ambition but remain skeptical of its current implementation landscape. The directive's long-term impact will likely depend on the emergence of coordinated guidance, enforceable clarity, and practical support structures that will enable organizations to translate its high-level aims into usable regulatory practice.

5.6 Limitations

Although our findings from the study offers an early approach to NIS2 adoption, they come with a few important caveats:

Sample Composition and Selection Bias: We ended up interviewing eight experts (six Danish consultants, one Spanish consultant, and one Norwegian consultant). Because they all advise companies that have already decided to tackle NIS2, we did not hear from

organizations that are ignoring or postponing the directive. Their views might be very different.

Limited Geographical and Sectoral Coverage: The study reflects primarily Nordic (and, to a lesser extent, Spanish) perspectives gathered before full national transposition. No interviews were secured with telecom, energy-operator, or pan-European conglomerate CISOs Results may look different once we cover more regions and sectors.

Timing of Data Collection: Data were gathered between February 2025 and May 2025, therefore all interviews happened before every EU country finished its local NIS2 law. Many companies are still waiting for final templates and audit checklists, so their answers are based on guess-work rather than lived experience.

Reliance on Self-reported Perceptions: Both interview and survey instruments capture perceived costs, maturity levels and improvements. They do not measure objective security outcomes, therefore we could not check incident logs, patch metrics, or budgets ourselves. Memory gaps, social-desirability bias and organizational narratives shaped by compliance marketing or "best-face-forward" answers are possible.

Qualitative Coding and Researcher Position: Thematic coding was performed by the student research team. Although intercoder checks were applied, interpretive bias cannot be ruled out. Moreover, the researchers' outsider status limited access to confidential artifacts (risk registers, audit findings) that might have corroborated or tempered interview claims. Considering all this, some personal bias might still be able to appear.

Survey Scope and Representativeness: The supplementary questionnaire yielded nine complete responses, insufficient for robust statistical inference. Results should be viewed as directional signals that complement the interview findings and help indicate broader patterns, not as stand-alone evidence.

Regulatory Overlap not fully explored: While DORA, CRA and sector-specific mandates were acknowledged, the study did not formally map every overlap in detail. This could be explored in future work.

Transposition Timing and Evolving Context: A further limitation stems from the fragmented state of NIS2 transposition at the time of this study. Because most Member States have yet to fully implement the directive, both interview and supplementary analysis findings reflect an evolving landscape. This limitation complicates the task of assessing long-term impact or cross-national effectiveness. While the supplementary transposition research offers valuable insight into early divergence patterns, these may shift as additional national laws are finalized. Future research should revisit these findings after full implementation has occurred across the EU.

5.7 Future work

Building on the limitations above, several research avenues could strengthen (or challenge) the study's provisional conclusions and deepen understanding of NIS2's impact.

Follow Organizations over Time: Rather than a single snapshot, future research should track the same firms for several years after NIS2 is fully in force. Remeasuring outcomes such as incident rates, patch times and audit findings would show whether early paperwork efforts later translate into real security gains.

Widen the Sample: Our data collection for the primary research comes mostly from Danish, Norwegian, and Spanish experts. Replicating the study in other EU countries would reveal whether the patterns seen can be verified and expanded further. Including telecom, energy and large multi-nationals would additionally balance the SMB focus of this work.

Measure Breach Costs and Savings: Once national incident-notification databases become available, researchers could link those records to cost estimates (e.g., insurer payouts, service downtime). A "before-and-after" or control-group design would clarify whether NIS2 actually lowers loss severity.

Compare Overlapping Laws: Many firms face NIS2, DORA, CRA and sector rules at the same time. A detailed control-by-control map would show where requirements clash, duplicate, or support one another (helping regulators streamline audits and reduce redundant paperwork).

Long-term Effects: Building on the supplementary research, future studies could focus on the long-term effects of legal divergence on cross-border security coordination. A comparative case study approach that examines organizations across high- and low-stringency Member States may reveal how regulatory fragmentation translates into operational variances.

Chapter 6

Conclusion

This thesis set out to examine the extent to which the NIS2 Directive leads to tangible improvements in cybersecurity practices, or whether it primarily drives minimal, compliance-oriented implementation. To address this, four research questions (see section 1.4) were developed and explored through qualitative interviews and a supporting survey (as detailed in chapter 3).

The findings reveal that patterns of NIS2 implementation vary significantly across organizational size, sector, and regulatory familiarity. Larger organizations and those in previously regulated sectors tend to progress faster, often due to better resource availability and internal compliance infrastructure. However, across all groups, a consistent challenge lies in the complexity of the directive's risk-based and organizational requirements. Financial constraints are not the sole barrier; limited awareness and knowledge also significantly hinder progress, particularly for smaller or less mature organizations.

The second research question focused on understanding why many organizations adopt a compliance-driven approach. The data indicates that this tendency results from a combination of vague directive language, delays in national transposition, and the perception that NIS2 is primarily a legal formality rather than a strategic opportunity. Fines and enforcement mechanisms appear to be key drivers. Nonetheless, several consultants argued that even minimal compliance can be beneficial, as it allows organizations to engage with regulatory expectations in line with their current capacity, which is seen as preferable to taking no action at all.

Regarding whether NIS2 leads to tangible security improvements, the evidence is mixed. For less mature organizations, the directive often acts as a catalyst for initiating security practices and improving structural capabilities. For more mature organizations, however, the directive offers less added value and is sometimes perceived as redundant. Despite this, participants noted that NIS2 is generally more actionable than past regulations such as GDPR, and it can support business growth by providing a form of assurance or license to operate that facilitates client trust and market access.

Experts overall view NIS2 as a step in the right direction. However, they identified several areas where the directive falls short. The most pressing concerns include inconsistent national transposition, a lack of actionable guidance, limited support resources, and un-

certainty about long-term regulatory enforcement. Respondents emphasized the need for clearer implementation instructions, timely transposition, and accessible advisory channels. Without these, the directive's effectiveness may be diminished due to uneven interpretation and implementation. The supplementary research further reinforces this concern, highlighting that the directive-based nature of NIS2 is itself a key driver of the slow and fragmented transposition across Member States. As a legal instrument, directives inherently allow for national discretion, which has resulted in substantial divergence in implementation timelines, scope, and enforcement structures.

Returning to the central aim of this thesis, it can be concluded that NIS2 has the potential to drive genuine improvements in cybersecurity practices. However, its success is conditional. The directive creates opportunities for progress, particularly among organizations that previously lacked formal structures. Yet it also risks producing minimal outcomes where awareness and guidance are insufficient. Many of the directive's weaknesses relate not to its substance, but to the environment in which it is introduced. To enhance its impact, implementers, regulators, and advisors must address these gaps collectively.

Given the predominantly advisory-based sample, the findings reflect cross-organizational patterns rather than deep internal implementation dynamics. This perspective provided valuable breadth, but future studies should consider additional viewpoints.

This thesis provides an early empirical foundation for understanding how organizations interpret and operationalize cybersecurity regulation under NIS2. The insights may help inform future implementation strategies, regulatory refinements, and advisory efforts. Future work could extend these insights by directly studying internal implementation strategies as organizations move closer to compliance deadlines and enforcement mechanisms mature.

Bibliography

[1] Aalborg University. *Rules for the Use of Generative AI*. Accessed: 2025-05-22. 2024. URL: https://www.students.aau.dk/rules/rules-for-the-use-of-generative-ai#to-which-extent-am-i-permitted-to-use-generative-ai-in-project-work.

[2] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2023*. [Accessed 16-05-2025]. Heraklion: EU Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf.

[3] *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148. [Accessed 16-05-2025]. 2016.

[4] Yelena Smirnova and Victoriano Travieso-Morales. "Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review". In: *International Journal of Law and Management* 66.3 (2024). [Accessed 16-05-2025], pp. 326–344. URL: https://www.researchgate.net/publication/377572957.

[5] *Regulation (EU) 2019/881 (Cybersecurity Act) on ENISA and ICT cybersecurity certification*. https://eur-lex.europa.eu/eli/reg/2019/881/oj. [Accessed 16-05-2025]. 2019.

[6] *Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA)*. https://eur-lex.europa.eu/eli/reg/2022/2554/oj. [Accessed 16-05-2025]. 2022.

[7] *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*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555. [Accessed 16-05-2025]. 2022.

[8] Tope Olufon, Madelein van der Hout, and Zaklina Ber. *Systemic Gaps and Geopolitical Tensions Define Europe's Cybersecurity Threats in 2024*. Forrester Research Blog, 25 Sep 2024 [Accessed 16-05-2025]. 2024. URL: https://www.forrester.com/blogs/systemic-gaps-and-geopolitical-tensions-define-europes-cybersecurity-threats-in-2024/.

[9] Jukka Ruohonen. *A Systematic Literature Review on the NIS2 Directive*. eng. arXiv preprint arXiv:2412.08084. [Accessed 16-04-2025]. 2024. URL: https://arxiv.org/abs/2412.08084.

[10] 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 (NIS2 Directive)*. *Official Journal of the European Union*, L 333, 80–152. 2022.

[11] European Commission. *The EU's Cybersecurity Strategy for the Digital Decade (COM(2020) 605 final)*. Brussels: European Commission. Available at https://digital-strategy.ec.europa.eu. 2020.

[12] *NIS2 Directive Information Hub*. Accessed: 2025-03-01. 2024. URL: https://nis2directive.eu.

[13] European Parliament and Council. *Regulation (EU) 2016/679 (General Data Protection Regulation)*. [Accessed 16-05-2025]. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[14] Sean Sirur, Jason R. C. Nurse, and Helena Webb. "Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)". In: (2018), pp. 88–95. URL: https://arxiv.org/abs/1808.07338.

[15] Edilson Teixeira, Ana Ferreira, and Lixia Liu. "Critical Challenges in GDPR Implementation: A Systematic Review". In: *Journal of Information Systems Engineering & Management* 4.1 (2019), pp. 1–21. URL: https://www.researchgate.net/publication/333581339.

[16] M. Lin and M. Saebeler. "Risk-based vs. Compliance-based Cybersecurity". In: *EBA-Net* (2019).

[17] W. Wang, S. M. Sadjadi, and N. Rishe. "A survey of major cybersecurity compliance frameworks". In: *Proceedings of the 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity)*. New York, NY, USA, 2024, pp. 23–34. DOI: 10.1109/BigDataSecurity62737.2024.00013.

[18] Danielle Barbour. *Small Business Guide to NIS 2 Compliance*. [Accessed 16-05-2025]. Oct. 2024. URL: https://www.kiteworks.com/regulatory-compliance/nis-2-compliance-small-business/.

[19] Vanta. *NIS 2 Compliance Checklist: 7 Steps You Need to Take*. [Accessed 16-05-2025]. 2024. URL: https://www.vanta.com/resources/nis-2-compliance-checklist.

[20] Robin Tatam. *NIS2: Compliance Requirements, Deadline & Instructions for the New NIS2 Directive*. [Accessed 16-05-2025]. May 2025. URL: https://www.puppet.com/blog/nis2.

[21] European Cyber Security Organisation (ECSO). *NIS2 Implementation: Challenges & Priorities (White Paper)*. [Accessed 16-05-2025]. 2025. URL: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf.

[22] Yelena Smirnova and Victoriano Travieso-Morales. "Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review". In: *International Journal of Law and Management* 66.3 (2024), pp. 326–344. URL: https://www.emerald.com/insight/content/doi/10.1108/IJLMA-08-2023-0170/full/pdf.

[23] Tiernan Connolly and Hannah Rossiter. *DORA vs. NIS2 vs. PSD2: Navigating the Evolving Regulatory Landscape*. [Accessed 16-05-2025]. Oct. 2024. URL: https://www.kroll.com/en/insights/publications/cyber/dora-vs-nis2-vs-psd2-navigating-evolving-regulatory-landscape.

[24] European Commission. *Commission Guidelines on the Relationship between NIS2 and DORA*. [Accessed 16-05-2025]. Sept. 2023. URL: https://www.nis-2-directive.com/.

[25] Setterwalls Advokatbyrå. *Drawing the Line – Managing the Overlap Between the Different Cybersecurity Regulations*. [Accessed 16-05-2025]. Nov. 2024. URL: https://setterwalls.se/en/article/drawing-the-line-managing-the-overlap-between-the-different-cybersecurity-regulations/.

[26] Alfredo Thomas Moretti and Nuria Talayero. *DORA, NIS2 and CRA: Decoding Europe's Cybersecurity Regulatory Landscape*. [Accessed 16-05-2025]. Jan. 2025. URL: https://www.telefonica.com/en/communication-room/blog/dora-nis2-cra-decoding-europes-cybersecurity-regulatory-landscape/.

[27] *Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act)*. https://eur-lex.europa.eu/eli/reg/2024/2847/oj. [Accessed 16-05-2025]. 2024.

[28] Eviden SAS. *Network and Information System Directive (NIS2) – Compliance Journey Whitepaper*. [Accessed 16-05-2025]. June 2024. URL: https://sec-consult.com/fileadmin/user_upload/sec-consult/Statisch/Home/NIS2/NIS_2_Whitepaper_20-06-2024_Final.pdf.

[29] Jonny Cameron. *NIS2 Checklist*. [Accessed 16-05-2025]. Feb. 2025. URL: https://simplynuc.eu/blog/nis2-checklist/.

[30] J. Ruohonen. "Early perspectives on the Digital Europe Programme". In: *Digital Policy, Regulation and Governance* 27.1 (2025), pp. 37–55. DOI: 10.1108/DPRG-11-2024-0162.

[31] European Criminal Law Associations. "Commission Report on the Application of the GDPR". In: *eucrim* (2021).

[32] PwC. *Preparing for GDPR: Survey Results*. PricewaterhouseCoopers. 2017.

[33] EY and IAPP. *GDPR Benchmarking Survey*. EY & IAPP. 2018.

[34] Cisco Systems. *2023 Data Privacy Benchmark Study*. [Accessed 16-05-2025]. Cisco Systems, 2023. URL: https://www.cisco.com/c/dam/en/us/products/collateral/security/2023-data-privacy-benchmark-study.pdf.

[35] Data Catalyst Institute. *Say It Ain't So: GDPR Data Regulation Hurts EU Economic Growth*. [Accessed 16-05-2025]. 2020. URL: https://datacatalyst.org/reports/say-it-aint-so-gdpr-data-regulation-hurts-eu-economic-growth/.

[36] International Association of Privacy Professionals and Ernst & Young. *Privacy Governance Report 2022*. [Accessed 16-05-2025]. 2022. URL: https://iapp.org/resources/article/iapp-ey-privacy-governance-report-2022/.

[37] Jian Jia, Ginger Zhe Jin, and Liad Wagman. *The Short-Run Effects of GDPR on Technology Venture Investment*. Tech. rep. [Accessed 16-05-2025]. Cambridge, MA: National Bureau of Economic Research, 2019. URL: https://www.nber.org/system/files/working_papers/w25248/w25248.pdf.

[38] Jennifer Huddleston. *The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More*. [Accessed 16-05-2025]. 2021. URL: https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more/.

[39] American Action Forum. *The Unintended Consequences of the GDPR*. American Action Forum. 2019.

[40] . Jia et al. *The Short-Run Effects of GDPR on Technology Venture Investment*. eng. [Accessed 2-03-2025]. Cambridge, Mass, 2018. URL: chrome-extension://efaidnbmnnnibpcajpcglclefin https://www.nber.org/system/files/working_papers/w25248/w25248.pdf.

[41] Data Catalyst Institute. *Europe's Privacy Rules Are Having Unintended Consequences - Data Catalyst — datacatalyst.org*. https://datacatalyst.org/europes-privacy-rules-are-having-unintended-consequences/. [Accessed 2-03-2025].

[42] Garrett A. Johnson, Scott K. Shriver, and Samuel G. Goldberg. *Privacy and market concentration: Intended and unintended consequences of the GDPR*. https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=.... [Accessed 2-03-2025]. 2023.

[43] H. Freitas and M. Silva. "GDPR compliance in SMEs: There is much to be done". In: — (2018). Explores SME-specific cost-benefit challenges.

[44] *SME definition — single-market-economy.ec.europa.eu*. https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en. [Accessed 09-05-2025].

[45] Svend. Brinkmann and Steinar. Kvale. *InterViews : learning the craft of qualitative research interviewing*. eng. 3. ed. Los Angeles, Calif: Sage Publications, 2015. ISBN: 9781452275727.

[46] Microsoft. *Enterprise Data Protection in Microsoft 365 Copilot and Microsoft 365 Copilot Chat*. Accessed: 2025-05-16. 2024. URL: https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection.

[47] John W. Creswell and J. David Creswell. *Research design : qualitative, quantitative, and mixed methods approaches*. eng. Fifth edition. Thousand Oaks, California: SAGE Publications, Inc., 2018 - 2018. ISBN: 9781506386706.

[48] Aalborg University. *Data classification and system use*. https://www.security.aau.dk/data-classification. Accessed: 2025-05-29. 2024.

[49] Virginia Braun and Victoria Clarke. "Using thematic analysis in psychology". eng. In: *Qualitative research in psychology* 3.2 (2006), pp. 77–101. ISSN: 1478-0887.

[50] DNS Research Federation. *Trends in the Transposition Journey of Article 28 of NIS2*. Blog post. Accessed: 2025-05-01. Apr. 2025. URL: https://dnsrf.org/blog/trends-in-the-transposition-journey-of-art-28-of-nis2/index.html.

[51] Konrad Sałek and Patryk Fajdek. "Analysis of the Implementation of the NIS2 Directive in the Weimar Triangle Countries". In: *Central European Review of Economics & Finance* (2025). Accessed: 2025-05-01. URL: https://journals.economic-research.pl/ceref/article/download/3677/2455/11887.

[52] KPMG Netherlands. *NIS2 Update*. White paper. Accessed: 2025-05-01. 2025. URL: https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/services/nis2-update.pdf.

[53] European Cyber Security Organisation (ECSO). *NIS2 Directive Transposition Tracker*. Webpage. Accessed: 2025-05-02. 2025. URL: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/.

[54] European Commission. *Commission calls on 19 Member States to fully transpose the NIS2 Directive*. Press release. Accessed: 2025-05-02. 2025. URL: https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive.

[55] Ronja Isaksson. *NIS2 & National Implementation: Which Local NIS2 Laws Are Available in Cyberday?* Cyberday blog post. Accessed 2025-05-2. 2025. URL: https://www.cyberday.ai/blog/nis2-national-implementation-which-local-nis2-laws-are-available-in-cyberday.

[56] Cyber Risk GmbH. *The NIS2 Directive | Transposition*. Webpage. Accessed 2025-05-2. URL: https://www.nis-2-directive.com/NIS_2_Directive_Transposition.html.

[57] Phil Muncaster. *Over Half of UK Firms Not GDPR Compliant*. Available at: https://www.infosecurity-magazine.com/news/over-half-of-uk-firms-still-not/. Accessed: 2025-03-16. 2025.

[58] Sean Sirur, Jason R. C. Nurse, and Helena Webb. "Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)". In: *MPS 2018 - Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, co-located with CCS 2018*. ACM, 2018.

[59] Ran Zhuo et al. *The Impact of the General Data Protection Regulation on Internet Interconnection*. Accessed: 2025-05-16. 2020. URL: https://www.nber.org/system/files/working_papers/w26481/w26481.pdf.

[60] Gonçalo Almeida Teixeira et al. *The Critical Success Factors of GDPR Implementation: A Systematic Literature Review*. Available at: https://www.proquest.com/docview/2559388433/fulltextPDF. Accessed: 2025-04-12. 2019.

[61] Brian DeVault. *How Compliance Can Create a False Sense of Security*. Available at: https://www.netrio.com/how-compliance-can-create-a-false-sense-of-security-for-business-operators/. Accessed: 2025-03-12. 2025.

[62] Forta - Tripwire. *Mind the Cybersecurity Gap*. Available at: https://static.fortra.com/tripwire/pdfs/guides/tw-mind-the-cybersecurity-gap-gd.pdf. Accessed: 2025-03-12. 2025.

[63] Forsyningsministeriet. *BEK nr 260 af 06/03/2025, Klima-, Energi- og Forsyningsministeriet – retsinformation.dk*. Available at: https://www.retsinformation.dk/eli/lta/2025/260. Accessed: 2025-04-12. 2025.

[64] Forsyningsministeriet. *LOV nr 258 af 06/03/2025, Klima-, Energi- og Forsyningsministeriet – retsinformation.dk*. Available at: https://www.retsinformation.dk/eli/lta/2025/258. Accessed: 2025-04-12. 2025.

Appendix A

Interview Consent Form

This appendix presents the original participant consent form that was distributed prior to each interview. It includes the purpose of the study, participant rights, data usage, and contact information for questions or withdrawal.

Do you want to contribute to our master thesis in understanding the efficacy of implementing legislatures in businesses?

Purpose

We are a student team creating a master's thesis through Aalborg University analysing the cyber-oriented legislatures and related legislative regulation on their actual efficacy in how well they are implemented in businesses, or the potential consequences of improper organizational implementation.

Who is responsible for this thesis?

Students at Aalborg University, The Technical Faculty of IT, Electronics, and Programming, in collaboration with professor Lene Tolstrup Sørensen as the internal supervisor.

Why did we ask you to attend?

Our student team has either been given your contact from our supervisor, Lene Tolstrup Sørensen, has been attracted to your knowledge as a Subject matter expert, or in any other way, a potential contributor to the success of the finalization of the project.

What does contributing mean for you?

It means you will be contributing in providing a better understanding of the usefulness in implementing legislations in businesses. This does not entail any obligations for you, and your personal information details will become anonymized.

It is voluntary to contribute

It is voluntary to contribute to this thesis. If you choose to participate, then it is within your right to retract your consent without providing any reason at any point in time. All of your personal information will be deleted. It will have no negative consequences for you if you choose not to participate or retract your choice later.

Your privacy - how we will store and use your information

We will only use the personal information about you for the purposes we have described in this article. We process the information confidentially and in accordance with the privacy regulations. In addition to the team itself, information will be visible to the thesis examiner at Aalborg University.

The participants (you who are interviewed) will not be able to be directly recognized in any publication, and all information will only be communicated in a compiled and anonymized form represented in a thesis which may be published at a later date. This guarantee is not only limited to this thesis, but a guarantee to any future re-published papers or references for the entire life period of the paper.

c

What happens with your personal data when the Thesis is finished
The information will be anonymized when the thesis ends, which is planned to be End of June 2025. Personal information, such as contact data (if collected), is only kept for as long as the thesis takes place, with the aim of being able to contact you again to correct any misunderstandings in minutes, and deleted by the thesis's end.

Your rights
If you can be identified in the data material, then you have the right to:

- Access the information which is registered about you, and get delivered a copy of said information,
- Be able to change information regarding yourself,
- Be able to delete information regarding yourself, and;
- Be able to send complaints to the Danish Data Protection Agency "Datatilsynet" about the use of your personal information.

What gives us the rights to work with your personal data
We treat your personal information based on your consent.

Where can I ask more questions
If you have questions regarding the studies, or wish to make use of your rights, please contact:

- Jacob Sylvest Krab-Johansen, Team leader, E-mail: bf44ro@Student.aau.dk
- Data Protection Officer at Aalborg University, E-mail: dpo@aau.dk
- Lene Tolstrup Sørensen, Supervisor at Aalborg University, E-mail: ls@es.aau.dk

Kind regards

Lene Tolstrup Sørensen
Supervisor/professor

Jacob Sylvest Krab-Johansen
Team leader

Declaration of consent

I have received and understood the information about the thesis is conducted by an Aalborg University student team, and have been given the opportunity to ask questions about said thesis. I agree to:

- participating in an interview
- the team working with the information I provide

(Signed by thesis participant - You who is being interviewed)

Appendix B

Interview Drafts

Table B.1: Final Interview Questions for implementers

Q#	Interview Question
1	Can you briefly introduce yourself, your role, responsibilities, and how long you've been with the company?
2	What industry does your company operate in, and how large is it in terms of employees?
3	Does your company fall under NIS2, and if so, which sector are you allocated to? How do you generally assess your cybersecurity strategy (risk-based, compliance-driven, or a mixture)?
4	When did you first become aware of NIS2, and how did it compare to your initial expectations?
5	What prompted your organization to start implementing NIS2, and how would you describe your current level of compliance (fully compliant, in progress, not started)?
6	Have you conducted a business impact or gap analysis regarding NIS2 requirements, and what internal or external resources have you relied on for guidance?
7	Has NIS2 affected your business significantly? Have your compliance efforts led to tangible security improvements, or has the focus been primarily on meeting regulatory requirements?
8	What major challenges have you encountered in implementing NIS2 (e.g., financial costs, expertise gaps, operational complexity, internal resistance)?
9	Do you see NIS2 as a growth driver, or is it mainly a regulatory requirement? Have you identified a minimum viable compliance level to balance cost and compliance?
10	If you could change anything about NIS2, what would it be?

Appendix C

Model Iterations

Figure C.1: First draft of coded interviews in general

f

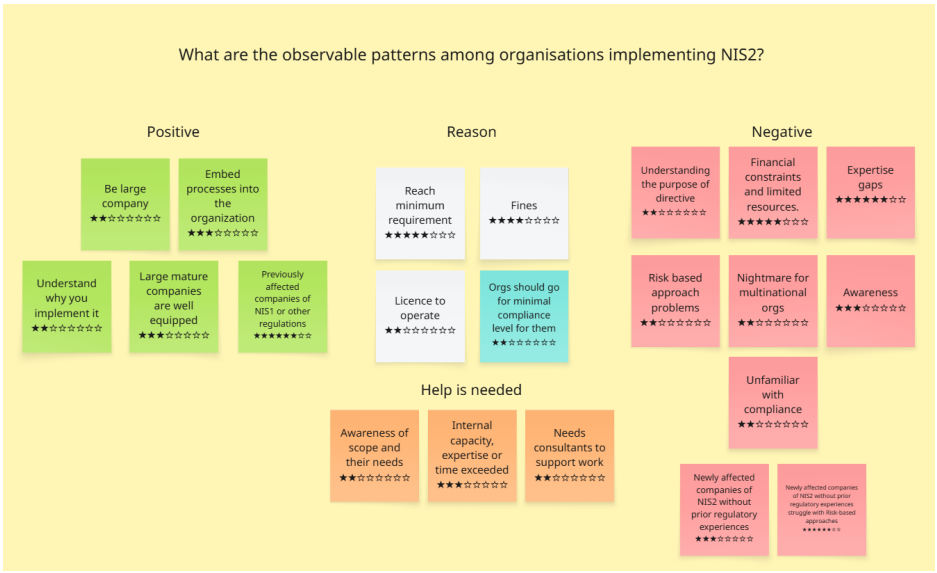


Figure C.2: First draft of coded interviews for RQ1

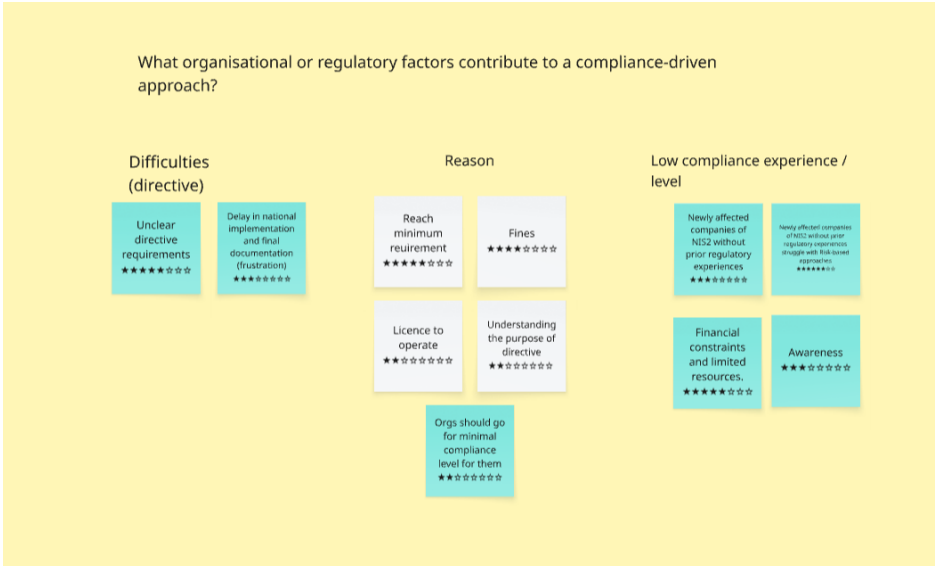


Figure C.3: First draft of coded interviews for RQ2

g

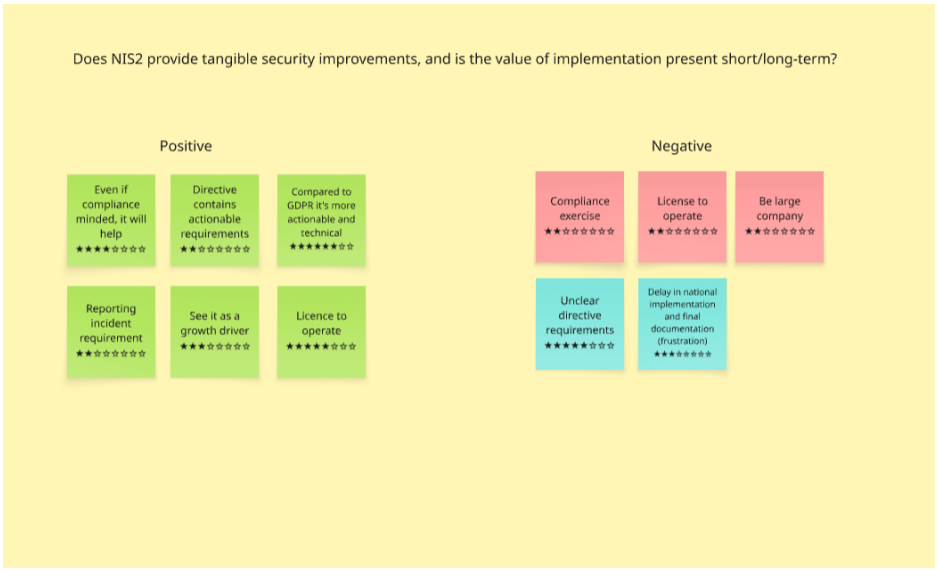


Figure C.4: First draft of coded interviews for RQ3

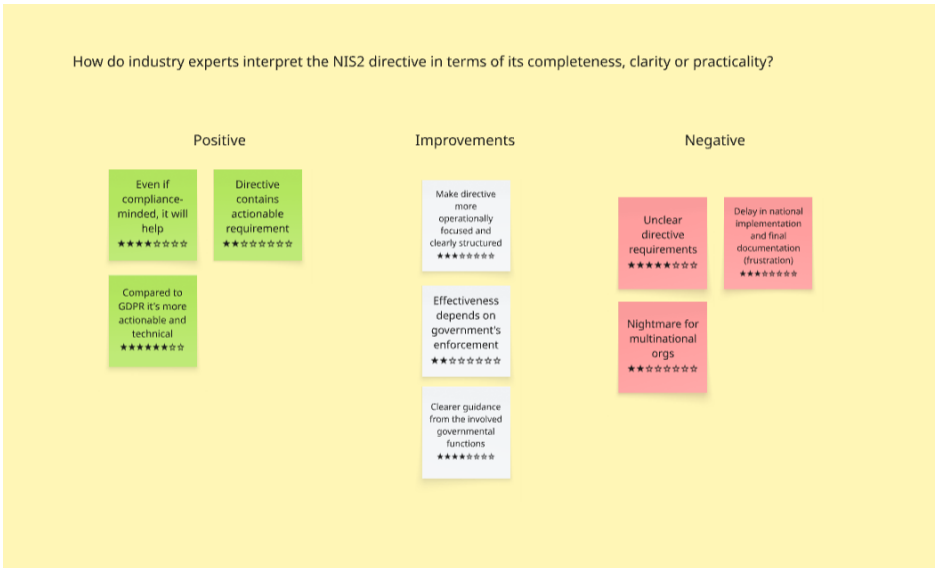


Figure C.5: First draft of coded interviews for RQ4

Appendix D

Supplementary Transposition Research

This appendix presents supplementary research on the national transposition of the NIS2 Directive across EU Member States. It outlines differences in scope, enforcement, and timelines to provide context for the findings discussed in the main study.

Divergent paths: A supplementary analysis of NIS2 transposition across EU Member States

Executive summary

The NIS2 Directive (Directive (EU) 2022/2555) marks a pivotal advancement in the European Union's cybersecurity legislative framework, building on its 2016 predecessor. Its fundamental aim is to establish a high common level of cybersecurity throughout the Union by broadening its scope to include a wider range of sectors and entities with the introduction of more rigid security and reporting obligations, to enhance cross-border collaborations, and to impose more substantial penalties for non-compliance. This comprehensive approach is designed to strengthen cyber resilience, standardize cybersecurity practices, and improve the EU's collective readiness against an ever-evolving landscape of threats.

Despite these clear objectives and the mandated transposition of Oct. 17-2024, the process of NIS2 integration into national law has presented significant unevenness across the 27 EU Member States. As of December 2024, two months after the transposition deadline, only four countries have successfully managed to transpose the directive, which has led to widespread infraction proceedings initiated by the European Commission against the remaining Member States.[2] Beyond mere delays, considerable variations are evident in how individual Member States interpret and implement key provisions.[2] These divergencies are visible in the scope of regulated entities, the specific cybersecurity measures imposed, the structure of supervisory bodies, and the mechanisms chosen for enforcement.[4]

This divergence poses significant obstacles to the broader aims of NIS2 it enables regulatory arbitrage, allowing companies to favour jurisdictions with more lenient compliance demands, which may weaken the directive's ambition to establish a uniform and robust level of cybersecurity across the EU.[2] For organizations operating in several Member States, this fragmentation creates added complexity and heightens compliance requirements, making it more difficult to implement coherent risk management and incident response strategies.[5] Ultimately, such inconsistencies threaten to create vulnerabilities within the Union's shared defence, undermining the resilience NIS2 had intended to enhance.[9]

Introduction: The NIS2 Directive and the transposition imperative

The NIS2 Directive represents a central element of the European Union's cybersecurity strategy, developed to overcome the shortcomings of the precedent directive and to respond to a cyber threat landscape that is growing in both scale and complexity.[1] At its core, the directive seeks to strengthen cyber resilience, promote more effective collaboration and information exchange, and bring greater consistency to cybersecurity measures across Member States. It notably extends its scope to include a wider set of sectors and entities, moving past the initial focus on national critical infrastructure. The updated framework now covers a broader group of "essential" and "important" entities, such as those operating in healthcare, digital services, manufacturing, and public administration. This shift reflects a recognition of the deep interdependencies in today's economies, where a single cyber incident in one area can have widespread ripple effects across multiple sectors, making a more expansive regulatory approach both necessary and justified.[1]

A key feature of EU law, and essential to understanding the current state of NIS2 implementation, is the distinction between a directive and a regulation. Unlike EU regulations, which apply directly and uniformly across all Member States, directives such as NIS2 require each country to transpose the provisions into national legislation.[2] This process typically involves the drafting of new national legislation, often followed by public consultations, subsequent revisions based on feedback, and eventual parliamentary approval.[2] While this approach allows Member States to account for national legal traditions and contextual nuances, it also introduces considerable variation in how the directive's objectives are carried out in practice.[8] This structural element of directives creates a persistent

tension between the EU's aim of harmonization and the preservation of national legislative autonomy. The divergence seen in NIS2's implementation is therefore not solely the result of state-level shortcomings but also reflect the inherent flexibility of the directive as a legal instrument. This underlying dynamic creates a fundamental challenge for achieving a truly uniform and "high common level" of cybersecurity across the Union. Such a tension may also suggest that future EU cybersecurity legislation could increasingly favour regulations to enforce greater uniformity, as some observers have expressed a preference for directly applicable regulations over directives that allow for national options and discretions.[8]

The deadline for Member States to adopt and publish the necessary measures to comply with NIS2 was set for Oct. 17, 2024, with those measures coming into effect on Oct. 18, 2024. This date carried significant weight, serving as a crucial point of coordination for strengthening cybersecurity across the Union in a timely and harmonized manner. It established a clear reference for national legislative efforts and was intended to promote alignment in implementation across Member States.

Evidence of divergence in transposition

The hypothesis that Member States have taken markedly different approaches to the transposition of NIS2 is well supported by evidence across several critical areas. These include the timing of national legislative processes, tremendous differences in how the directive's provisions are understood and incorporated, and uneven approaches to oversight and enforcement structures.

A. Timeliness of transposition

The most immediate and measurable indication of divergence is found in the widespread failure of Member States to meet the required transposition deadline. By December 2024, only four of the 27 EU Member States had successfully managed to incorporate the directive into national law within the prescribed period. This broad shortfall reflects a significant obstacle to meeting the Oct. 17, 2024, deadline. In response, the European Commission launched infraction proceedings against 23 Member states on Nov. 28, 2024. By early May 2025, reasoned opinions had been issued to 19 of these states for not fully notifying their transposition.[15] These formal notices provide a two-month period for corrective action. If the Member States fail to comply, their cases may be brought before the Court if Justice of the European Union, potentially leading to financial sanctions.

The extent of these delays reflects more than procedural complexity. It points to deeper differences in national administrative capacity, legislative efficiency, and the political prioritization of cybersecurity. While the democratic process of passing new legislation, including executive drafting, public consultation, iterative revisions, and parliamentary approval, is by nature time-intensive[2], the fact that only a small number of Member States met the deadline highlights significant variation in their ability to respond swiftly to new regulatory demands. In some cases, such as France and Germany, efforts to align NIS2 with other directives in a single legislative package introduced further complications, requiring more extensive consultation and review.[2] Though this strategy may offer long-term efficiency, it has contributed to immediate delays. Delays in transposing directives are not an isolated phenomenon for NIS2; in 2023, the average delay in transposing EU directives reached an all-time high of 18.3 months.[2] This broader pattern indicates a structural challenge in implementing EU legislation, suggesting that NIS2's transposition difficulties are symptomatic of a larger issue. The inconsistent ability to meet transposition deadlines reveals that the EU's goal of a "high common level" of cybersecurity is constrained not only by legal interpretation but also by divergent institutional capacities and political will among Member States.

The following table illustrates the varied transposition status across Member States, highlighting the significant delays and legal actions taken by the European Commission:

k

Table 1: NIS2 Transposition status by Member State (as of December 2024 / May 2025)

Member State	Transposition Status (Latest Info)	Notes on Specific Variations/Actions
Austria	Reasoned Opinion Issued (May 2025) [15]	Transposing Directive's text as originally drafted for Article 28.[2]
Belgium	Transposed by Deadline (Dec 2024) [2]	Goes beyond Directive terms for Article 28 [2]; closely aligns national law with minor adaptations.[6]
Bulgaria	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]
Croatia	Transposed by Deadline (Dec 2024) [2]	Included additional sectors; detailed entity categorization.[6]
Cyprus	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]
Czechia	Reasoned Opinion Issued (May 2025) [15]	Goes beyond Directive terms for Article 28 [2]; public consultation held.[2]
Denmark	Reasoned Opinion Issued (May 2025) [15]	
Estonia	Reasoned Opinion Issued (May 2025) [15]	
Finland	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]
France	Reasoned Opinion Issued (May 2025) [15]	Drafted new law transposing NIS2 and other directives simultaneously; faces delays due to political instability.[2] Public consultation held.[2]
Germany	Reasoned Opinion Issued (May 2025) [15]	Drafted new law transposing NIS2 and other directives simultaneously; coherent but incomplete framework.[2] Enforcement expected 2025.[16] Public consultation held.[2]

Greece	Infraction Proceedings (Nov 2024)	Public consultation held.[2]
Hungary	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]
Ireland	Reasoned Opinion Issued (May 2025) [15]	
Italy	Transposed by Deadline (Dec 2024) [2]	Transposing Directive's text as originally drafted for Article 28.[2]
Latvia	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]
Lithuania	Transposed by Deadline (Dec 2024) [2]	Public consultation held.[2]
Luxembourg	Reasoned Opinion Issued (May 2025) [15]	
Malta	Infraction Proceedings (Nov 2024)	Public consultation held.[2]
Netherlands	Reasoned Opinion Issued (May 2025) [15]	Transposing Directive's text as originally drafted for Article 28.[2] Public consultation held.[2]
Poland	Reasoned Opinion Issued (May 2025) [15]	Revised initial draft; faces challenges with institutional fragmentation and unclear enforcement.[4] Public consultation held.[2]
Portugal	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]
Romania	Infraction Proceedings (Nov 2024)	Public consultation held.[2]
Slovakia	Infraction Proceedings (Nov 2024)	Public consultation held.[2]
Slovenia	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]

m

Spain	Reasoned Opinion Issued (May 2025) [15]	
Sweden	Reasoned Opinion Issued (May 2025) [15]	Public consultation held.[2]

B. substantial variations in national implementation

Beyond the issue of timelines, the manner in which Member States are implementing NIS2 reveals notable substantial differences that contributes to a fragmented regulatory environment. The directive expands its scope to cover "essential" and "important" entities across 18 sectors: an increase from the original version. However, there is a clear "inconsistency among Member States in how they scope and classify entities".[5] This lack of alignment creates uncertainty and potential compliance challenges for organizations operating in multiple jurisdictions, as the obligations they face may vary depending on national interpretation.[5] For instance, Croatia has chosen to include sectors beyond those required by the directive.[6] Although NIS2 primarily targets large organizations, it can also apply to medium-sized and, in some cases, smaller entities, depending on the critical nature of their services as well as the organization's monetary revenue.[9] Divergencies in how Member States define size thresholds or determine sectoral relevance can result in entities being in scope in some countries while not in others, which further complicates efforts to establish a coherent EU-wide cybersecurity standard.[3]

Clear differences are also evident in how specific provisions are being implemented. Article 28, which requires domain name registers and related entities to verify and publish registration data in a manner consistent with GDPR, provides a clear example.[2] Some Member States, including Austria, Italy, and the Netherlands, appear to be incorporating the directive's wording directly into national law. Others, such as Belgium and the Czech Republic, are going beyond the directive's original language, while some countries have yet to incorporate the provision in their transposition efforts.[2] Article 28(6), intended to minimize redundant data collection within the DNS industry, remains partially contested. Its broader implications and financial impact are still uncertain, and the interpretation of this clause continues to generate debate.[2]

National transposition strategies also differ in terms of regulatory strictness. Some Member States have chosen a "more strict implementation" which raises compliance costs for organizations operating within their jurisdiction. Others have opted for a "less strict implementation", seeking to reduce the burden of affected entities.[8] For instance, Belgium, has largely mirrored the text of the directive in its national NIS2 legislation, introducing only limited national modifications.[6] By contrast, Croatia, has adopted a broader approach, expanding the list of covered sectors and introducing a more granular classification of entities within its national law.[6]

A comparative legal analysis of France, Germany, and Poland, commonly referred to as the Weimar triangle, highlights the "considerable divergencies in the timing and structure of implementation".[4] France, operating under a centralized administrative system, has proposed a "broad regulatory scope" that notably includes local authorities. Its implementation, however, has been delayed, in part due to political instability.[4] Germany, drawing in its own federal structure and the central role of the BSI (Bundesamt für Sicherheit in der Informationstechnik), has put forward a "coherent though still incomplete framework"[4], with the expectancy of enforcement in 2025.[16] Poland revised its initial legislative proposal after receiving stakeholder criticism but continues to face challenges stemming from institutional fragmentation and limited clarity around enforcement structures.[4] These national differences are not incidental. They are "largely shaped by governance models, historical cybersecurity policies, and institutional preparedness". [4]

The combined effect of these divergent national interpretations has resulted in a "patchwork of local

requirements" rather than the uniform regulatory environment envisioned by the directive.[5] This fragmentation significantly increases complexity for businesses, which must navigate differing standards and compliance obligations across Member States, ultimately weakening the directive's aim for a coherent EU-wide cybersecurity framework.[5] The pursuit of a "high common level of cybersecurity"[15] is fundamentally compromised when the results and their enforcement differ so remarkably from one jurisdiction to another. This environment leads to regulatory arbitrage, allowing companies to base or expand operations in countries with less demanding implementations, placing more rigorous Member States at a competitive disadvantage. In turn, this undermines the principle of fair competition within the single market and risks lowering cybersecurity standards, as some countries may feel compelled to ease compliance requirements to attract business. These variations are not incidental or technical; they reflect well-established national administrative practices and political choices. As a result, achieving meaningful harmonization will require more than shared legislative language. It will depend on addressing the deeper structural and historical differences that shape how laws are applied. This reality suggests that future EU cybersecurity measures may need to be more prescriptive in nature, or potentially take the form of directly applicable regulations, to ensure a consistent and effective implementation across the Union.

The following table provides a comparative overview of key NIS2 implementation divergences across selected Member States, illustrating the qualitative differences in their approaches:

Table 2: Comparative overview of key NIS2 implementation divergences (Selected Member States)

Key Aspect of Implementation	France	Germany	Poland	Belgium	Czech Republic	Croatia	Netherlands	Austria	Italy
Regulatory Scope	Extensive, includes local authorities [4]	Coherent, but still incomplete framework [4]	Scope challenges due to institutional fragmentation [4]	Closely aligns with EU Directive, minor adaptations [6]	Goes beyond Directive terms for Article 28 [2]	Includes additional sectors beyond NIS2 minimum [6]	Transposing Directive's text as originally drafted for Article 28 [2]	Transposing Directive's text as originally drafted for Article 28 [2]	Transposing Directive's text as originally drafted for Article 28 [2]
Supervisory Body Structure	Centralized administrative model [4]	Leverages federal expertise, centralized BSI [4]	Institutional fragmentation, unclear enforcement [4]	Designates national authorities [6]	Designates national authorities [6]	Designates national authorities [6]	Designates national authorities [6]	Designates national authorities [6]	Designates national authorities [6]

o

Enforcement Focus/Clarity	Delays due to political instability [4]	Enforcement expected 2025 [16]	Lack of clarity in enforcement [4]	Clear enforcement in national law [6]	Clear enforcement in national law [6]	Clear enforcement in national law [6]	Clear enforcement in national law [6]	Clear enforcement in national law [6]	Clear enforcement in national law [6]
Incident Reporting Nuances	Subject to general delays [4]	Subject to general delays [4]	Challenges with clarity [4]	Aligns with EU directive [6]	Goes beyond Directive terms for Article 28 [2]	Defined timelines [6]	Aligns with EU directive [2]	Aligns with EU directive [2]	Aligns with EU directive [2]
Overall Approach	Extensive regulatory scope, political delays [4]	Coherent but incomplete framework [4]	Legislative revisions, institutional challenges [4]	Minor national adaptations [6]	More stringent implementation [2]	More strict implementation, additional sectors [6]	Transposing as drafted [2]	Transposing as drafted [2]	Transposing as drafted [2]

C. Disparities in supervisory and enforcement mechanisms

The implementation of NIS2 also reveals notable differences in how supervisory and enforcement functions are structured across Member States. Although all EU countries are required to designate a National Competent Authority (NCA) to observe and enforce the directive locally, these bodies are also expected to coordinate at the EU level through mechanisms such as ENISA and the Cooperation Group.[7] National legislation further defines the specific roles and responsibilities of these authorities, including whether oversight is distributed based on sectoral expertise.[6] Supervision generally includes a combination of methods, such as on-site inspections, external monitoring, and formal security assessments. [17] Essential entities are typically subject to proactive oversight, involving regular audits, random inspections, and on-site checks. In contrast, important entities are more often monitored reactively, with supervisory actions initiated in response to signs of non-compliance.[17]

NIS was intended to bring greater consistency and efficiency to incident reporting by requiring organizations to report “significant incidents” to national authorities within defined timeframes. The directive establishes a structured, three-step reporting process: an early warning within 24 hours of detection, an initial notification with preliminary assessment within 72 hours, and a final report within one month outlining the incident and the mitigation measures taken. However, in practice, “each Member State maintains its own regulators, reporting portals, and sector-specific requirements”.[5] This fragmented system introduces the risk of “duplicate or even conflicting reporting obligations,” particularly in cross-border contexts.[5] This situation illustrates a clear paradox. Although the directive sets out a

framework for harmonized penalties, enforcement remains highly fragmented. While the theoretical maximum fines are consistent across the Union, the actual application of penalties, along with the triggers for enforcement and the practical accessibility of reporting channels, differs considerably between Member States. These variations affect both the predictability and the effectiveness of the enforcement regime.

NIS2 also establishes a unified penalty framework that clearly distinguishes between essential and important entities[9]. For essential entities, fines may reach up to €10 million or 2% of global annual turnover, whichever is higher. Important entities face a lower threshold, with penalties capped at €7 million or 1.4% of global turnover. In addition to financial sanctions, the directive allows for non-monetary measures such as compliance orders, mandatory security audits, and, in serious cases, criminal sanctions. These may include personal liability for senior management and temporary disqualification from holding managerial positions in the event of repeated violations. While NIS2 defines minimum penalty levels, "specific fines will vary depending on the Member State,"[19] allowing for higher or the introduction of additional national conditions. As a result, the real "cost of non-compliance" differs significantly across the Union. This variation contributes to regulatory arbitrage, as companies may view the risk of detection or enforcement as lower in some jurisdictions, regardless of the uniformity in maximum penalties. It also creates complications for cross-border incident handling, where a single event affecting multiple countries could lead to different reporting obligations and enforcement responses from national authorities.

Implications of divergent transposition

The dramatic divergences in NIS2 transposition across EU Member States carry significant implications, affecting market dynamics, corporate compliance strategies, and the overall cybersecurity posture of the Union.

A. Regulatory arbitrage and forum shopping

The inconsistencies in how NIS2 is applied across Member States give rise to clear opportunities for "regulatory arbitrage". This allows multinational companies to engage in "regulatory shopping", Choosing to establish operations in jurisdictions where compliance is viewed as less costly or less tightly enforced.[2] This behaviour stems directly from the uneven transposition of the directive.

The consequences for a fair competition and the coherence of the single market are substantial. Member States that delay implementation or adopt a more lenient approach may unintentionally provide a "higher return of equity for forms. Just because the cost for compliance is lower". This places other Member States, those committing to more comprehensive and rigorous implementation, at a competitive disadvantage by increasing the regulatory burden on their local companies. The result is a distortion of the single market and a risk that some regions may gradually lower their cybersecurity standards to remain attractive to businesses. This undermines the directive's central aim of enhancing the Union's overall cybersecurity posture.

B. Increased complexity for multi-jurisdictional Organizations

For organizations operating across multiple EU Member States, the current regulatory landscape presents a significant challenge. Rather than dealing with a coherent and uniform framework, they are confronted with a "patchwork of local requirements".[5] This fragmentation adds considerable complexity to compliance efforts, requiring businesses to adapt their internal policies, procedures, and reporting mechanisms to align with the specific standards and interpretations adopted by each national authority.[5]

This lack of standardization directly impedes the ability to streamline critical processes such as incident response and risk management, thereby increasing the risk of errors or delays.[5] For instance, a single cyber incident affecting operations across several countries can trigger "duplicate or even conflicting obligations" due to the varied national regulators and reporting portals in place.[5] Furthermore, organizations encounter challenges in establishing management body accountability, as the

definition of "management body" under NIS2 remains vague in both scope and implications.[5] This uncertainty requires tailored legal interpretation within each member state, particularly because national frameworks demand accountability from a designated legal representative who can be held personally liable. As a result, the overall "cost of compliance" for companies extends beyond direct financial expenses to include operational inefficiencies and greater exposure to risk. This encompasses the burden of managing multiple, and at times conflicting, compliance systems, a higher risk of human error from non-standardized procedures, and the disadvantage of lacking a unified cybersecurity approach across the EU. It is essential to recognize this broader notion of "cost" for both businesses and policymakers, as it demonstrates that even if an organization avoids financial penalties through regulatory arbitrage, it still faces substantial non-monetary costs originating from operational strain and increased cybersecurity vulnerabilities.

C. Compromising the goal of a high common level of cybersecurity

The inconsistent interpretation and implementation of the original NIS2 Directive had already led to "disparate security levels between EU Member States", which weakened its overall impact.[9] NIS2 was introduced to address these deficiencies and to promote a more cohesive and resilient cybersecurity posture.[9] Yet, the ongoing divergence in national transposition threatens to sustain these "weak links"[10] within the Union's digital infrastructure. This continued fragmentation leaves the EU exposed to advanced cyber threats that target the most vulnerable entry points, ultimately placing the collective security of the bloc at risk.

Ultimately, the Directive's aim of strengthening the EU's capacity to respond to cyberattacks[1] is seriously undermined when national implementation differs significantly. In a fragmented landscape, the coordination needed for timely and effective cross-border responses becomes far more difficult, which can delay essential measures and worsen the effects of cyber incidents throughout the Union.

Contributing factors to transposition differences

The divergencies observed in the transposition of NIS2 cannot be traced to a single cause. Instead, they arise from a combination of interrelated factors that reflect the varying institutional, legal, and political contexts across Member States.

A primary cause of substantial divergence lies in the national governance traditions and historical approaches to cybersecurity. As shown in the comparative analysis of the Weimar Triangle countries (France, Germany, and Poland), a country's administrative structure, whether centralized or federal, and its past engagement with cybersecurity play a major role in shaping its transposition strategy.[4] For instance, France's centralized system has led to a proposed broad regulatory scope, whereas Germany's federal experience has contributed to a coherent, though still incomplete, framework. Poland, on the other hand, continues to face institutional fragmentation and uncertainty around enforcement, reflecting its distinct history with cybersecurity governance.[4] These variations make clear indications that transposition is not merely a technical process. It is closely tied to each country's administrative and political traditions, as well as its historical approach to institutionalising and regulating cybersecurity.

Another key factor is the institutional readiness and capacity for individual Member States. The European Unios comprises countries with "varied maturity and capability levels" across its Member States when it comes to cybersecurity preparedness.[20] Some are considered "role-modelling" states, while others are still "advancing" or "establishing" their capabilities.[20] These differences have a direct effect on how efficiently and thoroughly a Member State can transpose and implement complex legislation such as NIS2.[20] A directive aiming to establish a "common level" must operate within a landscape of uneven starting conditions, where some national authorities may lack the necessary resources, expertise, or administrative structures to develop and pass detailed legislative measures in a timely manner.

The integration of NIS2 with existing national laws and other EU Directives add another layer of

complexity to its transposition. NIS2 does not operate within a vacuum; It must interact with established national cybersecurity frameworks as well as other EU legislation. A noteworthy example of this is the Digital Operational Resilience Act (DORA), which is specifically aimed at the financial sector. For financial entities that fall under the scope of both NIS2 and DORA, careful alignment is essential to prevent duplication or conflict, which in turn would complicate the national transposition efforts.[1] The recurring challenge of "integrating multiple compliance requirements" appears across various sectors and Member States, further intensifying the legislative process.[3]

Additionally, the uneven levels of cybersecurity maturity across sectors and within individual Member States pose distinct implementation challenges. ENISA's NIS360 report points to significant differences in maturity among sectors.[21, 22] Industries such as electricity, telecommunications, and banking tend to be more advanced, due to prior regulatory attention and sustained investment. In contrast, sectors like healthcare, space, and public administration often face specific difficulties, including dependence on outdated systems, complex supply chains, or limited awareness of cybersecurity issues.[21,22] This sectoral disparity means that national authorities must account for varying degrees of preparedness and capacity when applying NIS2 across their national industries.[3] These divergencies show that a "one-size-fits-all" approach is difficult to apply in practice. The issue extends beyond legal interpretation to include fundamental variations in national infrastructure and institutional capabilities.

Finally, ambiguity in the legal terminology of the directive itself contributes to divergent national interpretations. Terms like "management body" remain unclear in both scope and implication under NIS2.[5] This lack of clarity requires legal interpretation within each Member State, leading to different approaches to defining accountability and determining who holds liability within an organization. As a result, the effort to establish a unified compliance framework becomes more complex and fragmented.

Efforts of harmonization and outlook

Considering the challenges caused by divergent transposition, the European Commission and ENISA are taking active steps to support implementation and encourage closer cooperation among Member States.

The European Commission holds a central role in overseeing the transposition process, launching infraction proceedings against Member States that fail to meet the directive's requirements and deadlines. This enforcement mechanism is intended to compel compliance and showcases the commission's commitment to ensuring full implementation of NIS2. However, the number of Member States subject to these proceedings, 23 initially, followed by 19 reasoned opinions, illustrates the structural limitations of directives an achieving swift and consistent compliance across the Union. While such proceedings are an essential instrument for enforcement, they also demonstrate that directives are not automatically effective and rely heavily on national initiative, which varies significantly among Member States. This reflects a largely reactive approach toward harmonization. Although most Member States are expected to eventually complete the transposition process[2], the initial delays and inconsistencies contribute to a period of fragmented cybersecurity capabilities across the EU.

ENISA (European Union Agency for Cybersecurity) plays a key role in supporting the implementation of NIS2 by offering technical expertise, strategic guidance, and in-depth reports such as the NIS360.[7] The agency aims to help national authorities gain a clearer understanding of the cybersecurity landscape, set priorities, identify critical gaps, and track progress effectively.[21] ENISA places strong emphasis on enhancing collaboration both within individual sectors and across different sectors, promoting the development of tailored, sector-specific guidance, and encouraging greater alignment of cybersecurity requirements across borders.[21] It also works closely with national Computer Security Incident Response Teams (CSIRTs) and the cooperation Group to support coordinated, cross-border responses to cyber threats.[7]

To navigate the fragmented landscape, clear recommendations for both national authorities and organizations are essential. For national authorities, it

is critical to enhance cooperation, create sector-specific guidance that reflects the particular challenges of different industries, ensure consistency of requirements across borders, and offer targeted assistance to less mature sectors or entities.[3] Tackling institutional fragmentation and clarifying enforcement frameworks, especially in countries such as Poland, is also necessary for effective implementation.[4] For organizations, compliance requires thorough risk assessments, the development of comprehensive ICT risk management plans, and clearly defined procedures for incident reporting. Ongoing resilience testing, regular updates to cybersecurity protocols, and continuous employee training are equally important.[1] Emphasizing strong governance and accountability is vital, particularly through training for management bodies and raising awareness of personal liability. In addition, securing the supply chain by carefully evaluating third-party partners is a key component of NIS2 compliance.

Looking forward, although many Member States failed to meet the initial deadline, it is expected that most will complete the transposition of NIS2 by Oct. 2025, supported by the continued pressure of the European Commission's infringement proceedings.[2] The broader legislative trend within the EU indicates a growing preference for directly applicable regulations rather than directives, reflecting a possible shift in strategy aimed at reducing persistent inconsistencies in national implementation.[8] Ongoing contributions from ENISA and the cooperation Group will be crucial in promoting practical harmonization and addressing remaining challenges, especially in areas that demand coordinated cross-border oversight and information sharing. [7] These sustained collaborative efforts are essential for advancing towards a genuinely high and consistent level of cybersecurity across the EU's diverse Member States.

t

To conclude

The findings clearly support the hypothesis that the transposition of the NIS2 Directive has varied significantly across EU Member States. This divergence is demonstrated by the broad failure to meet the Oct. 2024 deadline, substantial differences in how national legislation interprets and incorporates the directive's provisions[2], and noticeable inconsistencies in supervisory and enforcement structures. [9]

These significant implications include the rise of regulatory arbitrage, where companies may gravitate toward jurisdictions with more lenient compliance demands, weakening the directive's goal of establishing a unified cybersecurity standard. Multi-jurisdictional entities also encounter greater compliance burdens, as they must navigate a "patchwork" of differing national requirements[5], making it more difficult to streamline vital processes such as incident response and risk management.[5] in the end, this level of fragmentation threatens to create "weak links"[10] in the EU's collective cybersecurity posture, placing the Union's overall resilience at risk in the face of increasingly sophisticated cyber threats.

These divergencies arise from a combination of factors, including the structural flexibility built into directives as a legal instrument[2], long-standing national governance traditions[4], differing levels of institutional capacity across Member States[20], and uneven cybersecurity maturity among sectors.[3] Although EU enforcement tools like the European Commission's infraction proceedings act as corrective measures, they also underscore the challenges directives face in securing timely and consistent compliance across the Union.

Despite these challenges, the continued efforts of the European Union and ENISA remain essential in supporting and coordinating implementation.[7] Ongoing attention and adaptability from both national authorities and organizations are vital to address the current fragmentation and to achieve the Directive's broader objective of building a genuinely high common level of cybersecurity across the Union.

Cited work

1. *Staying compliant with NIS2 regulation*: *Key insights - Moody's,* https://www.moodys.com/web/en/us/kyc/resources/insights/understanding-the-nis2-regulation-staying-compliant-key-insights.html
2. *Trends in the Transposition Journey of Art 28 of NIS2* https://dnsrf.org/blog/trends-in-the-transposition-journey-of-art-28-of-nis2/index.html
3. *Nis2 implementation: challenges & priorities - European Cyber Security Organisation* https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf
4. *Analysis of the implementation of the NIS2 directive in the Weimar ...* https://journals.economic-research.pl/ceref/article/view/3677
5. *NIS2 update - KPMG International* https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/services/nis2-update.pdf
6. *NIS2 & national implementation: which local NIS2 laws are available in Cyberday?* https://www.cyberday.ai/blog/nis2-national-implementation-which-local-nis2-laws-are-available-in-cyberday
7. *Understanding NIS2: supervision and penalties of non-compliance* https://www.cyberday.ai/blog/understanding-nis2-supervision-and-penalties-of-non-compliance
8. *The NIS 2 Directive* https://www.nis-2-directive.com/NIS_2_Directive_Transposition.html
9. *NIS vs. NIS 2: What's changed and what you should know* https://www.vanta.com/resources/nis-2-changes
10. *NIS vs NIS2: Key Differences Explained for EU Cybersecurity Compliance (part 1) – Indevlab* https://indevlab.com/blog/nis-vs-nis2-key-differences-explained-for-eu-cybersecurity-compliance-part-1/
11. *The NIS 2 Directive Guide: New Rules, Compliance Needs, and Strategic Implications* https://complianceandethics.org/the-nis-2-directive-guide-new-rules-compliance-needs-and-strategic-implications/
12. *What Is NIS2 (Network and Information Security Directive)?* https://sosafe-awareness.com/glossary/nis2/
13. NIS2: Requirements, Penalties & Implementation - Docusnap, tilgået maj 22, 2025, https://www.docusnap.com/en/it-documentation/nis2
14. Accessed
15. *Commission calls on 19 Member states to fully transpose the NIS2 ...* https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive
16. *NIS2 Compliance: Key Requirements & How to Prepare* https://www.dataguard.com/nis2/
17. *NIS2: A Roadmap to Compliance | Cyber and Data Resilliance – Kroll* https://www.kroll.com/en/insights/publications/cyber/nis2-roadmap-to-compliance
18. *Understanding NIS2: The New EU Cybersecurity Directive* https://www.deloitte.com/fi/fi/services/consulting-risk/blogs/Understanding-NIS2-Directive-The-New-EU-Cybersecurity-Directive.html
19. *NIS2 Fines & Consequences | Huge Penalties for Violations* https://nis2directive.eu/nis2-fines/
20. *ENISA: Fit for Purpose? -* https://www.interface-eu.org/publications/enisa-fit-for-purpose
21. *ENISA's NIS360 report guides NIS2 Directive implementation, maps sectoral maturity, flags cybersecurity challenges* https://industrialcyber.co/reports/enisas-nis360-report-guides-nis2-directive-implementation-maps-sectoral-maturity-flags-cybersecurity-challenges/
22. *ENISA NIS360 2024 report: A comprehensive look at cybersecurity maturity and criticality of NIS2 sectors* https://www.enisa.europa.eu/sites/default/files/2025-03/ENISA%20-%20NIS360%20-%202024_0.pdf