

Jade Karrila

**IMPROVING CYBERSECURITY INCIDENT RE-  
SPONSE CAPABILITIES IN THE FINNISH FI-  
NANCIAL SECTOR**  
From Compliance to Resilience

Master of Science Thesis  
Faculty of Management and Business  
Ilona Ilvonen  
Saeid Heshmatisafa  
November 2025

# ABSTRACT

Jade Karrila: Improving Cybersecurity Incident Response Capabilities in the Finnish Financial Sector: From Compliance to Resilience

Master of Science Thesis

Tampere University

Master's Degree Programme in Information and Knowledge Management

November 2025

---

This thesis examines how cybersecurity incident response capabilities can be improved in the Finnish financial sector by analyzing governance, communication, and skills coordination during cyber incidents. The study was motivated by the Nordea 2024 distributed denial-of-service attacks, which revealed challenges in resilience and communication despite the sector's high cybersecurity maturity. The main research question addresses how the Finnish financial sector can improve its incident response capabilities.

The study employs a qualitative, descriptive case study strategy based on a systematic literature review, document analysis, and six expert interviews. The theoretical foundation draws from cybersecurity governance frameworks, including ISO/IEC standards, NIST SP 800-61r3, and the European Cybersecurity Skills Framework.

Findings indicate that while preventative measures are advanced, communication rigidity, fragmented accountability, and limited integration of learning processes hinder agile incident response. The thesis highlights that effective incident response requires continuous learning, adaptive situational awareness, and clear role coordination. The study contributes by contextualizing the ECSF within financial-sector cybersecurity and by offering a novel framework for aligning competencies with governance structures to strengthen organizational resilience.

Keywords: cybersecurity, financial sector, incident response, resilience, governance, European Cybersecurity Skills Framework

The originality of this thesis has been verified using the Turnitin Originality Check service.

# TIIVISTELMÄ

Jade Karrila: Kyberturvallisuuden poikkeamienhallinnan kyvykkyyksien parantaminen Suomen finanssialalla

Diplomityö

Tampereen yliopisto

Tietojohdamisen diplomi-insinöörin tutkinto-ohjelma

Marraskuu 2025

---

Tässä diplomityössä tarkastellaan, miten kyberturvallisuuden poikkeamienhallinnan kyvykkyyksiä voidaan parantaa Suomen finanssialalla. Aihetta tutkitaan analysoimalla hallintoa, viestintää ja osaamisen koordinoitua kyberturvallisuuspoikkeamien aikana. Tutkimuksen taustalla ovat Nordean 2024 pitkittyneet palvelunestohyökkäykset, jotka paljastivat haasteita resilienssissä ja kommunikoinnissa huolimatta alan korkeasta kyberturvallisuuden kypsyydestä. Tutkimuksen päätutkimuskysymys käsittelee sitä, miten Suomen finanssiala voisi parantaa kyvykkyyksiään reagoida kyberturvapoikkeamiin.

Tutkimuksessa käytetään laadullista, kuvailevaa tapaustutkimusstrategiaa, joka perustuu systemaattiseen kirjallisuuskatsaukseen, dokumenttianalyysiin ja kuuteen asiantuntijahaastatteluun. Teoreettinen perusta rakentuu kyberturvallisuuden hallintokehyksiin, mukaan lukien ISO/IEC-standardeihin, NIST SP 800-61-r3 -viitekehykseen ja eurooppalaiseen kyberturvallisuuden osaamiskehykseen.

Tulokset osoittavat, että vaikka ennaltaehkäisevät toimenpiteet ovat edistyneitä, viestinnän jäykkyys, hajanaiset vastuut ja rajoittunut oppimisprosessien integrointi hidastavat ketterää reagointia. Tutkimuksessa korostetaan, että tehokas reagointi vaatii jatkuvaa oppimista, sopeutuvaa tilannetietoisuutta ja selkeää roolien koordinoitua. Tutkimus tuo lisäarvoa kontekstualisoimalla ECSF:n osaksi finanssialan kyberturvallisuutta ja tarjoamalla uudenlaisen kehyksen osaamisen ja hallintorakenteiden yhteensovittamiseksi organisaation resilienssin vahvistamiseksi.

Avainsanat: kyberturvallisuus, finanssiala, poikkeamin hallinta, resilienssi, hallinto, eurooppalainen kyberturvallisuusosaamisen viitekehys

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin Originality Check -ohjelmalla.

# USE OF AI IN THESIS

I have utilised AI tools in my thesis:

- No
- Yes

The AI tools utilised in my thesis and their purposes are described below:

DeepL Write  
Microsoft Copilot  
Scopus AI

Purpose of using AI tools: The use of AI in this thesis followed a predefined plan in the thesis outline. AI was intended to be used ethically and transparently in language enhancement, with the objective of refining academic writing style and ensuring grammatical accuracy.

AI was used to translate empirical document data and interviews from their original languages for direct quotations. Document material in Danish, Norwegian, and Swedish was translated using AI tools to have standardized coding and analysis process. The purpose was also to make the processing of foreign-language material more efficient and improve the accuracy of translation work.

AI translation was not used to translate the names of institutions and actors. Instead, English translations were obtained from official sources, namely the organization's own websites.

In addition, Scopus AI was utilized to identify additional literature review data that complemented the existing dataset. Material found and selected using Scopus AI is marked in the literature review table in Appendix A.

Sections where AI tools were used: Direct quotations appearing in Chapter 7 have been translated using AI tools if their original language was other than English. All translated quotations were checked manually.

I acknowledge that I am fully responsible for the entire content of my thesis, including the parts generated by AI, and accept accountability for any violations of ethical standards in publications.

## **PREFACE**

This thesis was written out of my genuine interest in cybersecurity and its particular relevance within the financial sector, given the sector's high level of digital maturity and the critical role of financial systems in society.

I would like to express my most sincere gratitude to my examiners, Ilona Ilvonen and Saeid Heshmatisafa, whose valuable feedback and support were instrumental throughout the writing of this thesis.

Finally, I am deeply grateful to my family and friends for their thoughtful feedback on my writing, and to the interviewees for generously sharing their time and insights, which significantly contributed to this research.

Tampere, 30 November 2025

Jade Karrila

# CONTENTS

USE OF AI IN THESIS .....	III
1. INTRODUCTION.....	1
1.1 Background and motivation .....	1
1.2 Research questions and objectives .....	3
1.3 Research structure .....	5
2. RESEARCH METHODOLOGY .....	7
2.1 Research design.....	7
2.2 Research strategy .....	9
2.3 Research methodology.....	10
2.4 Time horizon.....	11
2.5 Systematic literature review .....	11
3. CYBERSECURITY IN THE FINANCIAL SECTOR.....	14
3.1 The financial sector as critical infrastructure .....	14
3.2 Cybersecurity threat landscape and challenges.....	16
3.3 Regulatory environment and supervisory guidelines .....	19
4. CYBERSECURITY GOVERNANCE AND FRAMEWORKS .....	24
4.1 Cybersecurity governance models.....	24
4.2 Cybersecurity frameworks and standards.....	26
4.3 European Cybersecurity Skills framework.....	31
5. INCIDENT RESPONSE IN FINANCIAL CYBERSECURITY .....	34
5.1 Principles of incident response .....	34
5.2 Recovery and business continuity in the financial sector .....	39
5.3 Roles, coordination, and governance in incident response .....	42
6. DATA COLLECTION AND ANALYSIS.....	45
6.1 Document data collection.....	45
6.2 Semi-structured interviews.....	48
6.3 Data analysis.....	52
7. EMPIRICAL ANALYSIS RESULTS .....	58
7.1 Document analysis .....	58
7.1.1 Leadership and the role of management.....	58
7.1.2 Significance of communication.....	60
7.1.3 Regulation and responsibilities.....	61
7.1.4 Skills and ECSF roles .....	63
7.1.5 Technological and structural challenges .....	65
7.1.6 Organizational resilience and incident response .....	67
7.2 Results of interviews.....	70
7.2.1 Leadership and role of management.....	71

7.2.2 Significance of communication.....	72
7.2.3 Regulation and responsibilities.....	73
7.2.4 Skills and ECSF roles .....	75
7.2.5 Technological and structural challenges .....	76
7.2.6 Organizational resilience and incident response .....	77
8.DISCUSSION.....	79
8.1 Current state of incident response practices in the Finnish financial sector	
79	
8.2 Comparison with frameworks and best practices .....	80
8.3 The Role of the European Cybersecurity Skills Framework .....	83
8.4 Improving incident response capabilities.....	86
9.CONCLUSION.....	90
9.1 Key findings.....	90
9.2 Evaluation of the study .....	92
9.3 Suggestions for future research.....	93
REFERENCES.....	95
APPENDIX A: LITERATURE REVIEW TABLE.....	1
APPENDIX B: DOCUMENT ANALYSIS DATA.....	1
APPENDIX C: INTERVIEW GUIDE.....	1

## LIST OF ABBREVIATIONS

DDoS Attack	Distributed Denial-of-Service Attack
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECB	European Central Bank
ECSF	European Cybersecurity Skills Framework
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Authority
ESRB	European Systemic Risk Board
FIN-FSA	Finnish Financial Supervisory Authority
NBI	National Bureau of Investigation
NCA	National Competent Authority
NIST-CF	National Institute of Standards and Technology Cybersecurity Framework

# 1. INTRODUCTION

This chapter introduces the research topic, the background and motivation behind the research. The research questions related to this topic and the purpose of the research are discussed, and finally, the thesis structure is presented.

## 1.1 Background and motivation

Cybersecurity in the financial sector is fundamentally different from other industries. The financial sector is part of critical infrastructure, which makes it an attractive target for cyberattacks (Didenko, 2020). For this reason, the industry operates under heavy regulatory oversight from both international and national bodies, which enforce security and resilience measures.

The European financial sector operates under a complex regulatory landscape, with multiple authorities issuing guidance and oversight on cybersecurity. Key actors include the European Banking Authority (EBA), which sets industry-wide guidelines with strict standards and reporting requirements (EBA, 2019), and the European Central Bank (ECB), which oversees cybersecurity testing through frameworks such as TIBER-EU (Threat Intelligence-based Ethical Red Teaming) to strengthen institutions' resilience through simulated attacks (European Central Bank, 2023). Additionally, the European Union Agency for Cybersecurity (ENISA) provides coordination, threat intelligence, and support for implementing EU-wide directives such as DORA (Digital Operational Resilience Act).

Nationally, Finland's cybersecurity landscape in the financial sector is shaped by Traficom's National Cyber Security Centre and Financial Supervisory Authority (FIN-FSA), which guide, assist, and supervise organizations with implementing cybersecurity best practices in the industry. In Finland, the financial sector has previously been reported to be the third most advanced industry in terms of cybersecurity, after telecommunications and ICT and software (Huoltovarmuuskeskus, 2022). However, the pressure on the already targeted industry has grown. Internationally cybersecurity attacks, especially denial-of-service attacks have increased both in size and volume over the past few years (de Neira et al., 2023). National Cybersecurity Centre of Finland has reported that the amount of denial-of-service attacks has grown in Finland, however prolonged attacks disruptive to organizations are still rare (Kyberturvallisuuskeskus, 2024a).

In September 2024, Nordea experienced a prolonged denial-of-service attack, disrupting banking services across multiple regions. Nordea reported that the attack generated up to 15 million service requests per second (Toivonen, 2024). While this is a considerable amount, it is not unprecedented (de Neira et al., 2023). According to Nordea, other major Nordic banks, such as SEB and Swedbank, were also targeted at the same time and this attack was intended to disrupt the entire Nordic finance sector (Malminen, 2024). Notably, the attack coincided with a scheduled maintenance of Nordea's IT systems (Malminen & Kinnunen, 2024), which could raise questions about whether it exploited existing vulnerabilities.

Nordea claimed that this was part of a broader, organized attack targeted toward the entire Nordic financial sector, with indications that a state actor could be involved. Cybersecurity experts have found it exceptional that Nordea itself publicly suggested a possible state-sponsored attack. (Toivonen, 2024) Targets of cybersecurity attacks typically avoid attributing blame without definitive proof. However, it must be noted that Nordea's communication is not entirely impartial, as maintaining customer trust and reputation is crucial for its business. Another unique feature of the case is that Danish news media claimed Nordea had not conducted appropriate disaster recovery testing in decades and still relied on outdated systems and hardware that failed to recover as expected. Nordea denied these claims. (Vento, 2024)

Most cybersecurity guidelines focus on prevention measures instead of reaction and recovery. This is understandable, as it is much harder to mitigate denial-of-service attacks once they are launched (Zargar et al., 2013) and the best way in general to prevent damages is to prevent the attack from happening in the first place (de Neira et al., 2023). In this regularly stress-tested, heavily supervised, and regulated environment, the Nordea incident seems unusual. In theory, it should not have happened. But the question is whether cybersecurity can be designed in a resilient and sustainable way. Cyber resilience refers to the ability to absorb, adapt to, and recover from cyber disruptions while maintaining continuity of critical functions (Dupont, 2019; Petrenko, 2019). It is enabled by governance, preparedness, learning, and organizational culture (Petrenko, 2019). Cybersecurity research deems cybersecurity risks unavoidable (Uddin et al., 2020) and cyber resilience research even aims for cybersecurity as an industry to evolve into resilience where it is able to maintain organizational continuity during cyber events (Björck et al., 2015).

This thesis examines how organizations in the Finnish financial sector could improve their incident response capabilities using Nordea's September 2024 incident as a descriptive case. By analyzing the regulatory environment, best practices, and challenges

faced during an attack, the study aims to contribute to a more resilient cybersecurity approach for Finnish financial institutions utilizing information and knowledge management perspectives and processes.

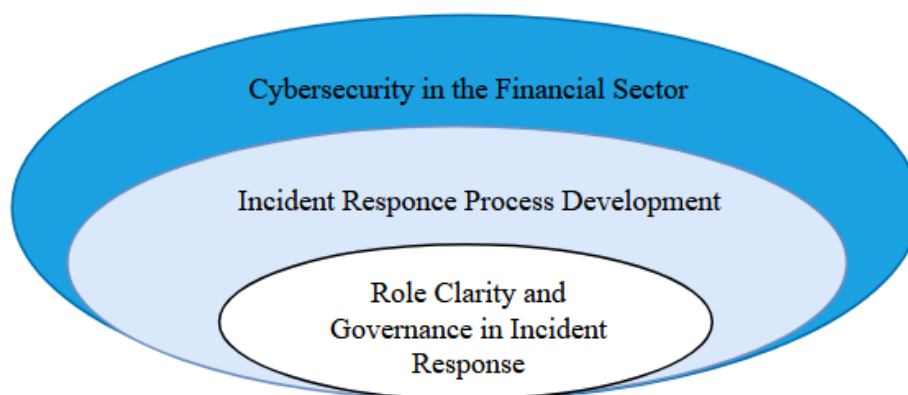
## 1.2 Research questions and objectives

The purpose of this study is to explore the current state of incident response in the Finnish financial sector and examine how incident response should be implemented when a cyberattack successfully disrupts business operations.

The financial sector is heavily regulated, with multiple frameworks, guidelines, and legislation designed to guide cybersecurity efforts (Calliess & Baumgarten, 2020; European Commission, 2025). However, these frameworks primarily emphasize preventive measures, focusing on identification and protection (ISO/IEC 27001, 2023). While such measures are essential, cybersecurity frameworks and cybersecurity research increasingly recognizes that not all attacks can be prevented, and incidents are inevitable (Naseer et al., 2024). This is when the ability to respond and recover effectively becomes crucial.

This study aims to address the existing gap by shifting the focus from prevention to response and recovery. By applying information and knowledge management practices, the research will aim to develop an incident response process model tailored to the specific needs of the Finnish financial sector. The goal is to enhance organizational resilience and improve existing incident response processes to avoid incidents like the Nordea case.

To better define the scope of the study, the research topic definition has been narrowed down, as illustrated below in Figure 1.



**Figure 1:** Scope and focus of the research

Figure 1 illustrates the progressive narrowing of this study's focus, which starts from the broad domain of cybersecurity in the financial sector and arrives at a specific emphasis on role clarity and governance in incident response. The narrowing reflects the research's pragmatic aim of producing practically applicable insights. This gradual specification reflects both the complexity of the topic and the necessity of defining clear boundaries for the research. Rather than concentrating on a single attack type, this study focuses on disruption to business operations, acknowledging that various forms of cyberattacks may lead to similar challenges in response and recovery. In addition, given the rapid evolution of attack and defense technologies, and the fact that successful attacks often exploit unknown vulnerabilities, it is not appropriate to focus on individual, currently known attack methods from a resilience perspective. The emphasis is on organizational resilience, rather than technical aspects of attack vectors.

In order to capture the full scope of roles and responsibilities involved in incident response, the research adopts a broader role-based perspective, drawing on the European Cybersecurity Skills Framework (ECSF) to identify the key professional roles and competencies required for effective response. While larger financial institutions such as Nordea provide illustrative context, the study does not limit its scope to them, and insights are intended to be relevant across the Finnish financial sector.

EU-level regulations such as DORA and NIS2 will be examined to understand the regulatory requirements and guidance shaping incident response responsibilities. The study remains focused on processes, governance structures, and role coordination during and after incidents and does not focus on specific technical implementations or tooling. While incident prevention remains a background consideration, the core interest lies in the response and recovery phases, where cyber resilience is most directly tested.

The main research question is:

- How could the Finnish financial sector improve its incident response capabilities?

The sub-research questions are:

- What is the current state of incident response practices in the Finnish financial sector?
- How do current practices differ from existing frameworks or best practice in incident response?
- How could the European Cybersecurity Skills Framework be used to identify and address skills gaps in incident response?

This study follows a qualitative empirical research approach to explore how the incident response capabilities of the Finnish financial sector could be improved. The purpose is to study the current state of incident response practices in the Finnish financial sector, how the practices differ from existing frameworks or best practices and how the European Cybersecurity Skills Framework could be used to identify and address possible skills gaps in incident response.

A descriptive case study strategy is used to gain in-depth insights into real-world cybersecurity incident response processes and practices. The theoretical background for the empirical research will be based on systematic literature review collecting the most relevant cybersecurity research of the financial sector, the most widely used frameworks, best practices, and standards as well as the most prominent regulations affecting cybersecurity in the Finnish financial sector.

Data will be collected through semi-structured interviews with cybersecurity professionals with experience in the financial sector and incident response. In addition, a document analysis on incident reports and news articles of the Nordea incident will be conducted. The interviews will provide professional insight into incident response processes, while document analysis will help contextualize these findings within existing practices and cases.

For data analysis, thematic analysis will be applied to identify key patterns and strategies used in reaction and recovery efforts. This approach ensures a comprehensive understanding of how leadership influences cybersecurity resilience beyond prevention-focused measures.

### **1.3 Research structure**

The first chapter of the thesis introduces the research topic, its significance and the motivation behind the research. The research questions and the objectives are discussed. The second chapter discusses the research methodology of the empirical research. The methodological choices will be presented, including research design, strategy and time horizon. The methodology for a systematic literature review for the theoretical background is presented. The methodology is presented before the theoretical chapters because these choices are relevant to the literature material, which partly become empirical data through standards and regulations, among other things. The data collection and data analysis relevant to the empirical part of the study are presented in later chapters.

The third chapter begins the theoretical background behind the research, which has been collected with systematic literature review. The third chapter focuses on cybersecurity in

the financial sector, exploring relevant research on the cybersecurity landscape and infrastructure, challenges, and the regulatory environment of the financial sector. The aim is to define what the state of cybersecurity in the financial sector is, what are the common challenges and how the regulatory and supervisory environment expects financial institutions to answer them.

The fourth chapter continues the theoretical background by discussing cybersecurity governance and frameworks. Governance models, frameworks and standards are analyzed to understand how cybersecurity is managed, governed and what the tools for implementing cybersecurity best practices are. Frameworks and standards are evaluated based on how they help the financial sector standardize these guidelines and enhance incident response. The European Cybersecurity Skills Framework roles are introduced and analyzed in terms of how they will contribute to incident response.

The fifth chapter discusses incident response in the financial sector. The principles of how incident response is managed and should be managed are discussed, the most relevant standards, and the current state of recovery and business continuity are analyzed. Lastly, the roles, coordination and governance in incident response are explored and how incident response can be enhanced by integrating role frameworks.

The sixth chapter introduces the data collection and analysis methodology for the empirical research. The chapter discusses how document data has been collected and semi-structured interviews have been conducted. Data analysis approach is introduced with examples of how data is coded and themes are derived. The results of the empirical study are presented in the seventh chapter where document data and interview data are presented separately.

Chapter eight focuses on the discussion, comparison, and combination of the results. The discussion takes into account the connection of the results to the theoretical chapters of the literature review. The final, ninth chapter is the conclusion of the study with key findings, evaluation of the study, and suggestions for future research.

## 2. RESEARCH METHODOLOGY

This chapter explains the research design, framework and methodological choices behind them. The choices have been made based on the objectives of the research and what it aims to achieve. Methodological choices are also selected to serve the research questions presented and are based on the available data sources and on the intended contribution to both academic knowledge and practical application. According to Puusa et al. (2020), the success of a study depends on the internal coherence and balance between its different components. This chapter presents the overall research framework by outlining the methodological choices made.

### 2.1 Research design

This study follows the scientific framework proposed by Saunders et al. (2019) to structure the research design systematically. The framework provides a logical and layered approach to research that helps align philosophical assumptions, methodological choices, and data collection techniques with the research objectives. Following Eriksson & Kovalainen (2008), understanding and explicitly articulating philosophical assumptions enhances transparency by revealing how knowledge is produced, what kind of knowledge it represents, and how it relates to existing bodies of knowledge. This reflection is especially important in qualitative research, where the researcher's interpretive role inevitably shapes the construction of meaning (Eriksson & Kovalainen, 2008; Puusa et al., 2020).

The chosen research philosophical stance for this study is **pragmatism**, as it provides the most suitable foundation for exploring and improving cybersecurity incident response within the Finnish financial sector. Pragmatism acknowledges that reality is complex and that knowledge is constructed based on the research context and the practical usefulness of findings (Saunders et al., 2019). It emphasizes problem-solving and actionable usefulness of knowledge rather than commitment to any single ontological or epistemological position (Farjoun et al., 2015; Saunders et al., 2019). Its central principle is that knowledge should be valued according to its consequences in action, meaning what it enables actors to do in complex real-world situations (Farjoun et al., 2015).

This research seeks not only to understand how incident response currently functions and identify possible gaps between frameworks and best practices, but also to generate actionable insights to improve incident response capabilities. As Goldkuhl (2012) notes,

pragmatism extends interpretivist thinking by emphasizing practical application of understanding in real-world contexts. While interpretivism focuses on generating deep insights into social meanings and experiences, pragmatism builds on this by valuing knowledge for its capacity to improve practice. Consequently, pragmatism therefore provides a fitting philosophical stance for a study that bridges theoretical understanding with applied problem-solving.

Moreover, pragmatism avoids rigid dualism between objectivity and subjectivity or between theory and practice (Farjoun et al., 2015). This flexibility is crucial for research in cybersecurity, where phenomena are socio-technical and constantly evolving (Walton et al., 2021). This approach allows the study to combine theoretical frameworks such as ISO standards and incident response models with empirical data from interviews and documents, producing knowledge that is simultaneously analytical and actionable. Pragmatism thus accommodates both the descriptive aim to depict how incident response is organized, and the prescriptive aim to identify how it could be improved (Farjoun et al., 2015; Goldkuhl, 2012).

Alternative philosophical orientations were considered. Constructivism was considered appropriate since the study acknowledges that understanding of cybersecurity practices is socially and contextually constructed (Eriksson & Kovalainen, 2008). Nevertheless, constructivism does not sufficiently emphasize the instrumental value of knowledge in improving practice. Pragmatism, in contrast, integrates these interpretive and constructivist insights while focusing on their practical consequences, making it the most suitable philosophy for a study situated at the intersection of theory and operational practice in cybersecurity (Goldkuhl, 2012; Saunders et al., 2019).

The study adopts an **abductive approach** to theory development and reasoning, which aligns with the pragmatist philosophy emphasizing iterative inquiry and learning from practice (Farjoun et al., 2015; Goldkuhl, 2012). Abduction bridges deduction and induction. While deduction tests theory and induction builds theory from observation, abduction moves iteratively between empirical findings and theoretical concepts to refine both (Eriksson & Kovalainen, 2008; Saunders et al., 2019). It is particularly suited for exploratory research where existing frameworks provide partial but incomplete explanations of real-world practices.

In this study, abduction was operationalized through repeated movement between data and theory. The initial framework was based on a systematic literature review, which guided interpretation, but empirical findings prompted theoretical refinement. This pro-

cess reflects the pragmatist view of inquiry as adaptive sensemaking, where understanding evolves through interaction between ideas and experience (Goldkuhl, 2012). Abductive reasoning also supports reflection on anomalies rather than their dismissal, enabling theory development grounded in the practical complexities of incident response (Farjoun et al., 2015). Consequently, abduction ensures methodological coherence by combining theoretical grounding with openness to emergent insights, producing knowledge that is both explanatory and actionable.

## 2.2 Research strategy

This study employs a **descriptive case study research** strategy to explore and explain how incident response and recovery are organized in the Finnish financial sector. Case study research is particularly appropriate when the research questions are descriptive and context-sensitive, focusing on what is happening and how it unfolds in a real-life context (Eriksson & Kovalainen, 2008; Yin, 2018). The aim of this study is to examine the Nordea DDoS attacks of autumn 2024 and the organizational response to them, which requires a detailed and holistic understanding of an event embedded within complex organizational, regulatory, and societal structures.

Case study research should be understood as a research strategy rather than a method, emphasizing rich, multi-source data and analytical depth over variable control or statistical generalization (Eriksson & Kovalainen, 2008). The descriptive orientation is suitable because the study does not attempt to build or test theory but to produce a comprehensive, empirically grounded account that reveals patterns, contradictions, and lessons relevant to improving incident response capabilities (Flyvbjerg, 2006). As Flyvbjerg (2006) argues, well-selected descriptive cases can yield transferable and practice-relevant insights even without formal generalization.

The case study approach is also consistent with the pragmatist philosophy underpinning this research (Saunders et al., 2019). Pragmatism values a situated, actionable understanding and recognizes that complex real-world phenomena such as cyber incidents cannot be captured by universal values (Farjoun et al., 2015; Goldkuhl, 2012). Instead, knowledge develops iteratively through engagement with practice and context. The case study allows this iterative movement between theory and data, which is also characteristic of abductive reasoning.

In this research, the Nordea incident forms a bounded and information-rich case through which sectoral practices, communication, and regulatory interactions are examined. Access to internal organizational data was not feasible, thus the study relies on triangulated

data sources to ensure credibility (Puusa et al., 2020; Saunders et al., 2019). This strategy reflects the pragmatist commitment to linking micro-level actions with macro-level structures, showing how individual, organizational, and sectoral processes co-evolved during crisis management (Farjoun et al., 2015).

### **2.3 Research methodology**

Methodology refers to the organizing principles that guide how research questions are approached and how knowledge is produced in practice (Eriksson & Kovalainen, 2008). The methodological choices of this study are grounded in the research purpose which is to describe, compare, and develop incident response practices, and in the pragmatist philosophy, which emphasizes problem-solving and methodological flexibility (Farjoun et al., 2015; Goldkuhl, 2012). Consequently, this study employs a multi-method qualitative methodology, integrating document analysis and expert interviews to produce a comprehensive, context-rich understanding of cybersecurity incident response in the Finnish financial sector.

A multi-method qualitative design was selected to capture the multifaceted nature of organizational incident response, which cannot be adequately understood through a single data source. Document analysis and expert interviews complement one another by providing distinct yet interrelated perspectives on the phenomenon. Document data, such as standards, media articles, and public reports offer insight into official narratives, institutional framing, and sector-level expectations, while expert interviews reveal practitioners' situated interpretations, reasoning, and tacit knowledge that are often absent from formal documentation (Eriksson & Kovalainen, 2008; Puusa et al., 2020; Yin, 2018).

Such triangulation enhances credibility by allowing cross-verification of findings and the identification of convergences or discrepancies between different forms of evidence (Shenton, 2004). The approach also supports iterative theorizing, as empirical insights from interviews can refine interpretations drawn from documents and vice versa. This methodological pluralism reflects the pragmatist view that complex problems are best studied through multiple, context-sensitive lenses rather than through a single methodological tradition (Farjoun et al., 2015; Goldkuhl, 2012). In combining document analysis with expert interviews, the study gains both contextual breadth and interpretive depth, producing a more comprehensive and credible account of incident response in the Finnish financial sector.

## 2.4 Time horizon

This study adopts a cross-sectional time horizon, i.e. data are collected and analyzed for a bounded period to capture the situation as it appears rather than its evolution over time (Flyvbjerg, 2006; Saunders et al., 2019). A cross-sectional design matches the descriptive and current state focus of the research questions, exploring what incident response practices are and how they operate now in the Finnish financial sector, rather than testing temporal change or causal trajectories (Eriksson & Kovalainen, 2008; Maier et al., 2023). It is also coherent with a descriptive case study strategy that seeks a rich, situated understanding of real-life contexts to inform practice (Yin, 2018).

Methodologically, a cross-sectional horizon supports the study's pragmatist aim of producing actionable knowledge for present decision-making in a complex socio-technical domain (Farjoun et al., 2015; Walton et al., 2021). The Nordea 2024 DDoS incident provides a bounded, information-rich snapshot that enables triangulation of expert interviews with documentary sources to characterize incident response capabilities at a specific moment of practical relevance (Saunders et al., 2019). This offers a credible baseline of current practices and gaps that can guide immediate improvements and scaffold subsequent studies (Maier et al., 2023).

A longitudinal horizon would be appropriate for analyzing role evolution or regulatory effects over time, which would require repeated organizational access and multiple waves of data to observe change mechanisms (Eriksson & Kovalainen, 2008; Saunders et al., 2019). Given access constraints and the thesis scope, such a design would be impracticable here and misaligned with the present research questions.

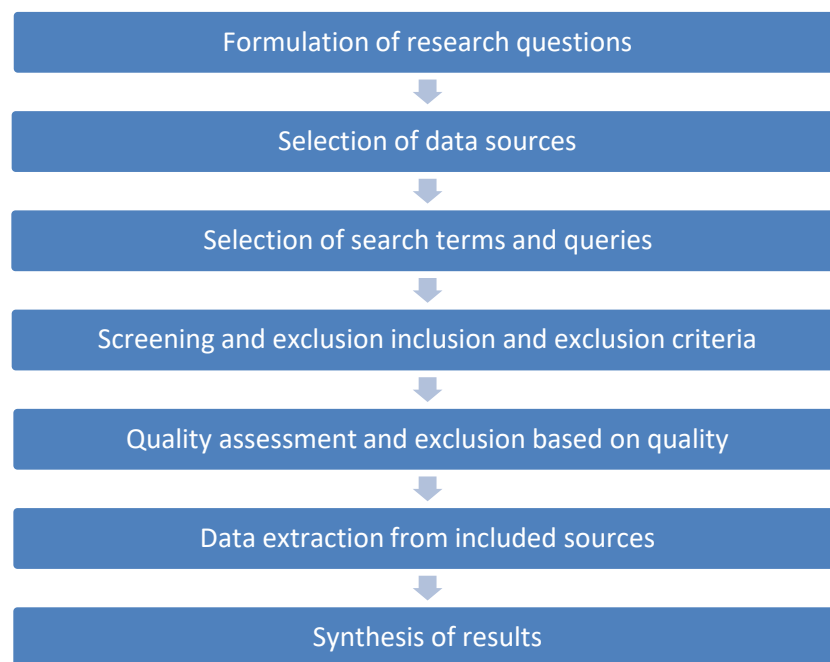
The cross-sectional horizon is also compatible with abductive reasoning since iterative movement between data and theory refines explanations without necessitating repeated measurements (Eriksson & Kovalainen, 2008; Saunders et al., 2019). Choosing a cross-sectional design is a methodologically coherent decision that aligns the research questions, strategy, philosophy, and practical constraints while delivering a rigorous, context-rich baseline of incident response practices.

## 2.5 Systematic literature review

Theory plays a central role in qualitative research, as its aim is to understand the perspective of the research subjects, which requires close contact with them (Puusa et al., 2020). For this reason, the theoretical framework for this study is compiled using a systematic literature review, as this allows for a sufficient understanding of the operating environment for expert interviews and the context for analyzing documents describing

the studied incident. A systematic literature review also enables careful examination of concepts, which is important in qualitative research where they are key building blocks, upon which empirical research later in this study is based on (Puusa et al., 2020).

Yin (2018) emphasizes that descriptive case studies must be guided by a theoretical framework. The theoretical background is defined through a systematic literature review following Fink's (2005) model for structured literature reviews. The purpose is to utilize a systematic literature review to construct a comprehensive understanding of a phenomenon, as it synthesizes and condenses existing research and expert knowledge into a structured overview (Salminen, 2011). Theoretical framework also helps to determine empirical data collection. The results will aid with defining key concepts of the study and the relationships between them to the subsequent qualitative research and data analysis (Tuomi, 2018). The process is illustrated in Figure 2.



**Figure 2:** Fink's model for structured literature review

The formulation of research questions was introduced in Chapter 1.2. Data for the literature review was collected from various sources. The legislation and regulations regarding cybersecurity and the financial sector were collected from the official websites of the European Union and the websites of the different institutions of the EU that offered guidelines and recommendations. In addition, publications from EU institutions discussing the current state of cybersecurity in the financial sector were selected. Reports of the national state of cybersecurity in Finland were selected from reliable organizations such as

Traficom's National Cybersecurity Centre and FIN-FSA. Frameworks and standards were collected from the websites of the organizations that had developed them.

The research articles discussing and evaluating how frameworks were implemented in the cybersecurity of the financial sector, what the current state of cybersecurity and incident response are, were collected from the database Andor, owned and managed by Tampere University as well as from Google Scholar and a few from Scopus AI. The focus was on peer-reviewed journals. The data sources included both financial and cybersecurity journals to assess both perspectives on the sector.

The search terms included cybersecurity, financial sector, incident response, business continuity, crisis response, and cybersecurity governance. The different inflections of the search terms were taken into account with the search commands. The search terms were used in order to construct appropriate search queries to the databases. In addition to the searches on databases, the bibliography of selected articles was manually searched in order to find relevant sources. The searches were done from March 2025 to April 2025. The publication date was limited to 2020-2025 because cybersecurity is evolving rapidly and knowledge becomes outdated very quickly. The language of the selected articles was solely English.

Articles that seemed to answer the research questions were selected based on titles and abstracts. Some articles were excluded in the reading phase, because on closer inspection, they did not address relevant topics for the research. The purpose of this selection process was to find research that discussed the current state of cybersecurity and incident response in the financial sector. The challenges, threats, and the implementation of frameworks as well as compliance with regulations were also analyzed in the articles.

In total 24 research articles were chosen for the systematic literature review. All the chosen articles were collected to a concise table to support transparency and the replicability of the literature review. Bibliographical details, transparency of the selection logic and information supporting quality assessment and search traceability are reported in the table. The table can be found in Appendix A.

During the reading phase of articles, irrelevant ones were pruned. The themes of the articles needed to contribute to the theoretical groundwork for the empirical research or answer the research questions. Notes from the articles were written and sorted by themes and by outlined chapters and topics.

## 3. CYBERSECURITY IN THE FINANCIAL SECTOR

The financial sector has distinct cybersecurity challenges due to its role as critical infrastructure, its heavy regulatory burden, and its reliance on both modern and legacy systems. As a highly targeted industry, financial institutions must navigate an evolving threat landscape while ensuring compliance with complex regulations.

This chapter discusses the significance of the financial sector, the threat landscape and challenges, and discusses how the regulatory environment and supervisory guidelines take into account both the high expectations of the industry and the complex challenges.

### 3.1 The financial sector as critical infrastructure

The financial sector is classified as critical infrastructure both in Europe and globally. Disruptions in this domain can cause widespread economic and societal consequences, making its resilience a national and international priority (Calliess & Baumgarten, 2020). Didenko (2020) notes that the financial sector has been prioritized for regulatory attention because of its central role in maintaining public trust and its deep interconnection with the broader economy. It has always been a primary target due to the critical nature of the information they handle (Didenko, 2020).

The European Union has classified both banking and financial infrastructure as critical infrastructure through the Directive on the Resilience of Critical Entities and requires its member states to adopt the regular risk assessment as part of national strategy (European Commission, 2024). In Finland, no national critical infrastructure, critical sector or operators were defined in legislation before 2025, when the legislation for the national implementation of this EU directive was finalized (Ministry of the Interior, 2025).

The National Emergency Supply Agency is responsible for planning and operational activities related to maintaining and developing Finland's security of supply. It has been defined that the role of the financial sector is to ensure that the services essential to the functioning of the society continue to operate in all circumstances, manage the business continuity of its own organization, and monitor the overall security of supply and resilience of the sector. The financial sector is responsible for ensuring the availability of products and services in the event of disruptions and exceptions. (Huoltovarmuuskeskus, 2025) This definition highlights the high expectations for continuity and trust for the sector. The Finnish financial sector is broad and consists of banks, investment funds, finance

companies, security brokers, life, pensions and non-life insurance companies (Finanssiala Ry, 2024).

Over the past two decades, the financial sector has become deeply dependent on technology for all its operations and services (Calliess and Baumgarten, 2020). For example, the number of transactions makes the operations of the sector infeasible without automated processing, networking and telecommunication (Varga et al., 2021). Digital infrastructure is the backbone of financial activity from trading platforms to customer interfaces. This is why also digital infrastructure is covered by the EU directive on the resilience of critical entities (European Commission, 2024).

As Uddin et al. (2020) observe, this increasing reliance on digital systems has significantly exposed the sector to systemic risks. The highly connected nature of financial networks means that a localized cyber incident could propagate through interdependent systems with cascading effects. This is also noted by Carilo (2023), as cybersecurity failures in the financial sector do not remain isolated incidents but they pose real threats to the economy as a whole. The sector can be seen as a vital enabler of the functioning of other sectors (Calliess & Baumgarten, 2020). Cyberattacks exploiting existing vulnerabilities in financial institutions can potentially escalate into systemic cyber risks, threatening the stability of the entire financial system (Carilo, 2023). Scholars argue that the financial sector suffers from systemic cyber risk due to its complexity, interconnectedness and centrality in economic infrastructure (Uddin et al., 2020).

In addition to the financial sector's dependence on information technology, people are increasingly dependent on financial services in their daily lives (Varga et al., 2021). In Finland, the most popular method of strong authentication is bank IDs. In this case, the user is dependent on the functioning of financial services to access Finnish e-government services (Suomi.fi, 2025).

In response to its role as critical infrastructure, the financial sector has made significant investments in cybersecurity. The financial sector takes cybersecurity very seriously, which is particularly evident in the large cyber technology investments in the sector (Uddin et al., 2020). According to some assessments, such as ENISA's, the sector has responded well to requirements and threats and is well developed in terms of cybersecurity maturity. Only the telecoms sector is assessed as more mature among the critical sectors in terms of cybersecurity. (ENISA, 2024) The rise of cyber incidents in the sector has made financial institutions increasingly outsource their IT infrastructure to third-party service providers (Clausmeier, 2023)

Activity in the Finnish financial sector is subject to authorization, so only applicants who meet the minimum regulatory requirements will be allowed to operate in the sector. In order to obtain a license, the operator must demonstrate operational risk management, meaning cybersecurity management is also examined before the start of operations. Cybersecurity management is assessed by an independent third-party conducting a cybersecurity audit. (Finanssivalvonta, 2020)

After authorization is granted, the operator becomes subject to supervision by the Financial Supervisory Authority and is subject to continuous supervision. This supervision includes assessing cybersecurity implementation, conducting audits, and evaluating outsourcing. Cybersecurity must also be considered in situations where services are discontinued. A plan for the termination or transfer of services is often required at the stage of applying for authorization to start operations. (Finanssivalvonta, 2020)

### **3.2 Cybersecurity threat landscape and challenges**

The cybersecurity threat landscape facing the financial sector is uniquely complex, shaped by interconnectivity, structural vulnerabilities, and evolving attack vectors. As a critical infrastructure, the financial sector not only faces frequent and sophisticated cyberattacks but also bears the risk that even localized incidents may trigger systemic consequences (Uddin et al., 2020). The European Union Agency for Cybersecurity (ENISA) has reported that cyber activity targeting financial entities increased notably during the first half of 2024. This trend is attributed to several factors such as geopolitical instability, matured incident detection and reporting, new legislation, and increased media attention to financial cyber incidents (European Union Agency for Cybersecurity, 2025). However, the number of reported incidents does not correspond to the number of attacks. Rather, it can signal heightened capacity for visibility and accountability.

ENISA's latest observations show that banks are the most frequently affected, while accounting for 46% of reported incidents. The dominant attack vector was distributed denial-of-service, representing half of all incidents, and remaining the most reported threat across all quarters in the period of January 2023 to June 2024. (European Union Agency for Cybersecurity., 2025) This pattern aligns with the findings of Varga et al. (2021), which identify the two primary cyber targets in the finance sector as the technical infrastructure of the markets and the human and organizational actors within them. The number of incidents was reported to rise significantly in 2024 (European Union Agency for Cybersecurity, 2025).

Beyond the frequency of attacks, the structural vulnerabilities of the sector make it especially susceptible to cascading effects. Carilo (2023) emphasizes that the tightly woven digital networks that enable modern financial operations create opportunities for systemic disruptions. A single disruption in a network can disrupt entire financial system. (Uddin et al., 2020) This vulnerability amplifies the global impact potential of cybersecurity incidents, meaning localized incident can quickly have international impacts (Carilo, 2023). This challenge of interconnectivity is also recognized by the National Emergency Supply Agency of Finland which has identified it as one of the main challenges for financial preparedness, the dependence on structures outside Finland. It has also complicated incident and crisis management, making it multidimensional and difficult (Huoltovarmuuskeskus, 2025).

Complicating the sector's resilience is the inherent uncertainty of estimating impact and likelihood of cyber risk. Unlike traditional business risks, cyber risks are by nature related to hidden vulnerabilities, unpredictable behavior, and potential for both direct operational damage and indirect reputational loss. Financial institutions often base their security investments on anticipated risk, yet the unpredictable nature of modern threats complicates resource allocation. Paradoxically, investments in cyber technologies can broaden attack surfaces, as no technology is without vulnerabilities (Uddin et al., 2020).

Reputational risk is perhaps the most severe consequence of cyber incidents in the financial sector. According to Varga et al. (2021), trust is fundamental to the functioning of financial systems, and a single breach can set off a negative sentiment and distrust that are difficult to contain. Erosion of customer trust may lead to depositor runs, liquidity shortages, and forced liquidation of assets before maturity, which in turn may destabilize markets and institutions (Uddin et al., 2020). This dynamic is more acute in finance than in other sectors, such as the healthcare sector, due to the instantaneous nature of capital flight and public reaction.

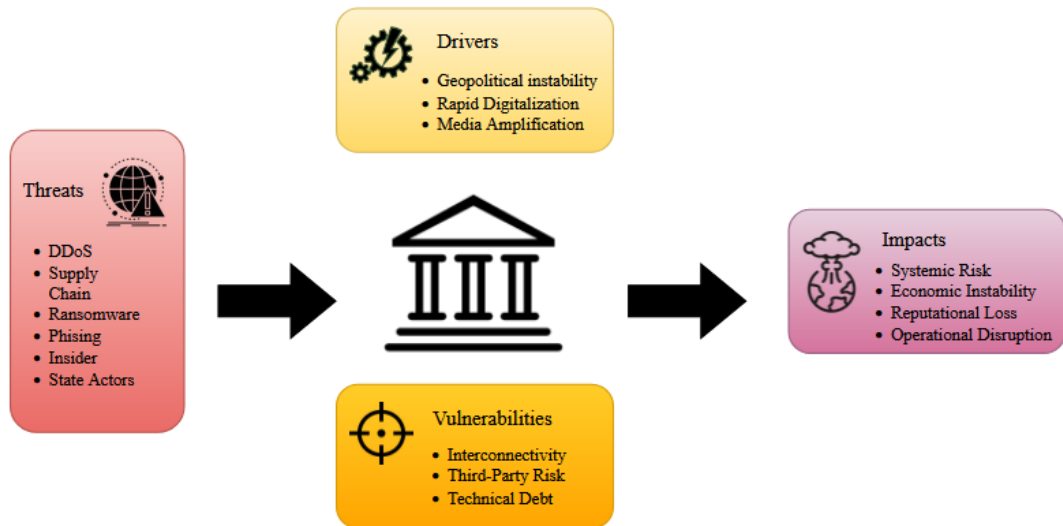
Despite the sector's high regulatory burden and technical investments, significant gaps remain in its ability to predict, detect, and adapt to evolving threats. Varga et al. (2021) note that many institutions still do not conduct real-time intrusion detection or gather threat intelligence themselves, delegating that responsibility to authorities or third parties. Moreover, many actors fail to analyze adversaries' motives or investigate the root causes of attacks. As Peihani (2022) argues that financial cybersecurity efforts have historically focused on narrow compliance goals, such as securing payment card data without fully addressing broader risks like supply chain vulnerabilities or third-party risks.

This challenge is also recognized in research by Darem et al. (2023) which highlights that outsourcing and vendor dependence introduce new vulnerabilities that financial institutions struggle with. Despite the existence of frameworks and guidelines, many organizations fail to enforce consistent cybersecurity standards across their supply chains (Darem et al., 2023). This leaves them vulnerable to indirect attacks through vendors and partners which are also recognized as a challenge in the research by Clausmeier (2023) as the finance sector is increasingly reliant on digital service outsourcing. ECB has found vulnerabilities in sector's IT sourcing strategies as supply chains remain complex, increasing the effort needed from finance sector organizations to monitor them. Additionally, concentration to a limited number of service providers in the industry has remained high, while dependency on outsourcing continues to rise. (ECB, 2025) The outsourcing of critical services being concentrated to a limited number of service providers may challenge operational resilience of organizations should one key provider become unavailable.

Fragmentation of regulatory frameworks further complicates the implementation of cybersecurity measures. Didenko (2020) argues that regulatory inconsistencies across jurisdictions hinder the implementation of harmonized cybersecurity policies, especially for financial institutions operating internationally. However, some argue that compliance-driven nature of cybersecurity in the finance sector limits flexibility and innovation, as organizations focus on audits rather than real-time threat mitigation (Peihani, 2022). Although EU regulation aims to reduce fragmentation within Europe, global alignment remains incomplete.

Figure 3 illustrates the complexity of the cybersecurity threat landscape in the financial sector by summarizing its key components sorted into different categories: threats, drivers, vulnerabilities, and impacts. The threats reflect the types of cyberattacks frequently observed in ENISA's reports and recent literature (European Union Agency for Cybersecurity., 2025; Varga et al., 2021). These threats are intensified by external drivers largely outside of the sector's control, including geopolitical instability, rapid digitalization, and media sensitivity to incidents in the finance sector. Together, these factors increase both the frequency and perceived severity of attacks. At the same time, the sector's inherent vulnerabilities, such as interconnectivity, third-party dependencies, and complex technical infrastructures make it particularly challenging to defend against these threats, as also emphasized by Uddin et al. (2020), Carilo (2023), and ECB (2025). These structural characteristics expose institutions not only to direct risks but also to cascading effects across the financial system. The resulting impacts go beyond operational disruption, en-

compassing reputational damage, economic instability, and systemic risk, which are especially severe in finance due to the sector's reliance on trust and its critical role in broader societal functions. Figure 3 provides a synthesis of how these dimensions interact to shape the sector's unique cyber risk environment.



**Figure 3:** Cybersecurity Threat Landscape of the Finance Sector

Financial institutions face a wide range of expectations from both internal and external stakeholders, and as threats become more sophisticated, the demands for compliance, transparency, and resilience increase (van der Kleij et al., 2022). However, while academic research often encourages disclosure of cyber incidents in order to foster trust (Uddin et al., 2020), there is also debate about whether transparency might also attract adversaries (Walton et al., 2021). The financial sector must now balance the pressures of compliance, the pace of digital innovation, and the necessity of building real-time resilience in a globalized threat landscape.

### 3.3 Regulatory environment and supervisory guidelines

Regulatory oversight of cybersecurity in the financial sector has intensified significantly as regulators and supervisory agencies have recognized cyber threats to be the most critical risk to the financial sector (van der Kleij et al., 2022). Of all industries, finance is arguably subject to the most comprehensive and advanced regulations related to cybersecurity (Didenko, 2020). Consequently, multiple European and national authorities are involved in governing and guiding the cybersecurity practices of financial institutions.

In the European Union, cybersecurity in the financial sector is supervised and guided by a multi-level network of authorities. The European System of Financial Supervision creates a network around the most notable supervisors which are the three European Supervisory Authorities (ESAs), the European Systemic Risk Board (ESRB) and the national competent authorities (NCAs) (European Central Bank, 2022). One of the persistent challenges of this structure is the coordination between multiple supervisory and regulatory bodies, which may lead to fragmentation or conflicting obligations across jurisdictions (Calliess & Baumgarten, 2020).

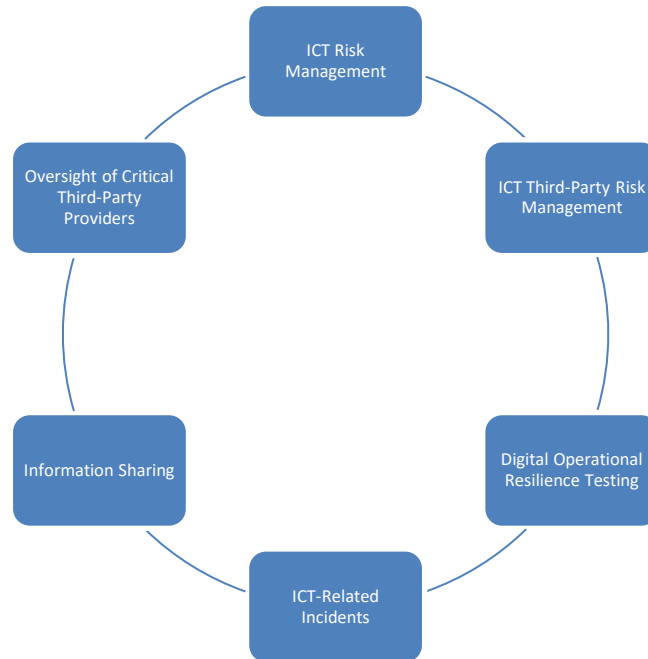
The European Systemic Risk Board supervises the financial system and collects relevant information on systemic risks, issues recommendations, and coordinates cooperation between authorities working closely with the European Central Bank (ECB) and the European Banking Authority (EBA) (European Central Bank, 2022). It guides information sharing, crisis management and the development of cyber resilience in the critical infrastructure sectors (European Systemic Risk Board., 2024). These supervisory authorities had an important role in providing guidelines for the financial sector that addressed cybersecurity prior to more advanced legislation such as NIS2 and DORA (Carilo, 2023).

The most important regulations for the cybersecurity of the sector are the NIS2 directive, the newly enacted regulation Digital Operational Resilience Act (DORA), guidelines from both EBA and other European authorities as well as the national legislation supervised by FIN-FSA for the Finnish finance sector.

Finanssiala Ry, the organization representing the interests of financial actors such as banks and insurance companies, has concluded that there is no need for further national legislation in Finland when it comes to cybersecurity of the financial sector (Finanssiala Ry, 2021). In Finland, national legislation mainly focuses on risk management practices with a notable focus on preventive measures. The most significant national instruments governing cybersecurity and incident response that include the Act on Arrangements for Ensuring Security of Supply in the Financial Sector (666/2022), as well as the FIN-FSA Regulation on the Principles of Contingency Planning for Credit Institutions.

The Digital Operational Resilience Act (DORA) is a regulation created in 2022 to enhance the digital regulation of the financial sector in the EU. DORA became applicable on January 2025 (Digital Operational Resilience Act (DORA), 2022). In Finland, the implementation of the act is supervised by FIN-FSA (Finanssivalvonta, 2025). DORA imposes requirements on how financial institutions should manage cyber risks and sets guidelines for financial institutions and third-party contractors. It also sets requirements

for protecting, detecting, containing, recovering and restoring operational capabilities after cyber incidents. Many of the areas covered by DORA were previously solely recommendations or part of best practices. (Carilo, 2023). The most important areas DORA aims to cover are depicted in Figure 4.



**Figure 4:** Topics covered by DORA (Adapted from EIOPA, 2022).

DORA has been seen as a major step forward in mainstreaming cybersecurity in corporate governance since it strengthens regulatory requirements for cybersecurity and is the most advanced legislative instrument of the EU in the field of cybersecurity in the financial sector (Carilo, 2023). It marks a shift towards cyber resilience as under it, organizations must ensure they can withstand, respond to, and recover from ICT-related disruptions and threats (Calliess & Baumgarten, 2020).

DORA follows risk-based approach, where requirements are calibrated to the size, complexity, and risk profile of the institution. The scope of it includes all entities regardless of their criticality for the sector. It also applies to less traditional organizations such as credit rating agencies, trade repositories and e-money organizations. (Clausmeier, 2023) DORA also significantly advances the integration of cybersecurity into corporate governance, requiring management actively oversee ICT risk management and resilience planning (Calliess & Baumgarten, 2020). However, some elements, such as technical standards for incident reporting deadlines, still need to be developed by the ESAs (Clausmeier, 2023).

NIS2 directive is an EU directive guiding cybersecurity strategies in 18 different critical infrastructure industries in the European Union and it aims to guide member states with defining national cybersecurity strategies. NIS2 aims to improve EU-wide cooperation with clear rules and stronger enforcement tools. It requires member states to enhance their cybersecurity readiness. (Kyberturvallisuuskeskus, 2024b) Before DORA, it was the main instrument governing cybersecurity in critical infrastructure, including the finance sector (Didenko, 2020). The financial sector is considered essential services under the directive, making it subject to specific risk management and incident reporting obligations (Calliess & Baumgarten, 2020).

NIS2 also regulates some aspects of third-party providers and aims to place the suppliers under EU supervision when serving financial institutions. NIS2 requires organizations to have appropriate and proportionate technical and organizational measures to combat cybersecurity risks. (Carilo, 2023) NIS2 requires organizations to implement risk analysis and information system security policies, incident handling procedures, business continuity and crisis management, supply chain cybersecurity, policies for evaluating effectiveness of cybersecurity measures and use encryption and multi-factor authentication. It also makes incident reporting mandatory meaning significant incidents must be reported to national CSIRTs or other competent authorities. The notification must be made within 24 hours, update of the situation within 72 hours and the final report must be delivered within one month. Significant incidents mean they cause substantial operational disruption or financial loss or otherwise impact other entities. NIS2 enhances cooperation between member states via the CSIRT's network and the European Cyber Crises Liaison Organization Network (EU-CyCLONe). (European Union, 2022)

NIS2 also enforces accountability by holding top management directly accountable for cybersecurity failures. Management bodies in organizations must approve cybersecurity practices and oversee cybersecurity risk management. NIS2 also allows for the imposition of fines and penalties for non-compliance. National authorities are empowered to conduct audits, issue binding instructions and impose administrative fines for organizations. The national authorities are usually sector-specific. (European Union, 2022) In Finland, FIN-FSA is the national authority guiding and supervising the finance sector (Kyberturvallisuuskeskus, 2025).

The European Central Bank's TIBER-EU framework (Threat Intelligence-Based Ethical Red Teaming) complements DORA by offering a structured way to test resilience through simulated real-life cyberattacks in a controlled way (European Central Bank, 2023). These exercises involve external ethical hackers, internal blue teams unaware of the test, and detailed threat intelligence tailored to the target entity (European Central Bank,

2023). The Finnish adaptation, TIBER-FI, is coordinated by the Bank of Finland and includes local governance adjustments, stakeholder cooperation, and reporting protocols (Bank of Finland, 2025).

Other instruments supporting cyber resilience include EBA guidelines on ICT and security risk management, which provide detailed requirements for governance, controls, outsourcing, and incident management (Didenko, 2020). These guidelines are part of the ESAs' wider rule-making portfolio, which often fills in operational-level detail for regulations like NIS2 and DORA.

Despite the presence of extensive regulatory frameworks, research suggests that fragmentation, compliance-driven cultures, and resource limitations still hinder the sector's overall cybersecurity posture. Uddin et al. (2020) note that the effectiveness of guidelines related to non-technical controls, such as awareness training or strategic planning, remain unclear. This may be because recommendations are mainly based on opinions of different IT experts and industry professionals. Researchers call for more evidence-based guidelines for financial institutions from regulators. (Uddin et al., 2020)

## 4. CYBERSECURITY GOVERNANCE AND FRAMEWORKS

This chapter explores the existing governance models and structures in cybersecurity. The most significant cybersecurity standards and frameworks are discussed, and the European Cybersecurity Skills Framework is introduced.

### 4.1 Cybersecurity governance models

Cybersecurity is no longer a purely technical concern as it has become a strategic necessity that directly affects the stability, reputation, and resilience of financial institutions. As the digitalization of financial services accelerates and the complexity of cyber threats grows, the need for clear and well-structured cybersecurity governance becomes more pressing. The ECB emphasizes that institutions must establish appropriate governance frameworks that define roles, responsibilities, and control mechanisms for ICT and outsourcing (ECB, 2025). Regardless of the internal allocation of responsibilities, the management body retains ultimate accountability under DORA (EIOPA, 2022). Clear definitions and contractual agreements are therefore not only regulatory expectations but key enablers of accountability and incident coordination.

Unlike operational management or technical incident response, cybersecurity governance focuses on the decision-making structures, responsibilities, policies, and resource allocation that define how an organization protects itself and reacts to evolving threats (Cortez & Dekker, 2022). Governance not only defines the decision-making but also determines the organization's capacity to coordinate response during disruptions. As Akinsulire & Ohakawa (2024) emphasize, governance-level deficiencies such as fragmented accountability and unclear leadership directly weaken the ability to execute coordinated incident response. This highlights that improving incident response capabilities requires embedding them within a broader governance structure, rather than treating them as technical or operational issues.

Cybersecurity governance refers to the structures, policies, and processes that ensure organization's cybersecurity efforts align with its business objectives, risk tolerance, and regulatory requirements. Governance models define who is responsible for cybersecurity decisions and how those decisions are made, monitored and improved over time. This includes accountability on all levels and the clear delegation of roles. (Cortez & Dekker,

2022). A well-designed governance model ensures that incident response, security investments, personnel training, and technology adoption are not isolated activities but part of coordinated strategic decision-making processes.

Despite advances in governance through regulations such as DORA, challenges remain. As ENISA (2024) has observed, many financial institutions still lack robust governance for cybersecurity risk assessment. Similarly, Varga et al. (2021) note that although cyber situational awareness is often treated systematically, there is insufficient integration between threat analysis and strategic decision-making. This suggests that cybersecurity governance is still maturing and that institutions need to move beyond technical fixes toward strategic resilience planning.

These findings illustrate that while regulatory progress has enhanced formal governance structures, practical deficiencies persist in linking strategic decision-making with technical implementation. This gap mirrors Akinsulire & Ohakawa's (2024) empirical findings, where institutions with unclear governance experienced delayed and inconsistent incident response, often compounded by a lack of alignment between IT and business objectives.

Cybersecurity governance is also critical in shaping technology-related decisions. Adetunji & Chinonso (2025) emphasize that the integration of rising technologies such as artificial intelligence and machine learning in cybersecurity must be strategically guided. Governance determines whether these technologies are deployed in alignment with the institution's risk tolerance, as the same capabilities are increasingly used by adversaries (Adetunji & Chinonso, 2025).

Governance is critical for cultivating a cybersecurity-aware organizational culture. Employee negligence and poor security hygiene are among the most common vulnerabilities in the financial sector (Varga et al., 2021). Governance must therefore ensure that responsibilities are distributed not only across technical teams but among all units. As Adetunji & Chinonso (2025) argue, fostering a culture of security awareness among employees, customers, and stakeholders is essential to minimizing human-centric vulnerabilities and reducing long-term risk.

As Weickert et al. (2023) argue, cybersecurity governance is embedded within an organization's cultural and behavioral context. Governance mechanisms and formal policies alone are insufficient unless they are internalized through culture, shared understanding, and incentives. Integrating behavioral dimensions into governance design can therefore help bridge the persistent last mile problem between strategic intent and operational practice. Frameworks such as NIST CSF, ISO standards, and the ECSF offer practical

tools for this integration by clarifying behavioral, organizational, and technical competencies.

Cybersecurity governance should not be viewed as a compliance burden but as a strategic investment directly influencing financial stability and operational resilience. Institutions with low security maturity face expected annual losses more than five times higher than those with mature governance models (Adetunji & Chinonso, 2025). This means robust governance is not only a regulatory necessity but also a business necessity.

## **4.2 Cybersecurity frameworks and standards**

Cybersecurity frameworks offer established best practices and well-regarded methodology. They support the implementation of regulations and legislation. Even though they are voluntary they have had a critical role in standardizing cybersecurity practices in the financial sector, as the sector has relied on well-established cybersecurity frameworks to mitigate risks and ensure regulatory compliance (Olutimehin, 2025).

Among the most widely adopted frameworks are ISO/IEC 27001 and ISO/IEC 27002 standards, and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The National Institute of Standards and Technology (NIST) is an institute in the United States that provides cybersecurity guidance across all industries, and its frameworks are widely used even in the European financial sector. The Cybersecurity Framework (CSF) is designed to guide organizations in cybersecurity management and implementation by presenting the desired outcomes of the organization by managing and mitigating cyber risks (National Institute of Standards and Technology, 2024). The CSF consists of six core functions, which promote organizational cybersecurity. The CSF was updated by NIST in 2024 to add the sixth core function, Govern. The functions are displayed in Figure 5.



**Figure 5:** The NIST Cybersecurity Framework 2.0 (Adapted from National Institute of Standards and Technology, 2024)

**Governing** consists of leading and strategically guiding cybersecurity in organizations. It contains the responsibilities of management, cybersecurity policies, risk management strategies and fulfilling the needs of stakeholders. These can be achieved through strong governance and compliance as well as with clear divisions of responsibilities. **Identifying** means recognizing the cybersecurity risks and threats, organization’s own resources, processes and relevant stakeholders. Identifying focuses on what needs to be protected in the organizations, and this realization can be built with resource mapping, risk assessment and analyzing business processes and dependencies. **Protecting** means implementing protective measures in order to protect the organization from recognized threats by preventing damage or limiting disruptions and impacts of risks. The measures include for example access management, awareness and training programs, data encryption and technical protection. (National Institute of Standards and Technology, 2024)

**Detect** means detecting security breaches and anomalies as quickly as possible. Suspicious activity and incidents can be detected with logging, anomaly analysis or with continuous monitoring practices. **Responding** means reacting to anomalies and attacks in an efficient way, and it includes incident response plans, communication and situational awareness. **Recover** means the ability to restore systems and operations in an orderly manner after a disruption. It includes recovery plans, backups, continuity solutions and

communication with stakeholders. (National Institute of Standards and Technology, 2024)

While NIST CSF offers comprehensive guidance, its voluntary nature may limit consistent implementation across the financial sector. Goodwin (2022) argues that this lack of enforceability contributes to uneven preparedness and accountability which is an issue partially addressed in the EU through regulations such as DORA. NIST CSF emphasizes a risk-based approach, which is critical for financial institutions in maintaining an adaptive and resilient cybersecurity posture (Akinsulire & Ohakawa, 2024)

Another limitation is that it provides a clear structure for managing risks and scholars argue that these frameworks largely remain reactive rather than adaptive (Adetunji & Chinonso, 2025). To effectively enhance incident response, financial institutions must move beyond compliance-based application toward continuous learning and improvement, which is also consistent with the resilience-oriented Govern area of NIST CSF 2.0 (National Institute of Standards and Technology, 2024).

The framework's Respond and Recovery functions closely align with the incident response processes identified as critical for resilience in the financial sector. Goodwin (2022) shows that these functions have helped institutions strengthen response coordination and recovery planning during large-scale disruptions. NIST is considered more adaptable and user-friendly than ISO 27001 which makes it attractive for organizations seeking a practical, risk-based approach rather than compliance-oriented documentation (Goodwin, 2022). Akinsulire & Ohakawa (2024) conceptualize governance as composed of four interdependent pillars which are IT governance, risk management, compliance, and internal controls. Frameworks such as NIST CSF and ISO standards operationalize these pillars by translating strategic oversight into measurable controls.

The International Organization for Standardization (ISO) has collaborated closely with the International Electrotechnical Commission (IEC) to establish significant cybersecurity standards ISO/IEC 27001 and ISO/IEC 27002. In addition, the ISO 22301 standard is examined because it provides requirements for developing security, resilience and business continuity which are all relevant to this study as the focus is the incident response aspect of cybersecurity.

ISO 27001 sets the requirements for Information Security Management Systems (ISMS) to systematically manage cybersecurity risks. The ISMS requirements consist of ten main sections introduced in Table 1.

**Table 1:** ISO 27001 ISMS requirements

Section	Description
Context	Understanding the internal and external environment of organizations and the needs of stakeholders
Leadership	Commitment of top management, cybersecurity policies, definition of responsibilities
Planning	Risk management, setting objectives
Support	The necessary resources, competences, awareness, communication and documentation
Operation	Implementation of risk management measures and controls
Performance evaluation	Monitoring, measuring, auditing and management reviews
Improvement	Reaction to nonconformity, continuous improvement and corrective actions

ISO 27001 also introduces 114 controls divided into four categories: organizational, people, physical and technological controls. Organizational controls focus on for example cybersecurity policies, dividing roles and responsibilities and managing cybersecurity procurement whereas people controls focus on cybersecurity awareness and education, physical controls focus on physical access control and hardware protection, and finally technological controls focus on encryption, digital access control, and for example firewalls and intrusion detection systems. Organizational and technological controls form the most of the controls. (ISO/IEC 27001, 2023) Organizations can assess the implementation of these controls based on their risk assessment and risk management practices. The consensus is that not all of them need to be implemented, but any deviations

should be justifiable. The ISO 27001 offers a holistic approach to cybersecurity combining both technical and organizational methods.

Unlike ISO 27001, ISO 27002 is not a certifiable standard but an indicative standard, which complements the ISO 27001 controls by explaining and delving into them deeper, and how they should be implemented. The standard provides practical guidance on implementation of the controls. It defines the objective, guidance and attribute table for each control specifying control type, information security properties, cybersecurity concepts, operational capabilities and security domains. (ISO/IEC 27002, 2022)

In the 2022 version of the ISO 27002, the number of controls was reduced from 144 to 93, but the four categories remained the same. Some controls removed handled assets, protecting application services transactions and technical review of application after operating platform changes. They were considered to be included in the other controls or were otherwise considered obsolete. Interestingly, in 2022 controls were also added, and the additions include controls which take into account threat intelligence, business continuity and information management among other things. Both of these discussed standards have the status of a Finnish national standard making them particularly important for the Finnish financial sector.

There are concerns about whether compliance-based security models are truly effective in preventing sophisticated cyberattacks even though financial institutions have invested heavily in compliance, risk management, and incident response strategies. Despite their value in establishing consistency, both ISO and NIST frameworks have been criticized for being overly compliance-oriented and insufficiently dynamic in addressing fast-evolving threats (Adetunji & Chinonso, 2025).

Research suggests that financial institutions certified under ISO 27001 experience fewer cybersecurity incidents and enhanced regulatory alignment because the framework mandates structured documentation and incident response planning (Olutimehin, 2025). Institutions are not audited in the same way for compliance with frameworks, such as NIST CSF. However, critics argue that rigid compliance structures of ISO standards can lead to excessive bureaucracy where institutions focus more on meeting audit requirements rather than actively improving their cybersecurity posture (Olutimehin, 2025). It should be also noted that these frameworks and standards do not provide sector-specific guidance, which may affect their effectiveness in addressing threats unique to the finance sector. However, the ECB often refers to standards in its sector-specific and risk-specific guidelines, so knowledge of the standards provides a basis for cybersecurity (ECB, 2025).

### 4.3 European Cybersecurity Skills framework

The European Union agency for Cybersecurity, ENISA, is an agency dedicated to enhancing cybersecurity across the entire European Union. Its purpose is to guide and support the member states, EU institutions and organizations in the EU to develop and improve their cybersecurity. (European Union Agency for Cybersecurity, 2022) Unlike the institutions such as European Central Bank or European Banking Authority, it is not a supervisory body. It guides the cybersecurity efforts of the EU through frameworks and guidelines but does not actively supervise regulatory compliance in cybersecurity.

ENISA's framework, the European Cybersecurity Skills Framework (ECSF) is a tool to build an understanding of the cybersecurity professional role profiles that determine what kind of skills and competences in cybersecurity are needed. The purpose of the framework is to support identifying the different responsibilities and tasks of cybersecurity professionals as well as the required knowledge, competences, and skills of them. The roles of the framework are introduced in Figure 6. (ENISA, 2022) It is targeted at both cybersecurity professionals and non-cybersecurity experts who need a comprehensive view of the industry and its needs.



**Figure 6:** Overview of cyber security profiles (European Union Agency for Cybersecurity., 2022a)

The framework enhances common terminology and understanding regarding what is expected of cybersecurity professionals. This tool, among other things, helps the cybersecurity industry with its skills shortage issues since it aids with the identification of what competences and skills are needed in the industry. (European Union Agency for Cybersecurity, 2022a) While governance frameworks define accountability and structure, their practical implementation depends on the human capabilities executing them. The ECSF provides a bridge between institutional governance and individual competencies by defining knowledge, skills, and roles necessary to operationalize cybersecurity and incident response strategies. It also supports the development of a cybersecurity culture within organizations by aligning training, role definitions, and expectations (Weickert et al., 2023).

The framework identifies 12 distinct roles as seen in Figure 6 that represent the most important requirements for a professional cybersecurity environment, so that key cybersecurity tasks, and missions are shared and taken care of. The 12 roles are typically required roles that are applied within organizations. (European Union Agency for Cybersecurity, 2022a) The key skills and main tasks are introduced in Table 2.

**Table 2:** Responsibilities of the cyber security roles (Adapted from (European Union Agency for Cybersecurity, 2022b))

Role	Key skills	Main tasks
Chief Information Security Officer	Cyber strategy, leadership, risk management, ISMS	Define and lead cybersecurity strategy, align with business, manage risk and resources
Cyber Incident Responder	Threat detection, log analysis, communication under pressure	Monitor systems, handle and report incidents, restore operations
Cyber Legal, Policy and Compliance officer	Legal expertise, data protection, regulatory compliance	Ensure legal compliance, assess privacy risks, advise on governance
Cyber Threat Specialist	Threat analysis, TTP tracking, intelligence reporting	Collect and analyze threat data, report intelligence, guide mitigation
Cybersecurity Architect	Secure design, system modelling, architecture planning	Design secure systems, define architecture, ensure security integration
Cybersecurity Auditor	Auditing methods, control assessment, impartial reporting	Evaluate systems, verify compliance, report findings and recommendations
Cybersecurity Educator	Pedagogy, awareness building, curriculum development	Train staff, develop learning materials, promote cybersecurity culture

Cybersecurity Implementer	Secure configuration, system hardening, troubleshooting	Deploy and maintain solutions, patch vulnerabilities, support users
Cybersecurity Researcher	Innovation, scientific analysis, R&D leadership	Conduct cybersecurity research, publish findings, develop new solutions
Cybersecurity Risk Manager	Risk analysis, mitigation planning, business alignment	Identify risks, plan mitigation, communicate with stakeholders
Digital Forensics Investigator	Evidence handling, integrity preservation, reporting	Collect and analyze digital evidence, support investigations
Penetration Tester	Ethical hacking, exploit discovery, creative thinking	Simulate attacks, identify vulnerabilities, report and suggest fixes

Table 2 summarizes the key skills and main tasks of the roles in the organizations which ENISA introduces in its documentation and user guide of the framework. Analyzing the roles and their different responsibilities, it can be concluded that the most important role for incident response is Cyber Incident Responder. This role is at the front line of incident response, reacting to attacks and breaches, responsible for containment and eradication, and ensuring business continuity. In the finance sector, this role is responsible for the continuous access to financial services where access to them has a real monetary value. This role can also be responsible for the CSIRT and SOC cooperation and collaboration.

There is limited research available on the implementation of ECSF. Before ECSF, there were multiple international efforts to develop effective cybersecurity skills frameworks, but they are not based on standards and do not address the specifications and structures of the national markets. The 12 profiles have been analyzed based on the EN 16234-1:2019 e-Competence Framework standard. (Polemi & Kioskli, 2023)

The main reason for the cybersecurity skills gap is the lack of common terminologies and taxonomies which the ECSF provides. The profiles hold main labels, as seen in Table 2, but each profile also holds synonymous labels found in the market reflecting the same capabilities which are merged in the role. The profiles can be considered to consist of components that connect the marketing needs with the training offer (Polemi & Kioskli, 2023). These can be seen as the key skills and main tasks columns in Table 2. Key skills are the training offer and learning perspective of what the role needs to know and be able to do, which includes skills, knowledge and competences. The main tasks are the marketing needs and workplace perspective of the missions, deliverables, and tasks of the role. (Polemi & Kioskli, 2023)

## 5. INCIDENT RESPONSE IN FINANCIAL CYBER-SECURITY

Incident response is the organized reaction and approach of an organization to cyber incidents. This includes response and recovery from cyber incidents. The aim of incident response is to minimize damage, reduce recovery time, losses, and costs as well as prevent future incidents.

This chapter discusses how incident response is implemented in financial cybersecurity, how it works as a process, how recovery and business continuity are ensured through it, and the governance and coordination behind the process, which involves multiple internal and external stakeholders in the financial sector. In this thesis, incident response is viewed both as a structured process and as a set of organizational capabilities that enable these phases and support overall resilience.

### 5.1 Principles of incident response

Incident response in cybersecurity refers to the structured and coordinated actions organizations take to address unexpected cyber incidents (Naseer et al., 2024). It encompasses both technical and organizational processes, management practices, and the capabilities that enable timely and effective reactions (Shin & Lowry, 2020). Incident response capabilities refer to those organizational, procedural, and technical functions, such as situational awareness, coordination, recovery, and learning, that allow the incident response process to be carried out effectively.

While incident response is often integrated into cybersecurity frameworks and standards, its success depends on detailed preparation in advance and continuous, iterative improvement and learning from incidents (Garcia-Perez et al., 2023). This need for iteration echoes He et al. (2022), who emphasizes that moving from linear to agile response cycles enables feedback loops between phases and supports rapid restoration of critical assets. Agile incident response refers to this non-linear, adaptive execution of incident response phases. For the financial sector, the significance is amplified, as it is frequently targeted, while being expected to maintain the continuity of its services (van der Kleij et al., 2022).

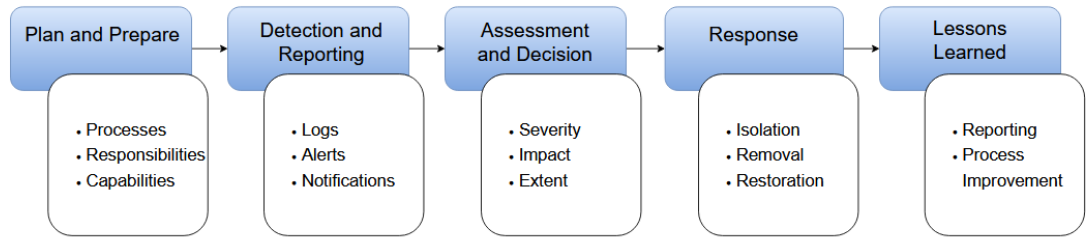
Financial institutions typically organize and structure their incident response through dedicated teams such as Security Operations Centers (SOC), Cyber Security Incident Response Teams (CSIRT), or Cyber Defense Centers (van der Kleij et al., 2022). These

teams can also be referred to more simply as Incident Response (IR) teams (Naseer et al., 2024). These teams are responsible for triaging, investigating, containing, and escalating incidents. The level of outsourcing of these teams to third parties differs in the financial sector. (van der Kleij et al., 2022). Collaboration between analytical and operational units remains a limiting factor as Naseer et al. (2024) observe that redesigning workflows between analytics and response teams could significantly improve situational awareness and containment effectiveness.

Effective coordination between such units and top management is essential, as leadership involvement has shown to directly correlate with higher levels of cyber risk management maturity and detection capabilities (ENISA, 2024). From the perspective of the European Cybersecurity Skills Framework, this underlines the importance of leadership roles where technical expertise as well as decision-making, governance, and communication competences are required.

ENISA has further highlighted the maturity gap in European CSIRTs, where alignment with internationally recognized practices remains low. The average EU score of 10 out of 100 in relevant indicators demonstrate that despite being well-integrated into international networks, structured certification and maturity remain limited. (ENISA, 2024) This contrasts with the dynamic capability perspective of Naseer et al. (2024), where mature institutions integrate sensing, seizing, and reconfiguring processes to adapt to rapidly changing attack conditions.

Several international standards and frameworks define principles and best practices for incident response. ISO/IEC 27035 is a three-part standard for information security incident management. It consists of principles of incident management, guidelines to plan and prepare for incident management, and for incident response operations. (ISO/IEC 27035, 2016) It has relevant and effective measures for the finance sector since incident response planning is considered the most effective and important organizational countermeasure for banking and financial services as it helps to ensure a timely and effective response to cybersecurity incidents (Darem et al., 2023). The standard introduces five-stage incident management process presented in Figure 7.



**Figure 7:** ISO 27035 Incident Management Process

The first stage of the incident management process in Figure 7, planning and preparation, is executed before incidents and the objective is for organizations to recognize the business environment they operate in, their own technical capabilities, processes and operations. Organizations need to plan how the operations should be protected, which responsibilities and roles need to be distributed, and what kind of training incident management requires for personnel. Detection and reporting contain the processes where anomalies are detected and how organizations detect them. These can contain log systems, alerting systems, and for example user notifications for logging in. Assessment and decision define the process by which organizations define which incidents are worth further investigation. Not all incidents are breaches or threats.

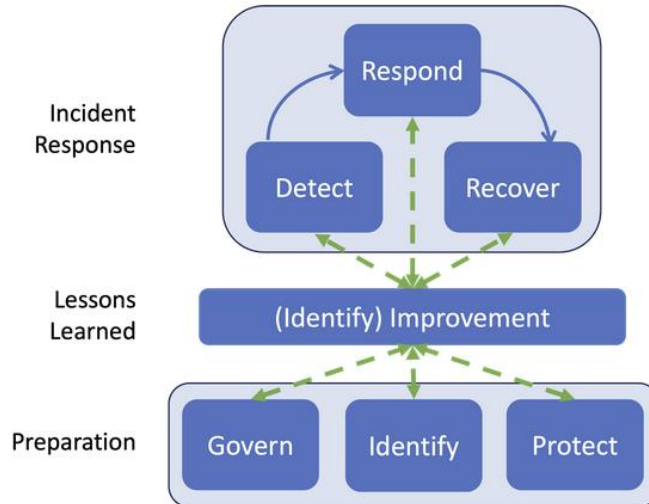
Assessment consists of severity, impact and extent of the incident which guides the decision of the organizations whether to react and in what way. This will lead to the response stage in the event of an attack. Organizations must have planned measures on how to respond based on the risk assessment. Response includes isolation, removal, recovery and communication with internal and external parties. The final stage is lessons learned consisting of post-incident analysis, reporting incidents, and responding to them to enable organizations to improve their incident management processes and develop their practices such as training and organizational capabilities. When interpreted strictly sequentially, these stages can limit the agility of incident response, even though the standard itself does not explicitly require a linear implementation (Shin & Lowry, 2020).

ISO 27035 instructs to construct an incident response plan which is documented plan for roles, processes and communication strategies in the event of an incident managing to disrupt operations. It also instructs to set up incident response teams, exercises, auditing, testing, and communication and coordination efforts with stakeholders. The operative actions in incident management the standard covers are classification and prioritization of events, technical investigation, coordination with internal departments such as legal and HR, restoration of the situation and recovery of services, and informing external

parties such as CERT and authorities. (ISO/IEC 27035, 2016) While the standard's approach to informing external parties is for them to be carried out when appropriate, in the financial sector this is absolutely essential. European frameworks and regulations emphasize threat intelligence sharing, and particularly in the financial sector, active communication.

Such linear models have also received criticism for discouraging real-time adaptation and learning, suggesting that incident response should incorporate iterative reviews even during ongoing crises rather than postponing analysis to post-incident phases (He et al., 2022). This shift from sequential execution to iterative adjustment is captured by the concept of agile incident response. Existing literature suggest incident response development should include predictive capability, automation, and continuous learning (Adetunji & Chinonso, 2025; He et al., 2022; Naseer et al., 2024)

Similarly, NIST among other notable institutions has contributed to incident response practices by developing Computer Security Handling Guide, referred to also as NIST SP 800-61r3. This was superseded by Incident Response Recommendations and Consideration for Cybersecurity Risk Management in 2025. The older framework consisted of preparation, detection, containment, eradication, recovery, and post-incident activity. The new model emphasizes a life cycle approach aligned with the NIST Cybersecurity Framework emphasizing continuous improvement and iterative processes. Compared to ISO 27035, this perspective stresses adaptability and integration into broader organizational processes. It also highlights that incident response capabilities are not isolated technical functions but are embedded in wider governance and improvement activities.



**Figure 8:** NIST Incident Response Life Cycle Model (Computer Security Division, 2024)

In the model displayed in Figure 8, the preparation activities are not part of the incident process itself. These activities can be recognized by NIST CSF. The preparation activities, govern, identify, and protect support incident response by developing and maintaining the wider organizational cybersecurity management. Incident response consists of detection, response, and recovery. All the incident response activity connects to improvement, also referred to as identification, which then enhances the supporting preparation activities. Improvement refers to need for continuous improvement which is achieved as all the activities provide lessons learned which are then analyzed, prioritized and used to improve all of the activities. (Computer Security Division, 2024)

Combining the adaptive life cycle logic of NIST with the procedural clarity of ISO 27035 could help financial institutions balance accountability with agility, as also advocated by Garcia-Perez et al. (2023), who link resilience to continuous learning and governance-level oversight. Cyber resilience can be understood as an organizational outcome that is enabled when incident response capabilities are both well-defined and enacted in an agile manner (Garcia-Perez et al., 2023). While ISO and NIST provide structured approaches, scholars increasingly argue that traditional, linear frameworks are insufficient for managing fast-evolving cyber threats (He et al., 2022; Naseer et al., 2024), as they lack the agility required in modern financial environments.

The literature suggests that the dynamic and evolving modern threat landscape requires a heightened level of cybersecurity awareness and more sophisticated incident response capabilities that can be enacted in an agile manner by financial organizations (Adetunji & Chinonso, 2025; He et al., 2022; Naseer et al., 2024). Incident response is not limited

to technical mitigation and structured reaction but increasingly relies on accurate situational awareness. Cyber Threat Intelligence (CTI) provides contextual information on adversaries' tactics, techniques, and procedures, thereby enabling more precise detection, faster containment, and improved prioritization of threats (Schlette et al., 2021). Integrating CTI into incident response processes can improve detection accuracy, provide shorter reaction times, and more effective containment strategies (van der Kleij et al., 2022). However, CTI is still underutilized in many organizations, often loosely integrated into response processes (Schlette et al., 2021). It can be interpreted to be part of building continuous improvement through analytics in the incident response frameworks and standards, but its ambiguous role can complicate design and implementation. Integrating threat intelligence and situational awareness into models not only strengthens detection accuracy but also contributes to the pervasive-learning capability described by Naseer et al. (2024), where threat profiling becomes continuous feedback mechanisms for adaptive defense. Incident response as a structured process is carried out through specific incident response capabilities, such as situational awareness, communication, coordination, recovery, and embedded learning (Naseer et al., 2024; van der Kleij et al., 2022), which must be enacted in an agile manner to cope with complex, evolving incidents. When these capabilities and agile practices are in place, they contribute to the broader organizational and sector resilience of the finance sector (He et al., 2022).

## **5.2 Recovery and business continuity in the financial sector**

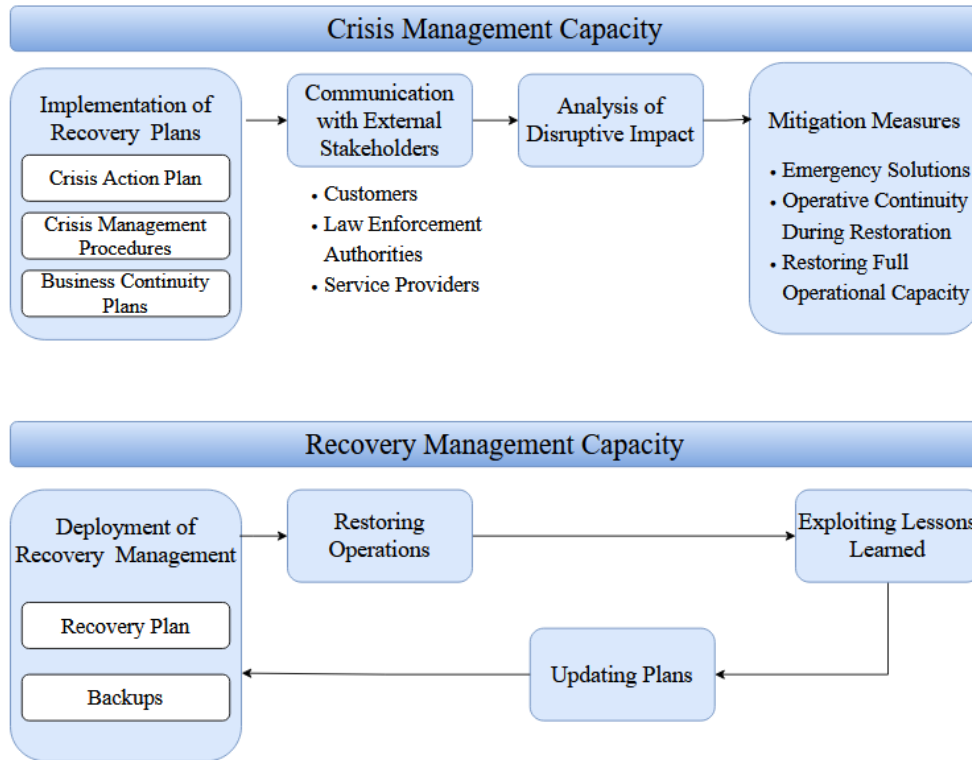
Business continuity in the financial sector is crucial, as both the national economy and critical infrastructure rely on its effectiveness (Iusan et al., 2020). As Iusan et al. (2020) note, the efficiency of integrated risk-management systems remains a permanent challenge, particularly when cyber and operational risks converge in critical infrastructure such as banking. Although financial institutions are often perceived as resilient due to their capabilities for continuous service, they are not invulnerable to threats (Carilo, 2023). Recovery and business continuity planning are not only a best practice but also a legal obligation.

The most important standard supporting this is the ISO 22301 standard for security and resilience, specifically business continuity. While not a cybersecurity standard, it complements ISO 27035 by offering a holistic approach to organizational resilience. It guides organizations with developing Business Continuity Management System (BCMS) with similar components to the ISMS displayed in Table 1. However, the scope gives a more comprehensive view of the entire business aiming to recognize the critical operations,

manage risks and incidents, recover from them as quickly as possible and continue operations despite disruptions. The standard sets out practical measures, including Business Impact Analysis to recognize critical operation and how they can be recovered, risk assessment to recognize which threats can disrupt operations, Recovery Time Objective and Recovery Point Objective to define tolerances for outages and data loss, continuity plans, exercises and testing. Whereas ISO 27035 focuses on incident detection and response, ISO 22301 broadens the perspective to ensure that essential financial services can continue despite disruptions.

Leo (2020) argues that business-continuity standards like ISO 22301 should evolve toward operational-resilience thinking, emphasizing adaptability, third-party dependency management, and systemic awareness, which is an argument reinforced by ECB (2025) requirements for proactive recovery planning and cross-providers testing. Operational resilience enabled financial institutions to recover from disruptive events (Leo, 2020) and in Finland, The FIN-FSA oversees the recovery and business continuity of the most important financial institutions under the supervision of the ECB.

These institutions include Nordea Bank Abp, OP Group, Municipality Finance Plc, and the Finnish branch of Danske Bank A/S (Finanssivalvonta, 2025). Due to the rise of cyberattacks, ECB has taken special notice of identifying and addressing resilience gaps in the event of cyber and other disruptions. Their yearly stress test in January 2024 included a hypothetical scenario in which all the bank's precautions failed, and a cyber-attack caused severe disruptions to its most significant databases and systems. This stress test particularly assessed the ability to respond to and recover from disruptions, not the ability to prevent them. (Finanssivalvonta, 2024) The results of these tests provide an indication of what is required in practice from financial institutions for a successful recovery. Figure 9 displays the interpretation of the reported requirements for success. The results recognized two vital capacities, crisis management and recovery management.



**Figure 9:** Crisis Management and Recovery Management Capacity of Financial Institutions

To succeed in recovery and maintain business continuity, institutions had to demonstrate their capacities illustrated in Figure 9. Crisis management capacity was needed from institutions, and it consisted of four different components. Institutions needed to have crisis action plans, internal crisis management procedures, and business continuity plans to activate during a crisis situation. Institutions had to communicate with all their external stakeholders, including customers, service providers, and law enforcement authorities. Institutions also had to analyze the disruptive impact of the crisis situation and implement mitigation measures such as emergency solutions to maintain operational continuity for the time required to restore the full operational capacity of its IT systems. (Finanssivalvonta, 2024) These capacities aligned with ISO 22301 and 27035, but it is noteworthy that cooperation with other financial institutions is not mentioned, even though the ECB emphasizes the role of collaboration in the development of incident response. On the other hand, it can be included in the recovery plans or communication strategies with external stakeholders.

The other necessary capacity was recovery management capacity which was needed in order to succeed in maintaining operations during testing. Efficient recovery management required the institutions to deploy a recovery plan and backups, restore operations,

and utilize lessons learned to update plans. (Finanssivalvonta, 2024) These capabilities can be assumed to occur at the same time and intermittently with the crisis management capacities. In the context of this thesis, these crisis and recovery management capacities are understood as part of the broader incident response capabilities that support organizational resilience in the financial sector. A permanent challenge for the management of institutions is the efficiency of an integrated risk management system even if it were in place. All aspects of the organizations should be taken into account both in terms of organizational functions and management. (Iusan et al., 2020) The iterative nature of these capacities echoes He et al. (2022) and Naseer et al. (2024), who both argue that agile post-incident processes shorten recovery cycles and reinforce learning.

### **5.3 Roles, coordination, and governance in incident response**

Incident response in the financial sector is not solely a technical process but also an exercise in organizational governance and coordination. Akinsulire & Ohakawa (2024) argue that fragmented accountability at the governance level weakens coordination which underscores that clear role definition is as critical as technical competence. Multiple actors, inside and outside the organization, must work together to ensure that response is effective, timely, and aligned with regulatory requirements (van der Kleij et al., 2022). Governance, coordination, and role clarity are therefore integral components of incident response capabilities rather than separate from the technical process.

The European Union has established the Systemic Cyber Incident Coordination Framework (EU-SCICF) to strengthen cross-border crisis coordination. The framework facilitates communication and coordination among the EU authorities and cooperation with key stakeholders at the international level when cyber incidents threaten the stability of the financial sector. (EU-SCICF, 2021) Designed for serious, large-scale cyber incidents and attacks, it is particularly relevant for the financial sector and other critical infrastructure where a single cyber-attack can cause systemic disruption across Europe and its member states. The main objectives of EU-SCICF are to enable common and rapid situational awareness of cyber threats across the EU and it aims to support decision-making and coordination between the EU and the private sector, and to ensure a coherent and coordinated response to systemic cyber disruptions. It has been established to complement, not replace national approaches and strategies. (EU-SCICF, 2021) The SCICF thus operationalizes Leo's (2020) concept of sector-wide operational resilience by institutionalizing cross-border learning and coordinated situational awareness.

EU-SCICF is most suited for systemic disruptions, such as massive DDoS attacks or cyberattacks on EU-wide payment systems or other attacks affecting several member

states in terms of scale and severity, requiring joint coordination. The framework consists of two different modes, non-crisis mode and crisis mode. During non-crisis mode the focus is on preparation and maintaining preparedness. Organizations develop and maintain documents, protocols, taxonomy and plans for crisis situations. (EU-SCICF, 2021) This dual-mode design reflects He et al. (2022) call for iterative adaptation as preparedness activities during non-crisis phases feed directly into real-time response improvement during crises.

They also exercise and test their procedures to ensure preparedness. Preparedness planning is maintained to establish an ad hoc team for crisis management. During crisis mode, the actors support each other, information sharing and crisis coordination are activated so that relevant and accurate information is exchanged among all stakeholders. (EU-SCICF, 2021)

Within financial institutions, coordination occurs three interconnected layers. The technical layers with SOCs and CSIRTs which are responsible for detection, containment, and forensic analysis (van der Kleij et al., 2022). This role is well-noted in standards and frameworks as presented in Table 3 below. Roles highlighting cooperation, compliance, and communication are also present functioning on an operational level. In addition, the strategic role of management in incident response has been recognized. The convergence between standards and legislation illustrates that effective incident response requires both vertical coordination, which links management and technical layers, and horizontal collaboration of teams, which He et al. (2022) identify as the principal advantage of agile approaches to incident response.

**Table 3:** Summary of Incident Response Roles in standards and frameworks

	ISO/IEC 27035	NIST SP 800-61r3	DORA & NIS2
Coordination	Incident Coordinator	Team Leader	Documentation of communication and schedule
Technical	Incident Responder	Technical Specialists	Risk Management and Assessment

Communication and Cooperation	Communication Officer	Legal & Compliance, Public Affairs	Reporting obligations to authorities and stakeholders
Management	Management and Decision makers	Management liaison	Management responsibility and involvement

The European Cybersecurity Skills Framework provides a useful lens for clarifying and developing the competences needed for incident response as it contains relevant profiles such as the Cyber Incident Responder for containment and eradication activities and the Cyber Threat Analyst for intelligence of prioritization and decision-making. However, it should be noted that ECSF does not take communication and cooperation into account with the same degree of precision as standards and legislation which focus on incident response and on the finance sector. The challenge is its universal interpretation codes do not take into account the important characteristics of the financial sector. Incorporating ECSF profiles into financial-sector organizations could address the behavioral gaps noted by Weickert et al. (2023), ensuring that habitual response routines and communication practices reinforce, rather than hinder, coordinated action. This further underlines that human roles and competences are central to shaping incident response capabilities in practice.

## 6. DATA COLLECTION AND ANALYSIS

This chapter introduces the data collection techniques of document data and expert interview data for empirical research. The inclusion criteria, datasets, and formulation of the interviews are presented. The thematic analysis approach is demonstrated using of examples that draw upon data.

### 6.1 Document data collection

The data collection in this study will combine document analysis and semi-structured interviews. These techniques will complement each other by providing both experiential insights from professionals and contextual understanding from official documents, reports and guidelines. These methods support triangulation and enhance the reliability of the findings (Shenton, 2004). Documents are never purely non-reactive because their production contexts and rhetorical functions matter (Karppinen & Moe, 2012). Pairing documents analysis with interviews makes those contexts visible and strengthens validity. This also ensures that the material reflects diverse perspectives and contexts (Billups, 2021).

Document analysis is used to examine the incident response of financial sector through news articles, standards, and public reports for the descriptive case study. Public narratives such as news coverage provide insight into how incidents are framed, communicated, and interpreted by stakeholders, thereby offering a complementary perspective to formal standards. According to Karppinen & Moe (2012), documents should be treated as artefacts with inscribed texts rather than neutral accounts. Therefore, the analysis focuses on how incident response is constructed and framed in public disclosures, rather than only on the factual contexts of the texts.

The purpose of this method is to provide a deeper institutional and contextual understanding of the environment in which cybersecurity professionals operate. This approach recognizes that, even in a highly regulated sector such as finance, standards and regulations do not just describe practice, they actively shape it by defining legitimate problem framings and acceptable responses (Karppinen & Moe, 2012). News articles construct the incident response process, communication, and the roles and different views on incident response in the financial sector.

Analyzing these documents ensures that the study aligns with industry standards and compliance frameworks. Treating documents as social products rather than as objective

sources (Karppinen & Moe, 2012) allows the analysis to capture how meanings and institutional priorities around cyber incidents are produced and circulated within the sector. This will also help to verify whether expert perspectives reflect broader industry practices and expectations. This method is particularly useful since access to internal processes is limited, as it allows the research to draw on publicly available, yet authoritative, materials to support both descriptive accuracy and analytical depth.

The document dataset consists primarily of publicly available news articles, public reports and decisions by FIN-FSA, and relevant international standards. These documents were selected to provide contextual background, illustrate public disclosure, and support the formulation of interview questions. The selection criteria were predefined to ensure transparency and reproducibility of the document analysis process. Purposeful sampling was applied, as suggested by Billups (2021), to ensure that documents were selected for their information richness and relevance to the research questions, particularly their potential to provide insight into the Nordea incident and related incident response practices.

The inclusion criteria were defined to ensure that the selected documents were relevant to the research context. Only documents published in English or one of the Nordic languages, Finnish, Swedish, Norwegian or Danish, were considered. The time frame for the article data collection was limited to documents published between September 2024 and December 2024, corresponding to the time period during which the events relevant to the case occurred and the media discussion was the busiest. The publication date of other documents, such as standards, was not relevant to the descriptive case researched.

Documents were excluded if they only referenced articles that were already included in the data and were completely identical in content, which is common in news reporting. Following Karppinen & Moe's (2012) caution that media texts are not entirely objective, attention was paid to their production context, origin, and rhetorical purpose to mitigate bias and reactivity during selection. Access to documents behind paywalls was obtained through institutional access. Expert comments, opinion pieces and analyses were also selected when published in reliable media, the expert was named by the media and had appropriate expertise to provide insight to the case.

A predefined set of search terms and keywords were used to identify relevant documents. Boolean search logic was applied where possible to increase precision. The queries included combinations of "Nordea", "Nordea palvelunestohyökkäys", "Nordea ddos", "Nordea disruption" and "Nordea överbelastningsattack". In most cases searching

“Nordea” during the selected timeframe provided documents discussing the case. The search terms were adjusted slightly depending on the platform or language used. The word for denial-of-service attack was translated into the language used by the local media.

Documents were collected from publicly accessible news outlets and databases in Nordic countries. These included national newspapers, online media archives, and professional news platforms. The main sources are provided in Table 4.

**Table 4:** Data sources of news article document data

Country	Media	Description	Number of documents
<b>Finland</b>	Yle Uutiset	National public broadcaster	34
	Helsingin Sanomat	Largest daily newspaper	16
	Tivi	IT and tech-focused news site	14
	Ilta-Sanomat	Popular tabloid newspaper	8
	Tekniikka ja Talous	Technology and business news	3
	Other	Nordea, Official announcements	10
<b>Sweden</b>	Aftonbladet	Popular tabloid newspaper	10
	SecurityUser	Cybersecurity focused news site	1
<b>Norway</b>	Aftenposten	Leading daily newspaper	1
<b>Denmark</b>	Finanswatch	Finance focused news site	2

The newspapers were accessed through online portals and ePress. All sources were selected based on credibility, regional relevance, and accessibility. In total 99 news articles were chosen for document analysis. As Table 4 shows, most of the news articles

were collected from Finland, where the largest number of sources discussing the case were available and where the research and research questions focus. However, foreign documents provide valuable comparisons.

In addition to media articles, the document data included formally approved standards and FIN-FSA's public reports and decisions. International ISO standards, which are also recognized as Finnish national standards, were included not only as theoretical reference points but also as empirical documents. These documents represent normative frameworks that guide institutional practices and serve as benchmarks for evaluating real-world procedures. Their role as theoretical constructs and practical governance tools makes them relevant for assessing alignment between institutional expectations and actual responses (Tuomi, 2018). Risk reports also published by selected Finnish financial institutions were included in the dataset. These reports provided insight into how banks publicly communicate their cybersecurity preparedness, roles, and recovery frameworks. They offered a structured view of the formal, institutional environment in which the studied incident response took place.

Each document was recorded in a structured format using a metadata table in Excel and Zotero. The use of predefined search terms, selection criteria, and metadata templates followed Billups (2021) recommendation that qualitative data collection tools should be designed, piloted, and refined before fieldwork to ensure consistency and transparency throughout the study. The metadata table is included in Appendix B for reference. This table supported both the systematic documentation of the material and the later stages of analysis.

## **6.2 Semi-structured interviews**

Semi-structured interviews were selected as a qualitative data collection method to complement the document data and enable an in-depth exploration of expert perspectives on incident response practices in the financial sector. This format combines a predetermined themes and set of open-ended questions with the flexibility to probe emerging topics which allows the researcher to adapt to the backgrounds of interviewees and to the direction of each conversation (Hirsjärvi & Hurme, 2022; Patton, 2023). Such flexibility makes semi-structured interviews particularly appropriate for investigating complex and dynamic environments where experiences, meanings, and institutional contexts intersect (Flick, 2021; Galletta, 2013).

Patton (2023) and Flick (2021) emphasize that semi-structured interviews are designed to understand participants' interpretations of events and the reasoning behind their actions, while the semi-structured format offers sufficient structure for comparability across participants and enough openness to pursue unanticipated insights. According to Saunders et al. (2019), this balance between structure and flexibility strengthens the credibility of findings by ensuring consistency while still encouraging elaboration. In this study, the semi-structured format allowed participants to discuss institutional practices freely while maintaining alignment with the predefined research themes derived from research questions, theoretical framework, and document data.

The interview guide was designed to follow Galletta's (2013) three-stage model of semi-structured interview flow. The opening should include establishment of trust and comfort with general and broad questions while a middle phase deepens discussion through targeted probing, clarifying questions, and tailored questions for participants' backgrounds. The concluding phase invites reflection and possible contradiction, and additional thoughts or final points from each participant. Recommendations by Hair (2023) and Flick (2021) for forming interview questions were taken into account as they guide how questions can be formed to guide the discussion while remaining open to interpretation. The main themes and subtopics were drawn from the theoretical framework and document data, ensuring that the interviews built upon prior findings rather than duplicating them. The interview guide is available in Appendix C.

The interview questions were not distributed in advance, although participants were informed of the themes prior to the meeting. Providing themes in advance was considered beneficial for directing attention to specific areas within the broad scope of incident response, while withholding detailed questions preserved the spontaneity and authenticity of the discussion (Puusa et al., 2020). This approach aligns with Flick's (2021) and Patton's (2023) recommendation to avoid over-structuring interviews, as doing so can constrain the emergence of new insights.

Interviews were conducted individually via Microsoft Teams due to flexibility and remote access. Literature suggests that online semi-structured interviews provide comparable depth and richness to in-person discussions, although they may take slightly longer to conduct (Hair, 2023; Saunders et al., 2019). Each interview lasted between 30–60 minutes and was recorded with informed consent. Participants were informed that recordings would be used solely for transcription and analytical purposes and would be deleted once no longer needed for the research. In total, 155 minutes of interview material were obtained. When permission to record was not granted, detailed notes were taken.

To ensure data quality, questions were tailored to each participant's expertise while maintaining comparability across interviews. Probing questions and purposeful pauses were used to encourage elaboration and reflection, a technique recommended by Hyvärinen et al. (2021) and Galletta (2013) to enhance narrative depth and contextual richness. The interviews were designed to explore incident response at a general level, rather than evaluating individual organizations or the Nordea incident. Establishing a relaxed and open atmosphere was prioritized to build trust and reduce desirability bias (Puusa et al., 2020). This could be a challenge in sensitive discussions, where cybersecurity is involved when going into detail.

Although no formal ethical review was required, ethical principles were observed throughout the research process. The study followed the guidelines outlined by Eriksson & Kovalainen (2008) and TENK (2019), including ensuring voluntary participation, informed consent, confidentiality, and protection of informants. Participation was entirely voluntary, and informed consent was obtained in writing and verbally before each interview. Participants were given genuine opportunities to decline without consequences, and no compensation or incentives were offered that might be interpreted as undue pressure or inducement to participate. Participants were informed of the study's purpose, the use of data, and their right to withdraw at any time.

Anonymity and confidentiality were safeguarded by avoiding the collection of personal identifiers. Participants were interviewed as individual experts in their field rather than representatives of their organizations. Their perspectives reflect personal expertise and experience related to the themes of the study, and do not represent the official stance of their employer. No personal information was collected, and identities of the participants and the research material were kept confidential. As Eriksson & Kovalainen (2008) stress, protecting informants' identities is a central obligation in qualitative inquiry. Audio files were securely stored and deleted after transcription and analysis, following the data protection recommendation of TENK (2019). If this study would have had beneficiaries, such as external financiers, all participants would have been informed as is ethically appropriate (Eriksson & Kovalainen, 2008; TENK, 2019). However, this study was conducted as an independent study without any external funding or assignment.

Informed consent includes relevant information of the study such as the research purpose, basic procedures, and the roles of interviewees and the researcher (Eriksson & Kovalainen, 2008). This information was provided via email upon contact and at the beginning of the interviews. Informed consent for recording was obtained both via email and before recording interviews. Informed consent includes also the information on the use of data as Eriksson & Kovalainen (2008) point out, and participants were informed

that the recording would only be used for transcription and analysis of the research material, it would be treated confidentially and deleted as soon as the transcription and necessary analysis have been completed.

The research also considered the relational context of the interviews. In some cases, participants were known to the researcher in advance. While this may have created a more relaxed interview atmosphere, it was also acknowledged that pre-existing relationships can shape how openly or critically interviewees share their views (TENK, 2019). In this study, interviews were generally characterized by a safe, respectful tone, allowing for both open and occasionally in-depth discussion of the topics.

The initial aim was to interview six experts with different backgrounds. Participants were identified by combining the researcher's networks, participant recommendations, and approaching relevant organizations. This approach was used to ensure that interviewees possessed relevant expertise in cybersecurity and the finance sector. Semi-structured interviews are especially effective when respondents are selected for their information-rich perspectives rather than representativeness (Patton, 2023). Six participants were interviewed, representing a diverse range of professional backgrounds, which was deemed sufficient to capture the variation required to support the document data. The number of interviews was assessed according to the principle of data saturation, meaning the point at which no new significant insights emerged (Saunders et al., 2019; Tuomi, 2018) The saturation threshold was reached after six interviews, as responses began to converge around consistent themes related to research topics. In total six professionals were interviewed, displayed in Table 5. The professionals had diverse backgrounds which gave versatile perspectives on the themes. For some interviewees, experience is only an estimate based on the interview discussion.

**Table 5:** Interviewees and their background information

Code	Background	Experience
I1	Academia	20+ years
I2	Consulting	<5 years
I3	Financial Institution	30+ years
I4	Financial Institution	10+in years

I5	Financial Institution	15+ years
I6	Supervisory Authority	10-20 years

### 6.3 Data analysis

The objective of data analysis is to identify issues that are pertinent to the research questions in both data sets (Tuomi, 2018). This allows conclusions about the phenomenon under study (Puusa et al., 2020). Data analysis of the research material will use thematic analysis as the primary approach for analysis. Thematic analysis is widely used and flexible method for identifying patterns, themes, and meanings within qualitative data (Saunders et al., 2019).

To enhance analytic rigor, reflexivity and transparency were emphasized throughout the analytical process. As Flick (2021) and Patton (2023) argue, qualitative interpretation is inevitably shaped by the researcher's prior understanding and assumptions. Therefore, reflexive notetaking and journaling were used to document analytical decisions. This practice increases the dependability of qualitative research by allowing others to trace how interpretations were derived (Saunders et al., 2019). Reflexivity also aligns with Braun & Clarke's (2006) reflexive thematic analysis approach, where the researcher's subjectivity is considered a resource for insight rather than a limitation.

A theme represents a meaningful pattern that captures something important about the data in relation to the research questions (Braun, 2022). Given the exploratory nature of this research, thematic analysis could offer a structured yet adaptable approach to identifying key insights from expert interviews and document material. The analysis technique fits the data collection techniques as well. The aim is not to test predefined hypotheses, but to allow themes to emerge from the data in a systematic yet flexible manner. (Saunders et al., 2019) This makes thematic analysis appropriate for handling complex, context-dependent material, such as expert reflection and institutional documents relating to cybersecurity roles and practices.

Initially, during the analysis, the areas of interest in the research were identified and grouped into categories. The categories are also combined to form broader categories from the subcategories that describe the material. (Tuomi, 2018) More precisely, the analysis will follow a six-phase model by Braun & Clarke (2006) for thematic analysis

1. Familiarization with the data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes
6. Producing results

The structured approach ensures rigor and transparency in the analytical process, while still allowing space for inductive insights to emerge from the empirical material. Following Saunders et al. (2019), the coding process was both data-driven and theory-informed, meaning that some codes emerged inductively from the data, while others were guided by sensitizing concepts identified in the literature and frameworks such as ISO 27035. As Morgan (2022) emphasizes, such a hybrid approach supports analytical depth by connecting empirical findings to conceptual understanding. In line with Billups (2021), iterative revising of earlier codes ensured internal consistency and that the list of codes remained aligned with the research objectives.

The first themes will be derived from document data, and recurring ideas or concepts will be coded and clustered under overarching categories that relate to the research objectives. The thematic analysis supports both depth and breadth in interpreting how incident response roles are constructed and practiced in the financial sector. The model by Braun and Clarke (2006) was first implemented on the document data so that the themes found in it could be used to design the interview questions and thus obtain additional material on themes important to the study in the form of expert interviews. The analysis process can be described as continuous, repeated, and circular dialogue with the data and pre-existing knowledge to create understanding and build a set of meanings for it (Tuomi, 2018). To improve trustworthiness, an explicit trail was maintained throughout the analysis, documenting coding decisions, category definitions, and theme revisions (Saunders et al., 2019). This systematic documentation enhances confirmability by allowing the analytic reasoning to be followed step by step.

The interviews were held via Microsoft Teams and recorded. The recording was exported for transcription and coding. Familiarization with the material was achieved through repeated readings and note-taking of both datasets. Swedish, Norwegian, and Danish material was carefully translated into English using back-translation and parallel automation tools to ensure translation accuracy. This was followed by generating initial codes based

on recurring ideas and meaningful units of data. To ensure interpretive accuracy, coded material was revisited at different stages and compared with earlier notes.

Coding was conducted manually and supported by tabular documentation to ensure traceability of interpretation. The codes were derived from sentences or short paragraphs in the data that presented distinct ideas, insightful findings, or relevant viewpoints to the research questions. There are no clear guidelines for coding in qualitative research, but the five important tasks of coding presented by Tuomi (2018) were taken into account during the coding process. The codes function as written notes as they structure what the researcher believes the material addresses, they serve as an aid in describing the text and as a tool for testing the structure of the material, and can be used to search for and review different parts of the material, i.e. they serve as an address (Tuomi, 2018).

For example, the sentence mentioned in D10, which was also discussed or mentioned in other documents was coded as “Management involved in crisis management and incident response”. The incident was so exceptional that it required much broader involvement from management and visible cooperation with authorities.

“The Economics Affairs Committee of the Parliament has summoned Nordea to a hearing on the problems of the online bank”

This was categorized under the broader theme of Leadership and the role of management, which sought to clarify the role of management in the incident and the division of responsibilities with authorities.

Another instance in the same document was coded as “Unclear role of regulation” under the broader theme of Regulation and responsibilities. The incident sparked much debate about the role of legislation and authorities in preventing such situations.

“Banks in Finland are supervised by the Financial Supervisory Authority, but the legislation on basic banking services is very general in terms of availability and quality, which makes it difficult to assess the adequacy of the availability of these services, Jussi Terho of FSA told Yle yesterday”

The next excerpt from D70 was coded as “Emphasizing unprecedentedness and scale” which was repeated several times when Nordea communicated the reasons for the prolonged incident. This is why it was organized under the broader theme of Significance of communication, as this communication style sought to maintain customer confidence.

“The Head of Personal Banking at Nordea, Sara Mella, emphasizes that the scale and volume of the attacks are unprecedented”

The following excerpt was coded from D87 was coded as “technical details of the attack”, which belonged to the subtheme “defensive and infrastructural weakness”, which belonged to the main theme Technological and structural challenges.

“It is unusual that a large portion of service requests have come from within the Nordic countries, which has made it difficult to combat them.”

These themes emerged across multiple documents and highlighted their importance in incident response of financial sector and enabled the discussion of the research questions. Providing clear examples of coding decisions strengthens the transparency of qualitative analysis (Braun, 2022; Saunders et al., 2019). These excerpts demonstrate how textual meaning was transformed into analytic categories and how interpretation remained anchored in the data rather than imposed from theoretical assumptions. This same process was applied to transcribed interview data. Table 6 provides a detailed coding example of this for the main theme of organizational resilience to increase transparency.

**Table 6:** Coding Example Table from Interview Data

Raw Excerpt	Initial Codes	Subtheme	Main Theme
<p>“Companies must have crisis management plans in place in case, for example a cloud service provider experiences security issues”</p> <p>“In a multi-vendor environment, cooperation must be established before incidents occur”</p>	<ul style="list-style-type: none"> <li>- Third-party risk identification</li> <li>- Multi-vendor co-operation</li> </ul>	Outsourcing management and third-party coordination	Organizational resilience and incident response
<p>“It does not make sense to keep forensic experts in-house, as they have work once or twice a year, and their skills need to be maintained”</p>	<ul style="list-style-type: none"> <li>- Balancing outsourcing</li> <li>- Cost-benefit of external expertise</li> </ul>	Balancing in-house and outsourced capability decisions	Organizational resilience and incident response

“Outsourcing must be balanced. What makes sense to buy from outside, and what should be kept in-house.”			
“The most important area for development right now is the use of third parties and the identification of risks involved in this”	- Reliance on third parties	Strategic dependency and risk visibility	Organizational resilience and incident response

As patterns began to emerge in the dataset, similar codes were grouped into candidate themes. During the reviewing phase, themes were assessed against the full data set to ensure internal consistency and external distinctiveness. Preliminary themes were first constructed based on the document data, but all the themes were validated and later refined also using the data from the interviews. The definitions and names of the themes were refined through iterative comparison with both datasets and the theoretical frameworks to ensure analytic fit (Braun, 2022). As Saunders et al. (2019) highlight, iterative validation enhances coherence between data, research questions, and emerging theory.

To strengthen transparency and reliability, each theme is supported by example codes and excerpts in Chapter 7. The coding framework was iteratively validated by comparing new codes with earlier ones and reflecting how well they fit the theme structure. Particular attention was paid to ensure that the codes were not overly descriptive but analytically meaningful so that latent patterns were reflected rather than only surface level content (Braun, 2022). Patton (2023) notes that qualitative rigor depends on moving beyond description to interpretation, connecting individual expressions to wider organizational and cultural patterns. Following Flick (2021), reflective questioning was used to test whether each theme contributed to new conceptual understanding rather than repetition of content.

Analysis of standards also provided normative reference points, allowing comparisons between actual practices and ideal models, especially regarding role clarity and incident handling structures. Thematic analysis served both as an interpretative and organizing tool, enabling systematic exploration of how incident response capabilities succeed, fail, and are demonstrated in the Finnish financial sector.

The quantification of data can enhance the value of qualitative research when the data set is sufficiently large to offer diverse perspectives on data interpretation and additional information about the results (Tuomi, 2018). This does not always apply in qualitative research when the data sets are too small, but the document data in the study was suitable for quantification. While the purpose of thematic analysis is primarily interpretive, presenting limited frequency counts can enhance transparency and provide an overview of data coverage (Saunders et al., 2019; Tuomi, 2018). Such quantification does not imply statistical inference but helps illustrate which issues appeared most frequently across the data and therefore warranted further interpretive attention.

Table 7 displays the quantification of the themes in document data. Main themes were derived from the subthemes and their codes and the frequency with which they appeared in the document data.

**Table 7:** Quantification of Document Data Themes

Main Theme	Subtheme	Example Codes	Frequency
Leadership and the role of management	Leadership taking responsibility	Leadership visibility during crisis	25
	Responsibility and accountability	Clarifying who is responsible	7
Significance of communication	Incident communications to the public	Customer reassurance	24
	Customer trust and reactions	Customer frustration	17
Regulation and responsibilities	Regulation expectations and oversight	Cooperation with FSA	15
Skills and ECSF Roles	Competence management	Unclear division of responsibilities	10
Technological and structural challenges	Defensive and infrastructural weaknesses	Technical details of the attack	34
Organizational resilience and incident response	Evolving operational environment	Geopolitical tensions	23
	Recovery from service disruptions	Lessons learned and improvement actions	20

## 7. EMPIRICAL ANALYSIS RESULTS

This chapter presents the results of the empirical analysis. The phenomenon is investigated through two complementary data sources, document data and interview data, introduced in Chapter 6. The analysis follows the thematic analysis approach as detailed in Chapter 6.3.

### 7.1 Document analysis

The document analysis revealed six central themes that reflect how incident response is shaped, governed, and challenged in the Finnish financial sector. These themes were developed through thematic analysis of institutional reports, relevant standards, and news articles about Nordea's DDoS attacks in September 2024. Each theme captures recurring patterns across multiple sources, linking empirical observations with theoretical and regulatory frameworks introduced earlier in the study.

#### 7.1.1 Leadership and the role of management

The first theme, **Leadership and the role of management**, describes how incident response during the Nordea case was framed as a leadership responsibility in organizational representation and public communication. Document data depict Nordea's senior executives as the primary public face of the incident as they express regret for service disruptions and provide reassurance to affected customers. In these accounts, management's role appears predominantly communicative and outward facing, whereas standards and regulations assign senior management a broader coordinating and accountable function. Frameworks such as DORA underline that responsibility remains with the institution and its senior management despite outsourcing and complex supply chains (Directive (EU) 2022/2555, 2022).

Parliamentary hearings further reinforced the expectation that major incidents require visible leadership engagement. Document data show that Nordea representatives appeared before both the Parliamentary Supervisory Council of the Bank of Finland and the Economic Affairs Committee, alongside several authorities including FIN-FSA, the Bank of Finland, and the National Cyber Security Centre. Media reports characterized this multi-party hearing as highly visible and institutionally significant, framing it as evidence that the incident was being addressed at the national level rather than as a purely technical disturbance.

“The Committee on Economic Affairs hear from Minister of Economic Affairs Wille Rydman (ps.) and representatives from the Ministry of Finance, the Bank of Finland, the Financial Supervisory Authority (FIN-FSA), the Financial Stability Authority, National Cyber Security Centre, Finnish Security and Intelligence Service (SUPO) and Nordea.” (D11)

Document data indicate that senior management played a central and highly visible role throughout the incident, particularly in public communication. Media coverage emphasized that Nordea’s executives reassured customers, explained the rationale for limited disclosure to avoid assisting attackers, and highlighted that professionals were actively working to maintain service continuity. Unlike in many international cases, no cybersecurity or information security officers appeared publicly in Finland. Instead, leadership assumed responsibility for external messaging and representation. Coverage also presented the incident as part of a broader pattern of attacks on Nordic banks, yet Nordea’s prolonged disruption in Finland received heightened attention. This framing positioned leadership not only as operationally accountable but also as responsible for reputational stewardship during the incident, especially as executives and public officials portrayed the attack as coordinated and international in scale (D43).

The documents also describe cooperation between Nordea and relevant authorities (D38). FIN-FSA emphasized that its role is supervisory rather than communicative, noting that any shortcomings would be reflected in its decisions under the Act on the Openness of Government Activities (D10, D57). The National Bureau of Investigation reported initiating a preliminary investigation into suspected telecommunications interference with international implications, which highlights coordination with domestic and international bodies (D57). Similarly, the National Cyber Security Centre commented that most attacks against banks do not become public or cause visible disruptions. These statements collectively reflect an institutional emphasis on legal compliance and investigative roles rather than public-facing crisis communication.

Taken together, the document data suggest that leadership and management were positioned as formally accountable but primarily communicative actors. Senior executives and authorities appeared visibly engaged, while the operational and coordinating aspects of management defined in frameworks such as DORA and ISO 27035 remained largely implicit.

### 7.1.2 Significance of communication

The second theme, **Significance of communication**, reflects a consistent perception in the document data that Nordea's public messaging during the incident was limited, ambiguous, and often insufficient for customers seeking clarity. Rather than presenting a steady flow of verified information, updates were described in media coverage as scattered and general, which contributed to uncertainty among users. This theme therefore illustrates the tension between institutional risk-management considerations, particularly avoiding disclosures that could aid attackers, and public expectations for clear and timely communication during service disruptions.

“Serious online banking problems that have been going on for more than a week have infuriated many of Nordea's Finnish customers. The malfunctioning online bank has caused people all sorts of problems, and several have said they are considering switching banks. Nordea's communication about the issues has been scarce. Customers have vented their anger on Nordea's social media channels, among others.” (D4)

Documents indicate that Nordea acknowledged the importance of clear communication to prevent customer uncertainty (D32). However, throughout September, updates remained limited. Nordea first informed Finnish media on 20 September that the continuing disruptions were caused by DDoS attacks combined with system updates (D48, D16). At this point, daily problems had been reported for more than a week and earlier issues already noted at the beginning of the month (D57). Although Nordea published disruption notices on its website, it declined to comment publicly despite extensive media attention. In contrast, Swedish media received earlier and more detailed statements on 16 and 19 September. Nordea informed Aftonbladet via email that login problems were caused by denial-of-service attacks coinciding with maintenance work, apologized for the disruptions, and stated that efforts to resolve them were ongoing (D22, D23, D24).

During the first weeks, media coverage repeatedly described the communication as scarce and ambiguous (D4, D10). Initial explanations attributed the disruptions solely to maintenance work (D17, D26, D27), and the unstable situation resulted in altering reports that problems had been fixed and then reappeared (D26, D27). Some customers stated that they received no information beyond what was reported in the media (D18), and several outlets argued that general statements about occasional disruptions did not meet reasonable expectations for customer communication (D61). Nordea responded that disruption notices were posted on affected platforms such as login pages (D32), although critics noted that these pages were often inaccessible during outages (D61). Nordea

justified its limited detail by emphasizing the need to avoid revealing defensive measures to attackers (D60).

Documents also highlight cross-country differences in tone and messaging. A Finnish press release on 23 September included an additional reassurance that customers' assets and information were safe, a statement absent from English-language versions (D37, D39). The Finnish version was signed by the Head of Personal Banking, whereas the English version was issued by the Chief Security Officer (D37). Across communications, Nordea repeatedly stressed that customer assets were not at risk, that most attacks had been repelled, and that the scale of the attack was unprecedented. Messaging emphasized the short-term nature of the disruptions, their linkage to maintenance and countermeasures, and that other Nordic banks were also targeted. The incident nevertheless received more attention in Finland than in other Nordic countries, even though problems reportedly continued in Sweden into December (D20). Nordea emphasized that 90 percent of malicious traffic had been blocked and that, across six weeks, total service unavailability amounted to 12 hours (D48).

By late October, Nordea's communication style shifted toward acknowledging the persistence of the attacks and the need for Nordic cooperation (D40). In response to criticism, Nordea maintained that any perceived ambiguity was necessary to avoid disclosing operational impacts to attackers (D48). At the same time, Nordea reported a dramatic increase in the volume of denial-of-service attacks. From 20 during the first half of the year to 360 in October alone (D12). Mid-October statements also suggested that a state actor might be responsible, arguing that the scale of resources involved made it unlikely that an individual perpetrator was behind the attack (D3, D32, D80). This unusual attribution drew considerable media attention, though it was later presented more cautiously. Investigative authorities and the chair of the Parliamentary Supervisory Council publicly described the attacks as unprecedented in scope, intensity, and duration, and consistent with an organized effort (D11, D57). In Danish media, Nordea's country manager commented that while no attribution would be made, previous attacks against the financial sector had been linked to Russia (D32). Subsequent Nordea communications no longer made direct accusations.

### **7.1.3 Regulation and responsibilities**

The third theme, **Regulation and responsibilities**, captures how document data characterized ambiguities in legislation, supervisory expectations, and accountability for service disruptions. Comments from authorities highlighted that although financial institu-

tions are supervised, legal standards for service continuity remain vague, making it difficult to determine whether the incident constituted a breach of regulatory requirements. The case occurred before DORA entered into force, but documents described how financial regulations, including cybersecurity requirements, often evolve during long-term IT system projects, such as Nordea's multi-decade core banking renewal, creating challenges in maintaining compliance with shifting EU legislation (D50).

Documents also criticized the fragmentation of cybersecurity regulations. While NIS2 applies directly to critical sectors, Finland does not have a comprehensive cybersecurity law covering all organizations, and the rapid increase in regulation can complicate understanding of legal obligations (D73). At the same time, IoT-related vulnerabilities raised questions about manufacturer responsibility since compromised Nordic devices were used in the attacks, and experts argued that ambiguous security standards make it difficult even for specialists to assess product security, enabling manufacturers to avoid investing in safeguards (D52). This was linked to the expectation that future EU standards would help correct these gaps.

During the incident, media repeatedly asked FIN-FSA how many disruptions banks are allowed to have. FIN-FSA stated that there is no strict legal limit, but recurring problems are addressed through continuous supervision and inspections (D27). Even prior to DORA, institutions were already required to notify FIN-FSA about disruptions, but the authority emphasized that it does not publicly comment on incidents because any short-comings would appear in its formal decisions (D10, D57). Documents noted that hundreds of online banking failures occur annually and that neither Finnish nor EU legislation defines an acceptable reliability threshold for online or mobile banking services, making intervention difficult (D84). Banking was repeatedly described in documents as a trust business, suggesting that market incentives naturally discourage prolonged disruptions.

Documents also highlighted gaps in regulatory expectations for adjacent services such as electronic identification. Traficom oversees eID services, yet there is no statutory requirement for their availability, and Finnish legislation defines a right to basic banking services without specifying quality or continuity levels (D84). FIN-FSA representatives noted that, in the absence of legal benchmarks for acceptable reliability, assessing whether service degradation warrants supervisory intervention is challenging. Although calls for clearer legislation were acknowledged, experts emphasized that defining such obligations in law would be difficult in practice. The overall picture presented in the documents is therefore one in which authorities require systems to be reliable and secure, but without concrete metrics against which reliability can be assessed.

FIN-FSA's investigation found no regulatory breaches or shortcomings in Nordea's practices, yet media reactions were strong. Although no customer funds or data were compromised, the service disruptions caused practical issues such as overdue payments (D18), and customers and experts publicly demanded greater responsibility from Nordea despite the institution operating within legal boundaries (D4, D18). Customers could file compensation claims, and Nordea reported receiving between 10 and 20 claims per day, which rose to over 500 by early October, and stated it would compensate for direct financial losses resulting from unavailability (D60, D64). Documents also noted that compensation is limited under law unless gross negligence occurred, which was not the case (D74).

The data further showed divided views on the seriousness of the situation. Some media reported that the disruptions significantly affected daily life (D18), while Nordea and representatives of the Bank of Finland noted that customers had not been unable to access banking services for an entire week (D25, D28). Nordea also commented that authorities were, ironically, relieved the attack targeted Nordea rather than a smaller bank, since a less-resourced institution might have faced outages lasting days (D48).

FSA can address recurring disruptions with warning and penalties. In 2023 it imposed several administrative penalties on S-Bank, including a €7.6 million fine for failing to address a vulnerability that enabled a significant theft and for a serious system weakness allowing users to access other customers' accounts (D84). This context reinforced the view that enforcement is possible, but only when clear legal obligations are breached. The media coverage does not directly indicate the severity of the incident, as this incident did not receive nearly as much attention as the Nordea incident did.

In addition, documents noted that Finland updated its national cybersecurity strategy in autumn 2024, indicating institutional recognition of these regulatory gaps and the need for more coherent guidance (D73). While this development was portrayed positively, commentators emphasized that the continuous expansion of cybersecurity legislation also increases complexity for organizations attempting to interpret and implement overlapping requirements (D73). This creates a dual challenge, insufficient clarity alongside regulatory expansion, which was presented as a structural factor contributing to uncertainty about responsibilities during large-scale disruptions.

#### **7.1.4 Skills and ECSF roles**

The fourth theme, **Skills and role clarity (ECSF)**, focuses on the institutional capacity to manage cyber incidents from a human capital perspective. While Nordea described

structured training programs and internal coordination models (D1, D2), there was little evidence of systematic alignment with European Cybersecurity Skills Framework (ECSF) or comparable competence models. This gap may hinder efforts to clearly assign, develop, and evaluate the roles involved in incident response. The lack of clarity of roles might also hamper communication and reduce trust when organizational communication is inconsistent and different parties communicate about the incident in different ways.

Across the Nordic region, documents identified a striking diversity of personnel speaking on behalf of Nordea. In Finland, the people responsible for giving statements included for example the two different Head of Personal Banking and Head of Communication, and the Head of Business Banking. In Sweden, Nordea's press contact was a Senior Communication Partner (D20, D23, D24), representative of Nordea's communications (D56) and a Senior Press Secretary (D21) and later statements were given by the CEO (D80). In Denmark, the incident was communicated by the country manager (D32) and in Norway by the Senior Communications Partner (D78) and the Chief Communicator (D80). The English announcements on Nordea's website were attributed to the Chief Security Officer (D37). However, these same statements were attributed to the Head of Personal Banking in the Finnish version. At the end of October, the President and Group Chief Executive Officer also commented the situation to media (D40). In addition to all this, Nordea's communications department provided situation updates to the media (D57).

While some degree of country-specific variation is expected in a multinational group, the number and diversity of roles involved in communication was unusually large. This fragmentation may have contributed to inconsistencies in tone, level of detail, and explanations provided to different audiences. Notably, no cybersecurity specialists appeared publicly in Finland, despite this being where the disruptions were most severe and where criticism of communication was strongest. As a result, individuals without technical expertise responded to questions about attack methods, defensive measures, and the interpretation of the disruptions (D24, D56). The lack of visible technical leadership stands in contrast with ECSF recommendations, which distinguish between communication roles, operational response roles, and strategic cybersecurity leadership. The document data suggest that these distinctions were not fully reflected in Nordea's public-facing structure during the incident.

During the incident, media covered that cybersecurity competencies within Finnish organizations have broader concerns. Human error and insufficient cybersecurity aware-

ness among staff were repeatedly described as major risks, particularly given the increase in cyberattacks targeting Finnish organizations over the past year (D36). Cybersecurity responsibilities remain disproportionately located within IT departments, and that embedding security awareness across organizational levels remains a challenge. This aligns with literature suggesting that human factors and organizational culture are central to incident preparedness.

The data also included a noteworthy example of evolving competence needs. Nordea was recruiting an expert in RACF security systems during September, despite having outsourced mainframe maintenance to IBM in 2019 under a €470 million contract (D56). This example illustrates a documented trend in which organizations seek to rebuild or reinforce in-house expertise in highly specialized areas that remain mission-critical during incidents. In the context of ECSF, this aligns with the need to maintain a balance between internal capability and outsourced functions, which is an issue that was visible throughout the communications and governance aspects of the Nordea incident.

### 7.1.5 Technological and structural challenges

The fifth theme, **Technological and structural challenges**, emerged from recurring references to vulnerabilities related to legacy infrastructure, system complexity, and recovery readiness in the Finnish financial sector. The data described the difficulties associated with defending a highly integrated, decades-old IT environment against modern large-scale cyberattacks.

Across documents, Nordea emphasized that it routinely repels cyberattacks without customer impact and that DDoS attacks are a known threat type (D28, D38). However, the institution stressed that the 2024 DDoS attacks differed from ordinary incidents due to their continually evolving patterns, large botnet involvement, and atypical distribution across Nordic IP addresses, which complicated detection and mitigation (D3, D32, D70). Nordea stated that the attackers changed methods throughout the incident and that the campaign displayed elements the bank had “never seen before.” This interpretation was reinforced by the Parliamentary Supervisory Council, whose chair described the attack as exceptional on a European scale (D42). Yet some commentators questioned the unprecedented framing (D49), noting that publicly reported attack volumes did not exceed the largest DDoS attacks documented globally in Cloudflare’s 2024 reports (Cloudflare, 2025). These contrasting views highlight how limited disclosure during incidents can hinder accurate comparison and feed uncertainty about institutional preparedness.

“Attackers used Finnish household appliances. Exceptionally, these attacks have come from Nordic IP addresses, which has made it difficult to combat. [The Head of Personal Banking] tells Turun Sanomat, that in practice the attackers have now exploited Finnish and Nordic devices and appliances connected to the network with weak protection.” (D3)

Concerns about preparedness were also reflected in external expert commentary. HiQ, a company specialized in DDoS defense, argued that Nordea “was not ready for the attack,” despite limited access to technical details (D48). Their CIO noted that while attack volume alone is not the primary challenge, diverse attack vectors and distributed sources across Nordic networks make filtering more difficult. He further suggested that reliance on traffic-blocking strategies such as geoblocking is increasingly outdated. At the same time, commentators acknowledged that only partial information is publicly available, and assessments are therefore necessarily constrained. Nevertheless, comparisons with Cloudflare’s capacity up to 200 million requests per second (D49), far above Nordea’s peak, indicate that scalable cloud-based mitigation could have reduced reliance on in-house defenses. Several documents noted that banks relying on private data centers face structural limitations since traffic filtering is more complex and less scalable than in cloud-native infrastructures (D92).

The incident also drew attention to structural characteristics of Nordea’s IT environment. As a result of decades of mergers and acquisitions, Nordea’s architecture consists of multiple layers of legacy systems, including IBM mainframes dating to the 1980s (D45, D50). These systems are renowned for reliability and security but are difficult to modernize, costly to update, and challenging to integrate with contemporary real-time payment and digital banking services (D45). Nordea has undertaken several large-scale renewal programs aimed at replacing or modernizing its core systems. One extensive reform launched in 2006 was discontinued after significant cost and schedule overruns (D56). A subsequent billion-euro project begun in the late 2010s aimed to unify fragmented systems into a modern digital platform; however, integration challenges have delayed completion, and the program was still underway in late 2024 (D56). These long-term transitions require phased migrations and iterative testing, increasing the likelihood of temporary mismatches between old and new components.

Documents noted that recent system upgrades were among the largest in Nordea’s history and involved transferring data between platforms, which can cause temporary account visibility issues (D45, D54). Nordea denied that the disruptions were directly caused by system upgrades (D54, D56) and stated that occasional malfunctions were the combined result of extensive DDoS attacks and reinforced defensive measures.

However, several sources suggested that legacy infrastructure inherently increases vulnerability by creating points of friction where modern applications interface with older systems (D45, D56). This aligns with FIN-FSA’s assessment that disruption causes are manifold in such complex environments, and that while DDoS attacks cannot be fully prevented by any single operator, planned system changes must be rigorously tested to avoid jeopardizing critical services (D27, D42).

Criticism also emerged from Danish media, which reported on a leaked document from 2020 claiming that Nordea had outdated hardware and shortcomings in disaster recovery testing, including an inability to perform failover tests for several years (D9). The document alleged that Nordea avoided failover testing due to risk of data loss and that a Danish data center had not been tested for scenarios such as power cuts. Nordea denied these claims and announced the data center in question was closed in 2021. The Danish country manager further noted that failover testing had indeed been lacking “a few years back” but stated that improvements had since been made (D9). FIN-FSA found no deficiencies in Nordea’s contingency planning or supervisory compliance (D8, D42), and therefore the allegations were not substantiated from a regulatory standpoint. However, the leaked report contributed to public debate about the adequacy of resilience testing in legacy-heavy environments.

Despite the controversies, the broader narrative across documents stressed the inherent complexity of the financial sector’s IT infrastructure. Financial institutions rely on systems that must maintain high reliability, strict security, and real-time processing capabilities. This operational environment constrains rapid re-engineering and creates long timelines for modernization. Through this lens, Nordea’s ongoing system renewal, described as one of the largest banking transformations in Europe since the financial crisis, illustrates the structural burden placed on major institutions attempting to reconcile decades-old architecture with contemporary cyber resilience requirements (D45, D56). The incident also highlighted sector-wide challenges, such as that banks continue to rely on mainframes for core processing, yet modern applications, cloud-based services, and international interoperability demand flexible, modular solutions that legacy systems are not designed to provide.

### **7.1.6 Organizational resilience and incident response**

The sixth theme, **Organizational resilience and incident response**, reflects how the documents portrayed Nordea’s and the wider sector’s ability to withstand, adapt to, and

recover from disruptive cyber events. This theme connects structural preparedness, procedural capacity, and contextual pressures that shape incident response in a rapidly changing threat landscape.

Document data revealed mixed perceptions of Nordea's preparedness. Experts questioned the technical explanations given publicly, and outlets noted that Nordea had experienced recurring mobile and online banking disruptions on most days over several weeks (D33). At the same time, Nordea consistently framed its response as evidence of resilience, repeatedly emphasizing ongoing investment in defense capabilities and the iterative strengthening of systems as attacks evolve (D37).

The disruptions affected not only online banking but also Nordea's authentication application (D13). Because bank credentials are the dominant method of strong authentication in Finland, customers were temporarily unable to access unrelated essential services such as government platforms. From a resilience perspective, this reflected a system-level single point of failure rather than a Nordea-specific technical limitation. Document data highlighted that authentication via the Mobile Certificate requires prior activation using bank credentials, making it unusable once disruptions began and unavailable to many users due to operator constraints. Customer support channels were also impaired, as chat services required online-bank authentication (D18).

Additional issues, such as disappearing account balances (D40), missing investment views (D64), sporadic card payment problems, ATM malfunctions, and difficulties in third-party service authentication (D57), illustrated how multiple interdependent services were affected. Not all issues occurred simultaneously as some were linked to DDoS activity and others to concurrent system updates, particularly in October. Nevertheless, the incident demonstrated that disruptions in one component of the digital banking ecosystem can cascade across essential public and private services, challenging assumptions about financial-sector resilience.

Nordea and external commentators also framed the incident as a catalyst for strengthening resilience. Nordea highlighted that its defense mechanisms had become "even more robust" as a result of the attacks (D32), and even critical voices acknowledged that the event would likely lead to improved defenses (D48). Nordea stated that thousands of updates and modifications are deployed annually, most invisible to customers, and that large-scale changes may occasionally require interruptions (D60). Nonetheless, documents also noted that service disruptions continued after the attack period, suggesting that the incident occurred amid broader infrastructural strain.

Sector-wide data contextualized Nordea's situation by showing that nearly half of Finnish companies had experienced serious cyberattacks within the past year (D36). While this survey did not focus on the finance sector specifically, it reflected a shift in the operating environment, including greater public concern and increased integration of cybersecurity into organizational strategies. Yet only half of surveyed companies reported having an action plan for cyberattacks (D36), underlining the unevenness of preparedness even as societal expectations rise.

Multiple documents linked the attacks to heightened geopolitical tensions, including Finland's NATO membership (D43), the war in Ukraine (D49, D92), and the broader increase in politically motivated cyber activity. Experts reported a dramatic surge in DDoS attacks across Europe in late 2024, with more than 900 attacks per week and an 86% annual increase (D51). In Finland the rise was lower but still significant at 23% (D51). Cloudflare's reporting indicated that DDoS attack strength has increased seventyfold during the war in Ukraine (D49), framing the Nordea incident within a wider shift from opportunistic disruption toward politically meaningful cyber operations.

Nordea repeatedly described the attack as intended to "undermine social peace" and create instability (D41). Members of Parliament similarly stated that the scale and persistence suggested state involvement. Although the group RootDos publicly claimed responsibility, experts doubted the attribution and suggested the justification offered was likely a cover story (D82). According to the National Bureau of Investigation, if state involvement were proven, the criteria for terrorist intent, such as serious societal fear or significant damage to critical infrastructure, could be met for the first time in Finland (D41). This reframing marks a significant shift because DDoS attacks have historically been characterized as digital vandalism, usually temporary and low-impact, but the Nordea incident revealed their increasing relevance as tools for geopolitical signaling and systemic disruption.

Although several major Nordic banks, including SEB, Danske Bank, Swedbank, and OP, were targeted during the same campaign, Nordea experienced the most prolonged and visible disruptions. Document data suggested contrasting interpretations. Nordea attributed the differential impact to its position as the largest Nordic bank and therefore the most attractive target (D32), while some experts questioned whether Nordea's existing system fragilities amplified the effects. The observation that the strongest attacks were reported in Sweden, despite lower public attention than in Finland, reinforces the need to evaluate resilience not solely through media visibility but through structural preparedness and recovery capability across institutions (D92).

Cybersecurity experts also cautioned that it is inherently difficult to assess an individual organization's resilience from the outside. They noted that given the volume of attacks targeting Finnish entities, the relative scarcity of large-scale disruptions indicates strong baseline resilience in the country (D92). However, Nordea faced recurring issues throughout 2024 and early 2025 (D46, D96), which may have shaped public perceptions and heightened scrutiny during the autumn incident.

## 7.2 Results of interviews

The interviews provided rich and diverse insights into incident response in the Finnish financial sector. The findings are presented corresponding to the themes identified in the document analysis. During the interviews, in addition to questions related to the themes, interviewees were asked preliminary questions about their work history and, for example, a general description of cybersecurity in the financial sector. The interviewees' descriptions of the financial sector were found to be very similar to one another, and consistent with the results of the literature review. The responses emphasized the high level of cybersecurity, heavy regulation of the sector, and the criticality of trust and business continuity.

“The financial sector is somewhat sensitive sector as it is highly dependent on information technology and is an obvious target for cyber-attacks, so they have been taking these issues seriously for many years. 15 years ago, when I conducted interviews there, it was clear they were all among the most progressive large companies.” (I1)

“Yes, in the financial sector, for example, cyber maturity and preparedness are at a much higher level [than in other sectors]. The financial sector is definitely one of the most mature I have seen.” (I2)

“One special trait that makes it different from a lot of other industries is that the financial sector is highly regulated. Also since this is a trust-based business, if customer data leaks somewhere else, it's unpleasant and embarrassing. But if it leaks here, it could mean the end of business in the worst case.” (I3)

“One special trait is that is a fairly well-regulated sector. There are a lot of national and EU-level regulation, as well as regulation within the industry itself.” (I4)

“I would say that in the financial sector, we are at a very mature level when it comes to information security in general and incident response has a long history with securing assets. I don't know how it compares to all other sectors, but among traditional industries, we are definitely at the most mature level.” (I5)

I6 also pointed out that there is much more IT expertise in the sector than is commonly understood. Many large organizations in the finance sector are large IT organizations themselves. The number of personnel can be very large. However, based on the interviews, it should be noted how much variation there is within the sector. It is not just a matter of size and personnel, but also of business model, revenue, resources, and even industry whether the company operates in banking, insurance, or pensions for example. Organizations vary greatly in nature, which can make assessing and comparing their cybersecurity capabilities rather difficult.

### **7.2.1 Leadership and role of management**

Leadership was consistently emphasized as critical to effective incident response. Academic and consultancy perspectives underline that top management must take accountability, both in public communication and in ensuring organizational structures remain functional during crises. The responses noted that management involvement depends on the size of the incident, in which case escalation plans play an important role as they should guide when management should be involved. The role of the management was described primarily as communicative, responsible for informing relevant parties.

“The upper management must be in line with the incident response team’s guidelines and their plans. But they also have to keep everything together, so they have their own ways of operating and must be clear as possible, especially in their communication role. And that also means ensuring that communication works internally and externally.” (I2)

Perspectives from financial sector confirmed that responsibilities are typically well defined in incident response. Incident response teams conduct the technical work while managers act as intermediaries, supporting communication with upper management and protecting the technical teams’ ability to focus and work in peace. This can be enhanced by interpreter roles that are needed between top management and technical teams to act as a link between them, understanding both sides, and helping management to gain an overview of situations (I3).

“Let’s say that (management support and role) stays far enough away from the situation and trust that the team will do the best they can, but then of course if there are big business decisions to be made, management is needed at the operational level to make those decisions.” (I5)

“It is important to respect incident management and crisis structures so that line management does not get confused in such situations. In my opinion, one important thing that reflects the maturity of an organization quite well is whether the incident management team is given trust and peace to work.” (I4)

Respondents emphasized that senior leadership involvement is not needed in all situations, as management’s role is mainly communicative and becomes critical in situations requiring cross-unit coordination. Responsibilities within the organization can be divided into major and minor incident management teams in some organizations (I4). However, risks remain if managers deviate from established crisis planning, potentially undermining trust and operational effectiveness (I4). DORA has reinforced management accountability by explicitly defining responsibilities. However, it has also increased complexity, as the responsibilities to keep multiple parties informed have increased and become more specific. This is not considered a challenge but rather a matter of prioritization, as it requires diverting personnel from maintaining normal operations during incidents to complete time-consuming reporting templates. Overall, the interviews highlighted the need for escalation plans clarifying when senior management must be involved and ensuring they are aligned with pre-defined incident response plans.

## **7.2.2 Significance of communication**

Communication emerged as both a technical and a reputational imperative. Respondents noted that financial institutions operate based on trust where customer confidence can erode quickly if communication is inadequate or ambiguous (I1, I3). Internal, external, and regulatory communications were deemed important. In internal communication, keeping relevant parties informed is essential for effective incident response (I2).

Interviewees highlighted the importance of pre-defined communication guidelines and exercises, determining who communicates with the media and stakeholders in different scenarios. The size and severity of the incident affect who is managing communication with stakeholders, for example communications, Chief Information Security Officer or even Chief Executive Officer.

“We have pretty clear roles and processes for [communications] which we have practiced. It depends a bit on the case whether there is a representative of communications talking with the media or does CISO give a statement. Or does even CIO or CEO need to give a statement.” (I5)

“We are part of market infrastructure, so we don’t have direct personal customers, but we have template check list in incident response which we then go through:

external communication, internal communication, and if there are customer effects then it is always communicated. That is always case-by-case.” (I4)

The need to balance openness and discretion was also mentioned, warning against both under-communication and unnecessary disclosure. Communication strategies seem case-dependent. Sometimes incidents are reported as technical disruptions, sometimes suspicion of cyber incident is communicated immediately but it depends on the situation at hand (I4). Overall, the communication of the finance sector was described as good (I1). Interviews also revealed criticism of communication in the financial sector, for example in cases of fraud or phishing attacks, which is perceived to describe incidents in a way that blames its customers and avoids accountability. Several interviewees noted that communication responsibilities usually rest with senior management or communication professionals rather than technical experts.

Stakeholder trust was identified as fragile yet crucial for business continuity. Attempts to conceal incidents could have severe reputational consequences, while transparency when paired with timely and accurate updates was seen as essential. Effective internal communication and control of the information flow can also prevent information leakage from the inside to the outside, which can be particularly damaging to reputation and trust (I2).

### **7.2.3 Regulation and responsibilities**

The regulatory environment was described both as a driver for resilience and a source of burden. All respondents acknowledged the sector’s high degree of regulation, several even used it to describe the significance of cybersecurity and incident response in the finance sector. Several interviews noted that Finland was already ahead of many requirements of DORA and already following the industry best practices (I3, I4). The reason for this was most of the requirements in DORA had previously been implemented from ECB guidelines or from the sector’s best practices. DORA made previous recommendations into mandatory regulations from the perspective of the finance sector.

“Well, there haven’t been that many new developments. It’s more a matter of basic principles, I would say, that if we had done things according to best practices, then they should have been done that way before at some level. However, our cooperation with our European colleagues has become closer because we have the same concerns.” (I3)

DORA introduced few genuinely new practices. However, it improved the overall cybersecurity by making recommendations mandatory, which affected especially smaller organizations. It was assessed that this was also influenced by Finnish legislation, which defined the finance sector critical to security of supply, resulting in broader development of the sector rather than focusing solely on banking (I3). It was also recognized that DORA has increased cooperation within the industry, as organizations discuss how they have interpreted its various requirements (I3). However, reporting duties were updated and identified as resource-intensive, occasionally diverting attention from incident handling itself (I4). Views on regulation diverged as some respondents argued regulations were essential in ensuring preparedness of the sector and mandating investment in resilience as they act as a driving force for cybersecurity development in the sector, while others noted ambiguities in interpretation and overlapping obligations that overcomplicated compliance.

“I can’t say whether there are any shortcomings in the regulations. It feels that the financial sector is heavily regulated, and let’s just say that perhaps there is no lack of regulations specifically on the reporting side.” (I5)

“Regulations are driving organizations to consider cybersecurity but on the other hand, the clarity of regulations is sometimes a challenge, as is how they actually achieve their objectives.” (I2)

The supervisory authority interviewed also mentioned this perspective as their role is to supervise what has been done, not how it has been done. The interviews mention that the regulations are not very specific, which is good in the sense that they are not unnecessarily detailed, difficult to implement, or require unreasonable investments. On the other hand, they may not necessarily achieve their objectives, as organizations can show that they comply with them and thus prove that their cybersecurity is on a sufficient level, but this does not necessarily improve cybersecurity in practice (I2).

Smaller organizations were speculated to struggle more with regulatory demands (I1). Despite these challenges, the consensus was that regulation ultimately strengthens resilience by enforcing a baseline of preparedness and ensuring management engagement, as well as harmonizing the application of best practices in the sector. The overlap between regulations is also a challenge from both the academic and supervisory perspective (I1, I6). This can make it difficult to assess what constitutes as enough, as regulations are not intended to be overly strict and watertight either.

## 7.2.4 Skills and ECSF roles

The interviews revealed generally strong recognition of skill requirements in incident response, though some gaps exist. Larger financial institutions maintain internal SOCs and CERT functions. However, highly specialized forensic expertise is often outsourced, as maintaining such skills in-house is not feasible given the rarity of large incidents (I4, I5).

“If very advanced forensic experience is needed, it doesn’t make sense for us to have it in-house, because those guys don’t really have that kind of work more than once or twice a year. So that they can even keep their skills up to date, it makes sense to buy this kind of work as outsourced.” (I4)

Respondents emphasized the necessity of technical expertise in incident response (I4, I5), particularly for understanding system architecture and having developed situational awareness of cybersecurity. At the same time, management and communication skills were viewed as equally important to support incident response. Training was described as proactive and continuous, with staff trained even with tailored courses as soon as skill gaps were identified (I5). As the sector is well-resourced, it enables rapid and efficient response to recognized training needs (I5, I6). This is likely most feasible in large, well-resourced organizations.

“[The finance sector] develops skills very actively. I would argue that the financial sector has more resources and interest in developing its own personnel and expertise in-house. However, quite a few actors rely on external actors when it comes to incident response.” (I5)

Roles identified aligned with Table 3 summary of roles and responsibilities appearing in widely used standards and frameworks. In addition, the special role of forensic experts in serious incidents was noted, which is described in more detail in ECSF framework. The Supervisory Authority also recognized that the small size of Finland limits the expertise available and partly explains the lack of specific expertise. An example of this was operational risk management experts who have advanced IT skills and knowledge, and in addition, expertise in cybersecurity risks.

The supervisory authority also recognized that the finance sector has strong and advanced IT skills. However, relying too heavily on outsourced expertise can create challenges for continuity management (I2, I6). The use of project-based consulting services can pose challenges for the development of sustainable long-term cybersecurity and incident response. This issue was not recognized as a concern among interviewees with well-developed internal capabilities.

## 7.2.5 Technological and structural challenges

All interviewees consistently pointed out legacy systems, system complexity, and extensive outsourcing as the primary technological and structural challenges. Respondents from financial institutions noted that some systems are only understood by a handful of individuals, creating possible single points of failure and complicating recovery. This can also lead to tacit knowledge to accumulate.

“Challenges in incident response in the sector include, for example, technology debt, lifecycle management, and strong ownership through the (supply) chain, which are certainly pain points for many.” (I3)

“Perhaps the most common challenges relate to finding the right owner of the asset. For example, who knows best about a server’s operations.” (I5)

“The complexity of the systems and the fact that many organizations have a lot of legacy systems of all kinds can make it difficult to form an overall picture of the situation. Especially in large organizations, it can be difficult to keep track of the big picture when, for example, a lot of system integrations have been made.” (I4)

The diversity of IT infrastructures and multinational operations were also mentioned as barriers to coherent recovery. It was also noted that failures should be interpreted as process breakdown rather than individual mistakes or technical failures, given the complexity of organizational networks. Large incidents could be better described as logistics issues than purely technical issues as large recovery operations just might need extensive amount of personnel (I3).

“Actually, almost always, the biggest technical challenge is posed by third parties and the outsourcing of services. Identification of risks is important and has previously led to incidents in the sector.” (I2)

Outsourcing was identified as both necessity and vulnerability. While external vendors provide essential services, resilience depends on visibility into the supply chain, robustness of contracts, and clear division of responsibilities (I2, I6). The supervisory authority also underlined that everything else can be outsourced, except responsibility. Exercises and simulations were regarded as crucial for testing these complex interdependencies before real incidents occur.

## 7.2.6 Organizational resilience and incident response

Organizational resilience was framed as both a cultural and structural capability (I1, I3). Respondents highlighted the importance of embedding resilience into everyday practices, ensuring it is not treated as a one-time project (I1, I3, I4). Resilience was described as supported by documentation, scenario planning, and sector-wide exercises. Important factors in developing resilience included mapping and understanding the organizational IT infrastructure, support and maintenance management, contract management, and managing how resilience requirements apply to service providers (I3).

Several respondents mentioned that resilience cannot rely on technical measures but requires management commitment, investment, and integration into the broader risk management system of the organization. Exercises and simulations were repeatedly emphasized as critical for revealing weak points and ensuring that roles and processes remain functional under pressure.

“Good instructions and clear roles (support resilience). Everyone know what their responsibilities are and we’ve practiced different scenarios. We are involved in attack exercises, and we also try to include business to them. Also, involvement in industry-specific exercises is important. Incident response is a process and well-done IT in practice. It could be exaggerated like this that information security is just well-done IT.” (I5)

Sector-wide cooperation during incident response was described as particularly advanced in Finland, with information-sharing networks, including informal messaging groups, enabling rapid coordination and mutual support during incidents (I3, I4, I5). This collaborative culture was seen as a major contributor to resilience, ensuring that even competitors act as partners in cybersecurity crises. There is room for further development, as there have been attempts for years to create a formal channel for sharing threat information (I3).

“It would benefit the whole sector if there was somewhere we could exchange threat information with each other. There is all sorts of problems with it as not one company can host for all others and there is not yet an authority for it and there are some bureaucratic challenges involved.” (I3)

The supervisory authority mentioned that unexpectedness is the greatest challenge of incident response in the sector, meaning situations that have not been prepared for or that are far beyond expected scale. Scenario analyses must be adequate. They are required, but their adequacy is not assessed, which means that the organizations’ analyses

may in reality be only superficial. The sector needs an understanding of what organizations are prepared for and where gaps remain.

Several interviews also highlighted outsourcing as a challenge for the sector when it comes to resilience and continuity management. For example, the supervisory authority noted that organizations should have more carefully planned supply chain management that takes better account of what happens if the service is discontinued or the supplier decides to pay contract penalties rather than comply with agreements, as outsourcing brings both good and bad outcomes. One of the greatest challenges in resilience and continuity management was identified to identify their own single points of failure (11).

## 8. DISCUSSION

This chapter answers the research questions using empirical results from both results with literature. The chapter examined where the datasets support, contradict, and expand each other as well as the literature explored through systematic literature review.

### 8.1 Current state of incident response practices in the Finnish financial sector

The Finnish financial sector demonstrates a high degree of cybersecurity maturity, yet the empirical findings reveal that incident response capabilities remain unevenly distributed and partly constrained by structural, communicative, and regulatory factors. This highlights that maturity at the systemic level does not automatically translate into organizational resilience.

Both empirical datasets converge on the view that Finland's financial institutions possess advanced prevention and detection capabilities, supported by extensive regulatory oversight and well-resourced ICT infrastructures. This is also supported by FIN-FSA's public documents, according to which it has rarely had to issue decisions on cybersecurity in the financial sector in recent years. However, the Nordea case and interview insights indicate that response and recovery processes are still challenged by fragmented communication, legacy systems, and limited learning integration, confirming earlier research suggesting that even a mature sector may struggle to operationalize resilience in practice (Björck et al., 2015; He et al., 2022). These challenges are interpreted as weaknesses in specific incident response capabilities rather than as a lack of technical maturity.

Communication practices further illuminate this gap between technical and organizational maturity. Documents highlighted fragmented and sometimes contradictory messaging during the Nordea incident, while interview data stressed the importance of predefined communication roles and internal control of information flow. This contradiction reflects what Varga et al. (2021) identify as the sector's central paradox, high technical competence coexisting with weak external transparency. The reluctance to disclose details was justified by the risk of aiding attackers, yet such discretion was perceived by the public as evasiveness, undermining trust which is a backbone of the financial market (Uddin et al., 2020). The comparison therefore extends the literature by showing that communication failures during cyber incidents can erode confidence more severely than the incident itself, particularly in highly digitalized banking environments where service continuity is equated with societal stability. These findings underline that communication

is not merely an external PR function but a core incident response capability that directly influences perceived resilience.

Technological and structural challenges persist despite advanced preparedness. Both datasets underscored the burden of legacy core-banking systems and complex supplier networks, which amplify recovery difficulty and blur accountability. The literature similarly associates such technical debt with resilience vulnerabilities (Carilo, 2023; Darem et al., 2023). Interviewees described difficulty in maintaining situational awareness across multiple integrated platforms and emphasized that outsourcing, while necessary, introduces dependencies that complicate incident coordination. The supervisory authority confirmed that everything can be outsourced except responsibility, reinforcing ECB (2025) guidance on contractual accountability. This alignment with prior research demonstrates that resilience increasingly depends not only on technological defenses but on incident response capabilities related to supply-chain governance and institutional learning from breakdowns.

Resilience culture in Finnish finance appears strong but unevenly embedded. Interviews described active participation in national and sector-wide exercises, informal threat-information exchange networks in the sector, and proactive training. Yet both data sources reveal that scenario analyses often underestimate unexpected, large-scale or prolonged incidents that fall beyond tested boundaries. The Nordea case thus illustrates that learning integration was limited. In practice, this also limits the development of embedded learning as an incident response capability.

The Finnish financial sector exhibits a paradoxical combination of formal maturity and limited adaptive capability. Governance structures, regulatory compliance, and technical defenses are highly developed, yet cultural and procedural agility in incident response remain limited. Finnish financial institutions demonstrate high preventive maturity but uneven operational agility in incident response. Structural dependencies, communication fragmentation, and limited learning integration constrain the sector's overall incident response capabilities, and consequently, their resilience.

## **8.2 Comparison with frameworks and best practices**

The comparison between the empirical findings and existing cybersecurity frameworks and standards reveals that Finnish financial institutions largely adhere to the spirit of international best practices but fall short of implementing them in the systematic and accountable manner envisioned by those frameworks. While interviewees consistently emphasized that DORA does not change anything substantial because the sector largely

already follows international best practices, the document data demonstrates that the practical application of these standards remains uneven, especially in communication, accountability, and post-incident learning. This gap invites a critical reflection on whether adherence to formal frameworks equates to genuine resilience in practice, or whether resilience depends on how incident response capabilities are enacted in real incidents.

According to the NIST CSF and ISO/IEC 27035, effective incident response encompasses preparation, detection, analysis, containment, eradication, recovery, and post-incident activity. Evidence from both datasets shows that Finnish financial institutions perform strongly in the preventive and detection phases. Interview data emphasized extensive monitoring capabilities, active participation in national exercises, and integration of threat intelligence into routine operations. These findings support previous research suggesting that Nordic financial entities demonstrate advanced detection maturity and inter-organizational cooperation (European Union Agency for Cybersecurity., 2025). However, the later stages of the incident response life cycle, particularly response, recovery, and post-incident learning, appear less consistent with the frameworks' intent, which raises the question of whether compliance-driven maturity adequately translates into agile and effective incident response when confronted with complex incidents (Computer Security Division, 2024).

The Nordea incident illustrates this misalignment clearly. While service continuity was sometimes restored quickly, the public communication was delayed, fragmented, and largely defensive in tone. This diverges from industry best practices and the necessary capabilities recognized by FSA which are essential for recovery and business continuity (Finanssivalvonta, 2024). Most frameworks stress stakeholder communication, accountability, and timely dissemination of verified information as integral to response effectiveness. The absence of a named accountable security officer in Finland contrasts sharply with best practices and with Nordea's Swedish operations, where incident briefings were more detailed. This gap suggests that formal alignment with framework requirements may serve symbolic legitimacy more than functional resilience, reflecting what Varga et al. (2021) describes as a tendency in the sector to prioritize reputation management over knowledge sharing during crises. The comparison suggests that while frameworks formally recognize communication and accountability as integral to incident response, these capabilities were not fully realized in practice, which weakened the contribution of incident response to overall resilience.

In terms of governance, ISO 27035, DORA, and NIST SP 800-61r3 emphasize the need for clear leadership structures and defined responsibilities during incidents. Interview confirmed that escalation mechanisms and internal playbooks exist, yet these are often

treated as compliance artifacts rather than dynamic operational tools. This interpretation supports Cortez & Dekker's (2022) argument that financial institutions frequently reduce governance frameworks to checklists, limiting their potential as mechanisms for organizational learning and agile incident response. This contrasts with some of the perspectives from the interviews, where structured processes and checklists were seen as an enabler for effective incident response when used dynamically.

Regulatory frameworks such as DORA, the EBA ICT guidelines, and the ECB's expectations have further institutionalized incident response in the Finnish financial sector. However, these regulations appear to reinforce procedural compliance rather than adaptive capability. Interviewees repeatedly stated that the requirements were already mostly met before DORA, suggesting that Finnish institutions perceive regulations as confirmation of their existing practices. Yet the Nordea case exposes limitations of this perception. While compliance metrics were fulfilled, the response lacked the clarity, accountability, and cross-border coordination that DORA aims to enforce. Although DORA was not yet in force during the Nordea incident, the interviewees emphasized that the sector already followed many of its forthcoming requirements through existing best practices, excluding new procedural elements such as reporting timelines. This contradiction between formal alignment and operational gaps reflects Peihani's (2022) notion of being secure on paper but not necessarily resilient in practice. In other words, regulations have helped standardize the existence of incident response processes but not necessarily the agility and effectiveness of incident response capabilities in dynamic conditions.

From a theoretical perspective, the findings both confirm and extend prior studies on the relationship between institutional maturity and adaptive response. Consistent with He et al. (2022), the data suggests that high technical preparedness can coexist with limited strategic flexibility and lack of agility in incident response processes. However, this study extends on the discussion by providing sector-specific evidence from Finland that even when frameworks are embedded at the policy level, their interpretive application varies depending on organizational culture and perceived reputational risk.

While Finnish financial institutions appear aligned with the principles of leading cybersecurity frameworks, their current arrangement may prove insufficient in unprecedented or large-scale situations. The implementation of them might often prioritize compliance visibility over the adaptive and communicative dimensions of incident response. The Nordea incident underscored that even highly mature organizations may falter in transparency, accountability, adaptability areas central to best practice. This research contributes to the literature by highlighting that framework adherence does not guarantee resilience, rather, the effectiveness of incident response depends on how frameworks

are internalized and enacted through concrete incident response capabilities and agile practice in real incidents.

### **8.3 The Role of the European Cybersecurity Skills Framework**

The European Cybersecurity Skills Framework (ECSF) provides a comprehensive structure for defining cybersecurity roles and competencies across organizations. Although it has not yet been widely adopted in the Finnish financial sector, the findings suggest that it could serve a valuable tool for clarifying responsibilities, managing outsourcing relationships, and improving communication and accountability in incident response.

Both document and interview data indicate that roles in the Finnish financial sector are currently defined through standards and regulations rather than through the ECSF. They are currently more in line with the roles presented in Table 3 in Chapter 5. This observation aligns with assessment of ECSF (Polemi & Kioskli, 2023), which note that the framework's uptake has been limited across sectors despite its potential to harmonize competence requirements.

Across both datasets, ECSF was not explicitly recognized as a guiding structure. Interview data revealed that incident response roles are already well established within financial institutions, typically reflecting regulatory expectations and industry best practices. During the Nordea incident, several executives commented publicly on the situation, yet no clear technical or security took visible responsibility. This pattern contrasts with the ECSF's approach, which emphasizes clear role definition and accountability chains extending from technical experts to strategic management. This also contradicts with the interview data results suggest that the Chief Information Security Officer often has a communicative role. However, the ECSF does not precisely define the communicative role and responsibility for stakeholder communication (European Union Agency for Cybersecurity., 2022b), which can be considered a major limitation especially in terms of its utilization in incidents similar to the Nordea incident. Clarifying these responsibilities would directly strengthen communication as an incident response capability.

On the other hand, it should be noted that there were discrepancies in the interview data about communication responsibility. Some emphasized the role of the CISO, some of senior management, and some of communication professionals. Consistent in the interview data was that roles and responsibilities should be clearly defined and exercised beforehand. Document data suggests that technical details cannot be completely ignored in cybersecurity communication, especially when ambiguity has already led to mistrust and narrative has been captured by the media. By contextualizing existing ECSF

roles such as the Cybersecurity Manager or Cyber Incident Coordinator, financial institutions could adapt the framework to incorporate communication accountability and stakeholder engagement. This adaptation would address one of the key deficiencies observed in the case data, the absence of visible, technically competent spokespersons capable of rebuilding trust during high-profile incidents.

Interview data confirmed that while institutions maintain skilled internal teams, specialized areas such as digital forensics are almost always outsourced due to their infrequent use and high expertise requirements. In addition, it must be taken into account that even though all participants had highly skilled internal incident response teams, they do not represent the entire finance sector which has been criticized for heavy outsourcing.

This finding however expands on the repeated perspective in the literature, where finance sector is criticized for excessive outsourcing (Clausmeier, 2023; Darem et al., 2023). Outsourcing can be a strategic decision in competence management, as long as risk management is also involved. This reliance on external providers highlights an area where the ECSF could support outsourcing management by offering a shared vocabulary for defining required competencies and responsibilities across organizational boundaries. This could enhance contract management of outsourcing, which is an important development area identified by the ECB (ECB, 2025), and would support more coherent governance in incident response capabilities.

The ECSF's role-based structure could help bridge the gap between internal and external expertise. Interviewees expressed concern that outsourcing complicates responsibility allocation and coordination during incidents. Current contracts often specify service levels and reporting requirements but do not necessarily ensure skill comparability or situational understanding between the institution and the vendor (ECB, 2025). By aligning contractual expectations with ECSF-defined roles, financial institutions could potentially improve transparency and reduce ambiguity in external collaboration. This would also respond to concerns raised in literature about fragmented accountability in incident management (Darem et al., 2023; He et al., 2022). The empirical findings thus extend the existing literature by illustrating that frameworks like the ECSF can contribute not only to training or recruitment but also to strategic governance of outsourced capabilities.

The empirical findings indicate cultural and institutional barriers to the framework's adaptation. Because Finnish financial institutions already operate within dense regulatory structures, there is limited perceived need for another framework. Several interviewees viewed new instruments as redundant unless they add clear operational value. This skepticism aligns with prior observations that ECSF's uptake depends on its ability to

integrate with existing standards rather than replace them (ENISA, 2023). The findings therefore suggest that ECSF’s relevance in the financial sector lies not in redefining roles but in improving the alignment of skills, responsibilities, and communication across internal and outsourced actors. Table 8 provides summary of ECSF role alignment with existing roles across frameworks and as they are observed in Finnish practice. Green signifies the roles is well represented in both theory and practice and that the frameworks and the Finnish financial sector share a common understanding of what the role does and where it fits in the incident response. These areas ECSF roles would reinforce without changing existing practice. Yellow signifies that role is present but interpreted differently in practice and not consistently defined. Red signifies that the role is not formally integrated in other frameworks or definitions.

**Table 8:** ECSF Role Alignment with Existing Incident Response Roles

ECSF Role	ISO/IEC 27395	NIST SP 800-61r3	DORA & NIS2	Observed in Finnish Practice
<b>Cyber Incident Responder</b>	Incident Responder	Technical Specialists	Incident Documentation	Internal SOC / Outsourced
<b>Cybersecurity Manager</b>	Incident Coordinator	Team Leader	Risk Management and Assessment	Internal
<b>CISO</b>	Management and decision-making	Management liaison	Management responsibility	Communicative
<b>Cybersecurity Legal, Policy and Compliance Officer</b>	Communication Officer	Legal & Compliance, Public Affairs	Reporting to authorities	Partial /shared responsibility across roles
<b>Digital Forensics Investigator</b>	-	Technical Specialists	-	Outsourced expertise

While ECSF is not currently visible in Finnish financial institutions’ incident response practices, the findings demonstrate several potential applications that could address the sector’s identified challenges. The framework could provide a structured basis for managing outsourced expertise, enhance transparency in role definition and accountability,

and support the development of more integrated communication practices during incidents. By linking technical roles to management responsibilities, the ECSF could strengthen both coordination and the credibility of incident response efforts. The results thus extend the literature by showing that frameworks like the ECSF, although designed primarily for workforce development, can also function as governance tools to enhance cross-sector consistency, outsourcing management, and stakeholder trust in the context of financial cybersecurity.

## 8.4 Improving incident response capabilities

The findings of this study indicate that while the Finnish financial sector demonstrate high technical maturity in prevention and detection, both datasets reveal that true resilience requires incident response capabilities that are enacted in adaptive and communicative ways. Similar to observations by He et al. (2022), the main challenge lies not in technical readiness but in the ability to dynamically manage prolonged and complex incidents.

Although frameworks such as ISO/IEC 27035 provide a strong procedural base, the empirical evidence suggests that their application in Finland remains largely sequential. This aligns with previous studies arguing that incident response frameworks risk becoming static when organizations interpret them as compliance checklists (Cortez and Dekker, 2022), which limits the potential for agile incident response. In practice, the Nordea incident revealed that these stages might overlap as new information can emerge while recovery is still ongoing, and communication to stakeholders must evolve continuously as the situation develops.

Interviewees similarly noted that during active incidents, several response functions such as technical containment, coordination with suppliers, and communication occur simultaneously and require repeated reassessment. On the other hand, the interview data repeatedly emphasized how structured and rehearsed processes, as well as clear roles and responsibilities, are key to successful incident response. Adaptability and scalability must therefore be incorporated into processes without disrupting existing roles, responsibilities, and incident response structures, so that structured playbooks can support rather than constrain agile incident response.

Consistent with He et al. (2022), this study provides empirical evidence that limited integration of learning and situational awareness during an ongoing incident leads to inefficiencies and credibility challenges. Frameworks might treat lessons learned as post-incident reflection rather than a continuous feedback process, leaving improvement phases retrospective rather than adaptive and agile.

Both empirical datasets indicate that current scenario-based preparedness does not sufficiently account for evolving, unpredictable threats. Interviewees acknowledged that exercises focus on known threat types, while literature highlights the need to integrate geopolitical and systemic risks into planning (Naseer et al., 2024). This gap demonstrates that scenario analysis must evolve into a continuous capability for adaptive situational awareness.

Naseer et al. (2024) argue that effective response depends on real-time sensemaking and dynamic threat profiling. The Nordea case supports this, showing that while technical detection functioned effectively, understanding of attacker intent and methods lagged behind the evolving situation. This finding underscores that preparedness for unprecedented incidents requires flexible processes, cross-unit cooperation, and adaptive situational awareness rather than new technologies alone.

Both datasets and previous studies (Uddin et al., 2020) underline that communication should function as a continuous operational component, not a post-incident PR. The Nordea incident exemplified how limited transparency can erode trust, echoing FIN-FSA's (Finanssivalvonta, 2024) emphasis on communication as a core recovery capability. Integrating technical expertise into public communication could therefore strengthen both credibility and coordination during crises.

Despite routine post-incident reviews, learning integration remains inconsistent. Echoing Carilo (2023) and He et al. (2023), the findings reveal that lessons learned often fail to become lessons applied. Embedding real-time documentation of decisions and hypotheses during incidents could ensure that contextual insights inform future playbooks and governance metrics. Expanding recovery metrics beyond technical restoration to include indicators such as customer sentiment or time-to-credible-update would align learning objectives with the realities of reputational resilience. The Nordea case, where services were restored swiftly but confidence lagged, illustrates the importance of this broader conception of recovery.

Among existing frameworks NIST SP 800-61r3 most closely represent adaptability through its iterative structure. However, it lacks explicit emphasis on communication, which is critical for the financial sector. Table 9 below synthesizes these findings by aligning identified improvement capabilities with NIST SP 800-61r3 and crisis and recovery management capabilities recognized by FIN-FSA.

**Table 9:** Incident Response Improvement Capabilities

<b>Capability Area</b>	Detection and Analysis	Response and Mitigation	Recovery and Restoration	Learning and Improvement	Preparation and Governance
<b>NIST SP 800-61r3</b>	Detect	Respond	Recover	Lessons Learned	Preparation
<b>Crisis and Recovery Management Capabilities</b>	Analysis of Disruptive Impact	Mitigation Measures	Deployment of Recovery Management and Restoring Operations	Updating plans according to lessons learned	Crisis and Recovery Management plans
<b>Identified Improvement Capabilities</b>	Adaptive Situational Awareness	Integrated and Transparent Communications	Scalable and Collaborative Recovery	Embedded Learning	Collaborative governance

In summary, the five improvement capabilities, adaptive situational awareness, integrated and transparent communication, scalable and collaborative recovery, embedded learning, and collaborative governance, represent interdependent incident response capabilities through which Finnish financial institutions can strengthen incident response. Together, they shift the focus from procedural compliance toward resilience based on agile incident response. Each capability directly addresses a specific weakness identified in empirical findings and extends existing models. Adaptive situational awareness advances traditional detection phases in NIST and ISO frameworks by introducing continuous sensemaking and feedback loops that mitigate delays in understanding attack intent and reduce fragmented communication between technical and executive teams.

Integrated and transparent communication complements technical response phases by embedding communicative competence and accountability into operations, countering the delayed and inconsistent public messaging observed in the Nordea incident. Scalable and collaborative recovery expands recovery concepts in existing models by emphasizing inter-organizational cooperation and flexible resource mobilization, tackling the uneven recovery coordination exposed in the findings. Embedded learning reframes the lessons learned stage as a concurrent rather than retrospective process, ensuring that ongoing documentation and reflection inform real-time adjustments instead of post-incident reports alone. Finally, collaborative governance redefines compliance-oriented leadership structures into participatory and cross-sector governance models, addressing

the fragmentation of accountability and oversight between outsourced, national, and cross-border actors.

## 9. CONCLUSION

This chapter concludes this study by providing key findings, evaluation of the study, and proposes further research suggestions for the future, which may delve deeper into various organizations in the financial sector, technical methods of incident response, and the recovery from certain types of cyber threats.

### 9.1 Key findings

This study provides new empirical insight how the Finnish financial sector can strengthen its incident response capabilities through adaptive governance, integrated communication, and embedded learning. From a managerial perspective, the findings highlight that resilience is not solely a technical achievement but a strategic and organizational one. Managers must view incident response as a continuous learning cycle that integrates iterative feedback between detection, response, recovery, and communication functions, as argued in previous literature (He et al., 2022; Naseer et al., 2024). In particular, embedding technically competent spokespersons and clarifying accountability across internal and outsourced teams can directly enhance stakeholder trust and recovery speed, which are two areas where even mature financial institutions still face challenges. The key findings are summarized in Table 10.

**Table 10:** Summary of Capability Development Directions

Capability Area	Current Gap	Improvement Direction
<b>Adaptive Situational Awareness</b>	Incident response functions are fragmented and not sufficiently iterative.	Embed continuous feedback and sensemaking across all incident response phases.
<b>Integrated and Transparent Communication</b>	Communication is decoupled from technical operations, causing inconsistent internal and external reporting.	Embed communication roles and protocols in operational cycles and appoint technically competent spokespersons.
<b>Scalable and Collaborative Recovery</b>	Recovery remains siloed and difficult to scale across units and providers.	Develop modular recovery playbooks and conduct joint recovery exercises with internal and external partners.

<b>Embedded Learning</b>	Lessons learned remain retrospective.	Integrate learning mechanisms into every function of incident response, not limited to post-incident reflection.
<b>Collaborative Governance</b>	Outsourcing fragments responsibility and weakens coordination.	Align internal and external roles and establish joint response protocols and accountability chains.

The significance of this research lies in its contextual and methodological contributions. By combining document analysis of the Nordea DDoS attack with expert interview, this study demonstrates that even in one of Europe's most advanced financial systems, resilience gaps persist between formal compliance and adaptive capability. This extends existing literature (Carilo, 2023) by revealing that regulatory maturity does not guarantee organizational agility. The results underscore that resilience emerges from independent managerial processes such as leadership, communication, and governance, rather than from regulatory conformity alone.

Novelty arises from integrating the European Cybersecurity skills framework (ECSF) into the discussion of incident response governance. The framework's role-based taxonomy, rarely applied in this context, offers a practical mechanism for aligning internal competences with outsourced capabilities, thereby addressing of the sector's most persistent vulnerabilities, fragmented accountability, especially prevalent in unprecedented and prolonged incidents. Unexpectedly, the study found that Finland's high cybersecurity maturity in the finance sector coexists with communication rigidity, which illustrates how reputation management can inadvertently weaken real-time transparency and undermine public trust. Consistent with previous research, the findings reframe incident response as a socio-technical management function where continuous adaptation, inter-organizational collaboration, and transparent communication form the foundation of sustainable cyber resilience in the financial sector.

Based on the findings, cyber security in Finland is highly developed and mature, and many practices in the financial sector are advanced in terms of both technology and internal cooperation within sector. Many sectors could learn a lot from the practices of institutions in the Finish financial sector. However, as part of critical infrastructure, maintaining and developing financial sector cyber resilience requires continuous effort. The European operational environment is changing, and in Finland in particular, organizations need to adapt their incident response capabilities across all areas in order to respond to changes in the threat landscape more flexibly and proactively.

## 9.2 Evaluation of the study

The quality and trustworthiness of this research were considered throughout the project rather than evaluated only at its end, following Eriksson & Kovalainen's (2008) view that continuous reflexive evaluation strengthens research integrity. The objective of the study, to explore how the Finnish financial sector could enhance its incident response capabilities and to identify strengths and weaknesses in current practices, was largely achieved.

The research design combined document analysis and semi-structured expert interviews, allowing both institutional and experiential perspectives to emerge. According to Patton (2023) and Flick (2021), methodological triangulation enhances analytic depth and credibility. In this study, it enabled a balanced understanding that considered both public evidence and insider reflections on the sector. The Nordea DDoS incident, as the descriptive case, met Patton's (2023) criterion of significance because it was both unique in the Finnish context and illustrative of broader European challenges.

Completeness was pursued by clearly defining the case boundaries and by including material that both supported and questioned the emerging interpretations. As Eriksson & Kovalainen (2008) stress, a convincing case study must display sufficient, and even contradictory evidence, so that readers can form an independent judgment. Evidence from news articles highlighting communication gaps was therefore analyzed alongside interview material emphasizing structural maturity. This duality contributed to a more nuanced and credible picture of the sector's resilience.

The study's trustworthiness can be assessed through Lincoln and Guba's (1985) four criteria. Credibility was enhanced by prolonged engagement with the data, transparent documentation of coding decisions, and clear logical links between observations and thematic categories (Saunders et al., 2019).

Transferability was addressed by providing rich contextual description, enabling possibility for readers to evaluate the applicability of findings to other financial or possibly critical infrastructure contexts. Confirmability was supported by maintaining an audit trail that connects interpretations to the original data, reducing the influence of researcher subjectivity. Dependability was ensured through a traceable and well-documented analytic process, consistent with the standards proposed by Eriksson & Kovalainen (2008).

Nevertheless, limitations must be acknowledged. As Puusa et al. (2020) note, interviews reveal participants' reconstructed perceptions rather than objective reality, which means reactivity and interpretation bias can occur through wording or researcher influence. The small number of interviews limits breadth, although the purpose of qualitative inquiry is

depth rather than statistical representativeness (Patton, 2023). The exclusive focus on written documents may omit non-textual discursive cues, which future research could address by including audiovisual or observational data, as recommended by Karppinen and Moe (2012). Finally, as Maier et al. (2023) note, methodological coherence between data, questions, and conclusions was continuously reviewed to avoid over-interpretation. Ethical considerations guided the study in line with Eriksson & Kovalainen (2008) and the Menlo principles (Macnish & van der Ham, 2020). Participants gave informed consent and were interviewed voluntarily with full awareness of the study's aims. Confidentiality was maintained, and quotations were anonymized to prevent reputational harm. Only publicly available materials were used for document analysis, respecting transparency and data-protection norms. The principle of beneficence directed the research purpose which is to contribute to improving incident response capabilities while avoiding potential harm to the institutions studied. As Macnish & van der Ham (2020) argue, ethical reflection in cybersecurity research must extend beyond data collection to include interpretation and publication, and these obligations were observed throughout.

### **9.3 Suggestions for future research**

This study has provided valuable insights into incident response capabilities in the Finnish financial sector and revealed several promising directions for further research, which remain unexplored due to the scope and limitations of this work. These topics are closely related to the findings and could significantly deepen the understanding of how the financial sector can enhance its resilience and preparedness against cyber incidents.

It is still too early to assess the real impact of the Digital Operational Resilience Act (DORA), which came only into effect in early 2025. Since no large-scale incidents have occurred under DORA so far, there is limited empirical evidence on its effectiveness or limitations in practice. Moreover, supervisory authorities focus primarily on whether institutions comply with the requirements rather than how they are implemented. Future studies could therefore investigate how DORA shapes organizational behavior, preparedness, and the quality of incident response over time.

There is also a clear need to develop and validate process models for incident response and structured approaches to information sharing. The findings of this research suggest that many incident response challenges stem from process-related shortcomings rather than technical issues. The technical incident response capabilities in the field appear to be undeniably advanced, while communication with stakeholders, for example, remains

contentious and divides opinion sharply. A more detailed comparison of incident response processes between various financial organizations could help identify best practices and sector-specific challenges as the current focus is largely on banking, even though the sector is diverse with different customers, structures, processes, and needs. Furthermore, international comparisons would provide valuable context for understanding how Finnish practices align with or differ from those in other EU countries. Such comparative studies could highlight both strengths and areas for improvement in Finland's incident response capabilities.

Although information exchange and networking among cyber security professionals in the sector is smooth and effective, attempts to develop official channels for sharing threat information have been ongoing for some time now. To refine this process, platform, and its practices, information and knowledge management can offer methods and processes that could be further researched and developed for testing in practice. Information and knowledge management could offer methods for effective, structured, and refined information sharing.

Another important direction for research involves developing methods to measure and monitor cyber resilience. As resilience becomes a strategic priority, organizations need clear metrics and tools to track their progress. Future research could explore how simulations, exercises, and collaborative information sharing can be measured in ways that systematically improve cyber resilience.

There also seems to be limited research available on the effectiveness of the European Cybersecurity Skills Framework (ECSF) and on how it has been applied in practice, making it difficult to evaluate its potential usefulness in the financial sector. Future work could assess whether adopting ECSF roles and skill profiles would make training and recruitment more effective and aligned with real operational needs.

## REFERENCES

- Adetunji, P.A. & Chinonso, P.O. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World J. Adv. Res. Rev.* 25, 1542–1556. <https://doi.org/10.30574/wjarr.2025.25.3.0909>
- Akinsulire, A.A. & Ohakawa, T.C. (2024). Enhancing Cybersecurity Governance in Financial Institutions: A Quantitative Study on Control Deficiencies and Regulatory Compliance (2024). *International Journal of Advanced Multidisciplinary Research and Studies*. Vol. 4 (6), 2127-2139. <https://doi.org/10.62225/2583049X.2024.4.6.4264>
- Bank of Finland. (2025). TIBER-FI Framework [WWW Document]. Bank of Finland. Available at: <https://www.suomenpankki.fi/en/money-and-payments/tiber-fi-framework/> (Accessed 5.8.25).
- Billups, F.D. (2021). *Qualitative Data Collection Tools: Design, Development, and Applications*. SAGE Publications, Inc. <https://doi.org/10.4135/9781071878699>
- Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition, in: Rocha, A., Correia, A.M., Costanzo, S., Reis, L.P. (Eds.), *New Contributions in Information Systems and Technologies*. Springer International Publishing, Cham, pp. 311–316. [https://doi.org/10.1007/978-3-319-16486-1\\_31](https://doi.org/10.1007/978-3-319-16486-1_31)
- Braun, V. (2022). *Thematic analysis: a practical guide*. SAGE Publications, London.
- Calliess, C. & Baumgarten, A. (2020). Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective. *German Law Journal* 21, 1149–1179. <https://doi.org/10.1017/glj.2020.67>
- Carilo, E.F.P. (2023). Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform. *European Business Law Review* 34, 1133–1166. <https://doi.org/10.54648/EULR2023052>
- Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *Int. Cybersecurity. Law Rev.* 4, 79–90. <https://doi.org/10.1365/s43439-022-00076-5>
- Cloudflare. (2025). DDoS threat report for 2024 Q4. Cloudflare Radar [WWW Document]. Available at: <https://radar.cloudflare.com/reports/ddos-2024-q4> (Accessed 11.3.25).
- Computer Security Division & I.T.L. (2024). Incident Response | CSRC | CSRC [WWW Document]. CSRC | NIST. Available at: <https://csrc.nist.gov/projects/incident-response> (Accessed 5.29.25).
- Cortez, E.K. & Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. *European Journal of Risk Regulation: EJRR* 13, 443–463. <https://doi.org/10.1017/err.2022.10>
- Darem, A.A., Alhashmi, A.A., Alkhaldi, T.M., Alashjaee, A.M., Alanazi, S.M. & Ebad, S.A. (2023). Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. *IEEE access* 11, 125138–125158. <https://doi.org/10.1109/ACCESS.2023.3327016>

de Neira, A.B., Kantarci, B. & Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. *Computer Networks* 222, 109553. <https://doi.org/10.1016/j.comnet.2022.109553>

Didenko, A.N. (2020). Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond. *Uniform Law Review* 25, 125–167. <https://doi.org/10.1093/ulr/unaa006>

Digital Operational Resilience Act. (2025). Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554: Training, Updates, Compliance [WWW Document]. Available at: <https://www.digital-operational-resilience-act.com/> (Accessed 3.13.25).

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity* 5. <https://doi.org/10.1093/cybsec/tyz013>

EBA. (2019). EBA ICT and Security Guidelines [WWW Document]. Available at: <https://www.eba.europa.eu/sites/default/files/2025-02/23684f95-f669-4852-94a0-dac6c2ae67ad/Final%20report%20on%20amending%20GLs%20on%20ICT%20risk%20and%20security.pdf> (Accessed 2.27.25).

ECB. (2025). ECB Guide on outsourcing cloud services to cloud service providers. European Central Bank. Available at: [https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603\\_draftguide.en.pdf](https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon240603_draftguide.en.pdf) (Accessed 9.2.2025).

ECB. (2025). Outsourcing trends in the banking sector. European Central Bank. Available at: [https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2025/html/ssm.nl250219\\_2.en.html](https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2025/html/ssm.nl250219_2.en.html) (Accessed 9.2.2025)

EIOPA. (2022). Digital Operational Resilience Act (DORA) - EIOPA. European Insurance and Occupational Pensions Authority. [WWW Document]. Available at: [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora\\_en](https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en) (Accessed 5.6.25).

ENISA. (2024). 2024 Report on the State of the Cybersecurity in the Union. European Union Agency for Cybersecurity. [WWW Document]. Available at: <https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf> (Accessed 5.19.25).

ENISA. (2022). European Cybersecurity Skills Framework (ECSF) | ENISA. European Union Agency for Cybersecurity. [WWW Document]. Available at: <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf> (Accessed 3.18.25).

Eriksson, P. & Kovalainen, A. (2008). *Qualitative Methods in Business Research*, 1st ed, Introducing Qualitative Methods. SAGE Publications, London. <https://doi.org/10.4135/9780857028044>

European Central Bank. (2023). What is TIBER-EU? European Central Bank. Available at <https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html> (Accessed 3.3.2025)

European Central Bank. (2022). European System of Financial Supervision. European Central Bank. Available at: <https://www.bankingsupervision.europa.eu/about/esfs/html/index.en.html> (Accessed 18.3.2025)

European Commission. (2025). Critical infrastructure resilience at EU-level. European Commission [WWW Document]. Available at: [https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level\\_en](https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en) (Accessed 4.16.25).

European Commission. (2025). Overview of financial services legislation - Finance - European Commission [WWW Document]. Available at: [https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/overview-financial-services-legislation\\_en](https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/overview-financial-services-legislation_en) (Accessed 11.12.25).

European Parliament and the Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 33, 80-152.

European Systemic Risk Board. (2024). Advancing macroprudential tools for cyber resilience: operational policy tools : April 2024 : a review of national and pan European frameworks. Publications Office, LU.

European Union Agency for Cybersecurity. (2025). ENISA threat landscape: finance sector : January 2023 to June 2024. Publications Office, LU.

European Union Agency for Cybersecurity. (2022a). ECSF, European cybersecurity skills framework. Publications Office, LU.

European Union Agency for Cybersecurity. (2022b). ECSF, European cybersecurity skills framework. Publications Office, LU.

EU-SCICF. (2021). Systemic Cyber Incident Coordination Framework (EU-SCICF) [WWW Document]. Available at: <https://www.eu-scicf.com/> (Accessed 5.8.25).

Farjoun, M., Ansell, C. & Boin, A. (2015). Pragmatism in Organization Studies: Meeting the Challenges of a Dynamic and Complex World. *Organization science* (Providence, R.I.) 26, 1787–1804. <https://doi.org/10.1287/orsc.2015.1016>

Finanssiala Ry. (2024). Mikä on Finanssiala ry? [WWW Document]. Finanssiala. Available at: <https://www.finanssiala.fi/mika-on-finanssiala-ry/> (Accessed 7.29.25).

Finanssiala Ry. (2021). Kyberturvallisuus ja tietosuoja [WWW Document]. Finanssiala. Available at: <https://www.finanssiala.fi/aiheet/kyberturvallisuus-ja-tietosuoja/> (Accessed 3.19.25).

Finanssivalvonta. (2025). Finanssivalvonnän vuoden 2024 valvontatoimenpiteet [WWW Document]. Finanssivalvonta Available at: <https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/toimintakertomukset/toimintakertomus-2024/valvonta/> (Accessed 5.30.25).

Finanssivalvonta. (2024). EKP testasi pankkien kyberhäiriöiden sietokyvyn [WWW Document]. Finanssivalvonta. Available at: <https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/verkkouutiset/2024/ekp-testasi-pankkien-kyberhairioiden-sietokyvyn/> (Accessed 5.30.25).

Finanssivalvonta. (2020). Tietoturvallisuus [WWW Document]. Finanssivalvonta. Available at: <https://www.finanssivalvonta.fi/finanssisektorin-toimijalle/vakuutus/fintech--finanssialan-innovaatiot/tietoturvallisuus/> (Accessed 6.3.25).

Flick, U. (2021). *Doing Interview Research: The Essential How To Guide*, First edition. ed. SAGE Publications, Ltd. UK, London.

Finanssivalvonta. (2025). Asetus finanssialan digitaalisesta häiriönsietokyvystä [WWW Document]. Finanssivalvonta. Available at: <https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/dora/> (Accessed 3.18.25).

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry* 12, 219–245. <https://doi.org/10.1177/1077800405284363>

Galletta, A. (2013). *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*, 1st ed, Qualitative studies in psychology. NYU Press, New York. <https://doi.org/10.18574/9780814732953>

Garcia-Perez, A., Sallos, M.P. & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. *Journal of Intellectual Capital* 24, 465–486. <https://doi.org/10.1108/JIC-06-2021-0166>

Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European journal of information systems* 21, 135–146. <https://doi.org/10.1057/ejis.2011.54>

Goodwin, S. (2022). The need for a financial sector legal standard to support the NIST Cybersecurity Framework, in: *SoutheastCon 2022*. Presented at the SoutheastCon 2022, pp. 89–95. <https://doi.org/10.1109/SoutheastCon48659.2022.9764006>

Hair, J.F. (2023). *Essentials of Business Research Methods - Tampere University Foundation*, 5th ed. Routledge, New York, NY.

He, Y., Zamani, E.D., Lloyd, S. & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International journal of information management* 62, 102435-. <https://doi.org/10.1016/j.ijinfomgt.2021.102435>

Hirsjärvi, S. & Hurme, H. (2022). *Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö*, [2. painos]. ed. Gaudeamus, Helsinki.

Huoltovarmuuskeskus. (2025). Finanssiala - Huoltovarmuuskeskus [WWW Document]. Available at: <https://www.huoltovarmuuskeskus.fi/toimialat/finanssiala> (Accessed 7.29.25).

Huoltovarmuuskeskus. (2022). *Toimialojen kyberkypsyiden selvitys 2022*. Huoltovarmuuskeskus. [WWW Document]. Available at: <https://www.huoltovarmuuskeskus.fi/files/bbdecbcd7921768bd3ac5496af7992a0460a9f2b/hvk-toimialojen-kyberkypsyiden-selvitys-2022.pdf> (Accessed 3.3.25).

Hyvärinen, M., Suoninen, E. & Vuori, J. (2021). *Haastattelut - Tietoarkisto* [WWW Document]. Available at: <https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-aineistot/haastattelut/> (Accessed 6.14.25).

ISO/IEC 27001, 2023. *ISO/IEC 27001:2023 - Information security management systems - Requirements*. International Organization for Standardization.

ISO/IEC 27002, 2022. *ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection - Information security controls*. International Organization for Standardization.

ISO/IEC 27035, 2016. ISO/IEC 27035-1:2022 - Information security incident management - Principles. International Organization for Standardization.

Iusan, C., Badea, D., Bucoveţchi, O.M.C. & Iancu, D. (2020). BUSINESS CONTINUITY MANAGEMENT IN THE BANKING AND FINANCE SECTOR. AN OVERVIEW OF SECTOR RELATED VARIABLES. *Journal of defense resources management* 11, 89–96.

Karppinen, K. & Moe, H. (2012). What We Talk about When We Talk about Document Analysis [WWW Document]. Available at: [https://www.researchgate.net/publication/299366807\\_What\\_We\\_Talk\\_about\\_When\\_We\\_Talk\\_about\\_Document\\_Analysis](https://www.researchgate.net/publication/299366807_What_We_Talk_about_When_We_Talk_about_Document_Analysis) (Accessed 10.29.25).

Kyberturvallisuuskeskus. (2025). Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2) [WWW Document]. Kyberturvallisuuskeskus. Available at: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa> (Accessed 5.8.25).

Kyberturvallisuuskeskus. (2024a). Palvelunestohyökkäystilanne Suomessa [WWW Document]. Kyberturvallisuuskeskus. Available at: <https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaystilanne-suomessa> (Accessed 3.3.25).

Kyberturvallisuuskeskus. (2024b). NIS2 - Euroopan unionin kyberturvallisuusdirektiivi [WWW Document]. Kyberturvallisuuskeskus. Available at: <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi> (Accessed 3.17.25).

Laki eräistä huoltovarmuuden turvaamisen järjestelyistä 666/2022. (2022). Edilex. [WWW Document] Available at: <https://www.edilex.fi/smur/20220666> (Accessed 9.6.25).

Leo, M. (2020). Operational resilience disclosures by banks: analysis of annual reports. *Risks (Basel)* 8, 1–15. <https://doi.org/10.3390/risks8040128>

Maier, C., Thatcher, J.B., Grover, V. & Dwivedi, Y.K. (2023). Cross-sectional research: A critical perspective, use cases, and recommendations for IS research. *International Journal of Information Management* 70, 102625. <https://doi.org/10.1016/j.ijinfomgt.2023.102625>

Malminen, U. (2024). Tässäkö syy pankkiongelmiiin? Tietojärjestelmät ovat 80-luvulla käyttöön otetun keskustietokoneen varassa [WWW Document]. *Yle Uutiset*. Available at: <https://yle.fi/a/74-20118006> (Accessed 2.20.25).

Malminen, U. & Kinnunen, P. (2024). Pankkivaltuuston puheenjohtaja Ylälle: Nordean ongelmista vaaditaan nyt selvitys Finanssivalvonnalta [WWW Document]. *Yle Uutiset*. Available at: <https://yle.fi/a/74-20116893> (Accessed 2.20.25).

Morgan, H. (2022). Conducting a Qualitative Document Analysis. *TQR*. <https://doi.org/10.46743/2160-3715/2022.5044>

Naseer, H., Desouza, Kevin, Maynard, Sean B., & Ahmad, A. (2024). Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems* 33, 200–220. <https://doi.org/10.1080/0960085X.2023.2257168>

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (No. NIST CSWP 29). National Institute of Standards and Technology, Gaithersburg, MD. <https://doi.org/10.6028/NIST.CSWP.29>

Olutimehin, A.T. (2025). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and Its Applicability to Decentralized Finance (DeFi). <https://doi.org/10.2139/ssrn.5133050>

Patton, M.Q. (2023). *Qualitative Research & Evaluation Methods: Integrating Theory and Practice*, Fourth edition. ed. SAGE Publications, Inc. US, Thousand Oaks.

Peihani, M. (2022). Regulation of Cyber Risk in the Banking System: A Canadian Case Study. *Journal of financial regulation* 8, 139–161. <https://doi.org/10.1093/jfr/fjac006>

Petrenko, S. (2019). *Cyber resilience*, 1st ed. ed, River publishers series in security and digital forensics. River Publishers, Gistrup, Denmark.

Polemi, N. & Kioskli, K. (2023). Enhancing Practical Cybersecurity Skills: The ECSF and the CyberSecPRO European Efforts. *Human Factors in Cybersecurity* 91, 93–100. <https://doi.org/10.54941/ahfe1003723>

Puusa, A., Juuti, P. & Aaltio, I. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus, Helsinki.

Salminen, A. (2011). *Mikä kirjallisuuskatsaus? Johdatus tyypeihin ja hallintotieteellisiin sovelluksiin*. Vaasan Yliopisto.

Saunders, M.N.K., Lewis, P. & Thornhill, A. (2019). *Research methods for business students*, Eighth Edition. ed. Pearson, New York.

Schlette, D., Caselli, M. & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials* 23, 2525–2556. <https://doi.org/10.1109/COMST.2021.3117338>

Shenton, A.K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for information* 22, 63–75. <https://doi.org/10.3233/EFI-2004-22201>

Shin, B. & Lowry, P.B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & security* 92, 101761–16. <https://doi.org/10.1016/j.cose.2020.101761>

Sisäministeriö. (2025). *Kriittistä infrastruktuuria koskevan sääntelyn uudistaminen [WWW Document]*. Sisäministeriö. Available at: <https://intermin.fi/hankkeet/kriittinen-infrastruktuuri> (Accessed 7.29.25).

Suomi.fi. (2025). *Miten kirjaudun Suomi.fi-tunnistusta käyttävään asiointipalveluun? - Suomi.fi-tunnistuksen ohjeet - Suomi.fi [WWW Document]*. Available at: <https://www.suomi.fi/ohjeet-ja-tuki/tunnistus/miten-kirjaudun-suomifi-tunnistusta-kayttavaan-asiointipalveluun> (Accessed 7.29.25).

TENK. (2019). *Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakoarviointi Suomessa*. Tutkimuseettisen neuvottelukunnan julkaisuja 3.

Toivonen, J. (2024). *Onko Nordeaan todella hyökätty suomalaisista koodista? Nämä viisi asiaa Nordean ongelmista tiedetään nyt [WWW Document]*. Yle Uutiset. Available at: <https://yle.fi/a/74-20118260> (Accessed 2.20.25).

Tuomi, J. (2018). *Laadullinen tutkimus ja sisällönanalyysi*, Uudistettu laitos. ed. Tammi, Helsinki.

Uddin, M.H., Ali, M.H. & Hassan, M.K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk management (Leicestershire, England)* 22, 239–309. <https://doi.org/10.1057/s41283-020-00063-2>

Valtiovarainministeriön asetus luottolaitoksen valmiussuunnittelun perusteista | 71/2025. (2025). Finlex. [WWW Document]. Available at: <https://www.finlex.fi/fi/lainsaadanto/2025/71> (Accessed 9.2.25).

van der Kleij, R., Schraagen, J.M., Cadet, B. & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & security* 113, 102535-. <https://doi.org/10.1016/j.cose.2021.102535>

Varga, S., Brynielsson, J. & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security* 105, 102239. <https://doi.org/10.1016/j.cose.2021.102239>

Vento, J. (2024). Tanskalaisväite: Nordea ei tehnyt järjestelmilleen katastrofitestausta vuosikausiin [WWW Document]. Tivi. Available at: <https://www.tivi.fi/uutiset/tanskalaisvaite-nordea-ei-tehnyt-jarjestelmilleen-katastrofitestausta-vuosikausiin/6578a72c-49f1-4216-93f6-175cb5107310> (Accessed 2.20.25).

Walton, S., Wheeler, P.R., Zhang, Y. & Zhao, X. (2021). An Integrative Review and Analysis of Cybersecurity Research: Current State and Future Directions. *The Journal of information systems* 35, 155–186. <https://doi.org/10.2308/ISYS-19-033>

Weickert, T.D., Joinson, A. & Craggs, B. (2023). Is cybersecurity research missing a trick? Integrating insights from the psychology of habit into research and practice. *Computers & security* 128, 103130-. <https://doi.org/10.1016/j.cose.2023.103130>

Yin, R.K. (2018). *Case study research and applications: design and methods*, Sixth edition. ed. SAGE, Los Angeles.

Zargar, S.T., Joshi, J. & Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials* 15, 2046–2069. <https://doi.org/10.1109/SURV.2013.031413.00127>

## APPENDIX A: LITERATURE REVIEW TABLE

Authors	Year	Title	Source	Data-base	Search Query	Notes
Adentuji & Chinonso	2025	The role of cybersecurity in safeguarding finance in a digital area	World Journal of Advanced Research Reviews	Google Scholar	"finance sector cybersecurity governance"	-
Akinsulire & Ohakawa	2024	Enhancing Cybersecurity Governance in Financial Institutions: A Quantitative Study on Control Deficiencies and Regulatory Compliance (2024)	International Journal of Advanced Multidisciplinary Research and Studies	Google Scholar	"finance sector cybersecurity governance"	-
Bederna et al.	2021	Further Strategy Analysis of Cybersecurity Incidents	Land Forces Academy Review	Andor	"incident response financial sector"	Peer-reviewed
Calliess & Baumgarten	2020	Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective	Cambridge University Press	Andor	"cybersecurity financial sector"	Peer-reviewed,
Clausmeier	2022	Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)	International cybersecurity law review	Andor	"cybersecurity financial sector"	Peer-reviewed
Cortez & Dekker	2022	A Corporate Governance Approach to Cybersecurity Risk Disclosure	European journal of risk regulation	Andor	"cybersecurity financial sector"	Peer-reviewed
Darem et al.	2023	Cyber Threats Classifications and Countermeasures in Banking and Financial Sector	IEEE Access	Google Scholar	"cyber threats financial sector"	Peer-reviewed
Didenko	2020	Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond	Revue de droit uniforme	Andor	"cybersecurity financial sector"	Peer-reviewed,
Garcia-Perez	2023	Dimensions of cybersecurity performance and crisis response in critical infrastructure organizations: an intellectual capital perspective	Journal of intellectual capital	Andor	"cybersecurity crisis response"	Peer-reviewed

Goodwin	2022	The need for a financial sector legal standard to support the NIST Cybersecurity framework	Proceedings of IEEE Southeastcon	Scopus	“utilizing NIST in finance sector or banking”	Scopus AI
He et al.		Agile incident response (AIR): Improving the incident response process in healthcare	International journal of information management	-	Reference tracking	Peer-reviewed
Iusan et al.	2020	Business Continuity Management in the Banking and Finance Sector. An overview of Sector Related Variables	Journal of defense resources management		“finance sector business continuity”	Peer-reviewed
Koibichuk & Dotsenko	2023	Content and Meaning of Financial Cyber Security: a Bibliometric Analysis	Financial Markets, Institutions and Risks	Andor	“incident response financial sector”	Peer-reviewed
Laib	2021	The Importance of Cyber Security in the Financial Sector in the Age of Digital Transformation	EL ACIL Review for Economic and Administrative Research	Andor	“cybersecurity financial sector”	Peer-reviewed
Leo	2020	Operational resilience disclosures by banks: analysis of annual reports	Risks (Basel)	Andor	“cyber resilience finance sector”	Peer-reviewed
Naseer et al.	2021	Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics	European Journal of Information Systems	Andor	“cybersecurity incident response”	Peer-reviewed
Peihani	2022	Regulation of Cyber Risk in the Banking System: A Canadian Study	Journal of financial regulatio	-	Reference tracking	Peer-reviewed
Polemi & Kioskli	2023	Enhancing Practical Cybersecurity Skills: The ECSF and the CyberSecPRO European Efforts	Human Factors in Cybersecurity	Google Scholar	“ECSF cybersecurity practical”	Discussion on ECSF
Şheau et al.	2022	Key Pillars for FinTechn and Cybersecurity	Acta Universitatis Danubius. Œconomica	Andor	“cybersecurity financial sector	Peer-reviewed

Schlettet et al.	2021	A comparative study on cyber threat intelligence: The security incident response persperctive	IEE Communica-tions Surveys & Tutorials	Andor	Reference tracking	Peer-re-viewed
Uddin et al.	2020	Cybersecurity hazards and financial system vulnerability: a synthesis of literature	Risk Manage-ment	Andor	"cybersecurity fi-nancial sector"	Peer-revie-wed,
Van Der Kleij et al.	2022	Developing decision support for cybersecurity threat and incident managers	Computers & se-curity	Andor	"cybersecurity fi-nancial sector"	Peer-revie-wed
Varga et al.	2021	Cyber-threat perception and risk management in the Swedish financial sector	Computers & se-curity	Andor	"cybersecurity fi-nancial sector"	Peer-re-viewed
Weickert et al.	2023	Is cybersecurity research missing a trick? Integrating insights from the psychol-ogy of habit into research and practice	Computers & se-curity	-	Reference tracking	Peer-re-viewed

## APPENDIX B: DOCUMENT ANALYSIS DATA

ID	Author(s)	Date	Title	Source Media	URL
D1	Nordea	19.3.2025	Detection, prevention, response	Nordea	<a href="https://www.nordea.com/en/news/detection-prevention-response-staying-ahead-of-cyber-threats">https://www.nordea.com/en/news/detection-prevention-response-staying-ahead-of-cyber-threats</a>
D2	Nordea	16.5.2025	Nordea On Your Mind	Nordea	<a href="https://www.nordea.com/en/news/nordea-on-your-mind-cybersecurity-ii">https://www.nordea.com/en/news/nordea-on-your-mind-cybersecurity-ii</a>
D3	Tauriainen & Kaivanto	15.10.2024	TS: Nordean hyökkäyksessä käytettiin suomalaisia kodinkoneita	Iltalehti	<a href="https://www.iltalehti.fi/digiuutiset/a/405d7a66-81ca-4963-8f77-ed849751c219">https://www.iltalehti.fi/digiuutiset/a/405d7a66-81ca-4963-8f77-ed849751c219</a>
D4	Korhonen	24.9.2024	Professori: Nordea voi kaatua, jos asiakkaat siirtävät rahat muualle	Iltalehti	<a href="https://www.iltalehti.fi/talous/a/90b96b0d-ba85-48d0-b406-917050a8f3a5">https://www.iltalehti.fi/talous/a/90b96b0d-ba85-48d0-b406-917050a8f3a5</a>
D5	Westberg	3.10.2024	Nordea drabbat av ny cyberattack	Finanswatch	<a href="https://finanswatch.se/news/bank/article17505924.ece">https://finanswatch.se/news/bank/article17505924.ece</a>
D6	SecurityUser	20.4.2025	Banker vill se lagändring efter attacker mot betaltjänster	SecurityUser	<a href="https://www.securityuser.com/se/Nyheter/Samhalle/banker-vill-se-lagandring-efter-attacker-mot-betaltjanster">https://www.securityuser.com/se/Nyheter/Samhalle/banker-vill-se-lagandring-efter-attacker-mot-betaltjanster</a>
D7	Yle Uutiset	18.10.2024	Finland's NBI probes wave of bank cyber attacks	Yle Uutiset	<a href="https://yle.fi/a/74-20118831">https://yle.fi/a/74-20118831</a>

D8	Vento	30.10.2024	Tanskalaisväite: Nordea ei tehnyt järjestelmilleen katastrofites- tausta vuosikausiin	Tivi	<a href="https://www.tivi.fi/uutiset/tanskalaisvaite-nordea-ei-tehnyt-jarjestelmilleen-katastrofites-tausta-vuosikausiin/6578a72c-49f1-4216-93f6-175cb5107310">https://www.tivi.fi/uutiset/tanskalaisvaite-nordea-ei-tehnyt-jarjestelmilleen-katastrofites-tausta-vuosikausiin/6578a72c-49f1-4216-93f6-175cb5107310</a>
D9	Valkama	9.10.2024	Analyysi: Tärkeä arjen toiminto kaatuilee jatkuvasti, mutta kukaan viranomainen ei ärähdä Nordealle	Yle Uutiset	<a href="https://yle.fi/a/74-20116834">https://yle.fi/a/74-20116834</a>
D10	Tolkki	16.10.2024	Talousvaliokunnan puheenjohtaja: Nordean verkkopalvelukatkojen takana ”järjestäytynyt toimija”, haluaa aiheuttaa haittaa		
D11	Toivonen	17.10.2024	Onko Nordeaan todella hyökätty suomalaisista kodeista? Nämä viisi asiaa Nordean ongelmista tiedetään nyt		
D12	Suutari	5.5.2025	Pankit   Nordea joutui palvelunestohyökkäyksen kohteeksi	Helsingin Sa- nomat	<a href="https://www.hs.fi/talous/art-2000011212898.html">https://www.hs.fi/talous/art-2000011212898.html</a>
D13	Suojelupoliisi	26.3.2024	Venäjän Suomeen kohdistuvan tiedustelun ja vaikuttamisen uhka säilyy koholla	Suojelupoliisi	<a href="https://supo.fi/-/venajan-suomeen-kohdistuvan-tiedustelun-ja-vaikuttamisen-uhka-sailyy-koholla">https://supo.fi/-/venajan-suomeen-kohdistuvan-tiedustelun-ja-vaikuttamisen-uhka-sailyy-koholla</a>
D14	STT-YLE	8.10.2024	Verkkopankkien käyttökatkoista järjestetään kuuleminen eduskun- nassa	Yle Uutiset	<a href="https://yle.fi/a/74-20116728">https://yle.fi/a/74-20116728</a>
D15	STT	25.9.2024	Nordea: Hyökkäykset jatkuneet, mutta tilanne on parempi	Yle Uutiset	<a href="https://yle.fi/a/74-20113988">https://yle.fi/a/74-20113988</a>
D16	STT	17.9.2024	Nordean palvelut toimivat jälleen normaalisti	Yle Uutiset	<a href="https://yle.fi/a/74-20112106">https://yle.fi/a/74-20112106</a>
D17	Siljamäki	24.9.2024	Nordean ongelmat ovat vaikuttaneet suomalaisten arkeen: synttärät Heurekassa ja futisturnaus jäivät väliin	Yle Uutiset	<a href="https://yle.fi/a/74-20113451">https://yle.fi/a/74-20113451</a>
D18	Siljamäki	23.9.2024	Miten Nordean häiriöt ovat vaikuttaneet elämäsi? Kerro kokemuk- sistasi	Yle Uutiset	<a href="https://yle.fi/a/74-20113300">https://yle.fi/a/74-20113300</a>
D19	Thurfjell	12.12.2024	Nordeas app fungerar igen	Aftonbladet	<a href="https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pin-edEntry=1315726">https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pin-edEntry=1315726</a>
D20	Öfwerman	3.10.2024	Nordea ligger nere efter en överbelastningsattack	Aftonbladet	<a href="https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pin-edEntry=1294762">https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pin-edEntry=1294762</a>

D21	Rosengart	21.9.2024	Bank har återigen störningar	Aftonbladet	<a href="https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1291302">https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1291302</a>
D22	Forsberg	19.9.2024	Svajigt på Nordea	Aftonbladet	<a href="https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1290551">https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1290551</a>
D23	Öfwerman	16.9.2024	Teknikstrul för Nordea	Aftonbladet	<a href="https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1290166">https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1290166</a>
D24	Santaharju	23.9.2024	Nordean palvelut takunneet jo päiviä – näin Suomen Pankin asiantuntija arvioi korvausvastuuta	Yle Uutiset	<a href="https://yle.fi/a/74-20113291">https://yle.fi/a/74-20113291</a>
D25	Santaharju	19.9.2024	Nordean häiriö korjattu	Yle Uutiset	<a href="https://yle.fi/a/74-20112672">https://yle.fi/a/74-20112672</a>
D26	Santaharju	19.9.2024	Häiriöt ja huoltokatkot pimentävät pankkipalveluita, mutta valvojan mielestä tilanne ei ole erityisen huono	Yle Uutiset	<a href="https://yle.fi/a/74-20112752">https://yle.fi/a/74-20112752</a>
D27	Sailaranta	19.10.2024	Kuka kantaa vastuun Nordean toistuvista it-häiriöistä? ”Ei mennyt suunnitelmien mukaan”	Tivi	<a href="https://www.tivi.fi/uutiset/kuka-kantaa-vastuun-nordean-toistuvista-it-hairioista-ei-mennyt-suunnitelmien-mukaan/5c1d9475-fb8e-4e54-b4c2-4ac9ac3247ac">https://www.tivi.fi/uutiset/kuka-kantaa-vastuun-nordean-toistuvista-it-hairioista-ei-mennyt-suunnitelmien-mukaan/5c1d9475-fb8e-4e54-b4c2-4ac9ac3247ac</a>
D28	Sailaranta	11.10.2024	HS: Asiantuntijalta tiukkaa kritiikkiä Nordealle – ”Syyllistetään kotikäyttäjiä”	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/art-2000010789361.html">https://www.is.fi/digitoday/art-2000010789361.html</a>
D29	Pitkänen	26.10.2024	Nordean verkkopankkihäiriö ohi	Yle Uutiset	<a href="https://yle.fi/a/74-20120334">https://yle.fi/a/74-20120334</a>
D30	Peltonen	25.10.2024	Miksi Nordean verkkopankin häiriökierre vain jatkuu? Näin vastaa johtaja	Yle Uutiset	<a href="https://yle.fi/a/74-20113188">https://yle.fi/a/74-20113188</a>
D31	Pantzar	22.9.2024	Nordea har været under cyberangreb 25 dage i træk	Finanswatch	<a href="https://finanswatch.dk/Finansnyt/Pengeinstitutter/article17522707.ece">https://finanswatch.dk/Finansnyt/Pengeinstitutter/article17522707.ece</a>
D32	Oxvig	10.10.2024	Nordean pankkiongelmät jatkuvat	Yle Uutiset	<a href="https://yle.fi/a/74-20113097">https://yle.fi/a/74-20113097</a>
D33	Oukanen	21.9.2024	Kuka kantaa vastuun Nordean toistuvista it-häiriöistä? ”Ei mennyt suunnitelmien mukaan”	Tivi	<a href="https://www.tivi.fi/uutiset/kuka-kantaa-vastuun-nordean-toistuvista-it-hairioista-">https://www.tivi.fi/uutiset/kuka-kantaa-vastuun-nordean-toistuvista-it-hairioista-</a>

					ei-mennyt-suunnitelmien-mukaan/5c1d9475-fb8e-4e54-b4c2-4ac9ac3247ac
D34	Aftonbladet	25.10.2024	Nordeas tjänster fungerar igen efter attack	Aftonbladet	<a href="https://www.aftonbladet.se/a/bmQ42v">https://www.aftonbladet.se/a/bmQ42v</a>
D35	Aftonbladet	3.10.2024	Nordeas problem lösta	Aftonbladet	<a href="https://www.aftonbladet.se/a/XjdArm">https://www.aftonbladet.se/a/XjdArm</a>
D36	Nyman	2.10.2024	Tietoevry: Nearly half of Finnish companies have been targeted by serious cyberattacks	Tivi	<a href="https://www.tivi.fi/uutiset/tietoevry-nearly-half-of-finnish-companies-have-been-targeted-by-serious-cyberattacks/a62447be-a920-4e8c-8bd3-5a8d03e60358">https://www.tivi.fi/uutiset/tietoevry-nearly-half-of-finnish-companies-have-been-targeted-by-serious-cyberattacks/a62447be-a920-4e8c-8bd3-5a8d03e60358</a>
D37	Nordea	23.9.2024	Päivitys: Palvelunestohyökkäykset voivat aiheuttaa hitautta Nordean digitaalisiin palveluihin kirjautumisessa	Nordea	<a href="https://www.nordea.com/fi/uutiset/paivitys-palvelunestohyokkaykset-voivat-aiheuttaa-hitautta-nordean-digitaalisiin-palveluihin-kirjautumisessa">https://www.nordea.com/fi/uutiset/paivitys-palvelunestohyokkaykset-voivat-aiheuttaa-hitautta-nordean-digitaalisiin-palveluihin-kirjautumisessa</a>
D38	Nordea	11.11.2024	Mikä on palvelunestohyökkäys ja miksi se hidastaa palveluja?	Nordea	<a href="https://www.nordea.com/fi/uutiset/mika-on-palvelunestohyokkays-ja-miksi-se-hidastaa-palveluja">https://www.nordea.com/fi/uutiset/mika-on-palvelunestohyokkays-ja-miksi-se-hidastaa-palveluja</a>
D39	Nordea	29.9.2024	Nordean digitaalisiin palveluihin vaikuttavat tekniset ongelmat	Nordea	<a href="https://www.nordea.com/fi/uutiset/nordean-digitaalisiin-palveluihin-vaikuttavat-tekniset-ongelmat">https://www.nordea.com/fi/uutiset/nordean-digitaalisiin-palveluihin-vaikuttavat-tekniset-ongelmat</a>
D40	Mauno	23.10.2024	Nordean asiakkaat joutuivat vaikeuksiin – ”Hyökkäykset eivät tule loppumaan, vaan ne jatkuvat”	Tivi	<a href="https://www.tivi.fi/uutiset/nordean-asiakkaat-joutuivat-vaikeuksiin-hyokkaykset-eivat-tule-loppumaan-vaan-ne-jatkuvat/0586f55a-9dcd-4930-bab7-7fd9308e4a38">https://www.tivi.fi/uutiset/nordean-asiakkaat-joutuivat-vaikeuksiin-hyokkaykset-eivat-tule-loppumaan-vaan-ne-jatkuvat/0586f55a-9dcd-4930-bab7-7fd9308e4a38</a>
D41	Mäntysalo	24.10.2024	Nordea-hyökkäyksissä voi olla kyse terrorismirikoksesta – asiantuntijat kertovat, miksi	Yle Uutiset	<a href="https://yle.fi/a/74-20119108">https://yle.fi/a/74-20119108</a>
D42	Mäntylä & Malminen	18.10.2024	Nordea sai puhtaat paperit pankkivaltuustolta – pankin toiminnassa ei puutteita, hyökkäys oli poikkeuksellisen laaja	Yle Uutiset	<a href="https://yle.fi/a/74-20118763">https://yle.fi/a/74-20118763</a>

D43	Mäntylä	10.10.2024	Analyysi: Nordean asiakkaat saavat nyt kärsiä päätöksistä joita on tehty jo paljon aiemmin	Yle Uutiset	<a href="https://yle.fi/a/74-20116824">https://yle.fi/a/74-20116824</a>
D44	Malminen & Kinnunen	9.10.2024	Pankkivaltuuston puheenjohtaja Ylelle: Nordean ongelmista vaaditaan nyt selvitys Finanssivalvonnalta	Yle Uutiset	<a href="https://yle.fi/a/74-20116893">https://yle.fi/a/74-20116893</a>
D45	Malminen	16.10.2024	Tässäkö syy pankkiongelmiin? Tietojärjestelmät ovat 80-luvulla käyttöönotetun keskustietokoneen varassa	Yle Uutiset	<a href="https://yle.fi/a/74-20118006">https://yle.fi/a/74-20118006</a>
D46	Mäklin	17.2.2025	Nordean verkkopankkihäiriö on ohi	Yle Uutiset	<a href="https://yle.fi/a/74-20144151">https://yle.fi/a/74-20144151</a>
D47	Magnussen	8.10.2024	Lækket rapport: Nordea kunne ikke katastrofe-teste it-setup	Version2	<a href="https://www.version2.dk/artikel/laekket-rapport-nordea-kunne-ikke-katastrofe-teste-it-setup">https://www.version2.dk/artikel/laekket-rapport-nordea-kunne-ikke-katastrofe-teste-it-setup</a>
D48	Linnake	2.12.2024	Asiantuntijalta kylmää kyytiä Nordealle – näin pankki puolustautuu	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/art-200010862819.html">https://www.is.fi/digitoday/art-200010862819.html</a>
D49	Linnake	4.12.2024	Asiantuntija odottaa Suomeen Nordeaa pahempia palvelunestohyökkäyksiä	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/tietoturva/art-200010873507.html">https://www.is.fi/digitoday/tietoturva/art-200010873507.html</a>
D50	Leskinen	4.5.2021	Nordean miljardiluokan järjestelmä uudistus – ”Se ei voi olla erillinen it-hanke”	Tivi	<a href="https://www.tivi.fi/uutiset/nordean-miljardiluokan-jarjestelmauudistus-se-ei-voio-lla-erillinen-it-hanke/e7b22dd4-184c-4c01-9074-67291621aad5">https://www.tivi.fi/uutiset/nordean-miljardiluokan-jarjestelmauudistus-se-ei-voio-lla-erillinen-it-hanke/e7b22dd4-184c-4c01-9074-67291621aad5</a>
D51	Leppälä	4.11.2024	Cyberattacks in Finland surge dramatically: over 900 attacks per week	Tivi	<a href="https://www.tivi.fi/uutiset/cyberattacks-in-finland-surge-dramatically-over-900-attacks-per-week/bf5dc2b6-c1a7-4fd3-8a23-b31cc627cff4">https://www.tivi.fi/uutiset/cyberattacks-in-finland-surge-dramatically-over-900-attacks-per-week/bf5dc2b6-c1a7-4fd3-8a23-b31cc627cff4</a>
D52	Leino	30.10.2024	A toaster can attack a bank – Finnish researcher develops solution to IoT device security issues	Tivi	<a href="https://www.tivi.fi/uutiset/a-toaster-can-attack-a-bank-finnish-researcher-develops-solution-to-iot-device-security-issues/dac739a4-e139-4e13-be9d-59f2eaff2661">https://www.tivi.fi/uutiset/a-toaster-can-attack-a-bank-finnish-researcher-develops-solution-to-iot-device-security-issues/dac739a4-e139-4e13-be9d-59f2eaff2661</a>
D53	Kononen & Seppä	6.10.2024	Nordean tilejä katosi – syy selvisi	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/art-200010744249.html">https://www.is.fi/digitoday/art-200010744249.html</a>

D54	Kolehmainen	21.10.2024	Nordea kärsii nyt ankarista häiriöistä – Pankki tekee samalla kertaa isointa järjestelmämuutosta 25 vuoteen: Nordea kiistää yhteydet asioiden välillä – Tässä asian taustat	Tekniikka & Talous	<a href="https://www.tekniikkatalous.fi/uutiset/nordea-karsii-nyt-ankarista-hairioista-pankki-tekee-samalla-kertaa-isointa-jarjestelmamuutosta-25-vuoteen-nordea-kiistaa-yhteydet-asioiden-valilla-tassa-asian-taustat/87f98dc4-c278-4bb2-8fda-8714819de015">https://www.tekniikkatalous.fi/uutiset/nordea-karsii-nyt-ankarista-hairioista-pankki-tekee-samalla-kertaa-isointa-jarjestelmamuutosta-25-vuoteen-nordea-kiistaa-yhteydet-asioiden-valilla-tassa-asian-taustat/87f98dc4-c278-4bb2-8fda-8714819de015</a>
D55	Kolehmainen	20.10.2024	”Törkeä tietoliikenteen häirintä” ja ”kansainvälistä ulottuvuutta”, mutta muuta poliisi ei sano – KRP käynnisti esitutinnan Nordean tapauksesta	Tekniikka & Talous	<a href="https://www.tekniikkatalous.fi/uutiset/torkea-tietoliikenteen-hairinta-ja-kansainvalista-ulottuvuutta-mutta-muuta-poliisi-ei-sano-krp-kaynnisti-esitutinnan-nordean-tapauksesta/b9dcd620-014c-4331-9c10-be5705d7324d">https://www.tekniikkatalous.fi/uutiset/torkea-tietoliikenteen-hairinta-ja-kansainvalista-ulottuvuutta-mutta-muuta-poliisi-ei-sano-krp-kaynnisti-esitutinnan-nordean-tapauksesta/b9dcd620-014c-4331-9c10-be5705d7324d</a>
D56	Kolehmainen	17.10.2024	Nordea kärsii häiriöistä keskellä miljardiluokan it-uudistusta – kiistää yhteyden	Tivi	<a href="https://www.tivi.fi/uutiset/nordea-karsii-hairioista-keskella-miljardiluokan-it-uudistusta-kiistaa-yhteyden/f004b47f-a5fb-4acb-b8de-b1e9a73f9e56">https://www.tivi.fi/uutiset/nordea-karsii-hairioista-keskella-miljardiluokan-it-uudistusta-kiistaa-yhteyden/f004b47f-a5fb-4acb-b8de-b1e9a73f9e56</a>
D57	Kavander & Santaharju	8.10.2024	Nordean ongelmat ohi tältä päivältä – vastauksia kysymyksiin on vaikea saada	Yle Uutiset	<a href="https://yle.fi/a/74-20116524">https://yle.fi/a/74-20116524</a>
D58	Kavander & Pantsu	20.9.2024	Syypäät Nordean verkkopankkihäiriöihin paljastuivat – pankki pahottelee	Yle Uutiset	<a href="https://yle.fi/a/74-20112889">https://yle.fi/a/74-20112889</a>
D59	Kärkkäinen	15.10.2024	HS: Nordean ongelmien tarkoitus on horjuttaa yhteiskuntaa	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/tietoturva/art-2000010764319.html">https://www.is.fi/digitoday/tietoturva/art-2000010764319.html</a>
D60	Kärkkäinen	23.9.2024	Nordea, mitä on oikein meneillään? Nyt pankki vastaa	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/art-2000010715956.html">https://www.is.fi/digitoday/art-2000010715956.html</a>
D61	Kärkkäinen	20.9.2024	Kommentti: Hei Nordea, miten menee noin niinku omasta mielestä?	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/art-2000010710521.html">https://www.is.fi/digitoday/art-2000010710521.html</a>
D62	Kangas	15.11.2024	Nordean palveluissa häiriö – saapuvissa maksuissa viiveitä	Yle Uutiset	<a href="https://yle.fi/a/74-20124790">https://yle.fi/a/74-20124790</a>
D63	Kangas	9.10.2024	Nordean liiketoimintajohtaja: Pankkiin kohdistuu koko ajan uusia hyökkäyksiä	Yle Uutiset	<a href="https://yle.fi/a/74-20116998">https://yle.fi/a/74-20116998</a>

D64	Jylhä	9.10.2024	USU: Yli 500 Nordean asiakasta sai tarpeekseen	Ilta-Sanomat	<a href="https://www.is.fi/digitoday/art-2000010752721.html">https://www.is.fi/digitoday/art-2000010752721.html</a>
D65	Joukanen	6.10.2024	Nordealla jälleen ongelmia verkkopankissa – tilin saldo näyttää nol- laa	Yle Uutiset	<a href="https://yle.fi/a/74-20116147">https://yle.fi/a/74-20116147</a>
D66	Jäärni	10.10.2024	Nordea toivoo, että asiakkaiden luottamus säilyy ongelmista huoli- matta, mutta Minnamari Dahlberg menetti sen jo	Yle Uutiset	<a href="https://yle.fi/a/74-20114346">https://yle.fi/a/74-20114346</a>
D67	Jäärni	9.10.2024	Harkitsetko pankin vaihtamista Nordean jatkuvien häiriöiden takia? Kerro kokemuksistasi	Yle Uutiset	<a href="https://yle.fi/a/74-20116809">https://yle.fi/a/74-20116809</a>
D68	Horppu & Niemi	6.10.2024	Asiakkaiden tilejä katosi Nordean verkkopankista – Nordea-pomo: Palvelunestohyökkäykset ovat lisääntyneet Pohjoismaissa	Yle Uutiset	<a href="https://yle.fi/a/74-20116159">https://yle.fi/a/74-20116159</a>
D69	Herrala	16.10.2024	Nordean johtaja kertoo, mistä on kyse – 360 palvelunestohyök- käystä kuukaudessa, tekijällä kymmenien miljoonien eurojen re- surssit	Tivi	<a href="https://www.tivi.fi/uutiset/nordean-joh-taja-kertoo-mista-on-kyse-360-palve-lunestohyokkaysta-kuukaudessa-tekijalla-kymmenien-miljoonien-eurojen-resurs-sit/343bc7e4-c5b7-47a1-89d6-dd12ebfcb6ed">https://www.tivi.fi/uutiset/nordean-joh-taja-kertoo-mista-on-kyse-360-palve-lunestohyokkaysta-kuukaudessa-tekijalla-kymmenien-miljoonien-eurojen-resurs-sit/343bc7e4-c5b7-47a1-89d6-dd12ebfcb6ed</a>
D70	Helakallio	22.10.2024	Leaders are the weak link in cybersecurity – 36% disable protec- tions	Tivi	<a href="https://www.tivi.fi/uutiset/leaders-are-the-weak-link-in-cybersecurity-36-disable-protections/b5adf379-1c56-4c72-99b0-f7f9d10f274b">https://www.tivi.fi/uutiset/leaders-are-the-weak-link-in-cybersecurity-36-disable-protections/b5adf379-1c56-4c72-99b0-f7f9d10f274b</a>
D71	Helakallio	15.10.2024	Finland strengthens its cyber readiness – new strategy unveiled	Tivi	<a href="https://www.tivi.fi/uutiset/finland-strengt-hens-its-cyber-readiness-new-strategy-unveiled/ae11e013-3b77-4280-906d-41aa101e4c87">https://www.tivi.fi/uutiset/finland-strengt-hens-its-cyber-readiness-new-strategy-unveiled/ae11e013-3b77-4280-906d-41aa101e4c87</a>
D72	Helakallio	9.10.2024	Fragmented cybersecurity regulations endanger organizations – "The weakest link endangers everyone"	Tivi	<a href="https://www.tivi.fi/uutiset/fragmented-cy-bersecurity-regulations-endanger-or-ganizations-the-weakest-link-endangers-everyone/fb1ea69b-284c-4a5d-bafa-25173cdb45a9">https://www.tivi.fi/uutiset/fragmented-cy-bersecurity-regulations-endanger-or-ganizations-the-weakest-link-endangers-everyone/fb1ea69b-284c-4a5d-bafa-25173cdb45a9</a>
D73	Heikkilä & Valkama	8.10.2024	Nordean ongelmista ei todennäköisesti voi saada korvauksia – laki antaa pankeille sopimusvapauksia	Yle Uutiset	<a href="https://yle.fi/a/74-20116722">https://yle.fi/a/74-20116722</a>

D74	Heikkilä	25.10.2024	Nordean häiriö ohi – verkkopankissa oli Pohjoismaiden laajuinen palvelunestohyökkäys	Yle Uutiset	<a href="https://yle.fi/a/74-20120325">https://yle.fi/a/74-20120325</a>
D75	Heikkilä	14.9.2024	Nordean verkkopankin häiriöt korjattu – ensi yölle luvassa mahdollisia katkoja	Yle Uutiset	<a href="https://yle.fi/a/74-20111558">https://yle.fi/a/74-20111558</a>
D76	Harjumaa	19.9.2024	Nordean verkkopankissa taas häiriötä	Yle Uutiset	<a href="https://yle.fi/a/74-20112784">https://yle.fi/a/74-20112784</a>
D77	Grasmo	21.5.2024	Siste nytt fra Norge og utlandet - Nordea har løst tekniske problemer	Aftenposten	<a href="https://www.aftenposten.no/norge/i/mBKed4/siste-nytt-fra-norge-og-utlandet?pinnedEntry=102732">https://www.aftenposten.no/norge/i/mBKed4/siste-nytt-fra-norge-og-utlandet?pinnedEntry=102732</a>
D78	Ekberg	8.10.2024	Nordea har teknikstrul	Aftonbladet	<a href="https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1295967">https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1295967</a>
D79	Forsberg	25.10.2024	Cyberattack mot Nordea	Aftonbladet	<a href="https://www.aftonbladet.se/a/LMk9B4">https://www.aftonbladet.se/a/LMk9B4</a>
D80	Aprea	8.10.2024	Teknikproblem hos Nordea under tisdagen	Aftonbladet	<a href="https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1295989">https://www.aftonbladet.se/nyheter/a/Rr77qd/aftonbladet-direkt?pinnedEntry=1295989</a>
D81	Ali-Hokka	6.10.2024	Nordeaa vastaan hyökkää ryhmä, joka väittää syyksi Koraanien polton Ruotsissa – tietoturva-asiantuntija ei selitystä niele	Yle Uutiset	<a href="https://yle.fi/a/74-20116174">https://yle.fi/a/74-20116174</a>
D82	Ahokas	4.6.2021	Pankkien it-toimittaja haluaa jättiuidistuksesta eroon – ”Meillä on voimassaoleva sopimus”	Tivi	<a href="https://www.tivi.fi/uutiset/pankkien-it-toimittaja-haluaa-jattiuudistuksesta-eroon-meilla-on-voimassaoleva-sopimus/187e1b9f-54a3-4cd6-92e2-2d0ec7f7414f">https://www.tivi.fi/uutiset/pankkien-it-toimittaja-haluaa-jattiuudistuksesta-eroon-meilla-on-voimassaoleva-sopimus/187e1b9f-54a3-4cd6-92e2-2d0ec7f7414f</a>
D83	Aaltonen	9.10.2024	Hundreds of technical failures in online banks annually – no legal upper limit	Tivi	<a href="https://www.tivi.fi/uutiset/hundreds-of-technical-failures-in-online-banks-annually-no-legal-upper-limit/4a090c42-ed85-407e-bdfd-df025f6669c4">https://www.tivi.fi/uutiset/hundreds-of-technical-failures-in-online-banks-annually-no-legal-upper-limit/4a090c42-ed85-407e-bdfd-df025f6669c4</a>
D84	STT	6.10.2024	Häiriöt   Nordean muutostoissa katosi joidenkin asiakkaiden tilitietoja – pankin mukaan vika korjattu	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010744256.html">https://www.hs.fi/talous/art-2000010744256.html</a>
D85	Juntunen	26.10.2024	Häiriöt   Tietoturva-asiantuntija moittii Nordeaa: ”Nyt syyllistetään kotikäyttäjiä”	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010789235.html">https://www.hs.fi/talous/art-2000010789235.html</a>

D86	Lassila	15.10.2024	Kyberturvallisuus   Yksi hönäytetty kone kunkin kotona voi olla osasyllinen Nordean verkkopankin piinaan	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010764466.html">https://www.hs.fi/talous/art-2000010764466.html</a>
D87	Junkkari	8.10.2024	Nordea kutsuttiin eduskuntaan kuultavaksi jatkuvien häiriöidensä takia   HS.fi	Helsingin Sanomat	<a href="https://www.hs.fi/politiikka/art-2000010750087.html">https://www.hs.fi/politiikka/art-2000010750087.html</a>
D88	Oksanen	8.10.2024	Pankit   Monen Nordean asiakkaan mitta täyttymässä: ”Tuntuu todella oudolta”	Helsingin Sanomat	<a href="https://www.hs.fi/suomi/art-2000010749728.html">https://www.hs.fi/suomi/art-2000010749728.html</a>
D89	Suutari	5.5.2025	Pankit   Nordea joutui palvelunestohyökkäyksen kohteeksi	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000011212898.html">https://www.hs.fi/talous/art-2000011212898.html</a>
D90	Raeste	15.10.2024	Pankit   Nordea: Verkkohyökkäysten voima ja kesto täysin ennennäkemätön, tarkoitus horjuttaa yhteiskuntaa	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010761540.html">https://www.hs.fi/talous/art-2000010761540.html</a>
D91	Lassila	9.10.2024	Pankit   Nordean häiriöt alkoivat sen jälkeen, kun Ruotsi hyväksyi ison Ukraina-tukipaketin	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010750389.html">https://www.hs.fi/talous/art-2000010750389.html</a>
D92	Oksanen & Vahtera	25.10.2024	Pankit   Nordean häiriöt ohi – hyökkäys aiheuttanut ongelmia useissa maissa	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010788804.html">https://www.hs.fi/talous/art-2000010788804.html</a>
D93	STT	16.9.2024	Pankit   Nordean mobiili- ja verkkopankissa oli laajoja ongelmia	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010699809.html">https://www.hs.fi/talous/art-2000010699809.html</a>
D94	Niemi & Kallionpää	20.9.2024	Pankit   Nordean palveluhäiriöiden syy selvisi: taustalla huoltotyöt ja palvelunestohyökkäykset	Helsingin Sanomat	<a href="https://www.hs.fi/suomi/art-2000010710794.html">https://www.hs.fi/suomi/art-2000010710794.html</a>
D95	Närhi	5.10.2024	Pankit   Nordean verkkopalveluissa oli taas häiriö, taustalla jälleen palvelunestohyökkäys	Helsingin Sanomat	<a href="https://www.hs.fi/talous/art-2000010743728.html">https://www.hs.fi/talous/art-2000010743728.html</a>
D96	Pietiläinen	10.10.2024	Pankkihäiriöt   HS selvitti: Nordean viimeaikaiset ongelmat ovat vain jäävuoren huippu	Helsingin Sanomat	<a href="https://www.hs.fi/tutkiva/art-2000010750754.html">https://www.hs.fi/tutkiva/art-2000010750754.html</a>
D97	Kantola	15.10.2024	Tietoturva   Isoihin organisaatioihin hyökätään nyt ovelalla taktiikalla – Tätä on ”mattopommitus”	Helsingin Sanomat	<a href="https://www.hs.fi/suomi/art-2000010760856.html">https://www.hs.fi/suomi/art-2000010760856.html</a>
D98	Oksanen	10.10.2024	Tunnistautuminen   Yhä useampi suomalainen haluaa nyt vaihtoehdon pankkitunnuksilla tunnistautumiselle – Näin toimii mobiilivarmenne	Helsingin Sanomat	<a href="https://www.hs.fi/suomi/art-2000010752537.html">https://www.hs.fi/suomi/art-2000010752537.html</a>
D99	Karvala	10.10.2024	Nämä merkit viittaavat siihen, että Nordea-sotkun takana on Venäjä	Ilta-lehti	<a href="https://www.iltalehti.fi/politiikka/a/9f0c07b4-5b72-452e-a881-4722f72c346b">https://www.iltalehti.fi/politiikka/a/9f0c07b4-5b72-452e-a881-4722f72c346b</a>

## APPENDIX C: INTERVIEW GUIDE

Theme	Main question	Follow-up/Variant
Leadership and the role of management	How should organizational leadership be involved in managing cyber incidents?	What kinds of roles and responsibilities have you had in your work?
	How should responsibilities be divided during an incident?	How do financial sector actors cooperate with each other?
Significance of communication	How does the Finnish financial sector communicate cyber disruptions externally?	Have you participated in crisis communication planning in your work?
	How can stakeholder trust be maintained and supported during incidents?	What role does communication have in incident response?
	How internal and external communication could be enhanced during cyber incidents?	How to enable flow of information?
Regulation and responsibilities	How clear do you consider the current regulation and guidance on incident response to be?	How does DORA affect your work?

	Does Finnish and European regulations support organizations to develop their incident response activities?	
	Are there any gaps or ambiguities in regulation or supervision that could affect the management of incidents?	
Skills and ECSF roles	How well do you think financial sector organizations are identifying and developing cybersecurity skills, especially in terms of incident response?	
	Have you identified skills gaps or development areas?	Can you assess the organization's own expertise at a sufficient level?
	Could a model such as the European Cybersecurity Skills Framework help to structure and develop skills?	What kinds of roles and skills are needed in incident response?
Technological and structural challenges	What are the main technical or structural factors that can make it difficult to respond to disruptions?	
	How do you assess the technical and infrastructural	

	capabilities of the Finnish financial sector for incident response?	
	How should organizations test recovery procedures?	How to ensure that development measures are permanent?
Organizational resilience and incident response	How would you describe the financial sector's ability to recover from large-scale cyber disruptions?	What are the biggest challenges in incident response?
	What factors support or undermine organizational resilience?	What is the incident process like in the financial sector?
Other	What would be the most important area for development to strengthen incident response capabilities in the Finnish financial sector?	
	Is there anything else you would like to raise on this topic?	