DORA: Friend or Foe?

A Qualitative Study into the Perceptions of the Financial Sector in the EU on the Expectation of the Digital Operational Resilience Act

J.B. ter Haar

TU Delft

An electronic version of this thesis is available at http://repository.tudelft.nl/

DORA: Friend or Foe?

Master thesis submitted to Delft University of Technology

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in **Engineering and Policy Analysis**

Faculty of Technology, Policy and Management

by

Jeroen ter Haar

Student number: 4454383

To be defended in public on the 28th of November, 2022.

Graduation committee

Chairperson:	Prof.dr.ir. P.H.A.J.M. (Pieter) van Gelder	Safety and Security Science
First supervisor:	Dr. S.E. (Simon) Parkin	Governance of Cybersecurity
External supervisor:	R. (Rabab) Laarabi	Cybersecurity consultant

TU Delft

Preface

Dear reader,

In front of you lies the Master Thesis report on 'A Qualitative Study into the Perceptions of the Financial Sector in the EU on the Expectation of the Digital Operational Resilience Act'. The foundation of this research is a combination of semi-structured interviews that was distributed among high-level security managers of Financial Services Organizations and ICT service providers. The report has been written as part of the completion of the Master Engineering and Policy Analysis at the Technical University of Delft. I have been engaged in researching this topic from April until November 2022.

I would like to express my gratitude to some people without whom I would not be where I am now. To start off, I would like to thank my first supervisor Simon Parkin. Thank you for your guidance, our interesting discussions about the thesis and life itself. Even though this qualitative angle of research was quite new to me, you have guided me through it and where I had ups and downs in the process you were always prepared to free up some time to help me. Secondly, I would like to thank Pieter van Gelder for being chair on my graduation committee. Although smaller than Simon's, your role and vision has helped me towards this final result. I also would like to thank the people at EY who have provided me with supervision over the past six months. To my EY supervisor, Rabab Laarabi, thank you for your insights as a cybersecurity consultant and helping me shape this project to what it is now. I would also like to thank Niels Wagenaar, although not my direct supervisor, for the moments in the office, however short, that have helped me accomplish great steps and make decisions in my thesis.

I am forever grateful to my parents, who have supported me throughout my entire education and were always there for me. I would not have been able to do this without them. Finally, I would like to thank my friends and especially my girlfriend Cathelijn, who were forced to listen to me ramble on about the digital operational resilience of the financial sector in the EU and have supported me always.

Thank you all, I hope you enjoy reading this report.

J.B. ter Haar

Amsterdam, November 2022

Management summary

Major disruptive events can have an enormous impact on the critical infrastructure. This has come to light through multiple incidents over the course of the past few years, such as the COVID-19 pandemic and the Russian invasion of Ukraine. These two events are physical threats affecting the critical infrastructure and society. There are, however, less explicit threats increasing in relevance: cyber attacks. Incidents like the Petya virus in 2016 or the Wannacry attack have had disastrous consequences. The rapid development of technology has given rise to many opportunities but also vulnerabilities for the critical infrastructure. The financial sector is especially prone to cyber attacks within the critical infrastructure. The financial sector must be available at all times. Even a minor disruption could cause wrongful or unexecuted transactions leading to cascading effects on careers, organizations, or entire industries. The way to cope with attacks and disruptive events is through operational resilience; for cyber attacks, this is digital operational resilience. But digital operational resilience is becoming harder to manage due to the complexity of operational processes, the reliance on third-party suppliers, the interconnectedness of the professional landscape, and the sophistication of malicious actors. This has made (1) digital operational resilience harder to manage, (2) the likelihood of disruption more significant, and (3) the impact of disruptions more severe.

In order to ensure digital operational resilience for the financial sector, many guidelines, frameworks, and regulations have been implemented. These were, however, often on a national level or for a specific sector within the financial sector, such as banking, insurance, or pension funds. In line with the rapid development of technology and associated threats, the European Commission has proposed the digital finance package in 2020. A part of this is the proposal for the Digital Operational Resilience Act. An act expected to enter into force at the end of 2022 aimed at harmonizing existing regulations and thereby ensuring a digital operational resilient financial sector in the EU. In order to estimate the regulatory performance of the DORA, insight is to be created into the perceptions of the stakeholders. Therefore, the research question of this thesis is:

What is the perception of the financial sector towards the expectation of the Digital Operational Resilience Act?

In order to answer this research question, interviews were conducted with high-level security managers of financial service organizations (FSOs) in the Netherlands. In preparation for these interviews, the DORA proposal was translated into 18 statements covering the requirements for the FSOs. In the first half of the interview, the participants had to give their organization a preparedness score for these 18 statements. The second half of the interview consisted of a semi-structured interview setup where the perceptions of the participant towards the DORA were studied. To create a more extensive insight into the stakeholders' perceptions towards the DORA, additional interviews were conducted with a security manager from a Dutch ICT service provider, a member of the European Banking Federation, and someone from the Dutch financial authority De Nederlandsche Bank (DNB).

From the insights gathered through the interviews, it can be concluded that most participants agreed on the fact that the DORA does not introduce any shockingly new concepts to the regulatory framework. Some participants regarded two aspects of the DORA as new: ICT major incident reporting and ICT third-party risk management. However, the larger part of the participants saw these two concepts' requirements merely as 'more detailed than previous regulation'. These two concepts were mentioned the most when asked for benefits that the DORA will bring to the financial sector, as well as the general awareness of the necessity for digital operational resilience in the changing professional landscape and rapid digitization of processes and services. The challenges identified were related to the fact that the DORA will be another paper to comply with due to the level of detail required by the DORA. Nevertheless, the participants were generally confident in their ability to comply within 24 months. They do not expect the financial sector to be resilient once everyone is compliant, but they perceive the DORA as a step in the right direction. In general, the perception of the financial sector towards the DORA is positive.

These conclusions lead to recommendations to both supervisory authorities and the financial sector. First, the perceptions towards the DORA are predominantly positive, which means that the regulation has a significant chance of success. Therefore, the supervisory authorities should aim for the DORA to be the single point of truth in ICT regulation in the EU for the financial sector. The second recommendation for the supervisory authorities is to take care in designing the technical standards of the DORA but publish them as soon as possible. An extended period between the implementation of the DORA and the publication of these standards can cause more discomfort with the regulation, leading to lower performance. Thirdly, the FSOs need to prepare for the DORA. They must get a good overview of their entire ICT supply chain and reach out to these ICT service providers to inform them about the coming of the DORA, as the regulation also entails significant changes for them. Fourth, the FSOs should focus on mapping the DORA criteria to their existing controls and identifying gaps and problems. Independent third parties might assist FSOs in avoiding overestimating present maturity or underestimating DORA requirements. It is encouraging to note that the majority of FSOs are confident in their capacity to comply with the legislation within the time frame specified, but they should be cautious about the actual work required to adapt to the new criteria.

Contents

Nomenclature

Abbreviation	Definition
API	Application Programming Interface
CERT	Crisis Emergency Response Team
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, and Availability
DDoS	Distributed Denial of Service
DNB	De Nederlandsche Bank
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EBF	European Banking Federation
EC	European Commission
EIOPA	European Insurance and Occupational Pensions Authority
EPA	Engineering and Policy Analysis
ESAs	European Supervisory Authorities
ESFS	European System of Financial Supervision
ESMA	European Securities and Markets Authority
ESRB	European Systemic Risk Board
EU	European Union
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSO	Financial Service Organisation
GDPR	General Data Protection Regulation
HREC	Human Research Ethics Committee
ICT	Information and Communication Technology
ISO	International Organization for Standardization
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OECD	Organisation for Economic Co-operation and Development
SaaS	Software as a Service
TLPT	Threat-Led Penetration Testing

List of Figures

List of Tables

1 Introduction

This section of the report contains the introduction. First, in Section 1.1, the topic's background will be discussed. Secondly, Section 1.2 defines the research problem. In Section 1.3, the scope of the study is explained. After defining the research problem and the scope Section 1.4 presents the research questions that this study aims to answer. Section 1.5 discusses the societal relevance followed by the fit with the MSc. program Engineering and Policy Analysis in Section 1.6. Finally, the outline of this thesis is presented in Section 1.7.

1.1 Background

Throughout the past few years, major global events have disrupted critical infrastructure. First, the pandemic in 2020 exposed the resilience of many companies, and now in 2022, the war in Ukraine has disrupted energy services, supply chains, and other critical infrastructures (Gumbau, 2022; Simchi-Levi and Haren, 2022). Critical services can be defined as *'services and products that are vital to the functioning of our societies and economies'* (National Research Council, 2002). The COVID-19 pandemic and the war in Ukraine are two major events, but there have been many disruptive events in the last 20 years. Some of these have a natural cause, such as the volcanic eruption of the Eyjafjallajökull in Iceland in 2010, shutting down air travel for seven days (Perkins, 2011), others with a man-made nature, such as the global economic crisis of 2008 (Williams, 2010).

There are, however, less tangible events that can disrupt the critical infrastructure on a large scale: cyber incidents. Cyber crises are a severe risk to societies because of their potential to cascade and seriously disrupt essential services (Boeke, 2018). For example, in 2015, a presumed Russian cyber attack successfully hacked the Prykarpattyaoblenergo power station in Ukraine, leaving over 230,000 people without power for 6 hours. The control systems of the power station were more secure than most systems in the world, emphasizing just how vulnerable these systems are globally. The sophistication needed for the cyber attack to be successful showed that the hackers could have permanently disabled the power station. The fact that this did not happen shows that the attack was meant as a message (Zetter, 2016). Ukraine was also the initial point of the Petya virus in 2016, after which it spread across the globe within hours. The virus had a major impact, causing container ports to shut down, drug production lines to come to a standstill, and even forcing a large French manufacturing company to return to work with pen and paper (Jacqué, 2017). The costs have been estimated to be over a billion euros (Untersinger, 2017). One of the other largest cyber attacks of the last decade was the Wannacry cyber attack. This attack encrypted data on computers using Microsoft Windows operating systems, demanding ransom payments in Bitcoin, affecting organizations worldwide, including 40 hospitals in the UK (Woollaston-Webber, 2017). These three attacks demonstrate the major disruptive impacts that cyber incidents can have. Dieye et al. (2020) studied the macroeconomic costs of cyber attacks. The main findings were that it is difficult to assess damage at the firm and the macro level due to the interdependencies between various economic sectors and the potential for cascading effects of cyber attacks. (Ali and Santos, 2015) showed

through a dynamic model analyzing a denial-of-service (DoS) attack that cyber attacks' cascading properties can cause ripple effects across different economic sectors.

Technology has seen rapid development over the past decades, transforming the professional landscape into a digital one. This digitization has enabled previously unimaginable opportunities across the globe but opened the door to new risks as well. The digital landscape brings a new kind of risk to organizations. Cybercriminals have become more sophisticated and better at attacking payment systems and digital infrastructures (Khiaonarong et al., 2021). The financial sector is especially at risk for cyber attacks within the critical infrastructure. It has been estimated to be three times more at risk of cyber attacks than any other sector (European Parliament, 2017), and the (European Systemic Risk Board, 2020) identified cyber risk as one of the sources of systemic risk to the global financial sector.

The way to cope with disruptive events is through operational resilience. Resilience is a *'fuzzy term'*, meaning there is ambiguity in the word's definition. For the sake of this research, a definition is needed. Björck et al. (2015) propose the following definition for cyber resilience, which will be used in this study: The ability to continuously deliver the intended outcome despite adverse cyber events. The digitization of the professional landscape has caused an increase in threats and vulnerabilities and has called for greater oversight and regulatory actions to ensure digital operational resilience. This has caused the regulatory landscape to be heavily fragmented. To harmonize the regulations, the European Commission has proposed the Digital Operational Resilience Act (DORA) (European Commission, 2020b). The DORA is focused on the digital operational resilience of the financial sector in the EU. It is proposed by the European Commission to enable and support the potential of digital finance while mitigating its risks. The DORA is expected to enter into force at the end of 2022, with the compliance date two years later, in 2024.

1.2 Research problem

The financial sector is subject to many regulations and guidelines for cyber security and resilience. The DORA aims to harmonize these regulations to draw one line for the entire financial sector in the EU and thus ensure a digital operational resilient financial system in the EU. Resilience, however, is hard to measure, as it entails the occurrence of an incident. It is the ability to deliver the intended outcome despite adverse cyber events. Something's resilience can only be measured after a disruptive event. There are theoretical models to measure resilience, but these are not applicable to a system as large and complex as the financial sector of the EU. Hence, the effectiveness of the DORA is hard to estimate. It is known, however, that the perceptions of a regulation's stakeholders impact its performance. The OECD (2012) published a report on measuring regulatory performance. This report is focused on using perception surveys to evaluate regulatory reforms because perceptions influence the final effectiveness of regulation. As the resilience of the financial sector is hard to measure, the effectiveness of the DORA will depend on the perceptions of the regulation. Because the regulation has yet

to go into force, the perceptions are towards the expectation of the DORA. This study's research problem is focused on measuring the DORA's stakeholders' perception to estimate the regulation's performance.

1.3 Scope

The DORA is a proposal done by the European Commission and will be effective in the entire EU. Financial Services Organizations (FSOs) located outside the EU but with operations in the EU will have to comply with the DORA as well in these areas. As this study relies on the DORA and tries to anticipate its effectiveness and effects, the scope will be digital operational resilience for financial services. Financial services are a crucial part of the critical infrastructure, and it is the sector with the highest cyber risk. Therefore, the scope of this research will be financial services organizations in the EU. This research will use the Dutch financial sector as a leading example.

1.4 Research Questions

This section presents the main research question that this study aims to answer, followed by sub-questions that will aid in answering the main research question. To give insight into the expected impact that DORA will have on the digital operational resilience of the financial sector in the EU, the perceptions of the entities that the DORA applies to are of great importance. Since the DORA has yet to enter into force, the perceptions will be on the expectation of the DORA. Therefore, the main research question that this study aims to answer is the following:

What is the perception of the financial sector toward the expectations of the Digital Operational Resilience Act?

In order to answer the main research question properly, sub-questions have been formed. The general perception of the regulation consists of many factors, such as novelty, preparedness, benefits, and challenges. These factors together make up the general perception. For this reason, the following sub-questions have been formed:

SQ1: ***What is the perception of the financial sector towards the novelty of the DORA?***
The first sub-question aims to give insight into whether the financial sector perceives the DORA as new. Over the years, guidelines, frameworks, and regulations have been introduced for the financial sector regarding cybersecurity. These have, however, always been from separate ESAs, so they applied only to one sector within the financial sector. The DORA aims to harmonize these guidelines; therefore, it is interesting to see whether the FSOs view this as merely a harmonization of existing guidelines or as a new regulation.

SQ2: ***What is the perception of the financial sector towards their preparedness for the DORA?***
The DORA is expected to go into force at the end of 2022. In line with the first sub-question, it is interesting to see how the FSOs view their preparedness for implementing the DORA. If they perceive the DORA as a mere harmonization of existing regulations, that should mean their preparedness is very high. Their perceived level

of preparedness will also affect the DORA's impact on the digital operational resilience of the financial sector.

SQ3: ***What is the perception of the financial sector towards the benefits of the DORA?***
The positive perception towards a new regulation and its benefits is crucial in its performance. If a regulation is perceived to bring benefits, it can influence firms' investment decisions and their compliance with regulatory requirements (OECD, 2012). Therefore, the perception of the benefits that the DORA is expected to bring affects the performance of the regulation. Conversely, a lack of awareness of benefits is harmful to performance.

SQ4: ***What is the perception of the financial sector towards the challenges of the DORA?***
In contrast to the perceived expected benefits, the challenges are also significant. The challenges will give insight into the pain points of the financial sector regarding the regulatory landscape in general and possible compliance issues with the DORA. Challenges could lead to irritation, which can have a more considerable impact on the overall perception of the regulation than the actual costs caused by the regulation (OECD, 2012). This irritation is not necessarily related to the administrative burdens imposed by the regulation (European Commission, 2009).

SQ5: ***What is the perception of the financial sector towards the expected impact of the DORA?***
The final sub-question aims to give insight into the impact that the DORA is expected to have in the eyes of the financial sector. Particularly the impact on digital operational resilience is interesting for the performance of the DORA, but for the scope of this study, the impact on the financial sector as a whole will be taken into account when answering this sub-question.

1.5 Societal relevance

We live in a turbulent world. Disruptive events have challenged organizations over the past decades. Therefore, operational resilience has become a more and more pressing matter for the critical infrastructure. In case of disruptions, critical business processes must keep running. An essential component of the increasing risks is cyber criminality. There has been a significant increase in cyber criminals, and the financial sector is three times more at risk than any other sector (European Parliament, 2017). At the same time, it is becoming harder and harder for security managers to make adequate security policies due to the rapid digitization and transformation of the landscape. The DORA aims to ensure digital operational resilience for the financial sector in the EU, which is part of the critical infrastructure. This research will explore the expected effects of the EU legislation on cyber resilience and security.

1.6 Fit with EPA

In the Master Engineering and Policy Analysis (EPA) at the faculty of Technology, Policy and Management of the Delft University of Technology, the focus is on grand challenges. EPA aims to provide decision-makers with good information to make the right decision under the given circumstances. The considered grand challenge in this thesis is cyber security. All grand challenges are essential, but in this case, the grand challenge of cyber

security overlaps with keeping the critical infrastructure safe and secure. The research will aid in providing decision-makers with information to help them make the right strategic decisions by identifying how the DORA contributes to ensuring cyber resilience in the critical infrastructure.

1.7 Outline

This report will first explain the key concepts in Section 2. After that, the literature review gives more insight into the background and states hypotheses in Section 3. Section 4 elaborates on the methodology used to answer the research question. The findings from this study can be found in Section 5. Next, a discussion of these findings and a reflection on the hypotheses can be found in Section 6. The research questions are answered, and recommendations are made in Section 7. Finally, the limitations and future research possibilities are in Section 8.

2 Key Concepts

Before analyzing the resilience of the financial sector and how the DORA will affect this, the main concepts are discussed. In this section, the concepts of critical infrastructure (Section 2.1), resilience (Section 2.2), cyber security versus cyber resilience (Section 2.3), the financial sector (Section 2.4), and the most common cyber threats (Section 2.5) are described.

2.1 Critical infrastructure

For the functioning of society, certain processes are so essential that failure or disturbance leads to serious social disruption and threatens national security (Ministerie van Justitie en Veiligheid, 2019). These processes form the critical infrastructure (CI). Electricity, access to the internet, drinking water, and payment transactions are vital processes within the CI. The Dutch CI consists of nine sectors identified by the NCTV. The increasing use of information and communication technologies makes the CI more complex, and it is becoming more dependent on each other's 'always on' availability (De Bruijne and Van Eeten, 2007). The increased interconnections and utilization of advanced networking technologies have caused societal and economic benefits but have made it harder to secure the CI as well (Kaufmann et al., 2015). Furthermore, the digital landscape brings a new risk to organizations: cybercriminals. Cybercriminals have become more sophisticated and better at attacking payment systems and digital infrastructures (Khiaonarong et al., 2021). Within the CI, the financial sector is especially at risk for cyber-attacks. The financial sector has been estimated to be three times more at risk of cyber-attacks than any other sector (Committee on Economic and Monetary Affairs, 2017), and the European Systemic Risk Board (2020) identified cyber risk as one of the sources of systemic risk to the global financial sector. In order to ensure a solid and reliable CI, resilience is needed.

2.2 Resilience

Before the concept of resilience entered the cyber domain, it had been a common term in fields such as engineering, ecology, psychology, and supply chain studies (Holling, 1996; Coutu, 2002; Sheffi and Rice Jr, 2005; Hollnagel et al., 2006). As the concept has been used in multiple areas, it is hard to give a single definition. For this study, it is essential to have a good understanding of the definition. A systemic review was performed by Birkie et al. (2014), analyzing formal definitions of resilience across different contexts. The authors found that all definitions of resilience consisted of five core functions: *sense, build, reconfigure, re-enhance*, and *sustain*.

- **Sense:** Resilience is focused on handling unanticipated, disruptive events that impact the organization or system. These are called unknown unknowns. Sensing is related to improving visibility and early detection.
- **Build:** Building the right capabilities—either naturally or through acquisition—is crucial for both proactive and reactive actions. The build core function designates a series of proactive actions. Depending on

the firm's responsiveness, these are often carried out before or after confronting altering conditions.

- **Reconfigure:** based on choice preferences and existing capabilities, the company strives to adjust to unexpected situations that have a significant impact. The answer might occur on two levels. At the most basic level, the company attempts to adapt to changing conditions by making relatively tiny incremental adjustments. At a higher level, the company may need to restructure its structure, assets, and so on to cope with long-term consequences with strategic ramifications and competitive advantage concerns.
- **Re-enhance:** This function is concerned with maintaining competitive performance levels after shocks or pressures have been felt. It is concerned with both the recovery from disruptive events and the enhancement of opportunistic events. It also emphasizes restoring performance levels that are equivalent to or better than those that existed before the incident.
- **Sustain:** The goal of adapting or reconfiguring is to keep company objectives on track. Continuing to perform in some capacity is a crucial quality that mitigates the unfavorable long-term implications of stopping and recovering.

Those five core functions encompass resilience definitions through the different fields of expertise. The authors define resilience as: *"The encompassing dynamic capabilities to sense, build, reconfigure, and re-enhance in the face of uncertainties in being able to sustain performance"* (Birkie et al., 2014). This can be understood as a broad, all-encompassing definition of resilience.

2.3 Cyber security and cyber resilience

For the purpose of this research, it is essential to understand resilience in the context of cyber and its difference with cyber security. Cyber security is a common term that has been used since the emergence of cyber and cyber threats. Cyber resilience, however, can be seen as a vague term. The definition, as given by Birkie et al. (2014), gives a better idea of how to view resilience in general. However, in the cyber area, it is essential to emphasize the difference between cyber security and cyber resilience. Cyberspace is a highly interconnected network of infrastructure, resident data, ICT devices, and components. Cyber security is the process of defending this cyberspace against intrusions by criminals and other foes. Any such assault carries risks depending on three variables: threats (who is attacking), vulnerabilities (whose weaknesses are being targeted), and impacts (how the attack affects the victims) (Fischer, 2017). An important aspect of cyber security is information security, which ensures confidentiality, integrity, and availability of information (Whitman and Mattord, 2021). This is also known as the CIA triad. Where cyber security is focused on defending against malicious actors and minimizing the impact of an incident, cyber resilience goes a step further and has a broader scope concerning not only what happens before an attack, but also including the actions during and after an attack to minimize the impact and continue operations as well as possible and bounce back to the original state or even a better state.

Björck et al. (2015) set out to define and analyze the difference and definitions of the two terms. The authors distinguish five defining characteristics to differentiate cyber resilience from cyber security: *objective, intention, approach, architecture,* and *scope.*

- **Objective:** The aim of cyber security is to protect networked IT and information systems. Cyber resilience, however, is focused on the higher-level objective of ensuring business delivery. As a result, a system is considered resilient when it can generate business value even in the face of unfavorable cyber occurrences, such as by using alternate ways of business delivery. As a result, any initiatives to improve cyber resilience must begin with business rather than information technology.
- **Intention:** The second aspect refers to the desired properties of a system. In cyber security, the intention is to design systems that the system should withstand cyber events, so they must be fail-safe. Resilient systems go one step further and must be able to fail in a controlled way. They must be safe-to-fail.
- **Approach:** A simplistic perspective of security is that it is implemented on a system. Encrypted communications, for example, can be used to secure communication between a system and its users. Another example is that corporations might establish special security teams that exclusively deal with system security. On the other hand, a resilience strategy would have a considerably more significant effect on the systems being" protected," necessitating the inclusion of resilience as an integral component of the IT systems and the organization's overall functioning. Resilience should be built in rather than added on.
- **Architecture:** The architecture of a system is concerned with its internal structure and is described as the system's component modules and their interactions. When it comes to resilient systems, the architecture must be designed to accommodate partial failure. As a result, rather than a hard exterior shell, the architecture should be viewed as a series of levels of protection. Each layer should therefore be constructed to adhere to the previously mentioned safe-to-fail approach.
- **Scope:** The scope of a cyber-resilient study cannot be limited to a single system or organization and its immediate surroundings. The reason for this is twofold: first, the danger might emerge from any of the system's numerous interconnections. Second, linkages with other systems (such as sub-suppliers) might be a source of strength regarding the systems' capacity to recover from cyber incidents.

Table 2.1 overviews the differences between cyber security and cyber resilience along the five aspects.

Table 2.1: Characteristics of cybersecurity vs. cyber resilience (Björck et al., 2015)

Aspect	**Cybersecurity**	**Cyber resilience**
Objective	Protect IT systems	Ensure business delivery
Intention	Fail-safe	Safe-to-fail
Approach	Apply security from the outside	Build security from within
Architecture	Single layered protection	Multi layered protection
Scope	Atomistic, one organization	Holistic, network of organizations

Björck et al. (2015) also propose a definition of cyber resilience in their paper, which is more concise and focused on cyber than the general and broad definition from Birkie et al. (2014). Therefore, the following definition for cyber resilience will be used in this study:

> *"Cyber resilience is the ability to continuously deliver the intended outcome despite adverse cyber events"*
>
> (Björck et al., 2015)

2.4 The financial sector

This study focuses on the digital operational resilience of the financial sector in the EU. Therefore, it is important to define the financial sector en emphasize the necessity for its resilience. The financial sector consists of all financial service organizations. As Asmundson (2017) describes it: *"at its heart, the financial sector intermediates. It channels money from savers to borrowers and matches people who want to lower risk with those willing to take on that risk"*. The author makes a broad split between FSOs: (1) insurance and related services and (2) banks and other financial service providers. Together, these form the financial sector. In this study, the FSOs are all the parties in the financial sector to which the DORA applies (see table B.1 in Appendix B). Digital operational resilience is of high importance for the financial sector. Due to risk concentration and a lack of alternatives, a business interruption of a financial market infrastructure or a group of large financial institutions might have a significant impact. For example, market participants would not be able to complete transactions if a payment and settlement system went down during the day, exposing them to liquidity and solvency risk. Similarly, equivalents of large banks that are disrupted and unable to conduct transactions would be in danger of liquidity- and solvency issues (Kopp et al., 2017). The financial industry is evolving. Institutions are implementing quicker, more responsive 24-hour internet services everywhere you look to fulfill client demand. However, as digital interaction grows, hacker organizations are enlarging their destructive footprints by using cutting-edge tools to enter operations, assault crucial programs, and steal data (Sydekum, 2018).

2.5 Most common cyber threats for the financial sector

The focus on cyber resilience within critical infrastructure, particularly the financial sector, is not superfluous. The development of technologies combined with the interconnectedness of the financial sector has made FSOs

attractive to malicious actors. Even though the actual data on cyber incidents are scarce, as organizations have no incentive to report them (Bouveret, 2018), VMware (2020) found a 238% increase in cyber attacks targeting financial institutions in the first half of 2020 through a survey with 25 Chief Information Security Officers (CISOs) from leading financial institutions. IBM and the Ponemom Institute assessed the financial sector's average cost of a data breach at $5,72 million (IBM and Ponemon Institute, 2021). Therefore, it is crucial to understand the most common cyber threats and vulnerabilities for FSOs. The most common cyber threats for FSOs that are mentioned across different sources (Bouveret, 2018; Khiaonarong et al., 2021; Kost, 2022; Ozarslan, 2022) are:

1. **Phishing**

   Phishing attacks, which have been around for decades and are still a huge issue today, pose a severe threat in the cyber world. Attackers are using a variety of innovative and inventive tactics to execute phishing assaults, which are on the rise (Alabdan, 2020). Phishing is a social engineering approach that seeks to persuade the victim of the attack to give personal information such as an email address, username, password, or financial information. The attacker subsequently exploits this information against the victim (Stavroulakis and Stamp, 2010). Email phishing is the most common form (Kost, 2022). It is estimated that 90% of successful cyber attacks start through phishing (Moramarco, 2021).

2. **Ransomware**

   Another serious cyber danger to financial institutions is ransomware. During a ransomware attack, attackers encrypt victims' computers with software, locking them out. Only by paying a ransom can the harm be repaired. Ransomware attackers utilize various extortion methods to get victims to pay a ransom. The most common strategy is to post larger chunks of confiscated sensitive material on criminal forums until a ransom is paid (Kost, 2022). The WannaCry cyber attack is an example of a successful large-scale ransomware attack (Woollaston-Webber, 2017).

3. **DDoS Attacks**

   A DDoS attack is an acronym for a Distributed Denial of Service attack. During a DDoS attack, the victim's server is overloaded with requests, forcing the system to go offline. This is a popular method for attacking financial institutions, as they have a large and diverse attack surface (Kost, 2022). Malicious actors could exploit the chaos created through a DDoS attack in two ways: launch a different cyber attack while focusing on solving the DDoS chaos or offer to solve the DDoS chaos for a ransom

4. **Supply Chain Attacks**

   In a supply chain attack, as the name suggests, the attackers enter the system through a vulnerability in the supply chain. As discussed in the previous section, the high level of interconnectedness of the financial sector and its heavy reliance on third-party IT suppliers makes this a significant threat to the financial sector.

3 Literature Review

This section of the report presents the literature review. First, the background of the DORA is discussed starting with the security focus (Section 3.1), the transformation of the professional landscape (Section 3.2), the struggle for security (Section 3.3), the shift to resilience (Section 3.4), and the existing regulations (Section 3.5). Next, the DORA and its contents are elaborated upon in Section 3.6, after which Section 3.7 goes into how the performance of the DORA can be measured. Section 3.8 compares the DORA to the GDPR and analyzes its perceptions to finally state some hypotheses for the perceptions on the DORA in Section 3.9.

3.1 Focus on security

The DORA is a regulation aimed at digital operational resilience. This is an advanced view and has developed over time. In the 1990s and 2000s, the focus was not yet on resilience but on security. The awareness of the risks of interconnected systems and networks grew, but the way to ensure a safe and secure cyberspace was to aim at cyber security (Hopcraft and Martin, 2018). This prioritization of safety and security flows through in the policies that are developed during the early 2000s (Coaffee et al., 2009). However, the early 2000s were different times than the technologically developed world we live in now. Back in 2001, there were no means to communicate quickly. Something that, through events such as 9/11, has become clear as crucial in disastrous times. Technological developments have improved communication capabilities and enabled rapid communication on a global scale. This brings benefits such as quick response in case of an incident but has also opened the door to new threats and risks. The threat has shifted from a physical one, such as a plane flying into a building, towards intangible threats, such as ransomware attacks, data leaks, and other cyber intrusions.

3.2 Transformation of the professional landscape

The examples of the Petya attack in 2016 and the global Wannacry virus illustrate how the critical infrastructure is prone to cyber attacks and how these cyber attacks can have cascading effects, with the possibility to have an enormous impact. Cyber attacks in the critical infrastructure can cascade on other firms and sectors they interact with (Ali and Santos, 2015). As mentioned before, the internal organization of a cybersecurity policy is complex (Adams and Sasse, 1999; Reinfelder et al., 2019), but other factors increase the cyber risk for organizations. Digitization has caused a transformation of the professional landscape that gives way to more vulnerabilities. The financial sector is especially at risk for cyber attacks within the critical infrastructure. The Committee on Economic and Monetary Affairs (2017) has estimated the financial sector to be three times more at risk for cyber attacks than any other sector. There are new concerns such as privacy, customer protection, cybercrime, and the interconnectedness of financial systems (Lautenschläger, 2018). Other factors, such as rapid digitization, the emergence of the complexity of financial instruments, and the expansion of operations, make resilience a more pressing matter than ever for the financial sector (Leo, 2020). These factors not only make

it harder to manage operational resilience but are also the reason that the impact of disruptions has become more severe. The increase in technological interdependencies has transformed the financial sector into a web of financial services, third-party suppliers, and other market players and infrastructures, making it possible for an IT disruption to escalate into a systemic crisis (Hernández de Cos, 2019). Along with the impact of disruptions being more significant due to the transformation, the likelihood of disruption has also grown. This can again be explained due to the complexity of operational processes, the reliance on third-party suppliers, the interconnectedness, and the sophistication of malicious actors (Khiaonarong et al., 2021). The transformation of the financial landscape has made (1) operational resilience harder to manage, (2) the likelihood of disruption more extensive, and (3) the impact of disruptions more severe. These factors have caused more concern from the regulators to ensure operational resilience in the financial sector.

3.3 The struggle for security

The security focus, in combination with the development of technologies and with that the emergence of cyber threats, has led to growing importance of cyber security. Cyber security protects networked IT and information systems (Björck et al., 2015). Cyber security is essential for the critical infrastructure, particularly the financial sector. But what makes cyber security so hard to manage?Adams and Sasse (1999) published a paper called *"Users are not the enemy"*. This research studies how security is managed in organizations and finds a tension between the ones responsible for security in organizations ("security managers") and employees whose primary tasks do not involve security ("users"). The authors portray how poor communication between the security managers and the users results in a non-functioning security policy. Users do not comprehend security concerns, and security departments do not understand users' perceptions, tasks, and needs. As a result, security departments stereotype people as "inherently insecure": at best, they are a security risk that must be managed and controlled, and at worst, they are the enemy inside. On the other hand, users see many security procedures as time-consuming and unnecessary - an impediment to their actual job. However, it is critical to refute the notion that users are never motivated to act securely. The paper concludes that most users are security-conscious as long as they perceive the need for it. Where users were often seen as the weakest link in security, Adams and Sasse (1999) illustrated how the lack of user-centered design in security mechanisms can be the problem, shifting the responsibility towards the security managers instead of the users themselves. Twenty years after the publication of this paper, Reinfelder et al. (2019) published the paper *"Security Managers are not the enemy either"* as a response to the paper of Adams and Sasse. The main recommendation from Adams and Sasse (1999) is to keep the user in mind when designing security mechanisms. However, little study has been conducted on security managers' attitudes toward users, how these attitudes develop, and how they impact decisions in security development processes (Reinfelder et al., 2019). The authors demonstrate that security managers are not the enemy either. They think and act within the confines of their scope, which is primarily defined by the organizational structures in existence. Because these institutions exclude users from the security development

process and generate a negative attitude of users, the resultant security measures, while well-intended, become unworkable. Inadequate organizational frameworks for involving users in the security development process lead to security managers' unfavorable perceptions of users and hence to a control-oriented approach rather than a user-oriented one. Implementing organizational frameworks for building user-centered security and offering relevant methodologies and tools to security managers is an important research direction that requires further development.

The papers from Adams and Sasse (1999) and Reinfelder et al. (2019) illustrate how complicated it is for an organization to design security efficiently.

3.4 Shift to Resilience

While the focus on cyber security was growing, a new term arose: resilience. The financial crisis of 2008 has caused resilience to be a prominent term in organizations and regulation but managing it has always been a critical topic (Dowell-Jones and Buckley, 2016). Coaffee (2013) demonstrates the shift from security to resilience as well. The author identifies three 'waves' of resilience policy in the UK. Resilience strategies have evolved over time and in response to various shifting socio-political and economic constraints (which have re-articulated the meaning, scale, operational role of, and responsibility for, resilience). The first wave of resilience, in the early 2000s, was primarily materially oriented, reactive by nature, and aimed to reduce security risk. However, as the 2000s progressed, more was done to emphasize the resilience cycle's preparatory components. The focus of second wave resilience policy shifted from shock absorption to the capacity of organizations, governments, and communities to absorb shocks and take preventative measures. The capacity of organizations, governments, and communities to foresee shocks and ultimately incorporate resilience into daily operations emerged as the third wave of resilience in the mid-late 2000s. Urban resilience policy has developed from a discourse of shock absorption to one of more excellent prevention, and finally to one that incorporates resilience thinking into daily activities. This focus on resilience can also be found in the cyber field. During the 2012 World Economic Forum meeting in Davos, cyber resilience was recognized as an area of growing importance, and commitments were made to improve the resilience against cyber risks (World Economic Forum, 2012).

3.5 Existing regulations

In order to establish a resilient financial sector and protect against the threats mentioned in section 2.5, several regulations and guidelines have entered into force over the last decade. In the EU, different authorities govern the financial sector. Together they compose the European System of Financial Supervision (ESFS). It consists of the European Supervisory Authorities (ESAs) and the European Systemic Risk Board (ESRB). The ESAs are three sector-specific authorities:

1. European Banking Authority (EBA)

2. European Insurance and Occupational Pensions Authority (EIOPA)

3. European Securities and Market Authority (ESMA)

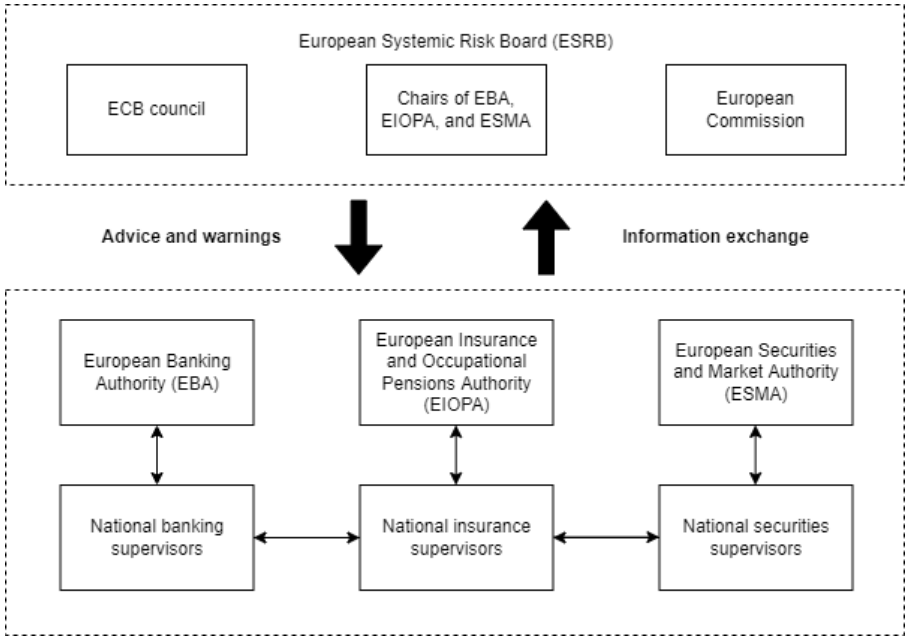

Figure 3.1: Governance structure of the ESFS

An overview of the governance structure of the ESFS is presented in figure 3.1. Together these authorities provide the financial sector with guidelines on how to operate and frameworks that authorities can use. Some existing guidelines are aimed at already ensuring cyber security or even cyber resilience. Examples are the *EBA Guidelines on ICT and Security Risk Management*, the *EIOPA Guidelines on ICT Security and Governance*, and the *ESMA Guidelines on outsourcing to cloud service providers*. These guidelines are from the ESAs on an EU level. However, they are sector-specific and thus not for the entire financial sector. In the Netherlands, there is the *DNB Good Practice on Information Security*, which is followed by all FSOs, but only in the Netherlands.

3.6 The Digital Operational Resilience Act

The DORA is part of the European Commission's priorities to make Europe fit for the digital age. This is called the Digital finance package, a strategy aimed at enabling and supporting the potential of digital finance in terms of innovation and competition while mitigating the risk arising from it. The digital finance package includes a new strategy on digital finance for the EU financial sector to ensure that the EU embraces the digital revolution and drives it with innovative European firms in the lead, making the benefits of digital finance available to consumers and businesses. Strengthening the digital operational resilience of FSOs is a necessary measure. The increased dependence on digital and remote technologies due to COVID-19 has emphasized this need (European Commission, 2020a). Digitization and operational resilience are two sides of the same coin. Digital or Information and Communication Technologies (ICT) give rise to both opportunities

and risks. These must be well comprehended and handled, particularly during times of stress. As a result, policymakers and regulators have become increasingly concerned about the risks associated with reliance on ICT. They have attempted to improve company resilience by establishing standards and coordinating regulatory and supervisory efforts. This work has been done on an international and European level and for several specialized industries and sectors, including financial services. ICT risks, however, continue to pose a threat to the EU financial sector. After the financial crisis of 2008, a reform strengthened financial resilience. The measures were focused on operational risks in general and only addressed ICT risks indirectly in some areas. These post-crisis changes to EU financial services legislation were aimed at governing financial risks but did not fully address digital operational resilience. Due to the need for more specific and comprehensive regulations on digital operational resilience at EU level, national regulatory initiatives (such as digital operational resilience testing) and supervisory techniques have proliferated (e.g., addressing ICT third-party dependencies). Due to the cross-border nature of ICT risks, there are better ways to ensure cyber security than these national regulations. These uncoordinated initiatives have an adverse effect, resulting in overlaps, inconsistencies, duplicate requirements, and high compliance costs (European Commission, 2020a). Therefore, the European Commission proposed the regulation for a comprehensive framework on digital operational resilience for the financial sector in the EU. The harmonization of the regulation that the DORA proposes is based on five pillars:

1. ICT Risk Management
2. ICT Incident Reporting
3. Digital Operational Resilience Testing
4. ICT Third-Party Risk Management
5. Information and Intelligence Sharing

Through harmonization of these five pillars on an EU-wide scale the FSOs should be helped in achieving operational resilience.

ICT Risk Management (DORA Art. 5 – 14)

The first pillar of the DORA is aimed at ICT Risk Management. To keep pace with the rapidly changing cyber threat landscape, the DORA requires FSOs to set up and maintain resilient ICT systems, continuously identify all sources of ICT risks, configure security and preventive measures, and rapidly detect anomalies. Implementation of the specific and comprehensive business continuity policy and disaster recovery and recovery plan, which are an integral part of the operational business continuity policy (European Commission, 2020a).

ICT Incident Reporting (DORA Art. 15 – 20)

The second pillar concerns streamlining the reporting of incidents. This is achieved through two actions: (1) a general requirement for the management of logging and reporting ICT incidents and (2) the obligation to classify the incidents based on criteria detailed in the regulation. These criteria are composed by the supervisory

authorities. In case of an incident, the FSO also needs to provide the authorities with an initial, intermediate, and final report and inform their users of possible financial consequences.

Digital Operational Resilience Testing (DORA Art. 21 – 24)

The third pillar of the DORA sets out requirements for testing digital operational resilience. These requirements depend on the size, business, and risk profiles of the FSO. Those FSOs that are found to be significant and cyber-mature by competent authorities must perform Threat Led Penetration Testing (TLPT). Penetration testing exposes and identifies the exploits and vulnerabilities in a cyber system by attacking or scanning it (Naik et al., 2009). Next to the requirements for the FSOs, this chapter lists the requirements for testers to become authorized to perform the tests.

ICT Third Party Risk Management (DORA Art. 25 – 39)

The fourth pillar is the most renewing and important of the regulation. It addresses the interconnectedness of the financial sector. FSOs have become heavily dependent on third-party ICT suppliers, complicating the supply chain and making it harder to manage security. This is also why the chances of disruption are higher and the impact more severe. Sound monitoring of ICT third-party risk is to be accomplished through this regulation. This will be achieved through (1) principle-based rules applying to the monitoring of third-party risk and (2) harmonizing the key aspects of the service and relationship with third-party ICT providers, thus allowing the FSO to fully monitor the ICT risk of third parties during the closing, execution, termination, and post-contractual phases of their relationship. There are strict requirements on the contents of the contract between the FSO and the ICT provider. Some examples of such contractual elements are a description of services, the indication of locations where data is to be processed, relevant provisions on accessibility, availability, integrity, security, and protection of personal data, and guarantees for access, recover, and return in the case of failures of the ICT third-party service providers. Next to the requirements regarding the monitoring and the contractual elements between FSOs and ICT third-party providers, the regulation proposes to construct a list of critical ICT third-party service providers. This list will be subjected to an EU oversight framework, putting the critical ICT providers under direct oversight. This oversight framework consists of two parts:

1. **DORA Oversight Forum**

   The Oversight Forum has the roles of preparing joint positions, appointing the Lead Overseer, consulting the Lead Overseer in exercising powers and addressing recommendations, fostering ICT risk management best practices, and ensuring cross-sectoral coordination to all matters on ICT risk in accordance with its tasks on cyber security.

2. **DORA Lead Overseers**

   The three ESAs are overseers and will be appointed by the Oversight Forum. They receive powers to ensure that ICT service providers that fulfill a critical role in the functioning of the financial sector are adequately monitored. They have the task of designating the ICT service providers as 'Critical Third

Party Providers', assessing these providers, and drafting oversight plans and guidelines for cooperation with national competent authorities. To do this, they have the power to request information, perform general investigations and on-site inspections, issue penalties for not providing information, and make recommendations.

Figure A.1 in Appendix A presents a visual representation of the ICT providers' oversight framework.

Information and Intelligence Sharing (DORA Art. 40)

The last pillar of the DORA aims to enhance digital operational resilience by raising awareness among FSOs regarding cyber threats. The regulation enables the FSOs to set up arrangements to exchange cyber threat information and intelligence.

3.7 Measuring resilience

The DORA aims to ensure digital operational resilience for the financial sector in the EU. The challenge with resilience, however, is that it is difficult to measure. Efforts have been made to measure resilience. Winderl (2014), for example, has reviewed measurements of resilience against natural disasters. It does, however, not consider more narrow-focused forms of resilience, such as cyber resilience. Platt et al. (2016) attempted to measure resilience and recovery in cases of an earthquake and found it very challenging. The authors propose analyzing data of historical events to build prediction models. This emphasizes the core problem of measuring resilience: resilience can only be measured after an incident. In the field of cyber, efforts have been made, but they mainly focus on cybersecurity, thus on access to the system and maintaining CIA, but there is little information on what happens after the system is breached (Jacobs et al., 2018). This challenge with measuring resilience is aggravated by the fact that the DORA is still in the proposal phase and that the technical standards have not yet been published. So it cannot be said what exact impact the DORA will have on the resilience of the financial sector. There are, however, ways to measure regulatory performance. The OECD (2012) published a report based on research and discussions on perception surveys to evaluate the effectiveness of regulatory reform programs. They found that positive perceptions and stakeholder support are critical for regulatory success. The report states that perception surveys can serve three primary purposes:

- evaluation of the success of a regulation from a user's perspective;
- identify areas of concern to stakeholders; and
- obtain information on stakeholders' awareness, confidence, interest, and recognition of regulatory obligations.

For this study into the coming DORA regulation, the stakeholders' perceptions will significantly impact the result of the implementation. Therefore, it is interesting to research the perceptions of the entities that DORA will apply. However, since the DORA has yet to enter into force and the technical standards are still to be

published, it is a challenge to measure the perceptions on a detailed level. Therefore, in the case of this DORA study, the perceptions of the expectation of the DORA will be studied.

3.8 The case of the GDPR

The DORA is not the first EU-wide regulation. Comparable regulations have gone into force over the past years affecting the financial sector in the EU. The best comparable example is the General Regulation Data Protection (GDPR), which entered into force in 2018. The GDPR is a comprehensive data protection regime with a larger scope than any similar law in the EU or elsewhere, with which the EU took an 'omnibus' approach to privacy law and data protection (Allen et al., 2019). For the case of this research, it is interesting to compare the perceptions of the GDPR with the final result of the law. This way, some hypotheses on both the perceptions of the DORA and the impact that these perceptions will have on the result of the regulation. These perceptions will be discussed along the same structure as the research questions: novelty, preparedness, benefits, challenges, and expected impact.

Perception towards the novelty of the GDPR

Baker (2017) wrote an article discussing the expected impact of the GDPR on the banking sector, discussing that this sector is a heavily regulated one, which is governed by a variety of stringent, onerous regulations that can require a lot of paperwork and appear to be continually added to by authorities all over the world. In addition, basic rules apply to everyone outside of business standards, which are only becoming stricter. Therefore, one might assume that an additional regulation can appear relatively harmless in an industry that is already overrun with compliance mandates, but that is not always the case, states the author. Therefore, the GDPR will also have an impact on the banking industry. The main reforms that the GDPR makes for all enterprises are mostly focused on securing the rights of data subjects, and the requirements for breach notification are stricter.

Zerlang (2017) highlights another aspect of the GDPR, which emphasizes how data is now central to an organization's success: whereas in earlier years, the challenge provided by cyberthreats would be addressed primarily by the department against whom the attack was performed, now every organization is required to have a Data Protection Officer.

The GDPR was generally perceived as a law that introduced new concepts. Individuals' rights would be strengthened, control over one's data would be enhanced, and organizations would face hefty fines if they could not comply with the regulation. The exponentially rising amount of data organizations work with correlates with greater levels of risk and necessity.

Perception towards the preparedness for the GDPR

The second aspect of the perception that was studied is the perceived preparedness for the GDPR of the financial sector. According to a study conducted by Deloitte in 2018, one-fifth of organizations only aimed for bare minimum compliance at the outset of the GDPR(Gooch et al., 2018), 92% of the organizations, however,

believed that they would be able to comply with the GDPR in the long term. A different study performed by McKinsey surveyed major European companies on their readiness for the GDPR. They found that only 10 percent had mature cybersecurity risk-management practices (Larsson and Lilja, 2019). Mikkelsen et al. (2017) howed that it could take companies years to complete all the necessary implementations, possibly with high costs.

The perception of the preparedness for the GDPR was predominantly positive, where most players expected that they could be compliant in the long term. However, research showed that 90% of the organizations were severely lacking when the GDPR was introduced (Larsson and Lilja, 2019). Even though the preparedness was low before the introduction of the GDPR, the positively perceived ability to comply turned out to be correct, as most organizations were able to comply with the regulation. A report from 2019 concluded that FSOs generally found it easier to comply with the GDPR than organizations in other sectors because of their experience in meeting strict privacy and data protection regulations set by financial regulators (Gooch et al., 2019).

Perception towards the benefits of the GDPR

The perceived benefits that regulation will bring are of great importance for its performance (OECD, 2012). Perceived benefits of a law can lead to a positive perception of it, which creates stakeholder support, and that is critical for regulatory success. Zerlang (2017) emphasizes that the advantages of implementing GDPR throughout an organization are apparent, but the drive toward digital transformation will necessitate extensive planning and assessment of the people, technology, and processes required to safeguard it. This may be a costly process, but organizations can take advantage of this process, utilizing advanced tools to analyze the big data at hand. Larsson and Lilja (2019) describe how the GDPR can be seen not only as a punitive measure but also as a stimulus for businesses to change how they handle data, manage risk, and comply with regulations, making them more competitive in the digital economy.

A year after the GDPR, Gooch et al. (2019) stated that despite the high compliance costs, the consensus among the industry is that a cost-benefit analysis would show that the benefits are higher.

Perception towards the challenges of the GDPR

The GDPR was not only perceived to bring benefits to the organizations. The main challenge that was perceived was related to compliance because 90% of organizations were not well prepared, and they would need to make large investments (Larsson and Lilja, 2019). It would also require significant people, systems, and process planning and review (Zerlang, 2017). In the financial sector, organizations were generally less confident about their compliance (Gooch et al., 2019). It might seem strange that the companies that operate in a heavily regulated area and are used to strict regulations and privacy or data laws are less confident about their compliance, but this shows that FSOs have a more realistic understanding of the difficulties of compliance.

But the compliance issues are not the only perceived challenges of the GDPR. Many also see it as a barrier to digitization. They worry that stronger data protection laws may restrict their ability to engage in digital

commerce and that they will have to put new policies in place to safeguard both consumer and employee data. Businesses are also concerned that the money required to comply with GDPR would take funding away from other digital initiatives. Finally, they also wonder if the more burdensome European regulations will disadvantage European businesses in the global marketplace (Mikkelsen et al., 2017).

These perceived challenges were partially correct. Some organizations had trouble initially with the new strict requirements of the GDPR, but most organizations were compliant at the given time (Hawker, 2018). The other challenge turned out to be a benefit. The GDPR forced organizations to invest in structuring and harmonizing customer data, which can be costly and time-consuming. It can initially seem as though such expenditures would only be made out of need rather than as a way to add value to the company. However, the business value of such investments is not simply wasted because the relevant data is cleaned, verified, and organized in a new structure that makes it easier to adhere to GDPR standards while also guaranteeing that the data is collected, stored, and used more wisely for data analytics and perhaps even for generating knowledge.

Perception towards the impact of the GDPR

The GDPR was expected to impact data protection and privacy across all industries greatly. The financial sector deals with a lot of personal data. Therefore, it was expected to have an enormous impact on FSOs (Arcuri, 2020). A report after the implementation of the GDPR showed that the FSOs found compliance a struggle because of its broad scope (Gooch et al., 2019). The GDPR was expected to have an effect outside of the EU as well since the location of the person whose data is processed matters and not the location where the data is processed. As it turns out, a survey from Gooch et al. (2018) shows that the impact of the GDPR goes beyond Europe's borders, contributing to the so-called *'Brussels effect'*, where the influence of EU rules is felt globally because of the size of the European market and the pressure on other nations to uphold the highest standards.

3.9 Hypotheses

Based on the perceptions of the GDPR before its implementation found through literature study and by comparing the GDPR to the DORA, some hypotheses can be made about the perceptions of the DORA expected to be found in this study.

Novelty and preparedness

First of all, the novelty of the DORA is expected to be perceived as lower than the GDPR. This is because the GDPR was a more radically new regulation than the DORA, which builds on existing guidelines and frameworks. Consequently, this is expected to result in a higher perceived preparedness since some of the DORA requirements are based on other requirements. But even though the chapters of the DORA might overlap with existing guidelines, the DORA does introduce some new concepts or more extensive requirements. Especially the ICT third-party risk management section is expected to bring new concepts and requirements.

Benefits

There are several benefits expected to be perceived. The hypothesis is that the FSOs will see the fact that EU-wide is being implemented aimed at the digital operational resilience of the financial sector with positive regard. More specifically, the chapter on ICT third-party risk management, since this is a tricky point for many FSOs.

Challenges

The expected perceived challenges will have to do with compliance issues. As expected and observed in the case of the GDPR as well: the financial sector is heavily regulated, which does not make it easier for them to comply with new standards. It simply means that they understand how much effort it takes. These perceived compliance challenges are expected to be caused for the same reason as with the GDPR: the broad scope of the regulation.

Impact

Finally, the expected perception of the impact that the DORA will have is that the DORA will have a positive impact on the resilience of the financial sector. However, in contrast to the GDPR, the DORA is not expected to have the same groundbreaking impact. Whereas the GDPR impacted all organizations that handle personal data and all individuals whose data is handled by organizations, the DORA is expected to increase the digital operational resilience of the financial sector in the EU. This is a lower impact than the GDPR, but it is the main objective of the regulation.

With these hypotheses stated, the following section goes into the methodology that is used to study the perceptions of the participants.

4 Methodology

This section presents the methods that are used to answer the research question and the sub-questions. First, section 4.1 explains the qualitative nature of this research with its benefits and challenges. Secondly, section 4.2 elaborates on how the participants for this study are recruited. The ecosystem representation and profiles of these participants are presented in section 4.3. Section 4.4 clarifies the ethical governance and data management of this research. Then, in section 4.5, the design of the study is presented. Finally, section 4.6 elaborates on how the data is analyzed.

4.1 Qualitative research

In order to answer the research question, qualitative research will be performed. As the study concerns a new regulation and its preparations, it is of an explorative nature. Therefore, a qualitative approach will be used to understand the attitude towards the DORA better. The data will be collected using interviews with high-level security managers in financial institutions and ICT providers. One of the main difficulties of qualitative research is that it rapidly generates an extensive, cumbersome database because of its reliance on prose in the form of such media as field notes, interview transcripts, or documents. Miles (1979) has described qualitative data as an 'attractive nuisance', because of its richness but the difficulty of finding logical paths through that richness. Unlike quantitative data analysis, there are few well-established and widely accepted rules for qualitative data analysis. Although learning the techniques of quantitative data analysis may seem painful at the time, they give an unambiguous set of rules about handling data. Qualitative data have not reached this degree of codification of analytic procedures, and many writers would argue that this is not necessarily desirable (Bryman and Burgess, 1994).

4.2 Participant recruitment

For the purpose of this study and the basis of participant recruitment, it is essential to define the scope of the research. As this study aims to give insight in the preparedness for and the perception of the DORA, the regulation has to apply to the participants. In the DORA proposal, 23 entities are defined that will come to fall under this regulation (European Commission, 2020b). They are divided into two groups: (1) financial entities, including parties such as banks, insurance companies, and pension funds, and (2) ICT third-party providers. An overview of all the entities that DORA applies to as defined in the proposal can be found in Table B.1 in appendix B. The participants of this research will be recruited from these two groups, with a focus on the first group: financial entities. As the technical standards of the DORA regulation are still under discussion, the proposal is high-level in nature. Therefore, the level of detail that can be extracted through interviews is limited. The interviews are designed to get an insight on a strategic level on the perception of the introduction of the DORA with its benefits and challenges. In order to get this information, the participant

needs to be in a high-level strategic position concerned with compliance with regulations such as the DORA and the organization's general ICT risk and operational security. This reduces the size of the group of possible participants, but for the aim of this research, these roles are needed to get the desired information. Additionally to the participants from the financial sector and the ICT suppliers, participants are included from supervisory authorities on both the European level (EBF) and the national level (DNB).

4.3 Ecosystem representation and interviewee profile

The participants were selected from high-level executives at the entities that DORA applies to. The DORA is a regulation for the financial sector in the EU. Therefore, the larger part of the participants is from FSOs. Since the DORA also entails some requirements for ICT service providers, one interview was conducted with an ICT organization. Additionally, two interviews were conducted with supervisory authorities involved in the discussions about the DORA proposal and in enforcing the regulation. Below is an overview of the participants per group.

- **Financial Service Organizations [P1, P2, P3, P4, P5, P7, P8]**

  The largest group of participants was selected from the FSOs. In particular, from three banks, three insurers, and one pension fund. All organizations differ in size from over 20.0000 employees to under 500 employees.

- **ICT service provider [P9]**

  As the DORA has severe consequences for the practices of ICT third-party service providers as defined in articles 25 to 39, it is interesting to see how the IT providers are concerned with DORA. One large Dutch ICT service provider was interviewed.

- **Supervisory Authorities [P6, P10]**

  Members of two supervisory authorities are included in the study: the EBF and DNB. The EBF is a consortium of 32 banking associations representing over 3500 banks in Europe (EBF, 2022). During the process from the DORA proposal towards the final implementation of the regulation, the EBF represents the voice of the banks in Europe and influences the content and technical standards of the regulation. Because of this involvement and closeness to the policymakers, an interview with a member of the EBF could give extra insights into DORA's driving forces and aims. The DNB is the Dutch authority for the financial sector. They are responsible for the national enforcement and supervision of the regulation. Perceptions from the DNB on the DORA and the financial sector could provide helpful insights into the execution of the regulation.

4.4 Ethical governance and data management

This research has been approved by the Human Research and Ethics Committee of the TU Delft. Due to the impact of COVID-19, most participants worked from home. Therefore, the interviews were conducted online through Microsoft Teams. They were recorded and transcribed. Two of the participants could not make time for an interview and participated through an online survey consisting of the same questions as the interview. One interview was conducted face-to-face, but the participant did not want the conversation to be recorded. After transcription, the recordings of the interviews were destroyed.

4.5 Study design

The report from the OECD (2012) provides a guide to using perception surveys to measure regulatory performance. In this case, however, surveys are not the optimal way to get the desired insights. The group of possible respondents is lower due to their needed level of experience and responsibilities in the organization. Therefore, interviews are chosen as the method. With a smaller number of participants, this can give more information than surveys, as through a semi-structured interview, more information, mainly implicit, such as perceptions, can be extracted. The interview consists of two parts: preparedness scoring and semi-structured questions.

4.5.1 Preparedness scoring

The first part is aimed at understanding the perceived preparedness and newness of the DORA proposal. The second part is focused on the general perceptions of the participant of the implementation of the DORA. In order to get a good view of the preparedness for the first part, the DORA proposal is translated into 18 statements that represent the requirements from the articles of the DORA. Participants were asked to score each statement on a scale from 0 to 5. This scale is an often-used scoring method for similar assessments. For example, the Dutch regulator DNB also uses this scale for maturity assessments on information security (DNB, 2020). The framework is originally taken from the international standards Control Objectives for Information and related Technology (IT Governance Institute, 2007). An overview of the framework with its meanings is presented in Table 4.1.

The 18 statements the participants had to score are interpretations of the articles in the DORA proposal. Each article was studied carefully and translated to a statement that aims to capture the essence of the re-requirement. The statements are divided into the five chapters that DORA consists of. The construction of the statements was an iterative process with external checks from academics and subject experts from the industry to ensure that the statements were both concise and exhaustive. The aim was to cover all the elements of the article in one sentence. An example of this is presented in Figure 4.1, where the colors represent the corresponding elements.

Table 4.1: Preparedness score framework

Score	Label	Meaning
0	**Non-existent**	No documentation. There is no awareness or attention for this control.
1	**Initial**	Control is (partly) defined but performed in an inconsistent way. The way of execution is depending on individuals.
2	**Repeatable but intuitive**	Control is in place and executed in a structured and consistent, but informal way.
3	**Defined**	Control is documented, executed in a structured and formalized way. Execution of control can be proved.
4	**Managed and measurable**	The effectiveness of the control is periodically assessed and improved when necessary. This assessment is documented.
5	**Optimized**	An enterprise-wide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.

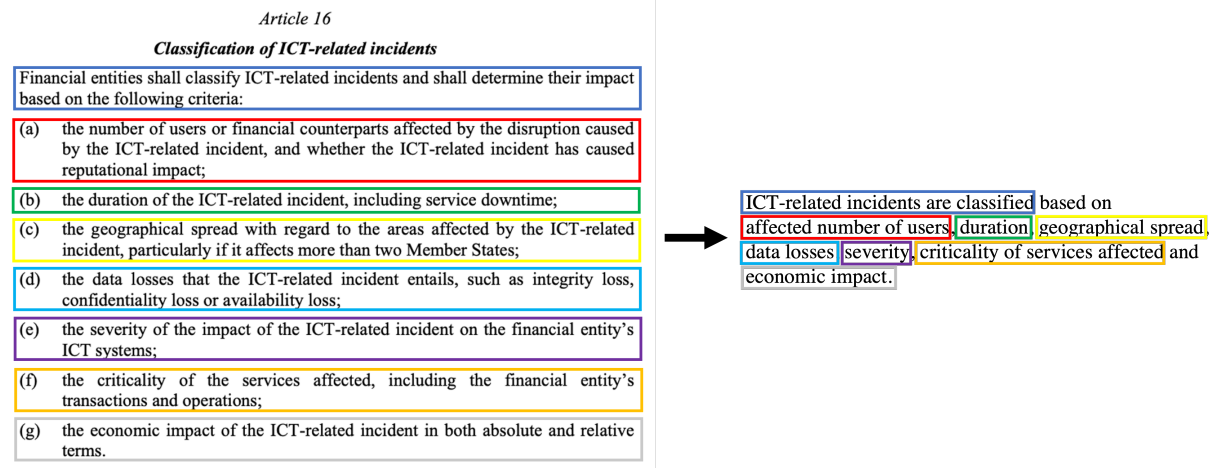

Figure 4.1: Conversion example of article 16 of the DORA

A complete overview of the 18 statements can be found in Appendix C, Table C.1, and the articles from the DORA related to the statements are presented in Table C.2.

4.5.2 Semi-structured questions

After the scoring of the preparedness statements, the second part of the interview starts. This is a semi-structured interview with guiding questions. The aim of this part of the interview is to get an insight of the participant's perception of the DORA. The question setup is presented in Table 4.2. The questions are designed so that the participant's perception can be interpreted from the answers. The participants were allowed to deviate from this list of questions to ensure that all possible information was extracted. The sub-questions were kept in mind during the interview, which are in line with the semi-structured questions, to make sure that the participant's deviation would allow the ability to answer the research question.

Table 4.2: Core questions of the semi-structured interview

Interview question	Scope and context
1) Are you aware of the EC proposal for the DORA?	Opening question to determine the participant's awareness of DORA
2) Do you think DORA is introducing any new concepts that previous regulations did not?	Participant is asked to elaborate on new concepts that DORA introduces in comparison with existing regulation and the participant's perception of it.
3) How prepared do you estimate your organization to the DORA at this point in time?	Participant is asked to determine their readiness for the DORA. Participant is asked to elaborate on the preparations they have taken.
4) What benefits do you think DORA is going to bring for FSOs?	Participant's positive perception of DORA is questioned.
5) What challenges do you think DORA is going to bring for FSOs?	Participant is asked which aspects of DORA could cause challenges.
6) Do you foresee any risks or implications in relation to those challenges?	Participant is asked to elaborate how the challenges of DORA could cause extra implications or risks.
7) Does the DORA address the challenges you have?	Participant is given the chance to address current challenges they have which could be resolved by the DORA.
8) Do you feel like the DORA makes it easier to comply to (international) regulations?	Participants can elaborate on compliance issues with existing regulations.
9) Do you think the 24 months for compliance after the DORA comes into force are sufficient for your organization?	The perception of participants is questioned regarding the possibility of compliance with the DORA.
10) Do you think that the financial sector will be resilient two years after the DORA is implemented?	Final question to see if the participant thinks the DORA will lead to resilience and gives participant the freedom to elaborate on things unmentioned.

4.5.3 Other participants

For the interviews with the participants from the ICT provider, the EBF, and the DNB, the first part of the interview with the preparedness scoring was omitted because these statements only apply to the financial institutions. These interviews consisted purely of a semi-structured question set. These questions can be found in Table D.1, in Appendix D, Table E.1, in Appendix E, and Table F.1, in Appendix F, respectively.

4.6 Data analysis

After transcription, the data are ready to be analyzed. First, a thematic analysis is performed to identify recurring themes in the interviews and to make sense of patterns of meaning across the data set. Braun and Clarke (2021) wrote a paper on quality practice in thematic analysis. This paper defines a six-phase process for data engagement, coding, and theme development. The process is as follows: 1) data familiarization and writing familiarization notes; 2) systematic data coding; 3) generating initial themes from coded and collated data; 4) developing and reviewing themes; 5) refining, defining, and naming themes; and 6) writing the report. This six-phase process is followed in the thematic analysis of the transcripts. Codes were gathered in a codebook,

where multiple codes related to the same theme were grouped, thus identifying topics of interest that were mentioned across different interviews. Finally, these grouped codes were translated into themes.

5 Findings

This section of the report presents the findings from the analysis of the interviews. The themes found through thematic analysis are presented in Table 5.1.

Table 5.1: Themes identified through the analysis

Theme	Description
New concepts of the DORA and previous regulations	Codes related to the novelty of the DORA with regard to existing regulations or standards
Benefits and challenges of the DORA	The opinions of the participants on the benefits and challenges of the DORA
Professional landscape of the financial sector	Codes related to the current landscape, third-party reliance, ICT supply chain, and changes herein
Preparation for the DORA and compliance	Codes related to compliance, including existing compliance issues, foreseen compliance issues with the DORA, and expectations for the future regarding compliance and its impact on resilience
Content of the DORA proposal	Codes related to the actual contents and requirements of the DORA. These can be across all chapters of the proposal
Impact of the DORA	Codes regarding to the participants' expected impact of the DORA on the financial sector and digital operational resilience

The findings will be discussed along these themes. The first theme of new concepts of the DORA and previous regulations will be discussed in Section 5.1. Next, the DORA's benefits and challenges from the participants' eyes are presented in Section 5.2. Statements regarding the professional landscape of the financial sector can be found in Section 5.3. Next, the preparations for the DORA and compliance issues are elaborated upon in Section 5.4. In Section 5.5, the perceptions of the participants on the content of the DORA are displayed. Finally, the participants' view on the expected impact of the DORA is explained in Section 5.6.

5.1 New concepts of the DORA and previous regulation

5.1.1 More detail

There is quite a difference in the participants' perception of the new concepts that the DORA introduces. Some feel that the DORA is merely a harmonization of existing regulations. For example, P2 mentions that *"most of it is already ingrained in the DNB best practice for information security [Dutch national guidelines]"* and identifies *"the only new thing"* as *"it really is something from EBA [European Banking Agency], so it's European. Our supervisor was the Netherlands, so the DNB. So that's just a bit different"*. P4 agreed with P2 that a lot of the requirements of the DORA are already defined in existing guidelines: *"[...] overall, our analysis for our own organization showed that most of the regulatory concepts are already defined by other supervisors (like in the DNB good practice information security [Dutch national guidelines]) which we have in place. However, the DORA shows more details about what is expected per concept opposed to other legislation that is more broadly defined"*. This perception that DORA offers more details is shared among other participants as well. For example, P1 compared the chapters of DORA with existing regulations but saw new requirements in the details. *"Regarding the ICT risks we had the implementation of the EBA guidelines on ICT and security risk*

management. There is a large overlap between DORA and the guideline. But DORA requires you to have all your critical business functions and underlying processes, system technologies, third-party contracts straightened out." and *"we always had to report incidents [...] but reporting vulnerabilities and threats to clients and the public is new from DORA"*. The DNB framework referred to by P2 and P4 is also mentioned by P7 when asked for new concepts of DORA: *"I was actually surprised what we had to do extra. There is of course the DNB self assessment [...] and we also have the EIOPA framework, and on top of that we have SOX. So taking all those in consideration then the real thing about it is that it is a legislation, and I think that's a good thing, it really becomes mandatory"*. P7 is the only participant emphasizing the fact that the DORA will be a legislation instead of the existing guidelines and frameworks. P5 agrees with P1, P2, P4, and P7 that DORA does not introduce new concepts but *"makes it more specific/SMART"*. So, the larger part of the participants sees the DORA not as something new but simply as a harmonization of existing regulations with some more detail.

5.1.2 New concepts

There are, however, some participants that did indicate some aspects of the DORA that they considered new. P8 identified two new concepts: *"a unified way for incident reporting for the entire financial sector in the EU [...] and the third-party risk management"*. These two aspects were confirmed by the participant from the EBF (P6), who said regarding the incident reporting: *"In principle DORA comes from the European Commission because they have seen in a number of incidents, there is actually too little reported among the financial institutions. The incident does happen, but the reporting process ends somewhere [...] not only for the ICT providers, but also for the banks, they are going to have to report major incidents"*. P9, the ICT provider, mentioned that they had already noticed a change in the relationship with the FSOs. This change was twofold: on the one hand, they noticed more pressure on assurances, and on the other hand, they noticed a shift in incident reporting and information sharing. P9 said regarding the incident reporting: *"The ICT providers are getting regulation that the financial sector has had for years, so we're kind of catching up. [...] It will be a step if they have to report. They are used to reporting to third parties, but really with direct oversight will be new though"*. The ICT providers already noticed some changes in the cooperation with the FSOs regarding incident reporting: *"we were asked to participate in the FS-ISAC, for information sharing [...] So there is an exchange of information, and the CERT of the FSOs knows who is in our CERT [...] That really wasn't the case before, so that's something new"* (P9). So the EBF indicates that the incident reporting will be a new concept of the DORA, P8 shares this perception, and P9 already feels the difference. The other concept that was mentioned to be new is the ICT third-party risk management. P8 mentioned the third-party risk management as a crucial part of the DORA: *"There are three large parties dominating the cloud market, now that they get direct oversight that is better"*. P6 emphasizes why this is an important step in the right direction towards resilience: *"it is a chain. Your service takes a cloud service consisting of the service itself, or a SaaS or an API, below that are a whole lot of sub-services from our provider. [...] And that's what hasn't actually been looked at until now"*. The ICT providers also notice that

"The FSOs are putting more pressure on assurances" (P9). This focus on third parties is also addressed by P3 as a new concept of the DORA, along with the information sharing in the form of incident reporting. These participants (P3,P6,P8,P9) agree that the really new concepts that are being introduced by the DORA are the incident reporting and the ICT third-party risk management but agree with the others that *"apart from that, a lot was already there"* (P8).

The participant from the DNB (P10) saw an explanation for this twofold in perceptions on whether the DORA is merely a harmonization of existing regulations or actually introducing new concepts. P10 saw that ICT risks are often in some articles of a regulation, but they are always *"ad hoc and fragmented"*. When asked whether the DORA was a harmonization or introduced new concepts P10 responded *"I think it has largely been shopping from existing guidelines [...], but there are some elements in it that are new such as a really greater focus on a strategy, greater focus on management involvement, greater focus on a truly holistic approach to ICT risk management. Oversight is of course a new element, outsourcing goes a bit further. So there are some extra elements in it"*. This statement explains how the DORA is seen by some FSOs (P1,P2,P4,P5,P7) as a more detailed harmonization of existing guidelines and how some participants (P3,P6,P8,P9) saw the third-party risk management and the incident reporting as new concepts.

5.2 Benefits and Challenges of the DORA

The next theme where multiple codes are grouped is the perception of the participants towards the benefits and challenges of the DORA. As mentioned in the previous theme, the participants were predominantly positive about the coming of the DORA. The benefits that got the most attention align with the new concepts identified by multiple participants (P6,P8,P9): ICT third-party risk management and incident reporting.

5.2.1 Benefits

third-party risk management

The majority of the participants (P1,P3,P6,P7,P8,P9) mentioned the ICT third-party risk management as one of the most significant benefits of the DORA. P7 explained why this is an essential aspect of resilience: *"Also with your third parties. You become more of a directing organization these days than you do it all yourself. We outsource a lot of our IT"*. Therefore, the participants see the focus on ICT third-party risk management of the entire supply chain as a benefit of the DORA. For this reason, P1 stated *"I think you should have an end-to-end overview of your ICT risk, whether that's internal or external"*. P3 also refers to the ICT supply chain requirements as a core benefit of DORA: *"The continuity, and in the entire chain, that is of course DORA, how on earth do you arrange that, what's behind it, subcontractors and stuff, those kind of issues"*. These ICT providers will get a direct oversight committee, which is a large change from the current course of business, where the FSOs are responsible for testing the assurances of the ICT providers. There are a few major parties who play a substantial role in this ICT supply chain, which are predominantly the American cloud providers:

"There are only three cloud providers who are dominating the market. Microsoft Azure, AWS, and Google. Now that they get direct oversight, that is better"(P8). This heavy reliance on ICT suppliers has given cause to a resilient supply chain. DORA is a step in the right direction, as P7 expresses: *"you will no longer buy an application from an ICT farmer on the corner that you will be dependent upon"*. So, DORA brings more attention to getting a good overview of the ICT supply chain and ensuring that the suppliers have the proper assurances and that critical suppliers are considered. This will be of large impact on the ICT supply chain of the financial sector: *"It will separate the good ones from the bad ones, and only the good ones will survive"* stated P6 regarding the ICT providers. The national authorities from the DNB also agree that *"a part of DORA that is necessary is the oversight on third parties"* (P10). The ICT providers have noticed the focus on assurances from the FSOs: *"often that is the reason for a number of important conversations with us to improve or adjust things"* (P9). This can also be seen from the other side, as P7 mentioned that *"We are notifying the ICT providers that this regulation is coming"*. The ICT providers agree that they are *"as a supplier, we are also very closely intertwined in the supply chain of the financial parties"*(P9). That emphasizes the need for a solid third-party risk management in order to ensure digital operational resilience. The ICT third-party (P9) had a generally positive perception about the DORA, seeing that it will make the relation with FSOs *"faster, more efficient, and I think more effective"*(P9), but also voiced concern on how this will bring a new challenge for the ICT suppliers, especially in getting direct oversight from one of the ESAs and having to report to another authority.

Incident reporting

The other benefit that multiple participants bring up concerns the incident reporting. DORA aims to harmonize the reporting for major cyber incidents in the financial sector in the EU so that *"If an incident happens in Italy, Spain, Denmark, the Netherlands, if all goes well, it will be reported, and it can no longer be the case that the hacker can go to another country after it attacked the first"* (P3). More participants were positive about the international standard for incident reporting: *"it's great, this is what we needed and it will make a great difference"* (P8). And P6 also said regarding the obligation for the reporting of major incidents *"and that's what's good about it, the harmonization"*. This harmonization that P6 mentioned is something that P1 agrees with, however, P1 has a side note regarding that: *"The idea of it is good, however, now there are a dozen templates and reporting periods. I don't see anything yet in DORA, but maybe that will come with the technical standards"*. This statement makes sense as the aim of the DORA is clear from the proposal, but since the technical standards have not been published yet, it cannot be said yet if the incident reporting will improve.

Raising awareness

Next to the benefits related to the concepts that some of the participants found new, there were some other benefits mentioned by participants. Two participants (P5 & P6) referred to the general raising of awareness for resilience as the largest benefit of the DORA. P5 said *"creating awareness of the necessity of resilience and preparations for resilience"*. The same goes for P6: *"I think the awareness will definitely go up"*. P9 also noticed

that *"Financial institutions have changed their mindset and it may very well be that DORA has been one of the drivers behind that"*.

ICT risk management

Even though the participants did not see the ICT risk management chapter as novel, simply as more detailed, the fact that it is there is called a benefit by some participants. P4 said the biggest benefit of DORA to be *"the level of detail that DORA describes in their expected IT risk management"* and P7 says *"There is more emphasis on the ICT risk part [...] people really need to emphasize the resilience, the dependence, the vulnerabilities that we have on ICT, and that's good"*. The DNB described the regulatory movement since the financial crisis and how this ICT risk management part is one of the benefits of the DORA: *"after the 2008/2009 financial crisis, the focus was mainly on mitigating financial risks, with operational risks being seen as a bit, well, of second order at times"* (P10). This caused the ICT risk regulation to be very *"ad hoc and fragmented"* (P10). P1 recognizes this fragmentation and elaborated on why the emphasis on the ICT risk management part is a benefit for their organization: *"Until now you had all kinds of financial laws, which had a paragraph that said something about ICT and risk management [...]. I had to wrestle through all those laws in search of the requirements of the ICT. The intention of DORA is to throw all those requirements of those financial laws and we now have one law that applies to the financial sector. I think that's a good intention"* (P1). This last quote from P1 entails another benefit as well, which is that the DORA aims to provide a single point of truth for the financial sector across the whole EU to which all FSOs have to comply. This is in line with the statement from P7 saying that it is a good thing that it is a legislation, so it will become mandatory. P4 said in line with these perceptions: *"the fact that the legislation has to be adopted EU broad which means all financial institutions have the same minimum level of maturity and this reduces systematic IT risk in the financial system"*. This is however easier said than done. As expressed by P1: *"I won't believe it until it's finished, so when all those paragraphs have been deleted, so all those other laws, and all those requirements expire, in such a way that DORA is the single point of truth for ICT risk management for the financial sector. But the intention is commendable"*.

Another benefit from the authorities' viewpoint is that *"it is cross-sectoral. This means that every time you want to change something on ICT risk management, you don't have to change all kinds of sectoral regulations, banks, insurers, all separately"* (P10).

5.2.2 Challenges

Next to the benefits that the participants mentioned, there were some challenges expected as well. Next to the benefits that were mentioned by the participants, there were some challenges expected as well. The perception that DORA is *"another paper to comply with"* (P8) is shared. P2 was particularly strong in expressing that they *"did not really see any benefits of DORA"* and *"we already have 100 different obligations [...] to which we have to comply. So if that is one or two, it doesn't really matter of course"*. However, P2 did elaborate on how an extra regulation can be hard to comply with: *"we are a small organization, so proportionality is*

a challenge for us. We cannot do everything according to the rules." And another challenge for them because of the size of the organization is that *"we approach it principle-based, because if you approach it rule-based we often get stuck"*. The challenge to comply with a new and extra regulation is also mentioned by P4: *"it might become inefficient for organizations to comply with different and all legislators, as legislators need to enforce their rules which in practice means different assessments of different supervisors about the same topic at financial institutions"*. The reason behind the fact that compliance can be a challenge is *"the factual realization of the change in policy and processes, paper is patient"* (P5), and the *"difference in theory and practice"* (P4). This can be related to the requirements regarding the ICT third-party risk management section for example. It can be a challenge to *"get an overview of the complete supply chain"* (P1), or on the other side for the *"overseeer to get a complete understanding of the supply chain"* (P6). One participant (P3) expressed that the details of the DORA will be a challenge because of *"the word 'all', you need to have 'all' your processes [...]"*. This level of detail is also pointed out by P6 as a challenge compared to existing regulations: *"The EBA guidelines describe a lot of things, but the emphasis was still placed on the critical important function, but not all"*. Overall, the participants see the largest challenge in complying with *"another paper"*, and the reason that this is a challenge is in the details. The DNB explains this level of detail in some sectioins of the DORA because they have been taken from existing guidelines: *"[...] because those guidelines are of course level 3 legislation, so that is very granular, very detailed. If you take that to level 1, i.e., legal text, and then you work it out further at level 2, then you run the risk that you will become very detailed. We also see that at DORA"*(P10). According to some participants the fact that the technical standards have not been published yet makes it even more problematic to comply. For example, P4 says: *"Changes in our ICT controls that we adapt now, might need further adaption every time a local supervisor defines another technical standard"*. P1 expresses the same concern regarding the publication of the technical standards: *"we worry about the overlap between the coming into force of the DORA and technical standards yet to be delivered"*.

5.3 Professional landscape of the financial sector

The third theme that was identified concerns the transformation of the professional landscape of the financial sector. This was often related to the relevance of the introduction of the DORA. Most of the benefits and challenges as expressed by the participants are related to this transformation. The financial sector has become heavily dependent on its ICT supply chain. The fact that *"our ICT is mostly outsourced"* (P7) is a statement that goes for almost all FSOs. Due to this interconnected web of FSOs and ICT service providers, a cyber incident can have a cascading effect. As P6 phrases it: *"People don't know in advance when I do this, what will happen on the entire chain"*. The cloud is often mentioned when discussing the DORA (P1,P2,P3,P6,P7,P8). This is a relevant concept because *"people work remotely, due to the pandemic, people work from home, a lot, via the cloud"* (P6) and this in relation with the fact that *"cyber hacks are increasingly sophisticated"* (P6) raises some concerns and explains the driving forces behind the DORA.

5.3.1 Cloud providers

A concern that multiple participants voice is that *"we don't see a cloud provider within Europe"* (P6). And because of this, P3 says *"with all due respect, but [Europe] is second tier. In fact, the Far East has now surpassed us in a number of facets, you have Alibaba Cloud"*. So the professional landscape is changing, and at the same time that more and more ICT is outsourced, Europe aims to *"be stronger and less dependent on others outside Europe"* (P6). Therefore, P7 expresses: *"I think it's a law that should have been passed 10 years ago, I think we've been taking it too easy for a long time"*. And the general feel among participants is that the DORA is aimed at this new landscape, to get an overview of the entire supply chain and *"comprehend all those processes, that is the core of DORA"* (P3).

5.3.2 Size of the organization

Another recurring topic within the theme of the professional landscape of the financial sector was that the size of an organization has a large impact. For example on how dependent an FSO is on its ICT suppliers: *"the large parties will certainly have other suppliers who can take over, but that is a bit more difficult for the small ones"* (P9), or the severity of an incident: *"a small incident can be major for a small bank"* (P6). Some parties are too small *"to program our own stuff"* (P3), or *"to approach frameworks rule-based"* (P2). The importance of size is not only mentioned by the FSOs, but by ICT providers as well: *"if we have to report to another supervisor, we have to invest time and effort. Larger internationally organized firms can simply divide that among all those other organizations, so it can also divide the costs. So for them that's much more manageable"* (P9).

5.4 Preparation and compliance

5.4.1 Confidence about compliance

The DORA is expected to go into force at the end of 2022, with the date of compliance being 24 months later. Even though there are participants who *"have not really looked into DORA yet"* (P2), most participants (P1,P3,P4,P7,P8) have started the preparations *"for some months now, on a low priority"* (P1). And they *"follow the development, so that means reading publications and such"* (P3). The most common way the organizations are preparing is to *"pull the legislation as it stands apart, and link it to our own ICT control framework"* (P7). The same goes for P8 where they *"mapped the current DORA proposal to existing controls and did a gap analysis"*. This preparation gives the organizations a kind of confidence where they express they *"have version 0.9 ready to go"* (P7), or *"only have to do a gap analysis between the latest and the final text, and nuance our gap analysis with that"* (P1). This confidence gained through preparing for the coming regulation can be noticed in the participants' attitude towards the time for compliance. The perception that *"24 months is enough for compliance"* (P4) is shared among the group (P1, P2, P4, P7, P8), even though they *"worry about the overlap between the coming into force of the DORA and technical standards yet to be delivered"* (P1).

Some are even stronger and state that *"if they had said six months we would make it"* (P7). These participants that are confident about their ability to be compliant within the given time tend to be the larger organizations. The DNB also noticed a certain confidence among the larger organizations, but also warned them *"not to underestimate the DORA"* (P10).

5.4.2 Compliance issues

Not all participants have such a positive attitude regarding the period given for compliance and see the 24 months as *"opportunistic and ambitious"* (P5). This is explained because *"paper is patient"* (P5). As P6 states the first two years are a *"learning process"* where the first months are all about *"identifying and documenting"*. Only then you have time to look at the underlying contracts and whether they are good in terms of agreement, because the DORA also requires that you impose certain obligations on your provider. They must, for example, report incidents that happen to the overseeer, instead of the FSOs. *"So you need time to put the contracts in order"* (P6). Another participant (P3) feels the same way and compared the introduction of the DORA to the introduction of the Euro in the Netherlands: *"Then, [the Euros] came straight out of the flapper. With this it's not as black and white. It will be transition, with stretch-goals"*. In line with this perception of the DORA being stretch-goals, P3 even states *"we will never be 100% compliant, compliant enough, but there will always be accepted risks. And this does not only go for us, but for everyone"*. The smaller organizations perceive more expected compliance issues.

5.5 Content of the DORA

This theme contains codes from the participants with specific mentions of the requirements inside the different chapters of the DORA. This part is structured along the five chapters of the DORA and includes the preparedness score that the participants have given for the statements. This preparedness scoring part was only included in the interviews with the FSOs (P1,P2,P3,P4,P5,P7). An overview of the frequency of each score is presented in Figure 5.1. In this Figure, the frequency of scores is illustrated by the size of the blue dot. A larger dot means that the score is given more often, a smaller dot means that the score is given less frequent. The graph is divided in the five chapters of the DORA.

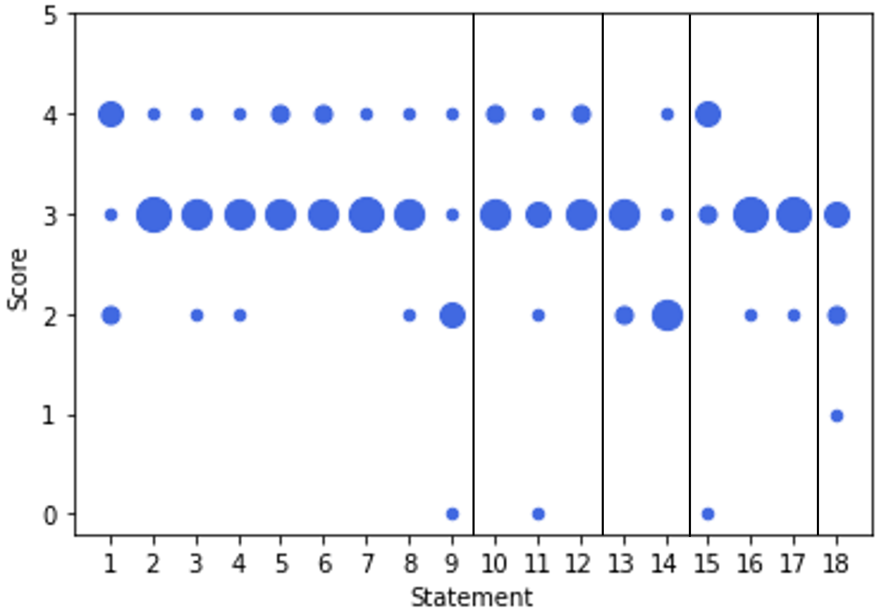

Figure 5.1: Frequency of preparedness scores

As can be seen from the Figure the scoring seems distributed around the score of 3 and no one gave a score of 5. This can be explained by the meaning of the scores. A score of 5 means that the score is "optimized", with *"An enterprise-wide risk and control program provides continuous and effective control and risk issues resolution"* (CobiT 4.1, 2007). For the aim of compliance, a score of 3 (meaning that the control is "defined", i.e., that the *"control is documented, executed in a structured and formalized way"* (CobiT 4.1, 2007)) is good enough for the authorities. Therefore, most organizations aim to score a 3 for the requirements, as it will show compliance to the requirements. A score below 3 is not compliant, but scoring a 5 on all requirements is not realistic and is also not the end goal of a regulation. If all organizations perceived themselves to comply with the requirements, all scores were at a minimum of 3.

Overall, the participants perceive their current preparedness as relatively high since there are few scores below a 3 given. A deeper dive into the distribution of scores dependent on the type of FSO gives more insight in the perceived scores. Figure 5.2 shows the individual scores of the participants. The color of the dot shows the type of FSO: orange for banks, blue for insurers, and green for pension funds. This graph is also divided in the five chapters of the DORA.

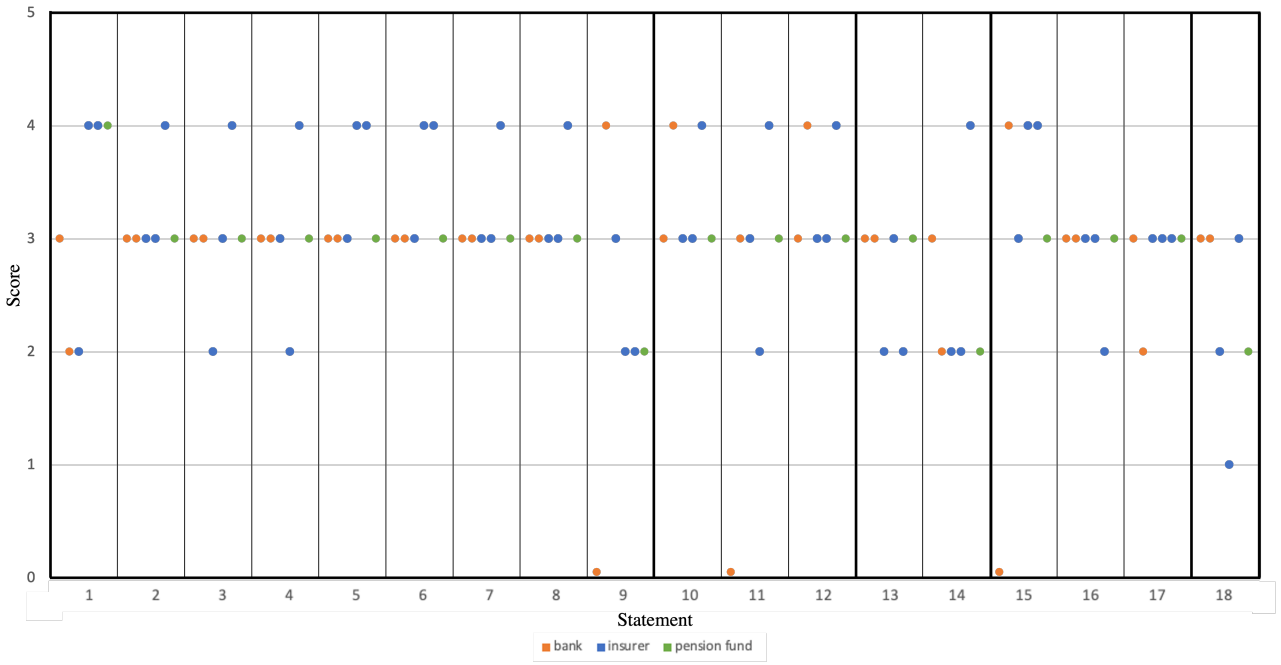

Figure 5.2: Preparedness score per type of FSO

The scoring per type of FSO does not give a clear answer on the difference between type of FSOs and their perceived preparedness. It was expected that the banks, on average, would score higher since they have been a more heavily regulated sector over the past years. The regulations for the banking sector are more advanced in the area of ICT risk management and cybersecurity compared to the insurance or pension funds sector. The perceived preparedness of the banks is, however, not higher. This could also be explained by the fact that because the banks are used to operating in a heavily regulated sector, they have a better understanding of what it means if a new regulation is introduced.

The following sections will go into the perceived preparedness scoring and other findings per chapter of the DORA.

5.5.1 Statement 1-9: ICT Risk Management

The general feeling about the first chapter of the DORA, the ICT risk management part is that *"there is a large overlap with the EBA guidelines"* (P1), but that *"DORA offers more detailed opposed to other legislation that is broader defined"* (P4). An example of this are the requirements DORA defines concerning communication plans (statement 9 in Table C.1, section B: Communication plans are in place for a responsible disclosure of cyber incidents or vulnerabilities to clients, counterparts, and the public.). Multiple participants call this *"a weak point for us"* (P7), or state that *"because of the word 'vulnerabilities' we score a 0 here"* (P1). Overall, the participants scored themselves the lowest for this statement.

Of all the chapters of DORA the first chapter concerns a topic that has had a lot of attention since the emergence of ICT. Therefore, it makes sense that a lot of the content of the DORA has already been covered in previous

regulations. However, these previous regulations and guidelines are mostly from sector specific authorities such as the EBA, EIOPA, or ESMA. This has caused the *"banks to be further along. Since the EBA guidelines were already stricter"* (P7). The DORA will harmonize the ICT risk management requirements for the financial sector in the EU, in the eyes of the participants from the banks this means they have to adjust some details in their processes, for other FSOs this has a larger impact. The participants scored, apart from statement 9, high on this chapter.

5.5.2 Statement 10-12: ICT Incident Reporting

As discussed in Section 5.1 and Section 5.2 the incident reporting chapter is seen as a new concept by some of the participants. DORA requires you to know your *"processes, people, and technology"* (P1) when you perform the classification of an incident. Almost all participants confirm to have a *"neat incident reporting system"* (P3), with for example *"For the severity of an incident, we look at which countries, how many users were involved, those kinds of things are all in our incident policy"*. This can also be seen in the preparedness scoring. The participants scored very high on this chapter, with only two scores below 3. This means that even though the unified incident reporting on a EU-wide scale is conceived as new, the participants find themselves prepared for the requirements related to these articles.

5.5.3 Statement 13-14: Digital Operational Resilience Testing

The third chapter of requirements concerns the testing programs. There are some new aspects in these requirements, related to the supply chain as well. For example that you *"not only test your main supplier, with whom you have your contract, but also ask your supplier, have you tested your supplier, subhosting, and what are the results."* (P6). There are participants, especially the banks, who are more familiar with testing: *"what we did so far was a lot, but partly because of TIBER EU, we did that"* (P1). TIBER-EU is a European framework for testing cyber resilience, and thanks to this framework the FSOs are familiar with testing, they only have to *"adjust the scope"* (P1). This can be seen in the preparedness score, where there are no scores above a 3 and more scores of 2 than in the other chapters.

5.5.4 Statement 15-17: ICT Third-Party Risk Management

The fourth chapter is the ICT Third-Party Risk Management. This chapter is seen as *"the most interesting"* (P7) and *"really good that it is integrated"* (P8). Some FSOs were *"already focusing on third-party risk management"* (P1), and others were aware that *"concentration risk of third parties is a weak point for us"* (P7). The ICT providers were not preparing so much for the DORA but they have noticed *"some changes in relation with the FSOs, behind which DORA could be the driver"* (P9). Even though this chapter entails the most new requirements, the participants find themselves well prepared, which can be deducted from the self-assessed preparedness scores.

5.5.5 Statement 18: Information Sharing

The information sharing is the last chapter of the DORA. There are already some ways to share threat-related information in the financial sector. The *"FS-ISAC"* (P9) is an example of an EU-wide information sharing community for banks, and in the *"health insurance sector, in this context we work together. But at the same time we are encouraged to compete with each other, which is a rather tricky paradox"* (P3). And this paradox is also voiced by P7: *"it is of course pretty confidential information"*. The information sharing arrangements as required by the DORA will change the way FSOs are sharing information, and the FSOs will have to adapt to this. The preparedness scores show that the banks perceive to be well prepared for the information sharing requirements, in contrast to the other FSOs, who score lower on this statement.

5.6 Impact of the DORA

The final theme contains codes where the participants articulate their view on the impact that the implementation of the DORA will have on the resilience of the financial sector. The problem with resilience is that it is inherently impossible to measure. This is mentioned by P6 who says that *"whether you are actually operational resilient, we will only see that in real life when [a cyber incident] happens"*. All participants agree that the DORA *"will not make the financial sector resilient"* (P1,P2,P3,P4,P5,P6,P7,P8,P9), but that it is a *"step in the right direction"* (P8) that will *"will bring more [resilience]"* (P7). A comparison was made between resilience through the DORA and privacy through the GDPR. Where *"privacy really took its flight once [GDPR] became a regulation"* (P7). So now that the focus on resilience is confirmed through a regulation and both FSOs and ICT providers have to implement the requirements of the DORA the *"awareness will go up"* (P5) and the *"operational resilience level will get better and better"* (P4). But this is not the final step: *"I don't think we're there yet [...] I think there will come a DORA 2"* (P6).

All participants agree that resilience is a nearly impossible goal to achieve, but that the DORA is a step in the right direction that will have a positive impact on the digital operational resilience of the financial sector in the EU. The impact of this regulation depends on whether *"all those other laws, and all those requirements expire, in such a way that DORA is the single point of truth for ICT risk management for the financial sector"* (P1).

6 Discussion

The purpose of this research is to get insights into the perceptions of the financial sector on the expectation of the DORA. A thematic analysis of semi-structured interviews with high-level security managers has been performed. All organizations included in this research are entities that DORA applies to and operate in the Netherlands. In Section 3.9, some hypotheses of the participants' perceptions of the DORA are made. This section provides a discussion of the study's main findings and reflects on the hypotheses.

The participants generally had a positive perception of the DORA. They acknowledged that the professional landscape is changing due to the increasing outsourcing of ICT services, which has caused a heavy dependence on third parties. Therefore, the DORA proposal did not come entirely unexpectedly. Overall, most participants feel that the DORA does not introduce shockingly new concepts that were never required before. However, it does add more detail to the existing guidelines and regulations. These details are mainly found in the incident reporting and the ICT third-party risk management parts of the DORA. For some participants, these aspects were seen as really new concepts. In general, the participants' attitude towards these concepts was positive regardless of their perception of their novelty. They thought it would be a step in the right direction toward a resilient financial sector. This perception of the novelty of the DORA is in line with the hypotheses that the DORA would be perceived as less new than the GDPR. The GDPR introduced really new concepts and changed the privacy and data protection landscape of not only the financial sector but of all organizations that handle personal data. This perception of a lower novelty than the GDPR also results in a higher perceived preparedness for the DORA than for the GDPR when it was introduced. Where the preparedness for GDPR was relatively low, the perceived preparedness for the DORA is generally high.

This positive perception can also be found in the perceived benefits of the DORA. The participants mainly saw benefits in the proposal, especially regarding the ICT third-party risk management and the incident reporting, which corresponds with the chapters that were perceived as new. The perceived benefits of the ICT third-party risk management are in line with the hypothesis stated in Section 3.9. There were, however, some extra perceived benefits, such as the fact that the DORA will raise awareness for the necessity of resilience and the dedicated section for ICT risk management. The challenges expressed mostly concerned that DORA will be an additional regulation to comply with, which is caused by the level of detail that DORA defines. This confirms the hypothesis that the DORA's broad scope and level of detail could cause some compliance concerns. In contrast to the GDPR, the participants did not voice many concerns regarding the investment costs needed for the DORA. This portrays how the timing of the DORA is good and that the FSOs are ready to work on their digital operational resilience. They do not see it as a hindrance to other possible technological developments.

Most participants have made the first preparations for implementing the DORA requirements. These preparations consist of mapping the DORA proposal to existing regulations and their security controls. These preparations have caused a certain confidence towards the 24 months that are given for compliance after the

DORA enters into force. The larger part of the participants felt this would be more than enough time to comply. There are, however, a few participants who saw some issues with this period. This was mainly based on the fact that paper is patient and that the DORA will not be a black-and-white transition but more of a stretch-goal kind of regulation. The general perception was, however, that the DORA will positively impact the digital operational resilience of the financial sector. Comparisons were made with the impact of the GDPR on privacy and data protection, where the introduction of the GDPR has made significant differences over time. The impact of the DORA is expected to be lower than the enormous influence that the GDPR has had on privacy and data protection.

The DORA is the largest regulatory movement the financial sector has faced since the GDPR. The impact will be significant, and most participants are aware of this fact. It was interesting to see how the larger organizations were more aware of the expected impact the DORA will have on their operations. They were, nevertheless, optimistic about their possibility of compliance with the requirements. The findings of this study confirm that larger organizations find it easier to comply with new regulations. This was explained by the fact that they have more workforce or can outsource specific changes and processes.

An important aspect of discussion in this context is the fact that in this research, compliance is often used as a measure of resilience. However, compliance with regulation does not inherently mean that the goal of that regulation is achieved. The ability to meet requirements in regulation does not portray the ability to absorb shocks. Therefore, full compliance with the DORA does not entail full resilience. For the aim of this research, compliance has been used to measure the regulation's expected performance.

7 Conclusion and Recommendations

This section will answer the research question, and recommendations will be made. The conclusion with answers to the research questions can be found in Section 7.1, followed by recommendations for the financial sector and the EC in Section 7.2.

7.1 Conclusion

Using a thematic analysis of semi-structured interviews with high-level security managers, this study aimed to understand the financial sector's perceptions of the expectation of the DORA. The research question to be answered is:

What is the perception of the financial sector toward the expectations of the Digital Operational Resilience Act?

To answer the main research question, sub-questions have been formed. Through answering these, the main research question can be answered.

SQ1: ***What is the perception of the financial sector towards the novelty of the DORA?***
The first sub-question aims to give insight into how new the financial sector perceives the DORA. The DORA can be seen as a harmonization of existing guidelines and regulations. A large part of the participants confirmed this perception. The general feeling was that the DORA was not a really new regulation but merely a more detailed harmonization of existing regulations. Where existing regulations might have had a chapter with ICT requirements, the DORA will provide the financial sector with a single point of truth regarding these concepts. Two chapters of the DORA were perceived as new by a few participants, namely the incident reporting and the ICT third-party risk management parts. The participants who perceived the DORA as a harmonization agreed that those chapters had the most new details in them, but in itself that they already existed. It can be concluded that the DORA does not introduce any groundbreaking new concepts in digital operational resilience, but that it is a single regulation for ICT requirements aiming at digital operational resilience, which applies to the entire financial sector in the EU, is new.

SQ2: ***What is the perception of the financial sector towards their preparedness for the DORA?***
The participants' perceived perception was measured through a preparedness scoring where they had to score their organization on a 0 to 5 scale, comparable to a maturity assessment which they are familiar with. A 3 means that the control is defined and implemented on this scale. Therefore, a 3 means that the organization largely meets the requirements. The participants were confident about their preparedness for the regulation since the number of scores below a 3 for any of the statements is very small. Most organizations have been preparing for the DORA, mapping the proposal to existing regulations and their controls. Some concerns were voiced regarding compliance, which focused on the level of detail that the DORA expresses and the moment of

publication of the technical standards. Only a few participants thought that more than 24 months for compliance with the DORA requirements would be needed. The larger part of the FSOs is confident that they will have enough time to comply.

SQ3: ***What is the perception of the financial sector towards the benefits of the DORA?***
Overall, the perception of the financial sector is that the DORA will bring many benefits. The benefits the participants touched upon were in line with the concepts perceived as the most new: incident reporting and ICT third-party risk management. The EU-wide policy for major ICT incident reporting is perceived to benefit the financial sector and its security and resilience. The ICT third-party risk management section was seen as beneficial primarily because of its relevance in the changing professional landscape. All participants emphasized their reliance on ICT service providers and the growing complexity of this supply chain. Therefore, it is perceived as a benefit that the regulation on this is tightened. Lastly, the general raising of awareness for the necessity of digital operational resilience in the current financial sector is perceived as a benefit of the DORA.

SQ4: ***What is the perception of the financial sector towards the challenges of the DORA?***
Even though it is seen as a benefit that the ICT third-party risk management gets more attention than before through the DORA, it also brings a challenge for the FSOs. Getting a good overview of the entire ICT supply chain and revising the contracts with the ICT service providers is perceived as a challenge. Besides this section, the participants did not voice any concerns about specific requirements that the DORA proposes. The only challenge that multiple participants expressed was the level of detail that the DORA entails. Where in previous regulations *'critical business processes'* had to be monitored and tested, the DORA requires this for *'all business processes'*, for example. This level of detail can become a concern or challenge for FSOs as they can perceive it as another paper to comply with. The fact that the technical standards have yet to be published adds to this concern and increases the challenge.

SQ5: ***What is the perception of the financial sector towards the expected impact of the DORA?***
The final sub-question aims to understand the perceived impact of the DORA's implementation on the financial sector and its digital operational resilience. The perception was unanimous among the participant that the DORA would not make the financial sector digital operational resilient simply because this is almost impossible. The perception was, however, that the DORA is a step in the right direction. All participants were optimistic about the impact that the DORA is expected to have. Resilience is not black-and-white; it is a stretch goal, and the DORA will help with this. Just like the GDPR has had a significant impact on privacy awareness and policies since its implementation.

To conclude, the answer to the main research question can be given through the answers to the sub-questions.

This study aims to understand the financial sector's perception of the expectation of the DORA. Through a thematic analysis of semi-structured interviews, results have been created, which have been discussed and answered the sub-questions. This allows the main research question regarding the perception of the financial sector towards the expectation of the DORA to be answered. First of all, it was found that FSOs share a predominantly positive perception of the coming regulation. This perception is driven by the transformation of the professional landscape, which has given rise to the necessity for a good overview of the entire ICT supply chain, which should be resilient in itself as well. Secondly, much emphasis was found on the fact that the DORA will be an EU-wide regulation for the entire financial sector. The perception of this was found to be positive as well, as it is seen as step in the right direction towards a digital operational resilient financial sector through the entire EU. This positive perception is extended to the fact that the regulation will raise awareness about the necessity for digital operational resilience for FSOs and their ICT suppliers. The participants' awareness of the DORA was high, which resulted in the fact that most FSOs in this study have made the first preparations for its implementation. This influences their perception of the possibility of compliance within the given 24 months after the moment that DORA enters into force. The primary perception within the financial sector is that this will be more than enough time to comply, and only a few participants perceived this period as concerning or ambitious. These compliance issues are perceived to be caused by the level of detail that the DORA contains in its requirements and the fact that contracts with ICT third parties have to be revised, which takes a lot of time. Another perceived challenge regarding the DORA and compliance is that this will be an additional regulation to adhere to. Concluding, the overall perception of the financial sector towards the expectation of the DORA is positive in the first place

7.2 Recommendations

From the results and conclusions of this study, recommendations to both supervisory authorities and the financial sector can be made regarding the implementation of the DORA. First, the recommendations for the supervisory authorities are given, followed by the recommendations for the financial sector.

7.2.1 Supervisory authorities

This research has provided insights into the perceptions of a coming regulation from the entities it will apply to. These insights are valuable for policymakers and authorities to measure how the regulation is perceived. The perceptions towards the DORA are predominantly positive, which means that the EC has made a good decision in proposing this regulation. They should not have waited longer to introduce such a regulation, as the general perception is that the FSOs have been waiting for such an act and are welcoming the DORA. The recommendation that can be derived from the conclusions is that the DORA should be the single point of truth. The aim of the DORA to harmonize existing guidelines, frameworks, and regulations can only be achieved if the existing ICT sections are dropped. Then, the DORA will be the single point of truth for the

entire financial sector across the EU. The second recommendation is to take care in designing the technical standards but publish them as soon as possible after the application of the DORA. An extended period before the publication of the technical standards can be worrisome for the FSOs, resulting in more compliance issues and discomfort with the regulation. Furthermore, the EC needs to take good care of the oversight of the ICT service providers. It is a new area for financial supervisors to oversee that kind of organization, and it will take time to understand the entire supply chain and system for them as well. Finally, it is vital for both the FSOs and the ICT service providers that the ICT service providers can give assurance of their compliance with the DORA. The EC should start a certification process to ensure a compliant supply chain. Again, it should be concerned that full compliance does not ensure complete resilience to adverse cyber events. The authorities should assess the impact of the DORA following the financial sector's compliance. If full compliance is achieved, only then can the performance of the regulation be measured, and only then will it be possible to see if the digital operational resilience of the financial sector is up to par. If this is not the case, the EC could introduce additional regulations or a revised second version. Overall, a fully digital operational resilient financial sector is a challenging goal, but the appropriate steps are being taken to come closer.

7.2.2 Financial sector

The DORA is expected to come into force at the end of 2022. This will have a significant impact on the ways FSOs operate concerning their ICT risks and cyber security. Whether the aim for a digital operational resilient financial sector in the EU will be achieved through the implementation of the DORA is the question, but based on the findings and conclusions of this study, some recommendations can be made to the financial sector for the implementation of the DORA. The first thing FSOs have to do is get an overview of their entire ICT supply chain. Then, all the ICT third parties have to be mapped to get an insight into their criticality and the FSO's dependence on this service provider. Subsequently, the FSOs have to open the conversation with these ICT service providers concerning their compliance with the DORA. It is recommended that the FSOs inform the ICT service providers about the coming of the DORA since their awareness is lower. Finally, it is recommended, based on the findings of this study, that all FSOs prepare for the coming of the DORA as much as possible before the publication of the technical standards so that when they are published, they can quickly adapt to the new requirements. The FSOs should intensify their mapping of the DORA requirements to their existing controls and take a critical look at where the gaps and challenges can be identified. Independent third parties could be of help to the FSOs to prevent overestimation of their current maturity or underestimation of the DORA requirements. It is good to see that most FSOs are confident about their ability to comply with the regulation within the given time, but they should be wary about the actual efforts needed to adapt to the new requirements. The predominantly positive perceptions of the regulation predict good compliance, but this optimistic attitude could also be a pitfall. Therefore, it is recommended to take the proactive measures proposed here to comply with the regulation.

8 Limitations and Future Work

In this final section of the thesis the limitations of the study will be discussed in Section 8.1 and possible directions for future work are proposed in Section 8.2

8.1 Limitations

The first limitation of this research is its exploratory nature because the DORA has yet to come into force. This leads to a limited possibility for generalization of the findings, and more research is needed to validate the found perceptions. The relatively small sample size adds to this limitation, as a larger number of participants in the study would contribute to the validity of the findings.

Secondly, the chosen research method of semi-structured interviews entails multiple biases resulting in limitations. The first is response bias, which occurs when participants are asked to self-report behaviors and can cause respondents to answer untruthfully or inaccurately. People tend to overestimate their own abilities, which can result, in this case, in higher preparedness scores than in reality. Another bias related to this type of research is the social desirability bias. Respondents could give untruthful or partially truthful answers because they provide answers according to society's, or in this case, the industry's, expectations. The effect of these two biases is in the same direction on the preparedness score.

Another limitation is that due to the impact of COVID-19, all interviews were conducted online. Interviews are preferably held in a face-to-face situation to prevent data loss. Furthermore, in all interviews, the interviewer plays a critical role in preserving the information-gathering process by soliciting comments and keeping an eye out for leading questions in all interviews. Being new to the field of social sciences and using interviews to gather data, it is inevitable that the objectivity of the information gathered has been impacted by the quality of the interviews.

8.2 Future work

The limitations of this study give way to possibilities for future research that can add to this area of study. This study was performed under a small population of stakeholders of the DORA in the Netherlands. This study should be performed among a larger group of participants to increase the generalizability. If this study were performed in other countries in the EU, then comparisons could be made between the perceptions of the FSOs in different countries towards the DORA and which national regulations play in these.

This study was performed in the last half year before the DORA will come into force. Therefore, it would be interesting to see how stakeholders' perceptions shift when the DORA has come into force. Once the technical standards are published, a gap analysis could be performed between the DORA and existing guidelines. These outcomes can be compared with the preparedness score that the FSOs have self-assessed in this study. Once

the technical standards are published, the perceptions can also be assessed in more detail, as opposed to the high-level strategic perceptions that this study found.

Finally, future research could be performed when the compliance date of the DORA has passed. Then the actual compliance of the financial sector could be assessed. As presented in the discussion, compliance does not equal resilience. Once the compliance date of DORA has passed, the compliance of the financial sector could be assessed in combination with its digital operational resilience. Even though the resilience of the financial sector is hard to measure, with the use of theoretical frameworks, an assessment could be made whether the digital operational resilience of the financial sector has improved as a result of the DORA and how the requirements of the DORA have influenced this digital operational resilience.

References

Adams, A. and Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12):40–46.

Alabdan, R. (2020). Phishing attacks survey: types, vectors, and technical approaches. *Future Internet*, 12(10):168.

Ali, J. and Santos, J. R. (2015). Modeling the ripple effects of it-based incidents on interdependent economic systems. *Systems Engineering*, 18(2):146–161.

Allen, D. W., Berg, A., Berg, C., Markey-Towler, B., and Potts, J. (2019). Some economic consequences of the gdpr. *Allen DWE, Berg A, Berg C, Markey-Towler B and Potts J (2019)'Some Economic Consequences of the GDPR', Economics Bulletin*, 39(2):785–797.

Arcuri, M. C. (2020). General data protection regulation (gdpr) implementation: What was the impact on the market value of european financial institutions? *Eurasian Journal of Business and Economics*, 13(25):1–20.

Asmundson, I. (2017). Financial services: Getting the goods. *IMF entry retrieved from http://www. imf. org/external/pubs/ft/fandd/basics/finserv. htm.*

Baker, L. (2017). The impact of the general data protection regulation on the banking sector: Data subjects' rights, conflicts of laws and brexit. *Journal of Data Protection & Privacy*, 1(2):137–145.

Birkie, S., Trucco, P., and Kaulio, M. (2014). Disentangling core functions of operational resilience: a critical review of extant literature. *International Journal of Supply Chain and Operations Resilience*, 1(1):76–103.

Björck, F., Henkel, M., Stirna, J., and Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In *New contributions in information systems and technologies*, pages 311–316. Springer.

Boeke, S. (2018). National cyber crisis management: Different european approaches. *Governance*, 31(3):449–464.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment.* International Monetary Fund.

Braun, V. and Clarke, V. (2021). One size fits all? what counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, 18(3):328–352.

Bryman, A. and Burgess, B. (1994). *Reflections on qualitative data analysis*, pages 216–224. Routledge, 1 edition.

Coaffee, J. (2013). Rescaling and responsibilising the politics of urban resilience: From national security to local place-making. *Politics*, 33(4):240–252.

Coaffee, J., Wood, D. M., and Rogers, P. (2009). *The everyday resilience of the city*, volume 10. Springer.

CobiT 4.1 (2007). *Appendix III - Maturity Model for Internal Control*, page 175. IT Governance Institute.

Committee on Economic and Monetary Affairs (2017). on FinTech: the influence of technology on the future of the financial sector. Technical Report A8-0176/2017.

Coutu, D. L. (2002). How resilience works. *Harvard business review*, 80(5):46–56.

De Bruijne, M. and Van Eeten, M. (2007). Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. *Journal of contingencies and crisis management*, 15(1):18–29.

Dieye, R., Bounfour, A., Ozaygen, A., and Kammoun, N. (2020). Estimates of the macroeconomic costs of cyber-attacks. *Risk Management and Insurance Review*, 23(2):183–208.

DNB (2020). Good Practice Informatiebeveiliging 2019/2020. https://www.dnb.nl/media/oabls2bx/good-practice-ib-2019-2020-nl.pdf.

Dowell-Jones, M. and Buckley, R. (2016). Reconceiving resilience: A new guiding principle for financial regulation. *Northwestern Journal of International Law and Business*, 37(1):1.

EBF (2022). ABOUT US.

European Commission (2009). Action Programme for Reducing Administrative Burdens in the EU Sectoral Reduction Plans and 2009 Actions. Technical Report COM(2009) 544 final.

European Commission (2020a). Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, 23 September 2020, COM(2020)591. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0591&from=EN.

European Commission (2020b). Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, Articles 28-29. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN.

European Parliament (2017). on FinTech: the influence of technology on the future of the financial sector.

European Systemic Risk Board (2020). Systemic Cyber Risk. Technical report.

Fischer, E. (2017). Cybersecurity issues and challenges. LIBRARY OF CONGRESS WASHINGTON DC.

Gooch, P., Bonner, S., Goethals, M., and Imeson, M. (2019). After the dust settles How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on. Technical report.

Gooch, P., Luysterbourg, E., Sponselee, A., Frank, D., Dewitt, B., Sehgal, M., and Batch, D. (2018). A new era for privacy: General data protection regulation ("gdpr") six months on.[online] deloitte.

Gumbau, A. (2022). Russia's war on Ukraine spotlights critical energy infrastructure. https://www.energymonitor.ai/tech/networks-grids/russias-war-on-ukraine-spotlights-critical-energy-infrastructure.

Hawker, E. (2018). Businesses struggling with gdpr compliance.[online] accountancy age.

Hernández de Cos, P. (2019). Financial technology: the 150-year revolution. https://www.bis.org/speeches/sp191119.htm.

Holling, C. S. (1996). Engineering resilience versus ecological resilience. *Engineering within ecological constraints*, 31(1996):32.

Hollnagel, E., Woods, D. D., and Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd.

Hopcraft, R. and Martin, K. M. (2018). Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region*, 14(3):354–366.

IBM and Ponemon Institute (2021). How much does a data breach cost in 2022? Technical report.

IT Governance Institute (2007). *Appendix III - Maturity Model for Internal Control*, page 175. IT Governance Institute.

Jacobs, N., Hossain-McKenzie, S., and Vugrin, E. (2018). Measurement and analysis of cyber resilience for control systems: An illustrative example. In *2018 Resilience Week (RWS)*, pages 38–46. IEEE.

Jacqué, P. (2017). Trois jours après la cyberattaque Petya, Saint-Gobain travaille « à l'ancienne ».

Kaufmann, H., Hutter, R., Skopik, F., and Mantere, M. (2015). A structural design for a pan-european early warning system for critical infrastructures. *e & i Elektrotechnik und Informationstechnik*, 132(2):117–121.

Khiaonarong, T., Leinonen, H., and Rizaldy, R. (2021). Operational Resilience in Digital Payments: Experiences and Issues. Technical report.

Kopp, E., Kaffenberger, L., and Wilson, C. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Kost, E. (2022). The 6 Biggest Cyber Threats for Financial Services in 2022 — UpGuard.

Larsson, A. and Lilja, P. (2019). Gdpr: What are the risks and who benefits? In *The Digital Transformation of Labor*, pages 187–199. Routledge.

Lautenschläger, S. (2018). Cyber resilience – objectives and tools.

Leo, M. (2020). Operational resilience disclosures by banks: Analysis of annual reports. *Risks*, 8(4):128.

Mikkelsen, D., Soller, H., and Strandell-Jansson, M. (2017). The eu data-protection regulation—compliance burden or foundation for digitization? *Risk*.

Miles, M. B. (1979). Qualitative data as an attractive nuisance: The problem of analysis. *Administrative science quarterly*, 24(4):590–601.

Ministerie van Justitie en Veiligheid (2019). Vitale infrastructuur.

Moramarco, S. (2021). Phishing attacks in the banking industry.

Naik, N. A., Kurundkar, G. D., Khamitkar, S. D., and Kalyankar, N. V. (2009). Penetration testing: A roadmap to network security. *arXiv preprint arXiv:0912.3970*.

National Research Council (2002). *Making the nation safer: The role of science and technology in countering terrorism*. National Academies Press.

OECD (2012). Measuring Regulatory Performance: A Practitioner's Guide to Perception Surveys. Technical Report http://dx.doi.org/10.1787/9789264167179-en.

Ozarslan, S. (2022). Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022.

Perkins, S. (2011). 2010's Volcano-Induced Air Travel Shutdown Was Justified. https://www.science.org/content/article/2010s-volcano-induced-air-travel-shutdown-was-justified.

Platt, S., Brown, D., and Hughes, M. (2016). Measuring resilience and recovery. *International Journal of Disaster Risk Reduction*, 19:447–460.

Reinfelder, L., Landwirth, R., and Benenson, Z. (2019). Security managers are not the enemy either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–7.

Sheffi, Y. and Rice Jr, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan management review*, 47(1):41.

Simchi-Levi, D. and Haren, P. (2022). How the War in Ukraine Is Further Disrupting Global Supply Chains. https://hbr.org/2022/03/how-the-war-in-ukraine-is-further-disrupting-global-supply-chains.

Stavroulakis, P. and Stamp, M. (2010). *Handbook of information and communication security*. Springer Science & Business Media.

Sydekum, R. (2018). Can consumers bank on financial services being secure with gdpr? *Computer Fraud & Security*, 2018(6):11–13.

Untersinger, M. (2017). Le virus Petya a coûté plus d'un milliard d'euros aux entreprises.

VMware (2020). Modern Bank Heists 3.0.

Whitman, M. E. and Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Williams, M. (2010). *Uncontrolled risk: lessons of Lehman Brothers and how systemic risk can still bring down the world financial system*. McGraw Hill Professional.

Winderl, T. (2014). Disaster resilience measurements: stocktaking of ongoing efforts in developing systems for measuring resilience.

Woollaston-Webber, V. (2017). NHS trusts affected by cyber attack.

World Economic Forum (2012). Partnering for Cyber Resilience. Technical Report 270912.

Zerlang, J. (2017). Gdpr: a milestone in convergence for cyber-security and compliance. *Network Security*, 2017(6):8–11.

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.

Appendices

A Appendix A

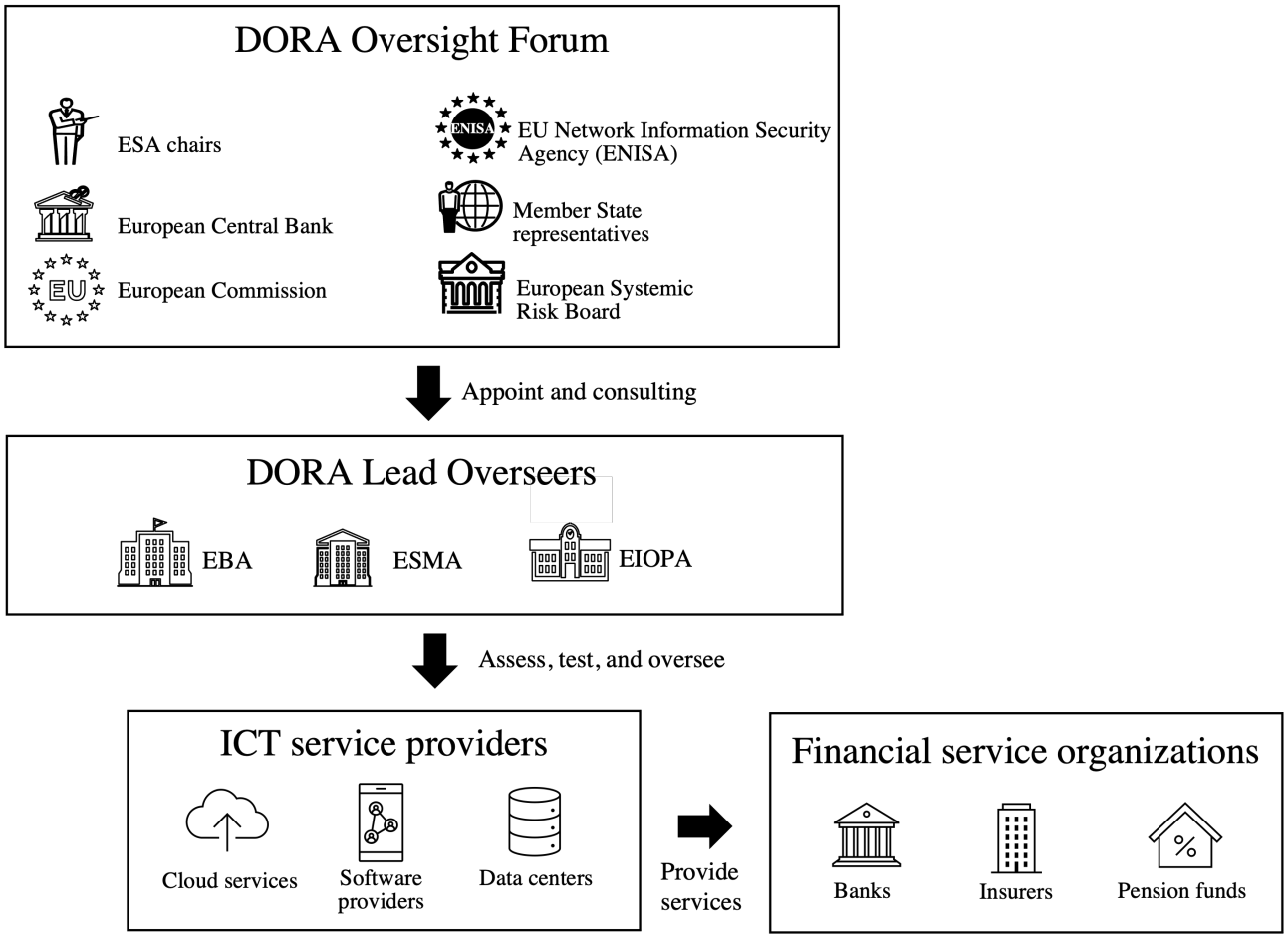

Figure A.1: Oversight framework of the ICT third parties

B Appendix B

Table B.1: Entities that DORA applies to (Committee on Economic and Monetary Affairs, 2017)

#	Entity
(a)	credit institutions,
(b)	payment institutions,
(c)	electronic money institutions,
(d)	investment firms,
(d)	crypto-asset service providers, issuers of crypto-assets, issuers of asset-referenced tokens and issuers of significant asset-referenced tokens,
(f)	central securities depositories,
(g)	central counterparties,
(h)	trading venues,
(i)	trade repositories,
(j)	managers of alternative investment funds,
(k)	management companies,
(l)	data reporting service providers,
(m)	insurance and reinsurance undertakings,
(n)	insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries,
(o)	institutions for occupational retirement pensions,
(p)	credit rating agencies,
(q)	statutory auditors and audit firms,
(r)	administrators of critical benchmarks,
(s)	crowdfunding service providers,
(t)	securitisation repositories,
(u)	ICT third-party service providers.

C Appendix C

Table C.1: 18 statements for the preparedness score

Domain	#	Statement
ICT Risk management	1	A comprehensive ICT risk management framework is in place for which the management body bears the responsibility.
	2	ICT systems, protocols and tools are being maintained and updated.
	3	ICT security strategies, policies and procedures aimed at ensuring resilience of ICT systems are designed and implemented.
	4	All ICT-related business functions are identified, classified, and documented.
	5	Mechanisms are in place and regularly tested to detect ICT-related anomalous activities.
	6	An ICT Business Continuity Policy and ICT Discovery Recovery Plan are in place and reviewed ensuring the continuity of critical ICT functions.
	7	A backup policy is in place ensuring minimum downtime and limited disruption of ICT systems.
	8	Vulnerabilities, cyber threats, and ICT-related incidents are analyzed with their likely impact on digital operational resilience.
	9	Communication plans are in place for a responsible disclosure of cyber incidents or vulnerabilities to clients, counterparts, and the public.
ICT Incident Reporting	10	Management processes are implemented to detect, manage, and notify ICT-related incidents and to ensure integrated monitoring, handling, and follow-up of the incidents.
	11	ICT-related incidents are classified based on affected number of users, duration, geographical spread, data losses, severity, criticality of services affected and economic impact.
	12	Major ICT-related incidents are reported to relevant authorities, with an elaborate incident report for the authority to determine the significance and impacts.
Digital Operational Resilience Testing	13	A digital operational resilience testing program is in place and part of the ICT risk management framework, where all critical ICT systems and applications are tested annually by independent parties.
	14	A testing program is implemented to execute of a full range of appropriate tests (e.g., vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing, or penetration testing).
Third-party Risk Management	15	ICT third-party risk is an integral component of the ICT risk management framework, and a Register of Information is maintained for all contractual arrangements with ICT service providers.
	16	Contractual arrangements with ICT third-party service providers that lead to multiple arrangements with the same party or to a third party that is not easily substitutable are considered.
	17	Rights and obligations of third parties are clearly allocated and documented (including, description and location of all functions and services, provisions on accessibility availability, integrity, security and protection of data, full-service level description, notice periods, requirements for 3d party to implement and test business contingency plans, the right to monitor the 3d party performance, and termination rights and exit strategies).
Information Sharing	18	Cyber threat information and intelligence is shared with other financial entities, including tactics, techniques, and procedures, aimed at enhancing digital operational resilience.

Table C.2: Statements with the related DORA articles

Statement #	DORA article
1	Article 5: ICT risk management framework
2	Article 6: ICT systems, protocols and tools
3	Article 7: Identification
4	Article 8: Protection and Prevention
5	Article 9: Detection
6	Article 10: Response and Recovery
7	Article 11: Backup policies and recovery methods
8	Article 12: Learning and evolving
9	Article 13: Communication
10	Article 15: ICT-related incident management process
11	Article 16: Classification of ICT-related incidents
12	Article 17: Reporting of major ICT-related incidents
13	Article 21: General requirements for the performance of digital operational resilience testing
14	Article 22: Testing of ICT tools and systems
15	Article 25: General principles
16	Article 26: Preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements
17	Article 27: Key contractual provisions
18	Article 40: Information-sharing arrangements on cyber threat information and intelligence

D Appendix D

Table D.1: Core questions of the semi-structured interview with the ICT providers

Interview question	**Scope and context**
1) What services do you provide to financial institutions?	Opening question to determine the relation and services between the ICT provider and the FSOs.
2) Are you aware of the EC proposal for the DORA?	Question to determine the participant's awareness of the DORA.
3) Which assurances do you currently have to demonstrate your security?	Participant is asked which assurances they currently have to see how DORA relates to this.
4) Do you experience any pressure from the financial sector that DORA is coming?	Question aimed at getting insight on the behavior of the FSOs with regard to the ICT third parties and DORA.
5) There will be an overseer per critical provider. What do you think about being under direct supervision?	Participant is asked for its perception towards a changing requirement that the DORA brings.
6) You have to report certain incidents to the supervisor and also to the customer (the financial institution). What is your opinion on this?	Participant is asked for its perception towards a changing requirement that the DORA brings.
7) Are you currently performing tests to test resilience?	Question to get insight on their current policy on testing.
8) How will you demonstrate that you are DORA compliant?	Participant's perception on future assurance of DORA compliance.
9) What do you see as benefits of DORA?	Participant's positive perception of DORA is questioned.
10) What do you see as the biggest disadvantages or challenges of DORA?	Participant is asked which aspects of DORA could cause challenges.

E Appendix E

Table E.1: Core questions of the semi-structured interview with the EBF

Interview question	**Scope and context**
1) How does the development of the DORA work and what is the role of the EBF in this process?	Opening question to get an understanding of the development process and the EBF's role herein.
2) What, in your view, were the motives behind the proposal for the DORA?	Participant's perception of the motivation for DORA is asked
3) Do you think the DORA introduces new concepts that current laws and regulations do not yet cover?	Participant is asked to elaborate on new concepts that DORA introduces in comparison with existing regulation and the participant's perception of it.
4) How do you see the current state of digital operational resilience of the financial sector in the EU?	Question aimed at getting insight on the participant's perception on the resilience of the financial sector
5) In your view, is an organization that fully complies with DORA fully resilient?	Participant is asked for its perception on whether DORA will ensure resilience
6) What do you see as benefits of DORA?	Participant's positive perception of DORA is questioned.
7) What do you see as the biggest disadvantages or challenges of DORA?	Participant is asked which aspects of DORA could cause challenges.
8) Do you expect DORA to make it easier for FSOs to comply with international laws and regulations?	Participant's perception on future compliance issues and DORA's role herein.

F Appendix F

Table F.1: Core questions of the semi-structured interview with the DNB

Interview question	**Scope and context**
1) What is the role of the DNB in the development of the DORA?	Opening question to get an understanding of the developmen process and the DNB's role herein.
2) How does the translation from EU to national legislation work?	Create insight in the difference between EU and national regulation
3) How do you see the current state of digital operational resilience of the financial sector in the EU? And the Netherlands?	Participant's perception of the current level of digital operational resilience is questioned.
4) Do you think the DORA introduces new concepts that current laws and regulations do not yet cover?	Participant is asked to elaborate on new concepts that DORA introduces in comparison with existing regulation and the participant's perception of it.
5) What do you see as benefits of DORA?	Participant's positive perception of DORA is questioned.
6) What do you see as challenges of DORA?	Participant is asked which aspects of DORA could cause challenges.
7) Do you think that the FSOs have the ability to comply within the given timespan?	Participant's perception of the compliance issues is questioned.
8) What role do the ICT service providers play in the digital operational resilience of the financial sector?	Participant's perception of the role of ICT service providers is questioned.
9) Do you think the DORA can be compared with the GDPR?	Question aimed at seeing where the DORA can be compared with the GDPR
10) What do you think about the fact the FSOs interviewed in this study ... ?	Open questions to be filled in with insights from the previous interviews. These questions aim to get the DNB's reaction to the found perceptions.