Master ICT in Business and the Public Sector

Navigating the DORA Landscape:
A Study of Service Provider Readiness

Name: Nicky Kos
Student ID: S3421295
Date: 20/09/2024

1st Supervisor: Dr. O. Gadyatskaya

2nd Supervisor: Dr. Y. Zhauniarovich

Master’s Thesis

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University
Einsteinweg 55
2333 CC Leiden
The Netherlands

Navigating the DORA Landscape:
A Study of Service Provider Readiness

Abstract

Critical infrastructure is increasingly vulnerable to disruptions caused by natural disasters, geopolitical tensions, and cyber-attacks. The highly digitized financial sector, in particular, faces a disproportionately high risk of cyber-attacks, which can undermine confidence in the financial system and have severe economic repercussions. In response to these threats, the European Commission introduced the Digital Operational Resilience Act (DORA), aimed at strengthening the digital resilience of financial organizations and their critical IT service providers by effectively mitigating IT and cyber risks.

This study examines the preparedness of service providers to support financial organizations in complying with DORA's regulatory requirements, which must be met by January 2025. Using a qualitative approach, the research includes document analysis and insights from fourteen semi-structured interviews with professionals from consulting and legal firms, ranging from consultants to partners, to assess their readiness in helping financial organizations adhere to DORA regulations.

The findings reveal that financial organizations face substantial challenges in managing DORA compliance internally due to limited resources and the increasing burden of regulatory requirements. As a result, these organizations often seek assistance from service providers for gap assessment validation, translating regulations into practical business applications, and offering implementation support. Key competencies for service providers include industry-specific knowledge, multidisciplinary expertise, and robust go-to-market strategies. Consultants should have a broad skill set that encompasses technical, legal, and general consulting capabilities. The study also provides a practical checklist that service providers can use to establish a DORA proposition or evaluate the completeness of their current offerings.

Keywords: DORA, Digital Operational Resilience Act, financial organizations, service provider readiness, cybersecurity, regulatory compliance, consulting services, operational resilience, service readiness checklist, digital regulations, financial regulations.

Statement of originality

This study was conducted by Nicky Kos, who takes full responsibility for the contents of this document. I declare that the text and the work presented in this document are original, and that no sources other than those cited in the text and references were used in its creation. I confirm that generative AI, such as ChatGPT and Gemini, was used solely for text rewriting purposes and not for generating content.

Acknowledgement

First, I would like to thank Dr. O. Gadyatskaya, my first supervisor, for her invaluable support and guidance throughout my thesis. Her expertise and constructive feedback have been crucial in shaping this study, and her dedication has been appreciated. I would also like to thank Dr. Y. Zhauniarovich for his assistance.

I also want to thank Mounaim Ben Touhami, my supervisor at Deloitte, for his exceptional mentorship and the time and effort he invested in me. His insights and support have been crucial in the completion of this study.

Additionally, I am thankful to all the interview participants who generously shared their time and insights, enhancing the quality of this study.

Finally, I would like to express my appreciation to my family and girlfriend for their support and encouragement during this journey. Their support has been a source of strength throughout the process.

I am grateful to each and every individual mentioned above for their contributions, without which this study would not have been possible. Thank you for being an important part of this and I wish you all the absolute best.

Opa, deze is voor jou. Ik hoop dat je er iets van meekrijgt.

Table of contents

List of abbreviations

Abbreviation	Full term
AI	Artificial Intelligence
AISPs	Account Information Service Providers
BCBS	Basel Committee on Banking Supervision
COBIT	Control Objectives for Information and Related Technologies
DNB	De Nederlandsche Bank
DDoS	Distributed Denial-of-Service
DORA	Digital Operational Resilience Act
DSPs	Digital Service Providers
EC	European Commission
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
EU	European Union
FSI	Financial Service Industry
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
ISO	International Organization for Standardization
IT	Information Technology
MiCA	Market in Crypto-Assets
NIST	National Institute of Standards and Technology
NIS2	The Second Directive on Network and Information Systems
OES	Operators of Essential Services
PISPs	Payment Initiation Service Providers
PRA	Prudential Regulation Authority
PSD2	The Revised Payment Services Directive
SOC	Security Operations Center
SS	Supervisory Statement
TLPT	Threat-Led Penetration Testing
TPRM	Third-Party Risk Management

List of figures

List of tables

1. Introduction

The first chapter of this study served as an introduction. Section 1.1 explores the background of the topic, highlighting the importance of digital operational resilience in the financial sector. Section 1.2 defines the problem statement, identifying the challenges faced by financial organizations in achieving compliance with DORA. The research scope in section 1.3 outlines the study's focus on assessing the readiness of Dutch service providers to assist in this compliance. The research questions in section 1.4 enumerates the main and subquestions guiding the study. Section 1.5 explains the contribution of this study. Finally, section 1.6 outlines the structure of this study.

Background

For decades, critical infrastructure has been the victim of disruptions from events of various sizes and origins, and is increasingly vulnerable to disruption (Heino et al., 2019). According to the Dutch Ministry of Justice and Security, the processes and services constituting vital infrastructure form the foundation upon which Dutch society relies. Any disruption to these processes can have significant effects on other vital processes, sectors, or even national security (Ministerie van Justitie en Veiligheid, 2023).

There are different events that can disrupt the critical infrastructure (UCP Knowledge Network, 2023). Examples of events that have caused disruption to critical infrastructure worldwide are the COVID-19 pandemic, and the financial crisis in 2008. Other events include geopolitical tensions, such as the conflict between Ukraine and Russia, natural disasters, such as the North Sea flood of 1953, and human-caused disasters, such as the Chernobyl nuclear disaster in 1986. These events are well-known, and we are familiar with their consequences and severity. However, there are also less tangible events that have the potential to disrupt critical infrastructure, such as cyber-attacks (Lehto, 2022). In 2010, a minimum of fourteen industrial facilities in Iran, including a uranium enrichment plant, were compromised by a 500-kilobyte computer worm as part of the Stuxnet attack. The final stage of this worm involved targeting the programmable logic controllers, which allowed its creators to both monitor the industrial systems and cause the centrifuges to self-destruct (Kushner, 2013). The centrifuges were used to separate nuclear material (Allianz, 2016). In 2017, a major cyber-attack struck a petrochemical plant in Saudi Arabia. The malware used in this incident, called TRITON, was engineered to specifically target, and manipulate safety systems within critical infrastructure (Trend Micro, 2019). Trend Micro assumed that the threat actor responsible for the attack appeared to be motivated to execute a high-impact attack resulting in physical damage (Trend Micro, 2017).

In a more recent cyber-attack, during 2022 and 2023, the pro-Russia hacktivist group KillNet targeted countries it considered to be supporting Ukraine (Rohner, 2023). This attack affected at least fourteen medical centers across the United States through Distributed Denial-of-Service (DDoS) attacks. In addition to DDoS, KillNet exfiltrated data from the websites and their databases, sharing this sensitive health and personal information on its own websites. The global cost of cybercrime continues to rise, with estimates projecting it will reach $10.5 trillion annually by 2025 (Cybersecurity Ventures, 2023).

These examples underscore the disruptive potential of cyber-attacks on critical infrastructure. The financial sector faces a risk of attacks three times higher than other critical infrastructure sectors (European Parliament, 2017). Recognizing this vulnerability, the European Systemic Risk Board (ESRB) has identified cyber risk as a source of systemic risk to the financial sector, noting that such risk can have severe negative impacts on the economy, such as eroding confidence in the financial system (European Systemic Risk Board, 2020).

The Financial Service Industry (FSI) is recognized as one of the most digitized sectors within the economy (Kun, 2024). Digitizing the business could increase efficiency and the competitiveness of businesses, but also bring risks (Saeed et al., 2023). To support financial organizations in benefitting from the potential, but also mitigate the associated risks that come with digitizing, the European Commission (EC) made a proposal for an act, the Digital Operational Resilience Act, abbreviated DORA (European Commission, 2020c). The DORA establishes requirements for organizations operating in the financial sector, as well as for critical third parties that provide IT-related services to them (DORA, 2023). The DORA aims to establish a framework for digital operational resilience for European financial organizations, outlining clear requirements to manage and mitigate IT and cyber risks (Krüger and Brauchle, 2021). The DORA became effective on January 17, 2023. All financial organizations in the European Union (EU) have until January 17, 2025, to comply with the regulation (De Nederlandsche Bank, 2023).

Problem statement

Financial organizations that do not comply with DORA by January 17, 2025, will face severe financial penalties, including a daily fine of 1% of the average daily turnover, with a maximum duration of six months (Secura, 2023). For example, ING Group, with an annual revenue of €17.6 billion in 2022, would incur a daily penalty of approximately €482,100, potentially reaching €87 million over six months for non-compliance (Yahoo Finance, 2023).

Given the high stakes, financial organizations must ensure compliance with DORA to avoid substantial fines and maintain operational stability. Various service providers[1], including Deloitte, Secura, and PwC, have positioned themselves to assist these organizations in meeting DORA's requirements (Deloitte, 2024b; Secura, 2024; PwC, 2024a). However, the readiness of these service providers to effectively support financial organizations remains uncertain.

This study investigates the preparedness of selected service providers to assist financial organizations in achieving DORA compliance. By examining the readiness and capability of these firms, the study aims to provide insights into how well-positioned these service providers are to support their clients in meeting the regulatory demands of DORA.

Study scope

The DORA is a proposal introduced by the European Commission that will be effective across all EU countries. Organizations fall under the scope of DORA if they have offices within the EU or provide services to a financial organization operating in the EU (Clarke, 2023). This study examines the extent to which service providers are ready to assist financial organizations in complying with DORA. The service providers examined in this study are consulting firms based in The Netherlands, such as Deloitte, Grant Thornton, and BDO on one hand, and law firms such as Houthoff, NautaDutilh, and Loyens & Loeff on the other. This study focuses exclusively on the readiness of the Dutch offices of these firms, as it was more practical to contact them.

Study questions

The aim of this study is to gain insight into the extent to which these service providers are prepared to support financial organizations in achieving compliance with DORA. Therefore, the question this study aims to answer is:

To what extent are service providers prepared to support financial organizations in complying with DORA?

In order to answer this research question, the following subquestions have been formulated:

- *SQ1: What does DORA require from financial organizations?*
- *SQ2: How do service providers perceive readiness to provide services related to DORA?*

[1] In this thesis, "service providers" refers to organizations that offer consulting services to financial organizations to help them comply with THE DORA requirements.

- *SQ3: What are the current offerings of service providers in assisting financial organizations with DORA compliance?*
- *SQ4: What are the factors that influence the decision of financial organizations to engage service providers for DORA compliance support?*
- *SQ5: What capabilities are essential for consultants to assist financial organizations in complying with DORA?*
- *SQ6: To what extent can the knowledge acquired by service providers in assisting financial organizations with other digital regulations be applied to adhere to DORA?*
- *SQ7: How can a checklist be designed to evaluate the readiness of service providers in delivering DORA services?*

Study contribution

This thesis makes a valuable academic contribution by addressing the gap in understanding the readiness of service providers to support financial organizations in complying with DORA. Because DORA is a new regulation, limited research exists on the role of service providers in this context. By analyzing service providers' capabilities and challenges through document analysis and interviews, this study offers new insights. Lastly, a checklist was developed to assess service provider readiness, which can be used by both academics and practitioners to evaluate and improve DORA service offerings.

Study outline

After the introduction, which outlined the research topic, context, and background, the thesis moves on to chapter 2, where the methodology is explained, including the data collection methods such as document analysis and expert interviews. Chapter 3 provides a review of existing literature related to topics such as DORA and service provider readiness. Chapter 4 presents a document analysis of DORA, detailing its objectives, pillars, and timelines, and comparing it with similar regulations to highlight key differences and similarities. The results of this study are presented in chapter 5, and they are discussed in chapter 6. Finally, chapter 7 concludes the thesis and proposes directions for future research.

2. Research methodology

The second chapter of this study outlines the methods used to answer the study's questions. Section 2.1 introduces the overall methodology, detailing how it aligns with the research questions. Section 2.2 provides an overview of the specific data collection methods used, including document analysis and expert interviews, and how these methods contribute to answering the subquestions.

Introduction

The method chosen for this study was a qualitative one. First, related literature was examined to learn from, and to get a basis to build further on. After that, a document analysis was conducted, examining both scientific literature and documents shared by private and public organizations, such as Deloitte, KPMG, and the European Commission. This was important in order to gain knowledge about DORA in general, the service provider landscape, and related regulations. To get more insights, interviews were held with DORA experts. In subsection 2.2.2, the interview process will be explained in more detail. As mentioned, the two primary research methods used in this study were document analysis and interviews. For a breakdown of which questions were addressed through document analysis and which were covered by the interviews, see Table 1.

Subquestion	Qualitative research	
	Document analysis	Interviews
SQ1: What does DORA require from financial organizations?	X	
SQ2: How do service providers perceive readiness to provide services related to DORA?		X
SQ3: What are the current offerings of service providers in assisting financial organizations with DORA compliance?	X	X
SQ4: What are the factors that influence the decision of financial organizations to engage service providers for DORA compliance support?		X
SQ5: What capabilities are essential for consultants to assist financial organizations in complying with DORA?		X
SQ6: To what extent can the knowledge acquired by service providers in assisting		X

financial organizations with other digital regulations be applied to adhere to DORA?		
SQ7: How can a checklist be designed to evaluate the readiness of service providers in delivering DORA services?	X	X

Table 1 - *Breakdown of subquestion answering method*

This study strived to design a checklist that provided practical guidance to service providers to assess their own service readiness. The checklist could help service providers align their DORA services with financial organizations' expectations and enhance their readiness in assisting financial organizations in complying with DORA effectively. This checklist underwent a validation check through an open discussion during one-on-one interviews with experts.

Data collection

2.1.1 Literature review

For scientific literature, the Google Scholar platform was employed. The documents used were thoroughly examined to ensure their relevance and reliability. This process included closely reviewing the authors' credentials and verifying that the articles were published in peer-reviewed journals. Recent publications (within the last 3-5 years) were prioritized to ensure that the gathered information reflected the current state of DORA compliance and service provider readiness.

2.1.2 Document analysis

As shown in Table 1, the document analysis aimed to (partially) address the first, third, and seventh subquestions. To achieve this, the Google search engine was utilized to locate industry reports and other relevant documents concerning DORA. Industry reports and grey literature were considered reliable if published on reputable organization websites such as Deloitte, EY, or the European Commission (EC), which introduced DORA. All documents related to DORA were sourced from 2020 onwards, aligning with the period when it was initially introduced by the EC.

2.1.3 Expert interviews

To gain insights into the current DORA landscape among service providers, interviews were conducted with fourteen employees from nine different firms offering DORA services. These firms were divided into two categories: consulting firms (e.g., Deloitte, BDO, Grant Thornton) and legal firms (e.g., Loyens & Loeff, Houthoff, NautaDutilh). Eleven participants represented consulting firms, and three were from legal firms, ranging from a senior consultant with three years of experience to a partner with over 25 years of experience. Detailed participant information is provided in Table 2.

Participant code	Background	Field of work	Function
C1	Operational Resilience, Security & Compliance	Cyber	Partner
C2	Cyber and Strategic Risk	Cyber	Junior Manager
C3	Cyber security	Cyber	Consultant
C4	IT Risk Assurance	Cyber	Partner
C5	Operational Resilience, Cloud & Digital Regulations	Cyber	Partner
C6	Cyber Strategy	Cyber	Manager
C7	Cyber Secure	Cyber	Senior Manager
C8	Technology Law	Legal	Manager
C9	Digital Risk Solutions	Cyber	Senior Consultant
C10	Cyber Risk	Cyber	Partner
C11	Cyber security & Privacy	Cyber	Director
L1	Regulatory & Finance	Legal	Attorney
L2	Financial Law	Legal	Partner
L3	Financial Markets & Products	Legal	Attorney

Table 2 *- List of interview participants*

Participants were identified through personal networks or firm websites and were considered suitable if directly involved in offering DORA-related services. The interviews, conducted online between June 6 and July 9, 2024, were held in English or Dutch depending on the participant's native language. Using a semi-structured format, the interviews adhered to a general plan of questions, which can be found in Appendix I, while allowing flexibility to explore emergent topics, thus enabling an in-depth exploration of participants' perspectives on DORA-related services.

At the beginning of each interview, participants were informed about the study's objectives, the interview process, and their rights, including confidentiality and the option to withdraw. Permission was obtained to record the session, use the information provided, and mention their position within the company. To ensure participant confidentiality, unique codes were assigned ("C" for consulting firms, "L" for legal firms), with full anonymization of transcripts and exclusion of company names. The recordings of the interviews were transcribed by the principal researchers. Only the principal researcher had access to the original and anonymized data. Given the competitive nature of the service provider landscape, the transcripts are not shared with this study.

All transcripts were reviewed and verified by the participants to ensure data accuracy, offering an opportunity for corrections or clarifications. One-on-one interviews were chosen to accurately capture the interviewees' perspectives with minimal external influence. An interview protocol, which can be found in Appendix II, guided the interviews. A mapping of the study's subquestions to the interview questions, which can be found in Table 3, ensured the coverage of the research objectives. Subquestion 1 was addressed solely through a literature review.

The interview questions explored various aspects of service provider readiness for DORA compliance, such as defining readiness for digital regulations, assessing current DORA service offerings, understanding factors influencing financial organizations to engage service providers, and identifying essential capabilities for DORA compliance.

Research questions	***Interview questions***
SQ2: How do service providers perceive readiness to provide services related to DORA?	Q1: How do you define readiness when it comes to providing services related to digital regulations like DORA?
	Q2: What criteria your organization use to assess its readiness to offer services for a new regulation like DORA?
SQ3: What are the current offerings of service providers in assisting financial organizations with DORA compliance?	Q3: How does your organization differentiate the services for DORA from other service providers?
	Q4: Which service that your organization offers do you consider the most important for financial organizations?
	Q5: What service is most frequently requested by financial organizations?
SQ4: What are the factors that influence the decision of financial organizations to engage service providers for DORA compliance support?	Q6: What are the main reasons why financial organizations opt to use service providers instead of addressing regulations like DORA internally?
	Q7: In your experience, do financial organizations prioritize cost-effectiveness or quality of service when choosing a service provider for (DORA) compliance support?
	Q8: Are there any other specific concerns or requirements that financial organizations have

	when considering potential service providers for the (DORA) compliance support?
SQ5: What capabilities are essential for consultants to assist financial organizations in complying with DORA?	Q9: What specific expertise or knowledge areas do you believe consultants must possess to assist financial organizations with DORA compliance?
	Q10: Are there any specific certifications or training programs your organization considers important for DORA readiness?
	Q11: Can you discuss any capabilities or skill sets that were beneficial in the past when supporting financial organizations with DORA compliance?
SQ6: To what extent can the knowledge acquired by service providers in assisting financial organizations with other digital regulations be applied to adhere to DORA?	Q12a: Which specific regulations (NIS2 for example) have provided the most valuable lessons that could be applicable to assisting with DORA compliance? Q12b: What knowledge and lessons learned are specifically applicable?
SQ7: How can a checklist be designed to evaluate the readiness of service providers in delivering DORA services?	Q13: Can you describe the components or criteria that you believe should be included in a checklist for assessing readiness for DORA compliance support?

Table 3 *- Mapping the research questions to the interview questions*

2.1.4 Checklist validation

The final deliverable of this study was a checklist designed to assess service providers' readiness to support financial organizations in achieving compliance with DORA. The checklist was developed based on insights gathered from both the document analysis and the interviews conducted. The checklist was validated through interviews with DORA experts.

Three additional interviews, which are not included in the table of participants, were conducted with DORA experts to validate the checklist. These experts provided critical feedback, allowing for iterative improvements to the checklist. This process ensured that the final product was well-rounded, practical, and aligned with industry standards and regulatory expectations. The goal was to refine the checklist, enhancing its accuracy and usefulness as a tool for service providers aiming to support financial organizations in complying with DORA requirements.

Coding process

After conducting the interviews and transcribing them, thematic analysis, as described by Braun and Clarke (2012), was applied to analyze the interviews. As mentioned earlier, some interviews were held in Dutch while others in English. Before uploading the transcripts to Atlas.ti for coding, they all had to be translated into English. Given the factual nature of this study, which places less emphasis on feelings and perceptions, the decision was made to focus on translating the core message of the interviewees, rather than translating their answers word-for-word. Instead of coding entire sentences, the approach focused on coding the key parts of each sentence, which aligns with Saldana (2013), who suggests that coding should target the most meaningful parts of a sentence to identify the central concept. For example, out of the sentence “many financial organizations, including larger ones, often do not have the capacity to manage this internally,” the phrase “do not have the capacity” was selected and assigned the code ‘lack of resources.’ In the initial open coding phase, 372 codes were applied. Towards the end of this process, the coding process stabilized with very few new codes emerging. During the second phase, the axial coding phase, these codes were grouped into 105 categories, which were divided into ten overarching themes. These themes are discussed in the results chapter. In Figure 1, the process from open codes to themes is visualized.

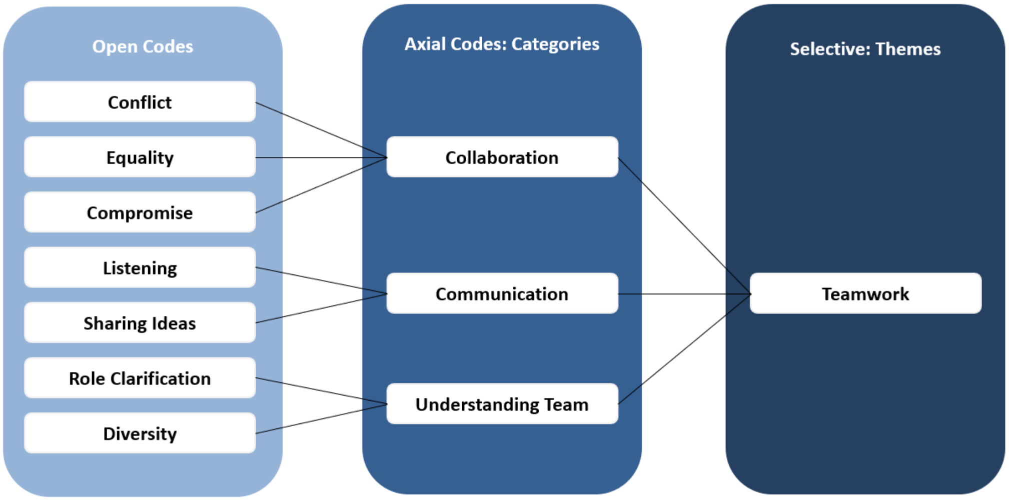

Figure 1 *- The process from open to selective coding (Williams and Moser, 2019)*

2.1.5 Coding reliability

To ensure the quality and reliability of the coding, the Inter Coder Agreement (ICA) tool in Atlas.ti was used with Krippendorff’s alpha formula to calculate intercoder reliability. The codebook, found in Appendix II, included comments to help the second coder understand each code. The Atlas file with the codes and transcripts was shared with the coder to ensure accurate coding. Each code had a comment explaining its meaning and how to interpret it. It's important to note that even if the same code is used, the score changes if it is applied to a different text segment, even if the difference is very small. After the coder completed coding a transcript, Krippendorff's c-Alpha-binary was used to calculate the reliability score, which was 0.709. After this, a second round of external coding took place, whereafter we again used the Krippendorff's c-Alpha-binary to calculate the reliability score, which was 0.868.

3. Related work

The third chapter of this study reviews the relevant research that informed this study's focus. Section 3.1 examines existing literature on DORA. Section 3.2 analyzes the role of service providers in regulatory compliance. Section 3.3 discusses studies related to the readiness of consultants and other service providers. Section 3.4 reviews studies in which interviews were conducted with security practitioners. Finally, section 3.5 describes the relevance of this related work to the current study.

Digital Operational Resilience Act

This section reviews the existing literature on DORA. Since DORA was a relatively new topic, research in this area was limited. At the time of writing, no scientific literature specifically addressed service providers in relation to DORA. The search terms used included combinations of the following keywords: “DORA”, “Digital Operational Resilience Act”, “Operational Resilience in the financial sector”, and “regulatory compliance in the financial sector.” However, the study that came closest was by Karakasilioti (2024), which provided an in-depth analysis of how DORA's implementation impacted the digital operational resilience of the financial sector. This study particularly focused on how financial organizations could enhance their compliance and operational stability, and included a case study on a fictitious bank to demonstrate the application of DORA assessment tool, indirectly highlighting the role of service providers in supporting financial organizations.

Another relevant study was conducted by Gusiv (2023), which aimed to develop a systematic approach for financial organizations to identify and address compliance gaps under DORA. Gusiv’s research included the validation of this compliance gap analysis method with DORA experts, something that this study also intends to do. One interesting aspect of Gusiv's work was the detailed explanation of the validation method, highlighting that not only professionals with direct DORA experience were interviewed, but also those with experience in only certain aspects of DORA. While Gusiv's validation process was conducted through a survey, and this study will conduct interviews, what made Gusiv's study particularly interesting was the inclusion of the interview questions used to validate the tool they developed. Gusiv deemed four responses sufficient for the validation.

In addition, more general research on DORA existed. For example, ter Haar (2022) explored whether DORA acted as a friend or an enemy to financial organizations by conducting interviews with security managers from Dutch financial organizations. Other studies that examined DORA, though not directly related to this research, included Waizel (2023), who investigated the impact of DORA on cloud adoption, and Kourmpetis (2022), who examined how DORA influenced the management of third-party risks.

Another study worth mentioning was conducted by Buttigieg and Zimmermann (2024), which focused on the challenges DORA presented within the EU, particularly regarding supervision and coordination of the oversight framework. They highlighted problems stemming from fragmented supervision at the national level and varying regulatory approaches. Their main argument was that although DORA represented a step forward in unifying digital operational resilience, it also brought challenges in achieving supervisory convergence and collaboration due to the divided supervisory framework. Duggan (2024) addressed concerns about financial organizations' ability to meet all DORA requirements before the implementation date. Research by Clausmeier (2023) demonstrated that DORA had some overlap with the NIS, which suggested that the NIS2 brought lessons learned to DORA, something this study will validate during the interviews.

Service providers’ role in regulatory compliance

This section reviews the existing literature on the role of service providers in ensuring regulatory compliance within the financial services industry. The search terms used included combinations of the following keywords: “service providers in regulatory compliance,” “consultants as intermediaries in financial regulations,” “role of service providers in compliance”, and “financial sector regulatory compliance support.” A study by Owen (2021) provided valuable insights into how these service providers contribute to regulatory compliance, with implications for the financial sector. Owen challenged the traditional view of a hostile relationship between businesses and regulators, emphasizing the role of consultants as intermediaries. These consultants not only assisted companies in adhering to regulations but also supported the public values underlying these rules. The study suggested that, similar to environmental consultants, financial service providers functioned as go-betweens, facilitating communication between regulators and institutions to help ensure compliance. This dual role was identified as crucial for the effective implementation of regulations and could even involve shaping regulatory frameworks, thereby enhancing their effectiveness. Owen's findings underscored the importance of these intermediaries in balancing regulatory compliance with business interests, a dynamic that was also relevant in the financial sector.

Another study by Butler and O’Brien (2019) explored the potential of Regulatory Technologies (RegTech), adding a new dimension to FinTech. RegTech had, according to the researchers, the potential to improve the efficiency of service providers in the financial sector by facilitating better regulatory compliance. As intermediaries, service providers, played a key role in bridging the gap between regulators and financial organizations. RegTech tools could streamline the compliance process by automating regulatory reporting and ensuring adherence to complex regulations. This technological integration allowed service providers to offer more accurate, timely, and cost-effective solutions, thereby improving the overall effectiveness of regulatory frameworks and supporting public values within the industry.

Service readiness

The third section aims to address the concept of service readiness, particularly in the context of providing services to organizations for regulatory compliance. It explores how service providers prepared to offer their services under new regulatory frameworks, the strategies they employed to ensure readiness, and the criteria used to assess their preparedness. The search terms used included combinations of the following keywords: “service provider readiness in regulatory compliance,” “DORA service providers,” “DORA readiness,” “client needs in DORA compliance,” “DORA consultant readiness,” “service provider strategies in compliance,” and “service provider readiness.”

A study by Christensen et al. (2016) emphasized the importance for service providers to focus on the specific tasks that customers aim to accomplish, referred to as "jobs to be done." They argued that service providers should not only meet functional needs but also consider the social and emotional dimensions that shape the customer experience. Understanding the context and circumstances in which their clients operate was crucial, enabling service providers to tailor their services to address the specific needs and challenges faced by the client. This study validated that the extent to which service providers focused on the jobs to be done of the financial organizations was deemed very important by service providers. Service providers also highlighted the importance of showing this in the go-to-market strategy, something which Christensen et al. (2016) also suggested. They said that service providers should design processes and experiences closely aligned with the jobs customers are trying to complete.

In line with this, Størkersen et al. (2023) investigated the role of risk and safety consultants in the oil and gas sector, highlighting how consultants serve as intermediaries to bridge gaps between risk regulations and industry practices. Størkersen et al. (2023) explored how consultants help organizations navigate regulatory standards, either by providing specialized knowledge in areas where the organization lacks in-house competence or by offering independent assessments to ensure compliance. The consultants do not just provide technical expertise but also act as translators and facilitators of regulatory intentions. They help organizations understand and internalize regulatory requirements, adapting their services to the specific context of the client. This aligns with Christensen et al.’s argument about addressing the unique "jobs to be done" for customers.

Interviewing security practitioners

This section reviews the existing literature on studies that conducted interviews with security practitioners. The search terms used included combinations of the following keywords: “interviewing security practitioners,” “interviewing cyber specialists ,” “thematic analysis in cybersecurity research,” “security professional interview studies,” and “qualitative research in cybersecurity.” There is a rich literature on interview studies with security practitioners. While to the best of our knowledge, nobody has focuses on the specific research question that we addressed, it is important to acknowledge the work in this field. For example, Bridges et al. (2018) aimed to close the gap between cybersecurity researchers and Security Operations Centers (SOCs) by examining the current practices, challenges, and future needs of SOC professionals. They carried out semi-structured interviews with 13 professionals from five SOCs, conducting these interviews either one-on-one over the phone or in person.

Furthermore, Bridges et al. (2018) utilized grounded theory to allow themes to emerge organically during their research. This approach of not presupposing outcomes mirrors the inductive analysis used in my own research. The emphasis they placed on the interviewer’s technical pre-knowledge also resonates with my study, as understanding DORA’s complex regulatory framework was crucial for interacting meaningfully with the participants. Thus, their methodology informed the design of my interviews, particularly in how to approach and engage experts in a way that fosters open dialogue.

Botta et al. (2007) interviewed twelve IT professionals from five organizations in a semi-structured interview, to gain insights into their workplace and tools. After the interviews, they analyzed the data using a variation of grounded theory and predesigned themes. The use of the combination of the grounded theory and predesigned themes is something that also could be considered for this study.

The studies mentioned above utilized a qualitative approach by conducting interviews and analyzing them using grounded theory or a variation of it. In the study by de Souza et al. (2011), which focused on the information needs of system administrators, two methodologies were combined, a qualitative study involving 20 semi-structured interviews and a quantitative study using a 45-question survey with over 200 respondents. The method where a survey is combined with interviews is another thing that could be considered for this study, however the small amount of DORA experts could be a problem there.

The combination of qualitative and quantitative methods, as seen in the study by de Souza et al. (2011), also provides an interesting contrast. Their mixed-method approach, which involved both interviews and surveys, could offer a broader view of expert perspectives. However, given the smaller pool of DORA experts available, this approach may not be feasible for my study. Nevertheless, de Souza et al.'s strategy of triangulating data from multiple sources reinforces the importance of supplementing interviews with other forms of evidence, such as document analysis, which I have incorporated into this thesis.

Finally, Axon et al. (2018) aimed to explore the attitudes of security practitioners toward the use of sonification in SOCs and to analyze the potential benefits, challenges, and design requirements for integrating sonification into SOC workflows. They conducted a survey of 20 respondents and interviewed 21 practitioners from various SOC roles, including managers, analysts, and engineers, providing diverse perspectives. Similarly, this study will interview a diverse set of roles to capture comprehensive insights into DORA compliance readiness, as understanding different viewpoints is crucial for a holistic analysis. The authors also addressed acquiescence bias by encouraging both positive and critical responses, fostering a balanced discussion.

The relevance of the related work

There was very little literature available on DORA, so the studies on DORA did not contribute as much as the document analysis, which provided more insight into DORA. However, studies like Karakasilioti (2024) and Gusiv (2023) emphasized the emerging nature of the regulatory landscape and the lack of scientific literature specifically addressing the role of service providers in the context of DORA. This gap confirmed the need for research focused on how service providers can assist financial organizations in achieving compliance.

Owen's study (2021) demonstrated the crucial role that intermediaries play in bridging the gap between regulators and financial organizations. This confirmed the suspicion that service providers are essential in helping financial organizations comply with new regulations. Butler and O'Brien (2019) further emphasized the potential of RegTech in assisting clients with achieving compliance.

The section on service readiness added a broader context to this study by exploring how service providers prepared to meet regulatory demands. Studies like Christensen et al. (2016) and Størkersen et al. (2023) underscored the importance of tailoring services to clients' specific needs, showing that organizations required not only technical expertise but also guidance in understanding and internalizing regulatory requirements. These service providers acted as translators and facilitators of regulatory intentions, helping organizations navigate the complexities of compliance. These studies confirmed the importance of service providers in regulatory compliance and therefore the necessity to investigate the extent to which service providers are ready to support financial organizations with DORA, as emphasized by the aforementioned studies.

Especially the last section provided some valuable lessons about interviewing security practitioners. Having knowledge about the topic of the interview was deemed crucial by Bridges et al. (2018). A solid understanding of the technical environment in which the participants operated was essential for meaningful interactions. This ensured that the discussions were relevant and that the interviewer could engage deeply with the participants' experiences.

Most of the examined studies utilized a qualitative method, by conducting interviews. Some studies combined interviews with a survey, but in this case, as the field of DORA experts in the Netherlands is relatively small, one-on-one interviews will be conducted.

Bridges et al. (2018) emphasized that security professionals might be reluctant to share operational details, so ensuring anonymity and confidentiality was vital due to the sensitive nature of their field. By guaranteeing anonymity and secure handling of data, it was possible to foster an environment where participants felt safe to share honest and detailed insights.

The study by Axon et al. (2018) showed that including a range of roles among participants provided a better understanding of the field. The studies reviewed included various roles, such as SOC professionals, IT professionals, and system administrators, but in my study, this could include partners, managers, and consultants. Gathering insights from a diverse group could reveal different perspectives and challenges based on their specific responsibilities and experiences, enriching the overall findings of the research.

4. Document analysis

The fourth chapter of this study presents the document analysis. Section 4.1 discusses the digital finance package, of which DORA is a part, highlighting its objectives and implications. Section 4.2 offers an overview of DORA, detailing its five key pillars, while section 4.3 compares DORA with similar regulations, identifying both differences and similarities. Finally, section 4.4 provides a comparative analysis of DORA against other similar regulations, while section 4.5 discusses the relevance of the document analysis.

Digital finance package

Since the financial crisis in 2008, the financial sector rapidly evolved, primarily due to advancements in fintech innovation (Mavļutova et al., 2022; Anagnostopoulos, 2018). Digital transformation, as defined by Gong and Ribiere (2021), drove this progress by utilizing innovative digital technologies and strategic resource leverage to fundamentally improve organizations and redefine their value proposition for stakeholders. This transformation led to the restructuring or replacement of entire business models (Downed and Nunes, 2013). To support financial organizations in benefiting from the potential, while also mitigating the associated risks of digitization, the EC introduced the digital finance package. The package aimed to enhance the digital friendliness of financial services in Europe, fostering responsible innovation and competition among EU financial service providers. Through the digital finance package, the EC aimed to prepare for the forthcoming digital transformation in the sector, believing that the package "will ensure that EU financial services rules are fit for the digital age, for applications such as AI and blockchain" (European Commission, 2020b).

Valdis Dombovskis, Executive Vice-President for an Economy that works for People, says the following about the package: *"The future of finance is digital. Technology has much more to offer consumers and businesses and we should embrace the digital transformation proactively, while mitigating any potential risks. That is what the Digital Finance Package aims to do. An innovative digital single market for finance will benefit Europeans and will be key to Europe's economic recovery by offering better financial products for consumers and opening up new funding channels for companies"* (European Commission, 2020b).

The digital finance package was introduced by the EC on September 24, 2020, and consisted of a digital finance strategy, a retail payments strategy, a legislative proposal for an EU regulatory framework on crypto-assets, and a proposal for an EU regulatory framework on digital operational resilience (European Commission, 2020a). Figure *2* illustrates the integration of DORA within the digital finance package.

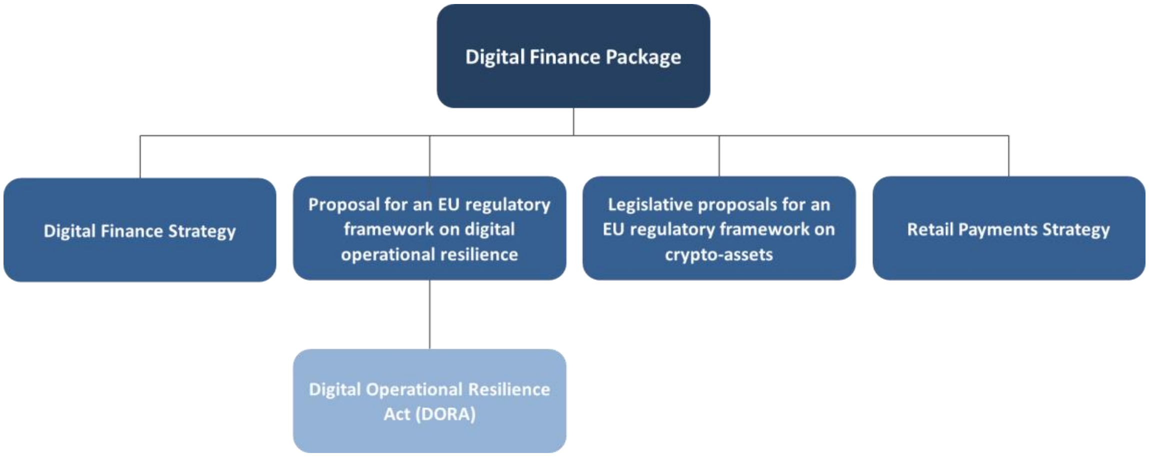
Digital Finance Package
Digital Finance Strategy
Proposal for an EU regulatory framework on digital operational resilience
Legislative proposals for an EU regulatory framework on crypto-assets
Retail Payments Strategy
Digital Operational Resilience Act (DORA)

Figure 2 *- Visualization of the digital finance package*

The Digital Operational Resilience Act

Cyber-attacks within the financial sector experienced a surge in recent years (Gulyás and Kiss, 2023). Not only did the frequency of these attacks increase, but they also became more sophisticated and destructive. Additionally, Clausmeier (2022) identified a growing trend where financial organizations increasingly opted to outsource their IT infrastructure to third-party service providers. The European Commission (2020c) emphasized the importance of strengthening the digital operational resilience of financial organizations as an essential, overarching measure.

The EC emphasized that the increased dependence on digital and remote technologies due to the Covid-19 pandemic further underscored the necessity for enhanced digital resilience. Another reason the EC gave for DORA was that the EU could not afford to have the operational resilience of its digital financial infrastructure questioned. As a result, DORA was recently proposed to unify and enhance IT risk management of financial organizations by recommending stricter rules (Neumannová et al., 2022). The EC stated that "*DORA will make sure the financial sector in Europe is able to stay resilient through a severe operational disruption*" (European Council, 2022). Lukács and Matek (2023) outlined the regulatory goal as aiming to safeguard against cyber threats, operational risks, and other potential disruptions that could threaten financial stability in the EU. While DORA's rules applied to all financial organizations, their implementation would vary depending on the size of the organization, its activities, and the level of risk it faced. This meant that micro-enterprises would experience a more flexible approach, with proportionate requirements for ICT risk management, digital resilience testing, reporting of major ICT-related incidents, and oversight of critical ICT third-party service providers (EY, 2023). To ensure this, DORA includes five pillars that financial organizations should cover, as outlined in Figure 3.

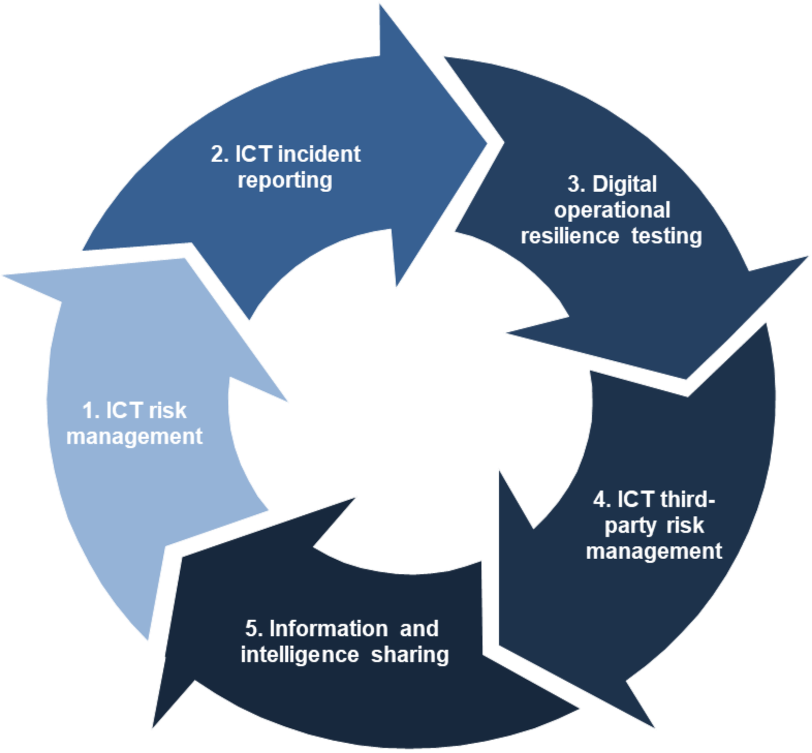
2. ICT incident reporting
3. Digital operational resilience testing
4. ICT third-party risk management
5. Information and intelligence sharing
1. ICT risk management

Figure 3 - *The five pillars of DORA (Thuama and Costigan, 2023)*

A visualized timeline of DORA could be seen in Figure 4.

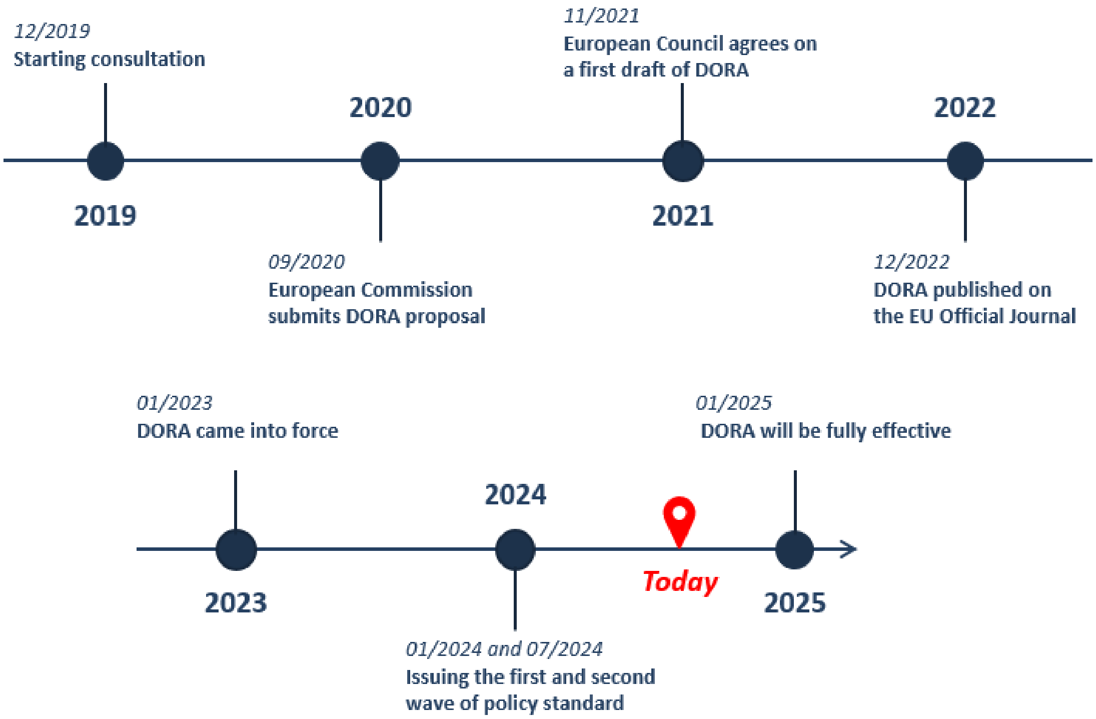
12/2019
Starting consultation
11/2021
European Council agrees on a first draft of DORA
2020
2022
2019
2021
09/2020
European Commission submits DORA proposal
12/2022
DORA published on the EU Official Journal
01/2023
DORA came into force
01/2025
DORA will be fully effective
2024
Today
2023
2025
01/2024 and 07/2024
Issuing the first and second wave of policy standard

Figure 4 - *Timeline of DORA (Eiopa, 2023)*

4.1.1 ICT risk management

The first pillar of DORA, ICT risk management, was addressed in Articles 5 to 14 (European Commission, 2020c). This pillar describes principles and requirements based on national, international, and industry standards, covering different functions within the ICT risk management process. The objective is to enable financial organizations to adapt to the evolving cyber threat landscape by maintaining resilient ICT systems and tools. The regulation emphasizes continuous risk identification, implementation of protective measures, prompt detection of anomalies, and the development of comprehensive business continuity and disaster recovery plans. Key standards and best practices for the financial sector include ISO/IEC 27001 for information security management (ISO, 2022), the NIST Cybersecurity Framework for improving cybersecurity posture (National Institute of Standards and Technology, 2024), and, industry-specific guidelines, such as the Basel Committee on Banking Supervision's (BCBS) principles for the sound management of operational risk (Basel Committee on Banking Supervision, 2014) and the European Banking Authority (EBA) outsourcing guidelines on ICT and security risk management (European Banking Authority, 2019). These standards and best practices ensure flexibility while aligning with supervisory instructions, helping financial organizations meet the robust requirements set forth by DORA without mandating specific standardization.

4.1.2 ICT incident reporting

The second pillar of DORA, ICT-related incident reporting, was addressed in Articles 15 to 20 and aimed to harmonize and streamline the reporting processes (European Commission, 2020c). Financial organizations are required to establish a process to monitor and log IT-related incidents. Furthermore, organizations are obligated to classify these incidents based on criteria outlined in the regulation. The European Supervisory Authorities (ESAs) established these criteria.

In the event of an incident, the financial organization has to furnish authorities with initial, intermediate, and final reports. Another focus of the ESAs was to craft the single rulebook, which aimed to provide a unified set of prudential rules that organizations across the EU had to adhere to (European Banking Authority, 2024). At the time of writing this study, a finalized rulebook was not yet available, but the EBA noted the need for flexibility in the rulebook implementation due to variations in credit and economic cycles. The ESAs applicable for this rulebook consisted of the EBA, the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA) (European Central Bank, 2024).

4.1.3 Digital operational resilience testing

The third pillar of DORA, digital operational resilience testing, was addressed in Articles 21 to 24 and underscored the importance of periodically evaluating the capabilities and functions incorporated into the IT risk management framework (European Commission, 2020c).

This testing aims to evaluate preparedness, identify weaknesses, deficiencies, or gaps, and facilitate the prompt implementation of corrective measures. DORA introduces a proportionate approach to applying digital operational resilience testing requirements, considering the size, business, and risk profiles of financial organizations. While all organizations are mandated to perform testing of IT tools and systems, advanced testing using Threat-Led Penetration Testing (TLPT) is only required for those identified by competent authorities as significant.

4.1.4 ICT third-party risk management

The fourth pillar of DORA, ICT third-party risk management, was addressed in Articles 25 to 39 and aimed to ensure that financial organizations managed IT third-party risk as an integral component of IT risk within their IT risk management framework (European Commission, 2020c). For instance, financial organizations have to evaluate whether a contractual arrangement involves a critical or important function. If it does, they are required to notify the competent authority promptly about the planned contract for such functions. Scott (2021) stated that DORA emphasized that financial organizations outsourcing technology services were ultimately responsible for managing IT risks.

4.1.5 Information and intelligence sharing

The fifth pillar of DORA, information and intelligence sharing, was addressed in Article 40 and aimed to enhance awareness of cyber threats, curbing their potential spread, and fortifying the defensive capabilities, threat detection techniques, as well as mitigation and response strategies of financial organizations (European Commission, 2020c). The European Commission (2020c) envisioned the implementation of this pillar through information-sharing arrangements designed to safeguard the sensitivity of shared information. These arrangements are to be governed by rules of conduct that fully respect business confidentiality, protect personal data, and comply with competition policy guidelines. Financial organizations are also required to inform the competent authorities of their participation in these information-sharing arrangements.

Current offerings regarding to DORA

This section examines the current services provided by service providers to assist financial organizations with DORA compliance. The first subsection discusses the common services offered by service providers. The second subsection explores services related to DORA where service providers sought to differentiate themselves from others. This section reviews Deloitte, EY, PwC, Capgemini, and Avenga.

4.1.6 Common services offered by service providers

All examined service providers offers comprehensive information on DORA on their websites. This included general information about what DORA entails, when it would go into effect, and details about its five pillars. Additionally, each service provider offers implementation actions, outlining steps that financial organizations could take to prepare optimally. Every service provider also provides a readiness assessment and gap analysis to evaluate current compliance levels and identify the most appropriate path for remediation (PwC, 2024b). Another commonly offered service is third-party risk management to comply with the fourth pillar of DORA. Capgemini mentions that they could conduct thorough risk profiling and assessment of suppliers and vendors (Capgemini, 2024), while Deloitte (2024b) states they could help with prioritizing the most important suppliers in order for organizations to ensure compliance with DORA and minimize their exposure to third-party risks.

4.1.7 Additional offerings

In addition to common services, EY also offers a resilience dashboard for monitoring and reporting resilience-related metrics and information to relevant stakeholders (EY, 2023). Avenga is the only one to offer a free readiness test in the form of a survey on its site. Within ten minutes, a financial organization could receive an initial estimation of DORA readiness (Avenga, 2024).

Comparative analysis of DORA with similar regulations

4.1.8 The second Directive on network and information systems

Following the adoption of the initial Directive in 2016, the second Directive on network and information systems (NIS2) was issued in December 2022. The first Directive aimed to establish a consistent cybersecurity level but required a revision due to evolving threats from digitalization and cyber-attacks. The NIS2 Directive strengthened security protocols, addressed supply chain security, simplified reporting, and implemented stricter supervisory measures (Vandezande, 2024). The first Directive applied to Operators of Essential Services (OES) in sectors like energy, banking, and healthcare, as well as Digital Service Providers (DSPs), such as online marketplaces and search engines. NIS2 expanded its scope to include organizations deemed 'important' in sectors like postal services, waste management, and the manufacturing of specific pharmaceutical or chemical products, as well as emerging digital services like social networking and cloud computing (Dekra, 2023). NIS2 classified organizations into two categories: essential and important, with identical requirements but distinctions in supervisory measures and penalties (Scheelen et al., 2023).

The NIS2 and DORA have some similarities, such as the fact that both sought to protect the EU's digital infrastructure from cyber-attacks and other digital threats. Moreover, both laws targeted entities within the EU and not outside it. However, there were logically more differences than similarities. The NIS2 aimed to standardize the overall level of cybersecurity in the EU, while DORA sought to enhance the operational resilience of digital systems in the financial sector (usd AG, 2023). Additionally, NIS2, functioning as a directive, required adaptation to the specific legal contexts of each European member state through national transposition. In contrast, DORA operates as a regulation, uniformly applying across all Member States upon enactment. As a binding legislative act, DORA mandated comprehensive enforcement without the need for individual adaptations (Palais, 2023). Finally, DORA focuses specifically on the financial sector, while NIS2 covered a broader range of industries. In instances of overlap between DORA and the NIS2, DORA overrides the application of the NIS2 (Hildner et al., 2022).

With the NIS2 directive deadline set for October 17, 2024, there were no concrete results available at that time. Similar to the situation with the first directive, where some countries, such as Belgium, only transposed the framework in 2019 despite the initial deadline of May 9, 2018 (Vandezande, 2024), Dutch Minister of Justice and Security Dilan Yeşilgöz-Zegerius concluded in a letter to the Dutch Second Chamber that the implementation deadline for NIS2 would not be met (Tweede Kamer, 2024).

4.1.9 The revised Payment Services Directive

The Revised Payment Services Directive (PSD2) built upon the original Payment Services Directive (PSD), introduced by the EC in 2007 to regulate payment services and providers across the EU (EUR-Lex, 2007). The evolving digital landscape significantly impacted the payment sector, leading to the emergence of new services and market players. Some of these newcomers operated outside the existing regulatory framework, prompting the need for a revised framework to ensure industry stability (Foa and Davola, 2024). The EU saw this trend and adopted PSD2 on October 8, 2015 (EUR-Lex, 2015), establishing a framework to enhance various aspects of electronic payments within the EU. Effective from January 13, 2018, the PSD2 introduced new categories of service providers, including Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs). Companies such as PayPal, iDeal, Tikkie, and Trustly were then authorized to initiate payments directly from users' bank accounts and aggregate financial data from multiple accounts. By formalizing the regulation of these third-party providers, the PSD2 aimed to foster a more interconnected and efficient payment ecosystem while ensuring transactional security and data privacy (Gounari et al., 2024).

The DORA and the PSD2 share some common objectives, particularly in safeguarding consumers through secure and reliable financial services. They both prioritized implementing security measures against cyber threats and operational disruptions. However, they differ in focus: the PSD2 emphasizes open banking and robust authentication for online payments, while DORA aims to enhance operational resilience across the financial sector. Moreover, the PSD2 regulates payment services and providers, whereas DORA extends to all financial organizations and their critical third-party vendors. Another difference is that the PSD2 is a directive, while DORA is a regulation.

Studies indicated that PSD2 plays a significant role in advancing the European payments sector, enhancing customer safeguarding, and fostering efficiency, transparency, and diversity in payment options (Eckhardt, 2023). Research done by Tsanakas (2023) found that financial organizations struggled to apply PSD2 while simultaneously complying with the General Data Protection Regulation (GDPR). This struggle resulted in organizations prioritizing mere compliance by focusing solely on the minimum requirements of the directive.

4.1.10 EBA outsourcing guidelines

The EBA outsourcing guidelines are a set of directives issued by the European Banking Authority with the goal of promoting consistent supervision of outsourcing practices across the EU (European Banking Authority, 2019). The EBA outsourcing guidelines became effective in September 2019 and applied to competent national authorities across the EU, financial organizations, payment organizations, and electronic money organizations (Bird & Bird, 2021). The guidelines outlined the internal governance arrangements, including risk management practices, that payment and electronic money organizations were required to implement when outsourcing functions. These guidelines also helped competent authorities by providing instructions on how to evaluate and monitor these arrangements, ensuring ongoing compliance by the organizations involved (Deloitte, 2019).

According to the law firm NautaDutilh (2023), the requirements of the EBA outsourcing guidelines and DORA show many similarities. For example, both set out requirements for arrangements with third-party service providers. One key difference between DORA and the EBA outsourcing guidelines is that DORA focuses on all ongoing digital and data services provided through ICT systems, not just those that qualified as outsourcing. In contrast, the EBA outsourcing guidelines applies to all outsourcing arrangements, whether they were ICT-related or not.

According to a report by Bird & Bird (2021), some EU Member States introduced stricter national requirements than the original ones set out in the EBA outsourcing guidelines. This could have been due to the perception that the guidelines were not strict enough. The EBA outsourcing guidelines became effective in Dutch national law after the Dutch competent authority, de Nederlandse Bank, incorporated them into its policy. With the introduction of DORA, the EBA began conducting a gap analysis to compare existing guidelines with the new requirements of DORA to ensure alignment with the updated regulatory framework of DORA (Pinsent Masons, 2024).

4.1.11 PRA SS2/21

The Supervisory Statement (SS) outlined the Prudential Regulation Authority's (PRA) expectations for how PRA-regulated organizations should manage outsourcing and third-party risks. The SS built upon existing operational resilience policies and requirements, such as those in the PRA Rulebook and SS1/21 on impact tolerances for critical business services. It also sought to promote the use of cloud services and other emerging technologies, as recommended in the Bank of England's 'Future of Finance' report, while aligning with the EBA outsourcing guidelines on outsourcing arrangements, thereby clarifying the PRA's expectations for banks. The statement was relevant to all banks, insurance and reinsurance organizations, and PRA-designated investment organizations in the United Kingdom, among others (Bank of England, 2021).

With PRA SS2/21 being effective from March 31, 2022, financial organizations in the UK had a head start of almost three years in implementing their own operational resilience framework. The operational resilience regimes of both the UK and EU shared similarities, such as a mindset shift towards assuming inevitable disruptions and building resilience to recover critical business functions promptly. Both frameworks required firms to enhance their mapping of policies, people, technology, data, and suppliers that supported their core business (Reynolds & Hill, 2021). However, there were differences. DORA was more prescriptive, with legally binding requirements, including regulators' oversight of critical third parties and specific incident and threat reporting protocols. In contrast, SS2/21 was a principle-based supervisory framework. Despite these differences, both aimed to protect against unexpected disruptions and enhance overall operational resilience.

The Bank of England conducted a survey from September to October 2023, targeting a sample of firms under the supervision of the PRA to evaluate the effectiveness and quality of the supervisory framework and its approach (Bank of England, 2024).

The results of the survey indicated that firms were finding the PRA Rulebook challenging to navigate. In response, the Bank of England launched a new PRA Rulebook in April 2024, designed to be more user-friendly. Additionally, firms expressed a desire for earlier and more frequent engagement with the PRA during policy formulation. In response to this feedback, the PRA planned to actively involve stakeholders to support informed policymaking and better address UK-specific circumstances (Bank of England, 2024).

The relevance of the document analysis

Firstly, and most importantly, the document analysis provided a thorough understanding of DORA in general, including its objectives, pillars, and timeline. It also helped in understanding the bigger picture of DORA within the digital finance package, clarifying the necessity of this regulation for financial organizations. This knowledge was crucial for formulating relevant interview questions and identifying gaps in the documents that were good to discuss during the interview. The knowledge was also important for having in-depth discussions about DORA during the interviews.

For instance, the section of the document analysis that focused on DORA's pillars enabled more targeted questions during the interviews, such as which of these pillars are most demanded by financial organizations and which are considered the most critical. Additionally, the analysis of current service provider offerings and the comparison of DORA with similar regulations, such as NIS2, were useful for formulating interview questions. Questions like, "Which specific regulations have provided the most valuable lessons for DORA compliance?" helped validate whether the regulations covered in the analysis were indeed the most influential.

During the interviews, the PRA SS2/21 was frequently mentioned by participants, but it was not covered in the document analysis. It became clear during the interviews that the PRA SS2/21 taught service providers important lessons that could be brought to DORA. Because of this, the PRA SS2/21 was incorporated into the document analysis. After asking the question about the regulation that provided the most valuable lessons learned, the follow-up question, "What knowledge and lessons learned are specifically applicable?" was designed to gain deeper insights into how these lessons could help service providers assist financial organizations in complying with DORA.

While analyzing the similarities between regulations, such as the EBA outsourcing guidelines and DORA, a hypothesis emerged. It suggested that the similarities between the EBA outsourcing guidelines and DORA allowed the lessons learned from the EBA guidelines to be directly applied to DORA. This hypothesis was later confirmed during the interviews. It became clear that experience gained from these similarities could indeed be transferred to DORA.

For instance, the requirements for managing third-party service providers, a significant component of the EBA outsourcing guidelines, were confirmed to be relevant to DORA as well. Interviewees highlighted that the approach to third-party requirements in the EBA was closely aligned with DORA's requirements. Therefore, the lessons learned from the EBA outsourcing guidelines can provide significant value when implementing the TPRM requirements under DORA.

5. Results

The fifth chapter presents the findings of this study. Section 5.1 addresses the first subquestion using insights from the document analysis. Section 5.2 provides answers to the remaining subquestions. Each subsection of the chapter, for example, 5.2.1, 5.2.2, and 5.2.3, is related to a subquestion of this research.

Analysis of DORA

The first subquestion was solely answered by the document analysis. More in-depth information regarding DORA can be found in the fourth chapter, but this section explains concisely what DORA requires from financial organizations.

5.1.1 DORA requirements for financial organizations

This subsection will give answer to the first subquestion of this study. The DORA is part of a bigger initiative of the EC. On September 24, 2020, the EC introduced the digital finance package, which aims to support the financial sector's digital transformation while mitigating associated risks. The DORA sets requirements for financial organizations to improve their digital resilience so that EU financial organizations can withstand severe operational disruptions, particularly cyber-attacks. Several updates have been made to DORA since September 2020, and the final version will be in full effect from Jan. 17, 2025. The DORA is built around five pillars:

1. ICT risk management: financial organizations must implement robust ICT risk management frameworks. This includes continuous risk identification, the implementation of protective measures, and the creation of business continuity and disaster recovery plans. Adherence to international standards like ISO/IEC 27001 and guidelines from authorities such as the EBA is encouraged.

2. ICT incident reporting: financial organizations are required to monitor, log, and classify IT-related incidents. They must provide authorities with reports detailing these incidents to ensure swift action and transparency. The reporting process is designed to be harmonized across the EU, aiding in unified regulatory oversight.

3. Digital operational resilience testing: financial organizations must periodically evaluate their digital operational resilience to identify and address weaknesses in their IT risk management frameworks. Depending on their size and risk profile, this may include advanced testing methods like TLPT.

4. ICT third-party risk management: DORA mandates that financial organizations manage risks associated with outsourcing IT services to third-party providers. Organizations must assess and monitor these relationships, especially if they involve critical functions, to ensure they maintain overall responsibility for managing IT risks.

5. Information and intelligence sharing: to enhance awareness and defense against cyber threats, financial organizations are encouraged to participate in information-sharing arrangements. These arrangements must comply with data protection, confidentiality, and competition guidelines.

Through these pillars, DORA requires financial organizations to strengthen their operational resilience, ensuring they can adapt to and mitigate risks associated with digital transformation and innovation in the financial sector.

Interviews

The remaining subquestions, the second until the seventh, were addressed by obtaining information during fourteen interviews. In this section, the results on those subquestions will be explained.

5.1.2 Service providers' perception of readiness for offering DORA services

This subsection will give answer to the second subquestion of this research: *"how do service providers perceive readiness to provide services related to DORA?."*

The answers to the interview questions designed to address this subquestion varied, but there were a few elements they felt every service provider should have, such as the importance of having multidisciplinary teams within the organization for delivering DORA services to financial organizations. Participants C7 and L2 emphasized that service providers could not effectively help financial organizations comply with DORA without knowledge and expertise across all aspects of the regulation. According to participants C2, C4, and L1, this included areas such as third-party risk management and cybersecurity. Additionally, they stressed the necessity for organizations to understand and explain legal aspects, such as contract law, according to Participant C8.

> *"A multidisciplinary approach is essential. It requires expertise in legal matters, business continuity, cyber, risk management and technical knowledge (e.g., pentesting)."*
> *(Participant C7)*

Participants C2 and C5 highlighted that having knowledgeable consultants was crucial in order to help the client as best as possible. According to Participant C9, being a knowledgeable consultant involved having an in-depth understanding of the relevant laws and regulations, including how DORA connected with them. The interviewee deemed it important to be able to present a view of these interrelationships between different laws and regulations. More essential expertise and knowledgeable areas for consultants are discussed in subsection 5.2.4. The interviewee added that, by doing this in the right way, the service provider could help financial organizations meet multiple requirements more efficiently at the same time. Participant C6 agreed, stating that DORA was the starting point for digital resilience and that implementing DORA could also be beneficial for upcoming regulations, such as the AI Act.

> *"During client projects, it's important to look beyond just DORA and consider other relevant laws and regulations, such as the AI Act. This approach can help organizations meet multiple requirements more efficiently at the same time and can serve as a unique selling point for the service provider."*
> *(Participant C9)*

A recurring theme among the interviewees was the importance of having the right tools to maximize effectiveness and efficiency. Participant C7 identified four key components of DORA readiness: the right consultants, processes, data, and tools. Additionally, Participant C6 emphasized that automation provided significant added value, such as using GenAI to upload and cross-check policies against DORA legislation.

> *“We have found that automation offers significant added value, for example, using tools like GenAI to upload and cross-check policies and DORA legislation.”*
> *(Participant C6)*

Other important aspects mentioned by the interviewees included having a go-to-market strategy, according to Participants C2 and C6, and securing access to decision-makers within financial organizations, as emphasized by Participants C6 and C9. Participant C6 highlighted the latter as crucial, explaining that without access to decision-makers, even the best go-to-market strategy would remain ineffective.

> *“Readiness includes having a strong go-to-market strategy”*
> *(Participant C2)*

Participant C5 defined readiness as the ability to use lessons learned from previous regulatory compliance, such as the PRA SS2/21 in the UK, to create a checklist for financial organizations to meet the minimum requirements set by the regulator and to understand that not all requirements could be met by the deadline. The interviewee added that having early conversations with regulators to define acceptable criteria was also important before starting to help financial organizations comply with DORA.

> *"Readiness involves having early conversations with regulators to define acceptable criteria."*
> *(Participant C5)*

When asked if the service providers used any criteria or tools to assess their own readiness, Participant C7 said that at their company, no specific review had taken place to assess their own readiness. Participant L3 also mentioned that they did not have a specific process or department to assess their readiness to offer DORA services. The interviewee stated that at their company, they studied the legislation themselves and discussed obligations and completeness internally. Participant C11 noted that their company used peer reviews and standard work programs to ensure the quality and completeness of their services. The company where Participant C5 worked used a tool to assess their readiness, employing checklists that included various criteria and benchmarks against best practices. Finally, Participant C4 stated that at their company, the quality of service is guaranteed by the expertise of individual partners and internal audits.

5.1.3 Current offerings of service providers

This subsection will answer the third subquestion of this research: "What are the current offerings of service providers in assisting financial organizations with DORA compliance?"

The document analysis looked at current offerings regarding DORA services from service providers toward financial organizations. However, during the interviews, some follow-up questions were asked about this, which can be seen in Table 3 on page 17 and are further elaborated on in this subsection.

During the document analysis, it was found that each service provider examined was able to provide financial organizations with a readiness assessment and a gap analysis to evaluate the current level of compliance and determine the most appropriate path for DORA compliance. Another commonly offered service was third-party risk management. Few other services were offered at that time, at least not on the service providers’ websites. However, there was no doubt that the service providers did much more than just the above, which eventually became clear during the interviews.

During the interviews, the discussion focused on how the service providers tried to differentiate their DORA services from those of other service providers. The aspects the interviewees identified as their unique selling points aligned with the previously mentioned must-haves for service providers, such as having multidisciplinary teams, industry-specific knowledge, and in-depth expertise in regulations and cybersecurity, among others. This was noted by Participants C5, C9, and C11. Some unique perspectives included the view of Participant C1, who highlighted their ability to deliver an end-to-end DORA solution as a unique selling point. Participant L3 pointed to their cooperation with industry associations and the development of standard clauses aligned with regulators as a key differentiator. Additionally, Participant C11 mentioned their integrated global network of international member firms as a unique selling point. Interestingly, Participant L1 noted that they were still exploring where their added value as a legal firm lay.

“As a legal firm, we haven't quite mapped out where the added value lies yet.”
(Participant L1)

Participant C1 highlighted the difficulty of pinpointing one specific service because DORA was an integral process, but if they had to choose the most important DORA services, they were third-party risk management and disaster recovery services. Participant C4 agreed, saying that most work was with third-party risk management. Another important service for financial organizations was the gap analysis, as it allowed a financial organization to clearly see where it stood, where it needed to go, and how it could overcome that gap, according to Participant C11. Participant C6 added that the gap analysis often served as the starting point from which service providers could undertake other projects within the financial organization.

“The most important service is the gap analysis, as this usually serves as the starting point. From there, we can offer program management and third-party risk management, which are often significant challenges for financial organizations.”
(Participant C6)

The services that were considered most important for financial organizations by the interviewees were, most of the time, also the most demanded by the financial organizations. However, some other services with high demand were also discussed during the interviews. Participant L1 said that financial organizations usually sought advice on how to integrate DORA requirements into the organization and what concrete steps were needed to do so. There was also significant demand for modifying contracts with vendors and for explanations about the exact content of DORA and its relevance to organizations, as noted by Participant L3. Participants C6 and C7 added that there was a growing demand for implementation support, such as assistance with privileged access management and third-party risk management. Participant C4 also saw a lot of demand for implementation support. Another important service was helping the board members of financial organizations become familiar with DORA, as mentioned by Participant L2.

> *"At this moment, advisory services on the interpretation of new laws and regulations and gap assessments are mainly in demand. However, the focus is shifting to actual implementation and elaboration."*
> *(Participant C7)*

Another service that had high demand was the validation of the financial organizations' own gap assessment by a third party. This was highlighted by Participants C3, C7, and C11. This was because an external party, in this case, the service provider, could provide an independent perspective, as explained by Participant C6. The most demanded services at a legal firm included drafting, modifying, and reviewing contracts, and determining which services were covered by DORA, according to Participants C8 and L2. Financial organizations also looked for assistance in translating the regulations into a business context, as mentioned by Participants C4 and L3. Another frequently mentioned need during the interviews was support in implementing DORA requirements, as noted by Participants C3, C6, and C11, as well as the ability to offer benchmarking with similar financial organizations, according to Participant C4.

> *"Clients are also often interested in having their own gap assessment reviewed by a third party so that it is truly validated."*
> *(Participant C7)*

5.1.4 Factors influencing financial organizations' engagement with service providers

This subsection will give answer to the fourth subquestion of this research*: "what are the factors that influence the decision of financial organizations to engage service providers for DORA compliance support?."*

Financial organizations often chose to use service providers due to a lack of resources. They did not have the necessary means to manage DORA compliance internally. Complying with DORA requirements was an intensive task that demanded specialized knowledge and experience, which financial organizations often lacked, according to Participant C8 and L1. Participant C8 added that, although financial organizations often took the first steps toward DORA compliance themselves, they eventually had to seek help from service providers due to the enormous amount of work required within a short timeline.

> *"One of the reasons is a lack of internal resources and expertise. You really need a serious amount of time, energy, and people to master such a new subject."*
> *(Participant L1)*

Participant C11 further noted that, besides the lack of knowledge and experience, financial organizations often lacked the internal capacity in terms of manpower to address DORA compliance. Participant C2 agreed, stating that financial organizations did not have the manpower or expertise to meet DORA requirements. A reason for this lack of capacity is that financial organizations are being overloaded with new regulations, as noted by Participant C4.

> *"Many financial organizations, including larger ones, often lack the capacity to manage DORA compliance internally. Their specialists are already occupied with existing regulations, leaving limited resources to address new regulatory requirements." (Participant C4)*

Other factors influencing the choice of service provider included the prioritization of cost-effectiveness or quality of service when seeking DORA compliance support. Regarding whether the cost or the quality of the service was more important, the responses varied. According to Participants C2 and C7, this depended on the organization and the specific DORA service in question.

> *"For assessments and program management, organizations often prioritize quality. However, for the execution phase, where most hours are spent, cost-effectiveness sometimes becomes more important." (Participant C2).*

Participant C9 noted that clients appreciated a good balance between price and quality, while Participant L3 mentioned that for loyal clients, price is less important compared to clients who use different service providers for each project. There were also interviewees who stated that cost-effectiveness is more important than the quality of the service, including Participants C5, C8, and C11. On the other hand, Participants C6 and C10 stated that the quality of service was more important than cost-effectiveness.

> *"Costs are often a bottleneck and are usually considered more important than the quality of service. This means that many financial organizations have budget constraints that force them to be cost-conscious when choosing a service provider. Although quality is also important, in practice, price often is the decisive factor in choosing a service provider."*
> *(Participant C8)*

In addition to the price/quality balance playing a role in deciding which service provider a financial organization chooses, the timeline is also an important factor, according to Participants L1 and C8. Financial organizations also regularly ask for examples of similar DORA projects that service providers have completed for other financial organizations, in the form of use cases or references, as mentioned by Participants C4 and C7.

> *"Besides costs and quality, timelines are a crucial focus. Financial organisations often face tight deadlines and expect service providers to work quickly and efficiently to meet these deadlines. The availability of the service provider and their ability to operate within the required timelines play an important role in the decision-making process." (Participant C8)*

5.1.5 Essential capabilities for consultants in assisting with DORA compliance

This subsection will answer the fifth subquestion of this research: "w*hat capabilities are essential for consultants to assist financial organizations in complying with DORA?"*

In subsection 5.2.2, it became clear that, for the interviewees, readiness meant having knowledgeable consultants. During the interviews, the expertise and knowledge areas that consultants must possess to assist financial organizations with DORA compliance were discussed, along with the certifications and training deemed important for these consultants.

The most frequently mentioned areas of knowledge and expertise during the interviews were the importance of consultants having experience working with financial organizations. The interviewees stated that industry-specific knowledge was crucial, according to Participants C5, C8, and C9. They explained that if service providers were familiar with the existing standards and practices within the sector, they could assist clients more effectively, as noted by Participant C8.

> *"Understanding the playing field and the specific needs of the client are critical."*
> *(Participant L2)*

Another frequently mentioned aspect was the importance of knowing the client. According to Participant C7, by knowing the client well, service providers could assist the client much better. Participant L1 added that understanding the critical functions and core business lines of a specific organization was important. Additionally, Participant C9 noted that understanding the context of an organization was crucial to identify which components were most important to the customer and where the most risk could be hedged. Other, more general consulting skills, such as analytical abilities, communication skills, and problem-solving capabilities, were also considered important by Participants C10 and C11.

> *"Analytical skills, knowledge of regulations, and the ability to solve complex problems have always proved useful. Communication skills are also crucial, as it is important to be able to work effectively with different departments within an organization."*
> *(Participant C11)*

Knowledge of operational resilience was considered important by a large part of the interviewees, including knowledge of recovery management, business continuity, and crisis management. This was highlighted by Participants C1, C2, and L2. Besides this, knowledge of IT risk management (Participants C4 and L1), cybersecurity (Participants C2 and L1), and knowledge of IT in general (Participants C3 and C8) were deemed important. Technical expertise was also considered an important area of expertise for consultants. According to Participant C2, knowledge of network security is an important skill for consultants. Experience with pentesting was another important technical skill that consultants needed to possess, as noted by Participants C1, C10, and L3.

> *"Service providers should have a team of experts who understand the ins and outs of DORA. In addition, they should have experts in crisis management, pentesting, among others."*
> *(Participant C1)*

In terms of legal knowledge, proficiency in IT outsourcing contracts, contract law, and the ability to translate DORA requirements into actionable steps were highlighted as crucial by Participants L1, L2, and L3.

> *"Service providers should be able to cover a wide range of legal topics, including financial supervisory law, IT, and governance. Deep understanding of clients' specific needs and operational practices is essential."*
> *(Participant L2)*

Regarding training programs and certifications, none of the interview participants indicated that following specific training or obtaining a certification was mandatory. However, Participant C10 mentioned that while trainings and certifications were not mandatory for a consultant to work on DORA projects, they were deemed beneficial. Certifications such as CISSP and CISM were seen as valuable for understanding the technical aspects of DORA.

> *“There are no mandatory certifications, but our company organizes both internal and external training sessions to share knowledge and prepare our associates for DORA. This includes strategic sessions for partners as well as operational training for junior and senior associates.”*
> *(Participant L2)*

Most participants mentioned that they did not have any internal DORA training programs, including Participants C4, C7, and L3, but that knowledge transfer within the organization was important, as noted by Participant C4.

> *"Security trainings like CISM and CISSP, as well as IT and Cloud training, provide a solid foundation for meeting DORA requirements. However, these are not strict requirements set by the company to work on DORA projects."*
> *(Participant C6)*

Most service providers teach their consultants the necessary skills through a ‘learning while doing’ approach, by organizing internal knowledge-sharing sessions, and by having more senior employees as mentors for junior staff, according to Participants C4, C8, and L2. Additionally, Participant C10 mentioned the establishment of an international DORA working group with multiple member firms, which facilitates knowledge exchange and the development of tools. Also, Participant C11 noted that their company has an integrated global network, which enables close cooperation between different member firms in Europe.

> *“We have set up a working group at the EU level with countries that form the financial heart of Europe, including the UK, Netherlands, Luxembourg, and Switzerland.”*
> *(Participant C10)*

5.1.6 Lesson learned from other digital regulations to DORA adherence

This subsection will give answer to the sixth subquestion of this research*: “to what extent can the knowledge acquired by service providers in assisting financial organizations with other digital* *regulations be applied to adhere to DORA?."* In section 4.4, similar regulations were discussed and formed a basis for the interviews on this topic. However, the four regulations identified as similar were not the only regulations from which lessons learned could be brought to DORA. The regulations, guidelines, and best practices discussed during the interviews included the EBA outsourcing guidelines, GDPR, PRA SS2/21, DNB Good Practice, EIOPA, ESMA, ISO 27001, KRITIS, and NIS2.

The EBA outsourcing guidelines, the GDPR, ISO 27001, PRA SS2/21, and NIS2 were the most frequently mentioned regulations from which lessons learned could be applied to DORA. Lessons learned from the EBA outsourcing guidelines, particularly in reviewing third-party suppliers and drafting contractual agreements, closely aligned with DORA's requirements, making the previously gained experience directly applicable, as explained by Participant C8.

Participant C6 noted that NIS2 was also comparable to DORA in terms of third-party risk management. According to Participant C7, the GDPR taught service providers that financial organizations could apply their third-party risk management approaches from the GDPR to DORA, as the processes were closely aligned. Additionally, Participant C6 mentioned that the structure of conducting DORA gap assessments at financial organizations was similar to that of the GDPR. This approach provided a framework for identifying compliance gaps and determining necessary actions to achieve DORA compliance. Participant C11 added that the GDPR particularly provided valuable lessons regarding uniformity and the need to constantly keep up with changes.

"The GDPR has a similar structure with its gap analysis approach."
(Participant C6)

Another regulation deemed interesting in relation to DORA was PRA SS2/21, which was about 1.5 years ahead of DORA, as mentioned by Participant C6. Valuable lessons learned from PRA SS2/21, that are directly applicable to DORA, included the importance of creating detailed checklists, understanding regulatory expectations, and engaging with regulators early to define acceptable compliance criteria, according to Participant C5.

"The UK's PRA SS/21 regulation has provided valuable lessons that are directly applicable to DORA compliance."
(Participant C5)

Besides the ones most frequently mentioned during the interviews, some other regulations were also considered relevant in terms of bringing their lessons learned to DORA. One of these was the DNB Good Practice, according to Participants C3 and C11. They pointed out that the DNB guidelines offer insights into different maturity levels and compliance dynamics, which are essential in understanding the varying needs of financial organizations. Participant L2 stated that ESMA and EIOPA provided key lessons regarding correctly interpreting and implementing outsourcing guidelines and understanding the operational resilience and IT security requirements. These aspects are crucial in DORA compliance, where the robustness of operational resilience is a focal point. Lastly, Participant C9 mentioned that MiCA, which is part of the digital finance package like DORA, had provided valuable lessons in aligning regulatory requirements with industry practices.

"The DNB Good Practice and ISO 27001 are in particularly relevant because the DNB guidelines offer insights into different maturity levels and compliance dynamics, while ISO 27001 provides a robust risk management framework."
(Participant C3)

ISO 27001 was highlighted as a crucial framework that service providers could leverage to enhance DORA compliance efforts. Its comprehensive approach to information security management systems aligns well with DORA's focus on ensuring the security and resilience of digital operations within financial organizations. This standard helps in implementing structured processes for identifying, managing, and mitigating information security risks. Participants emphasized that integrating ISO 27001's principles into DORA compliance strategies can lead to a more robust and systematic approach, allowing service providers to address both regulatory and security requirements effectively.

5.1.7 A checklist to evaluate the readiness of service providers

This subsection will give answer to the seventh subquestion of this research*: "how would a practical checklist help service providers assess their readiness and identify the gaps look like?."*

The checklist was designed to serve as a tool for service providers looking to establish a DORA proposition or assess the completeness of their current offering. Service providers could also partially implement the checklist into their existing services. Based on the findings from the document analysis, interviews, and validation discussions, there was a possibility that some topics not identified in these stages might be missing from the checklist. Nonetheless, the checklist aimed to outline what was, according to this study, necessary for service providers to effectively support financial organizations.

The checklist emerged primarily from the interviews, incorporating the insights gathered from all the interview and research questions. After creating a final draft, the checklist was further refined and validated through three separate interviews with DORA experts. This process resulted in the final checklist, which can be found in Table 4. It consisted of six phases, each addressing a specific aspect of the service delivery process, with the sixth phase, continuous improvement, serving as an ongoing process that surrounded and influenced all other phases. A visualization of the figure can be found in Figure 5.

The influence of the interviews on the checklist's development was evident in various phases. For instance, in the first phase, which included expertise development and go-to-market strategy, these topics directly reflected the discussions in subsections 5.2.2 and 5.2.4. The sixth phase, continuous improvement, covered elements such as internal audits and knowledge sharing, discussed in subsections 5.2.1 and 5.2.4. Most of the phases were designed and fine-tuned during the expert interviews, who provided valuable suggestions and identified areas for improvement.

One suggestion incorporated into the checklist was the inclusion of a continuous improvement cycle that encompassed all five phases, rather than confining activities like knowledge sharing or lessons learned to a specific phase. This change acknowledged that service enhancement is an ongoing process, not limited to any particular stage. For example, the development of tools is a continuous effort, not restricted to the gap assessment phase. During another interview with a DORA expert, tips were given about the gap assessment phase. He had worked on many DORA gap assessments already and was able to explain which important steps should have been part of that phase, such as the importance of validating the findings, which was not part of the checklist yet but was directly included after the validation interview.

Additionally, the wording of the checklist was refined to make it clearer and more accessible from the perspective of service providers. Another notable revision based on participant feedback was the use of bullet points instead of numbering the actions within the phases. Numbering had initially given the impression that the actions needed to be completed in a specific order, which was not necessarily the case.

Although the interviews and validation interviews provided the most input for the checklist, the document analysis also contributed. While reviewing service provider offerings related to DORA, insights were gained into the components of a gap analysis, such as conducting interviews and workshops with clients, as well as reviewing their documentation to identify gaps. These insights were used to draft the initial version of that specific part of the checklist.

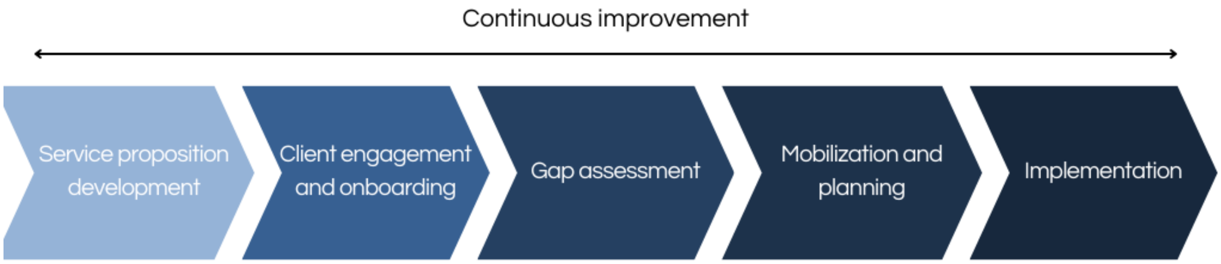
Continuous improvement
Service proposition development
Client engagement and onboarding
Gap assessment
Mobilization and planning
Implementation

Figure 5 *- Visualization of the phases of DORA readiness checklist*

Phase 1: Service proposition development

The first phase began with the creation and design of the service proposition. This phase emphasized the importance of defining the scope of DORA services, developing expertise, acquiring necessary technological tools, and creating a go-to-market strategy. These elements were essential for engaging potential clients and establishing the foundation for a successful service offering.

Phase 2: Client engagement and onboarding

In the second phase, the focus shifted to initiating client relationships and understanding their specific needs. This phase involved acquiring clients, conducting initial consultations, and planning the project. It was crucial to have access to decision-makers within the client organization to ensure that the project aligned with their expectations and business context.

Phase 3: Gap assessment

The third phase involved performing a gap assessment to identify compliance needs. This included conducting workshops and interviews with key personnel, reviewing existing documentation, conducting the actual gap assessment, and validating findings with the client. The outcome was a roadmap outlining the steps needed to achieve DORA compliance for the financial organization.

Phase 4: Mobilization and planning

In the fourth phase, a strategy and plan were developed to address the identified gaps. This included prioritizing gaps based on their impact, ensuring the availability of required skill sets, selecting necessary technology and tools, and developing an implementation plan. The strategy and plan needed to be approved by key stakeholders to proceed.

Phase 5: Implementation

The fifth phase focused on executing the implementation plan to achieve DORA compliance for the financial organization. This involved updating policies and procedures, implementing technical controls, conducting quality assurance audits, and delivering the final report to the client.

Phase 6: Continuous improvement

The sixth phase was dedicated to maintaining and enhancing the quality of DORA proposition. It included internal audits, knowledge-sharing, peer reviews, and the development of technological solutions. The aim was to equip service providers with the necessary tools and strategies to deliver reliable and up-to-date support for financial organizations, ensuring compliance with DORA regulations while maintaining high standards and adaptability in their services.

Phase 1: Service proposition development **Objective**: Establish the service offering, develop expertise, and create a market strategy.	
• **Service scoping**	
○ The scope of DORA services is clearly defined, emphasizing the organization's strengths, and identifying areas for enhancement.	
○ Service descriptions are developed to align with the needs and expectations of financial organizations, fostering confidence in the service provider.	
• **Expertise development**	
○ A team with technical expertise in third-party risk management, pentesting, cybersecurity, business continuity, and recovery management is developed.	
○ A team with legal expertise in IT outsourcing contracts, contract law, and the ability to translate DORA requirements into actionable steps is in developed.	
○ A team with general consulting expertise in analytical abilities, communication skills, and problem-solving capabilities is developed.	
○ A team with deep expertise in DORA and the ability to understand its correlation with other relevant regulations is developed.	
○ A team of people who understand what DORA is, who have a holistic view, and are able to convince clients are in place.	
• **Go-to-market strategy**	
○ A marketing and sales strategy to promote DORA services is developed.	
○ Promotional materials, case studies, and client testimonials are created.	
○ Access to decision-makers within potential client organizations is ensured.	
Phase 2: Client engagement and onboarding **Objective**: Utilize client relationships, understand their needs, and plan the project.	
• **Client acquisition**	
○ The go-to-market strategy is leveraged to attract potential clients.	
○ Networking, industry events, and digital marketing are utilized to generate leads.	

• **Initial consultation and needs assessment**	
o Initial meetings to understand the client’s specific requirements and business context are conducted.	
o The client is assessed to determine which DORA requirements are applicable, ensuring proportionality.	
o The project scope, objectives, and deliverables are clearly defined.	
• **Project planning**	
o A detailed project plan, including timelines, technology accelerators, and resource allocation, is developed.	
Phase 3: Gap assessment **Objective**: Perform a gap assessment to identify all gaps and compliance needs.	
• **Client workshops and interviews**	
o Workshops and interviews are conducted to gather detailed information from key personnel.	
• **Documentation review**	
o Existing policies, procedures, and contracts are reviewed.	
o Automation tools are used to review the client’s documentation.	
• **Requirement analysis**	
o The client’s documentation is mapped against DORA requirements.	
o Automation tools are used to identify gaps and areas needing improvement.	
• **Validate findings**	
o Findings are validated with the client to ensure accuracy and completeness.	
• **Client delivery**	
o A roadmap outlining the steps needed to close the gaps and achieve DORA compliance is delivered.	
o Gaps identified are prioritized based on their impact on compliance and operational risk.	
o The roadmap is presented to key stakeholders for approval.	
Phase 4: Mobilization and planning **Objective**: Develop a strategy and planning to address the identified gaps and achieve DORA compliance.	
• **People planning**	

○ The right people with the required skillsets are identified and made available within the necessary period.	
• **Technology and tool selection**	
○ The technology and tools required for implementation are assessed and confirmed to be available.	
○ If the necessary technology and tools are not available, they are actively being developed to meet project requirements.	
• **Implementation plan**	
○ A detailed implementation plan, based on the documents delivered in the third phase, is developed.	
• **Stakeholder approval**	
○ The strategy and implementation plan are presented to key stakeholders for approval.	
Phase 5: Implementation **Objective**: Execute the implementation plan to achieve compliance with DORA requirements.	
• **Policy and procedures**	
○ Policies and procedures are updated or created to align with DORA requirements.	
• **Technical implementation**	
○ Implement necessary technical controls and security measures to meet DORA requirements.	
○ Conduct testing of technical controls to ensure effectiveness.	
• **Incremental delivery**	
○ Incremental updates are delivered to the client within short timeframes to ensure alignment with their expectations.	
○ Necessary adjustments are facilitated based on client feedback and evolving requirements.	
Phase 6: Continuous improvement **Objective**: Ensure ongoing service enhancement through internal audits, knowledge sharing, peer reviews and technology development.	
• **Internal audits**	
○ Internal audits are conducted to ensure the quality and effectiveness of DORA services.	

o Findings from audits are documented, and corrective actions are promptly implemented.	
• **Knowledge sharing**	
o Knowledge sharing platforms and internal guidelines for effectively performing DORA services are established.	
o Internal training sessions are organized to ensure all team members are well-versed in the services and regulatory requirements.	
o All relevant documents are maintained in a centralized repository for easy access and reference.	
• **Peer reviews**	
o Regular peer reviews are conducted, and lessons learned are documented to improve DORA services.	
o Insights from reviews are used to identify areas for improvement and refine service delivery.	
• **Technology development**	
o Technology solutions are continuously enhanced and developed based on lessons learned and the latest innovations.	

***Table 4** - The DORA readiness checklist*

6. Discussion

In this sixth chapter of the study, the answers to the subquestions are addressed. In chapter 5, the answers to these research questions were provided. In this chapter, these answers are discussed, including the answer to the main research question. Section 6.1 discussed the limitations of this study.

RQ: To what extent are service providers prepared to support financial organizations in complying with DORA?

Based on the research conducted and the interviews held, it became evident that service providers are well-prepared to support financial organizations in achieving DORA compliance. The interviews provided valuable insights into how service providers assist financial organizations in meeting regulatory requirements. It became clear that most service providers offer services across each of DORA's five pillars. Additionally, they demonstrated a strong understanding of the challenges financial organizations face in becoming compliant, such as a lack of resources and specialized expertise. The strengths of service providers also emerged, including having multidisciplinary teams and utilizing automation and AI to improve the quality and efficiency of their services. Service providers mentioned significant investments in tools and technologies, highlighting their commitment to their role as intermediaries. Service providers appear well-prepared to help financial organizations overcome obstacles and achieve compliance.

Moreover, service providers are proactive in reaching out to financial organizations and actively offering their support. While these outreach efforts are undoubtedly driven by marketing, they also raise awareness among financial organizations that assistance is readily available if needed. Another indication of service providers' readiness is the extent to which they leverage their experience with other regulatory frameworks, such as NIS2, GDPR, and the EBA outsourcing guidelines, to ensure preparedness for DORA. Service providers are not only focused on being well-prepared at the moment but also on staying up to date with the latest developments around DORA by offering internal and external training for their consultants. They also organize (international) working groups to share knowledge and experiences within their firms.

Lastly, a further demonstration of service providers' preparedness is their engagement with regulators. Some interviewees highlighted the importance of having early conversations with regulators to discuss key aspects of DORA compliance, which further ensures they remain well-positioned to assist financial organizations effectively.

SQ1: What does DORA require from financial organizations?

The answer to this subquestion was that financial organizations were required to implement robust ICT risk management, report ICT incidents, conduct regular resilience testing, manage third-party ICT risks, and share cyber threat information to enhance overall digital operational resilience.

In my opinion, the requirements set by the EC for financial organizations seemed fair, and I agreed with the EC that, given the increasing digitalization of Europe, a new regulation to enhance the digital operational resilience of European financial organizations was necessary. The reason the EC demanded significant investment from financial organizations was precisely this increasing digitalization and the complexities that come with it. Nevertheless, the European Commission should have focused more on identifying overlaps between various regulations, such as DORA, GDPR, and the AI Act, to streamline compliance efforts for financial organizations. Participant C9 (2024) mentioned that it was already possible to meet multiple regulatory requirements simultaneously, but during the interviews, it appeared to me that this was not yet being done actively. By promoting this approach more actively, the European Commission could have made compliance easier for financial organizations and helped them better understand the broader purpose of these regulations. Currently, some organizations were primarily aiming to "tick the box" for compliance rather than embracing the overarching goal of strengthening their digital operational resilience. This was recognized by the service providers during the interviews, with Participant C4 stating that financial organizations, even larger ones, felt overwhelmed by the influx of new regulations.

Fortunately, DORA includes a proportionality principle that offers smaller organizations some flexibility in terms of compliance. However, as noted by Participant L3 (2024), this proportionality can sometimes be unclear to service providers and should therefore be better explained, allowing smaller organizations to fully benefit from this principle.

In response to ter Haar's (2022) study, which questioned whether DORA was a friend or a foe, I assumed that financial organizations viewed DORA as an enemy due to the enormous workload it brought. With more regulatory harmonization, there is potential for these regulations to become, in ter Haar's words, a friend.

SQ2: How do service providers perceive readiness to provide services related to DORA?

The answer to this subquestion in overall, service providers perceived readiness as having multidisciplinary teams, knowledgeable consultants, effective tools, go-to-market strategies, and leveraging lessons from previous regulations.

The interviews revealed varied responses regarding what service providers needed to be ready for DORA. However, some common themes emerged concerning the essential elements of readiness. A key requirement identified was the importance of having multidisciplinary teams to ensure that service providers could address the full scope of DORA requirements for their clients. This seemed logical to me, as DORA encompasses a wide range of expertise areas. Most of the companies I spoke with had access to multidisciplinary teams, but some legal firms lacked in-house technical capabilities and, therefore, did not offer services related to the third pillar of DORA, which involves digital operational resilience testing. Participant L1 (2024) even stated that, as a law firm, it was not realistic to cover the entire DORA spectrum, which I fully agree with. I think it is better for service providers to recognize their limitations rather than offering low-quality services to financial organizations.

Another expected requirement was that service providers needed consultants who thoroughly understood DORA and related regulations. Although this might seem obvious and not worth mentioning, it was one of the most frequently cited requirements for being prepared to help financial organizations comply with DORA. Additionally, using the right tools was highlighted as crucial for maximizing effectiveness and efficiency in delivering DORA services. For instance, Participant C6 mentioned using GenAI to cross-check policies against DORA legislation, which provided significant added value. The integration of (Gen)AI into the digital regulations landscape had been anticipated by Butler and O'Brien (2019), who recognized the potential of RegTech at that time. In terms of automation and efficiency, it was encouraging to see that many service providers were already embracing these tools to the fullest, and I am a strong advocate for using technologies to improve both quality and efficiency.

Christensen et al. (2016) emphasized the importance of understanding the "jobs to be done" for financial organizations, a concept that closely aligned with the interview findings on the necessity of a go-to-market strategy. This strategy was frequently highlighted as crucial during the interviews, underscoring its role in effectively addressing client needs. Additionally, gaining access to decision-makers within financial organizations was identified as a critical factor. Without such access, even the most well-crafted strategies would likely fail to achieve their intended impact.

While the service providers appeared to know exactly what was needed to assist financial organizations with DORA compliance, an interesting discrepancy arose when discussing their own readiness. Some companies did not have specific processes in place to assess their own readiness. Several high-profile consulting and legal firms interviewed for this study did not have a structured process, instead relying on internal discussions and the expertise of individual partners. This highlighted the need for a DORA readiness checklist and demonstrated how it could be highly beneficial for service providers.

SQ3: What are the current offerings of service providers in assisting financial organizations with DORA compliance?

The answer to this subquestion is that service providers offered readiness assessments, gap analyses, third-party risk management, implementation support, legal advice, and validation of gap assessments.

Initially, DORA services offered by service providers were explored during the document analysis. On the websites of service providers, gap assessments and readiness checks were primarily identified. While these two services were important starting points for both service providers and financial organizations, the interviews revealed many other offerings that were deemed crucial for financial organizations. It remains unclear why service providers don’t market other services, such as third-party risk management, digital operational resilience testing, regulatory reporting support, and incident response. During the interviews, it was frequently emphasized that a gap assessment serves as the starting point on the path to DORA compliance. We could assume that, from the perspective of service providers, a gap assessment is the first step, which is why they only promote it on their websites. Later, during follow-up conversations, they outline a pathway that includes the remaining services. I think this approach is not very customer-friendly, as it obliges clients to start with a gap assessment, even if they have already made internal progress and need specific help with third-party risk management. In that case, a client would have to reach out to the service provider to inquire whether they offer that specific service related to DORA. This situation seems even stranger when considering that many service providers highlighted their ability to offer end-to-end DORA solutions during interviews.

Both the document analysis and interviews indicated that almost every service provider offered the same services. A logical follow-up question was how they attempted to differentiate themselves from other service providers. Interestingly, the answers were also almost identical; they claimed to have multidisciplinary teams with both technical and legal expertise. They also mentioned using technologies such as automation tools and AI and having extensive experience with clients in the financial industry. Although they believed they knew what made them stand out, it became clear that these selling points were not as unique as they thought. One could assume that service providers did not pay enough attention to their competitors and did not clearly understand what truly set them apart.

Legal firms faced challenges in offering end-to-end DORA services due to their lack of technical capabilities, which is understandable. I agree with them that their expertise in DORA lies in its legal interpretation, policy drafting, contract management, etc. This led some legal firms to focus on specific pillars within DORA rather than providing a complete service offering. One large international legal firm even admitted that they were unsure where their added value as a company lay.

Service providers recognized a high demand for their DORA services, indicating that they were increasingly being called upon to act as intermediaries, translating regulatory requirements into actionable steps aligned with their clients' unique operational contexts. This intermediary role, as suggested by Owen (2021), was critical in facilitating communication between regulators and financial organizations, helping ensure that the goal of financial organizations in being compliant with DORA was reached. At the same time, they also supported the underlying values of the regulation, enhancing the digital operational resilience of financial organizations throughout the EU.

SQ4: What are the factors that influence the decision of financial organizations to engage service providers for DORA compliance support?

The answer to this subquestion is that factors included a lack of internal resources, specialized knowledge, cost-effectiveness, service quality, timelines, and proven experience of the service providers.

The key factor identified was the lack of internal resources and expertise, which was a logical driver for seeking external support, particularly given DORA's specialized nature. Financial organizations felt overwhelmed by the influx of new regulations and struggled to allocate the necessary time and personnel to ensure DORA compliance. Additionally, since legal topics are generally not the core business of financial organizations, it made sense that their employees did not have the specialized knowledge required to handle the complexities of DORA compliance. Even when these organizations attempted to start a compliance program, the workload quickly became unmanageable after the initial steps, forcing them to seek external support from service providers, as mentioned by Participant C8. This aligns with findings from Owen (2021), who highlighted the intermediary role of service providers in bridging the gap between regulatory requirements and organizational capabilities.

It was surprising that even larger financial organizations faced resource constraints, suggesting that the challenge of DORA compliance was not limited to smaller entities. One would expect that larger financial organizations would have dedicated departments that deal with compliance to various regulations daily. This pointed to a broader issue within the sector, where the rapid influx of regulations overwhelmed even those organizations typically perceived as well-resourced, something the research done by Tsanakas (2023) also indicated.

Once a financial organization decided to seek help from service providers, the next question became which service provider to choose. During the study, the balance between cost and quality emerged as another critical factor. Some participants noted that financial organizations prioritized quality for assessments but leaned towards cost-effectiveness during the execution phase, indicating that it was not simply a matter of choosing between cost and quality but rather a decision dependent on various factors. However, other participants argued that cost often became the decisive factor due to budget constraints. This aligned with Owen's (2021) argument that service providers had to navigate a complex landscape where they acted as both compliance enablers and cost-effective solutions. However, given the high stakes of DORA compliance, it is surprising that cost sometimes outweighs quality. Non-compliance poses significant financial and reputational risks, making a focus on short-term savings over long-term quality seem short-sighted.

Timelines of service providers also influenced decisions. Financial organizations often faced tight regulatory deadlines, making the ability to operate quickly and efficiently a crucial consideration. Additionally, organizations frequently requested examples of similar DORA projects from service providers to ensure they possessed relevant expertise. The focus on timelines and experience was expected, given the rigid implementation dates for new regulations. This finding aligned with Christensen et al. (2016) on the importance of service providers understanding the "jobs to be done" for their clients, which required both speed and competence.

SQ5: What capabilities are essential for consultants to assist financial organizations in complying with DORA?

The answer to this subquestion is that the essential capabilities included sector-specific knowledge, technical skills such as IT risk management and cybersecurity, legal expertise like contract law, and general consulting skills.

The essential capabilities identified during the interviews were deemed essential for consultants when assisting financial organizations with DORA compliance. These capabilities ranged from having industry-specific knowledge and soft skills like communication and problem-solving, to having technical-, and legal expertise. Of course, not each consultants needs to have knowledge of all of these capabilities, but that is the reason why the multidisciplinary teams were so important.

Industry-specific knowledge and a strong understanding of the client were crucial for a holistic approach to regulatory compliance. Service providers needed to navigate the unique operational and strategic aspects of each client to develop effective compliance strategies. Owen (2021) also emphasized the importance of consultants acting as intermediaries, understanding both regulatory requirements and the business context.

Technical expertise, especially in cybersecurity and IT risk management, was another essential capability. Knowledge of areas like network security and penetration testing was necessary to meet DORA's technical requirements. This emphasis on technical skills made sense, given DORA's goal to enhance digital operational resilience in financial entities.

A more surprising finding was the lack of mandatory training programs or certifications for consultants working on DORA projects. While certifications like CISSP and CISM were seen as beneficial, they were not required. Most service providers relied on a 'learning while doing' approach, supplemented by internal knowledge-sharing sessions and mentoring from senior staff. However, this approach might be insufficient for a regulation as complex as DORA. Although experiential learning is valuable, a more formal training approach could lead to a better understanding of DORA's requirements. Given the potential consequences that financial organizations face in cases of non-compliance, it would be wise for service providers to invest in structured training programs and certifications, rather than just relying on the skills of their consultants and hoping for the best. A combination seems crucial: laying a foundation through training programs and certifications, then applying that knowledge in practice with the support of senior staff.

Legal knowledge was also highlighted as crucial. This included understanding IT outsourcing contracts, contract law, and the ability to translate DORA requirements into actionable steps. Given the regulation's strong legal component, this emphasis was expected. Service providers needed to bridge the gap between legal requirements and operational implementation, ensuring that contracts and governance structures aligned with DORA's mandates.

DORA's focus on regulating third-party risk and IT outsourcing made legal expertise particularly important, as managing third-party risk was often mentioned as one of the biggest challenges for financial organizations. Translating the regulation into an understandable framework was also seen as vital. These findings made it clear why consultants with strong legal knowledge were indispensable.

In addition to technical and legal expertise, soft skills such as analytical abilities, communication, and problem-solving were crucial. This made sense, as every consultant should possess these skills to support clients effectively.

SQ6: To what extent can the knowledge acquired by service providers in assisting financial organizations with other digital regulations be applied to adhere to DORA?

The answer to this subquestion is that knowledge from other regulations, like PRA SS2/21 and EBA outsourcing guidelines, was directly applicable, especially for managing third-party risks and ICT resilience.

The results of this study showed that service providers had a lot of experience from assisting financial organizations with various digital regulations, such as the GDPR and the EBA outsourcing guidelines. This experience gained while helping clients comply with these digital regulations could, to a certain extent, be leveraged to facilitate compliance with DORA.

Each of the regulations mentioned during the interviews shared elements with DORA, particularly in third-party risk management. This led me to think, why wouldn't all these regulatory bodies, such as the EBA and the EC, develop a single regulation on third-party risk management for all organizations across Europe? I realized that this would involve many complexities, but it could potentially be much easier for both the regulators and the (financial) organizations in the long term. Currently, financial organizations have to conduct a gap assessment for every new regulation to check if there are new requirements regarding third-party risk management—a rather cumbersome process if you ask me.

The GDPR, for example, had similarities with DORA, particularly in its gap analysis approach. This indicated that the gap analysis initially applied to the GDPR could serve as a useful blueprint for assessing DORA readiness. In terms of efficiency, it was good to see that service providers recognized the similarities between different regulations. By drawing on their experience with these regulations, they could build on existing processes rather than reinventing the wheel for DORA compliance. This transferability of knowledge allowed for a more efficient approach to achieving compliance, leveraging established best practices.

Another regulation frequently mentioned was the PRA SS2/21 from the UK, which was, according to interviewees, about 1.5 years ahead of DORA. It provided valuable lessons on detailed checklists, understanding regulatory expectations, and early engagement with regulators to define compliance criteria. One interviewee even said that PRA SS2/21 was like DORA but in the UK, as both focused on enhancing operational resilience in the financial sector. This suggested that many lessons learned from PRA SS2/21 could be applied to DORA, both in terms of challenges and successes. However, quite a few interviewees had never heard of PRA SS2/21 until I brought it up. To be honest, during the document analysis, where I conducted a comparative analysis of regulations, I did not find PRA SS2/21 either. Once it was pointed out to me during the interviews, I decided to include it in the document analysis. In my opinion, there was still significant room for improvement in terms of the lessons learned by service providers.

While the findings indicated that much of the knowledge acquired from other regulations could be applied to DORA, it was crucial to recognize the limitations of this transferability. Each regulation, including DORA, had unique elements and required a specific approach. For instance, DORA placed a strong emphasis on digital operational resilience, which went beyond traditional data protection and risk management. Over-relying on frameworks like the GDPR or ISO 27001 without tailoring them to DORA's unique focus could result in inadequate compliance.

There was a risk in assuming that what worked for the GDPR, the EBA guidelines, or ISO 27001 would automatically suffice for DORA. While transferable knowledge provided a strong foundation, each regulation had its own requirements and nuances. Over-relying on previous frameworks without adapting them to DORA's specific context could lead to compliance gaps. To avoid this, service providers had to tailor their existing knowledge to meet DORA's unique requirements, which I observed they were indeed doing.

SQ7: How would a practical checklist help service providers assess their readiness and identify the gaps look like?

For this research question, there is no box with a short summary to the answer, because the answers to this question is the checklist itself. The development of this checklist, which aimed for service providers to assess their readiness for offering DORA services, emerged as an outcome of almost everything done during this study, such as the document analysis, the interviews, end eventually the finetuning during the validation interviews. This checklist addresses a gap identified during the interviews, namely that many service providers, even the larger ones, with a lot of experience in regulatory compliance, did not have a structured approach to assess their own readiness.

The checklist serves to standardize this process, offering a set of criteria that ensures all, according to this study, critical aspects of DORA are considered. You could say that the checklist is also, in an indirect way, beneficial for financial organizations, because if service providers enhance their ability to support them, they will profit of service with higher quality. After the first draft of the checklist was made, it was finetuned during three separate validation interviews. After each interview, the suggestions were implemented to the checklist, and each time, it became it little better, more complete, and better structured. In the end, I think the checklist can be considered as quite complete because during the last validation interview, almost no revisions were made.

Limitations

Like any other study, this study had several limitations that should be acknowledged:

1. Limited to a Dutch perspective. This study solely focused on Dutch service providers or the Dutch branches of international firms. This limited scope may not have fully captured the broader European perspective on DORA readiness. While DORA’s requirements are uniform across Europe, the interpretation and implementation of these requirements might differ among service providers in different countries. Including service providers from other EU countries could have offered interesting insights and provided a better understanding of DORA readiness across Europe.

2. Limited sample size. The study examined a relatively small group of experts, chosen through the researcher's network rather than through a random sampling method. This approach may have introduced selection bias and limited the diversity of perspectives. Future research could benefit from expanding the sample size and using a more randomized selection process to gather a broader range of expert insights.

3. Lack of insights from financial organizations. This study engaged solely with service providers and did not include any insights from financial organizations. Including their perspectives, challenges, and needs would have added another interesting and important angle to the study. It could have helped validate the needs identified by service providers, ensuring a more comprehensive understanding of DORA compliance landscape.

4. Conducted before DORA compliance deadline. This study was conducted before DORA compliance deadline of January 17, 2025, and therefore only addressed the preparatory phase.

Studies conducted after the compliance deadline will be essential to evaluate the effectiveness of DORA services offered by service providers and to identify any evolving challenges faced by financial organizations.

5. Need for further validation of DORA readiness checklist. The applicability and effectiveness of DORA readiness checklist require further validation across a broader range of service providers and financial organizations. During this study, the checklist was validated with three different DORA experts through open interviews. It would be useful to validate this checklist with more experts and evaluate its effectiveness with different service providers.

7. Conclusion

In the seventh and final chapter of this study, the research question is revisited. Section 7.1 presents recommendations for future research.

This study aimed to understand to what extent service providers are ready in supporting financial organizations to comply with DORA. Given the growing reliance on digital infrastructure and the increasing threats to critical systems, particularly within the financial sector, DORA represents a crucial regulatory framework to enhance digital operational resilience. The research aimed to provide insights into how prepared service providers are to assist financial organizations in meeting DORA's requirements, especially given the impending compliance deadline of January 17, 2025.

Through a combination of document analysis and expert interviews, the study revealed several key findings. First, it became evident that service providers recognize the importance of a multidisciplinary approach in offering DORA services. Expertise in areas such as third-party risk management, cybersecurity, legal, and operational resilience emerged as crucial components of an effective DORA service proposition. The gap analysis and readiness assessments offered by these firms were identified as essential services that help financial organizations understand their current state of compliance and the steps required to meet DORA's stringent requirements.

The study also highlighted the factors influencing financial organizations to engage with service providers for DORA compliance support. A lack of internal resources and expertise within financial organizations was the biggest driver for them, along with the complex and intensive nature of DORA's regulatory requirements. Cost-effectiveness and quality of service were found to be primary considerations for financial organizations when selecting a service provider, emphasizing the need for a balanced and value-driven approach by service providers.

A key contribution of this research is the development of a checklist designed to evaluate the readiness of service providers in delivering DORA-related services. The checklist offers a structured approach, emphasizing critical phases such as service proposition development, client engagement, and gap assessment. This tool aims to help service providers establish a complete and effective DORA service offering, ensuring they can meet the needs of financial organizations towards their goal to DORA compliancy.

While this research provides valuable insights into the readiness of Dutch service providers, it also acknowledges certain limitations. The focus on Dutch service providers may limit the generalizability of the findings across the broader European context. Additionally, the study's timing, conducted before DORA compliance deadline, means that it addresses the preparation phase rather than the post-implementation outcomes. Future research could expand on this work by including the perspectives of financial organizations and by evaluating the actual effectiveness of service provider support after the compliance deadline.

In conclusion, this study sheds light on the readiness of service providers to assist financial organizations in navigating DORA landscape. By offering an analysis and a practical checklist, the study contributes to a deeper understanding of the challenges and capabilities required for successful DORA compliance. As the financial sector continues to evolve and face new digital threats, the role of service providers will remain pivotal in ensuring operational resilience and regulatory adherence.

Recommendations for future work

In terms of future work, there are several directions into which the research could be extended:

1. Expand to an international scope. A study with a broader international focus could offer valuable additional insights. This study was limited to Dutch service providers and the Dutch branches of international firms. Future research could expand the scope by including service providers from other European countries. This would help determine whether the findings of this study are consistent across different countries and, in addition, assess whether the checklist developed in this study is applicable to more European service providers.

2. Focus on the perspectives of financial organizations. Another insightful study would be to focus on the perspectives of financial organizations themselves to understand their specific challenges, needs, and expectations regarding DORA compliance support. This would help validate whether the perceived challenges, needs, and expectations identified by service providers align with the actual experiences of financial organizations, ensuring a better understanding of DORA compliance landscape.

3. Assess the long-term effectiveness of the current DORA service offerings. Another important area of study would be to evaluate how financial organizations maintain DORA compliance over time and how service providers continue to offer support beyond the initial compliance deadline. While this study focused on preparing organizations for the initial deadline, future research could evaluate the effectiveness of current DORA service offerings and identify the challenges that organizations face in maintaining their operational resilience.

Scientific references

- Alharahsheh, H. H., & Pius, A. (2020). A review of key paradigms: Positivism VS interpretivism. Global Academic Journal of Humanities and Social Sciences, 2(3), 39-43.
- Alturki, R. (2021). Study onion for smart IoT-enabled mobile applications. Scientific programming, 2021, 1-9.
- Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. Journal of Economics and Business, 100, 7-25.
- Axon, L., Alahmadi, B., Nurse, J. R. C., Goldsmith, M., & Creese, S. (2018). Sonification in security operations centres: What do security practitioners think? Proceedings of the Workshop on Usable Security (USEC), Network and Distributed System Security (NDSS) Symposium, 1–12. Retrieved from https://www.cs.ox.ac.uk/files/9802/2018-USEC-NDSS-aangc-preprint.pdf
- Braun, V., & Clarke, V. (2012). Thematic analysis. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological (pp. 57–71). American Psychological Association. https://doi.org/10.1037/13620-004
- Butler, T., & O’Brien, L. (2019). Understanding RegTech for digital regulatory compliance. Disrupting finance: FinTech and strategy in the 21st century, 85-102.
- Buttigieg, C. P., & Zimmermann, B. B. (2024, June). The digital operational resilience act: challenges and some reflections on the adequacy of Europe’s architecture for financial supervision. In ERA Forum (pp. 1-18). Berlin/Heidelberg: Springer Berlin Heidelberg.
- Christensen, C. M., Hall, T., Dillon, K., & Duncan, D. S. (2016). Know your customers’ jobs to be done. Harvard Business Review, 94(9), 54–62.
- Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). International Cybersecurity Law Review, 4(1), 79-90.
- D. Botta, R. Werlinger, A. Gagn´e, K. Beznosov, L. Iverson, S. Fels, and B. Fisher. Towards understanding it security professionals and their tools. In Proceedings of the 3rd symposium on Usable privacy and security, pages 100–111. ACM, 2007.
- De Souza, C. R., Pinhanez, C. S., & Cavalcante, V. F. (2011, December). Information needs of system administrators in information technology service factories. In Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology (pp. 1-10).
- Downes, L., & Nunes, P. (2013). Big bang disruption. Harvard business review, 44-56.
- Duggan, D. (2024). The impact of the Digital Operational Resilience Act on financial market infrastructures in Europe. Journal of Securities Operations & Custody, 16(4), 344-350.

- Eichengreen, B., & Uzan, M. (1992). The Marshall Plan: economic effects and implications for Eastern Europe and the former USSR. Economic Policy, 7(14), 13-75.
- Foa, D., & Davola, A. (2024). Assessing the authorization regime under PSD2: do (different) supervisory practices prevent the achievement of a level playing field in the EU? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4726086
- Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. Technovation, 102, 102217.
- Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with Cyber security frameworks and standards. International Cyber security Law Review, 1-42.
- Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial organizations. Procedia Computer Science, 219, 84-90.
- Guo, J., Pan, J., Guo, J., Gu, F., & Kuusisto, J. (2019). Measurement framework for assessing disruptive innovations. Technological Forecasting and Social Change, 139, 250-265.
- Heino, O., Takala, A., Jukarainen, P., Kalalahti, J., Kekki, T., & Verho, P. (2019). Critical infrastructures: The operational environment in cases of severe disruption. Sustainability, 11(3), 838.
- Kourmpetis, S. (2022). Management of ICT Third Party Risk Under the Digital Operational Resilience Act. In Digitalization, Sustainability, and the Banking and Capital Markets Union: Thoughts on Current Issues of EU Financial Regulation (pp. 211-226). Cham: Springer International Publishing.
- Krüger, P. S., & Brauchle, J. P. (2021). The European Union, cybersecurity, and the financial sector: A primer. Carnegie Endowment Int. Peace Publications Dept., Washington, DC, USA.
- Kun, E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. Computer Law & Security Review, 52, 105931.
- Kushner, D. (2013). The real story of stuxnet. ieee Spectrum, 50(3), 48-53.
- Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber Security: Critical Infrastructure Protection (pp. 3-42). Cham: Springer International Publishing.
- Lincoln, Y., & Guba, E. G. (1985). Lincoln, Yvonna, and Egon G. Guba, Naturalistic Inquiry. Beverly Hills, CA: Sage, 1985.
- Mavlutova, I., Spilbergs, A., Verdenhofs, A., Natrins, A., Arefjevs, I., & Volkova, T. (2022). Digital transformation as a driver of the financial sector sustainable development: An impact on financial inclusion and operational efficiency. Sustainability, 15(1), 207.

- Neumannová, A., Bernroider, E. W., & Elshuber, C. (2022, December). The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Regulations analysis. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 570-585). Cham: Springer Nature Switzerland.
- Ngulube, P. (2022). Using simple and complex mixed methods research designs to understand research in information science. In Handbook of research on mixed methods research in information science (pp. 20-46). IGI Global.
- Ni Thuama, R., & Costigan, S. S. (2023). DORA - Understanding the new regulatory framework on digital operational resilience. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4549564
- Owen, D. (2021). Private facilitators of public regulation: A study of the environmental consulting industry. Regulation & Governance, 15(1), 226-242.
- Robert A. Bridges, Michael D. Iannacone, John R. Goodall, and Justin M. Beaver. 2018. How do information security workers use host data? A summary of interviews with security analysts. Retrieved from http://arxiv.org/abs/1812.02867.
- Saunders, M., Lewis, P. & Thornhill, A. (2012). Research Methods for Business Students. 6th edition, Pearson Education Limited.
- Scott, H. S. (2021). The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3904113
- Størkersen, K., Hayes, J., Standal, M. I., Ognedal, M., & Skogstad, M. R. (2023). We're in the middle of it: Consultants' role in risk management in the Norwegian petroleum sector. Safety Science, 167, 106258.
- Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and trends of financial technology (Fintech): a systematic regulations analysis. Information, 11(12), 590.
- ter Haar, J. (2022). 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.
- Vandezande, N. (2024). Cyber security in the EU: How the NIS2-directive stacks up against its predecessor. Computer Law & Security Review, 52, 105890.
- Waizel, G. (2023). The potential effects of recent EU Cyber security and resilience regulations on cloud adoption and EU cyber resilience. Centre for European Studies (CES) Working Papers, 15(3).
- Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. International management review, 15(1), 45-55.

Non-scientific references

- Allianz. (2016, June). Cyber attacks on critical infrastructure. Allianz Commercial. Retrieved January 19, 2024, from https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html
- Avenga. (n.d.). Digital Operational Resilience Act (DORA) Compliance Ensured – Avenga. Retrieved March 26, 2024, from https://www.avenga.com/dora-readiness-assessment/
- Banco de España. (n.d.). The introduction of the euro. Banco De España. Retrieved February 14, 2024, from https://www.bde.es/wbe/en/sobre-banco/actividad-europea/eurosistema-sebc/historia-eurosistema/euro/introduccion-euro/
- Bank of England. (2024, July 15). Results of the firm feedback survey 2023. Retrieved July 21, 2024, from https://www.bankofengland.co.uk/prudential-regulation/publication/2024/july/results-of-the-firm-feedback-survey-2023
- Basel Committee on Banking Supervision. (2014). Sound management of risks related to money laundering and financing of terrorism. Retrieved October 8, 2024, from https://www.bis.org/bcbs/publ/d353.pdf
- Bhattacharyya, D., Dietz, M., Edlich, A., Höll, R., Mehta, A., Weintraub, B., & Windhagen, E. (2023). Global Banking Annual Review 2023: The Great Banking Transition. In McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review
- Bird & Bird. (2021). The European Banking Authority’s Guidelines on Outsourcing - as transposed by national competent authorities across the EU Member States. In Bird & Bird. Retrieved July 2, 2024, from https://www.twobirds.com/-/media/pdfs/news/articles/2021/global/bird--bird-pan-european-outsourcing-guide_june-2021.pdf
- Capgemini. (2024, March 14). Digital Operational Resilience Act (DORA) - Capgemini. Retrieved March 26, 2024, from https://www.capgemini.com/solutions/digital-operational-resilience-act-dora/
- Clarke, B. (2023, September 6). Exploring DORA: What is the new EU legislation and who will it impact? Panaseer. https://panaseer.com/business-blog/exploring-dora-new-eu-legislation/#does-dora-apply-outside-of-the-eu
- CVCE. (n.d.). The provisions of the Single European Act - Historical events in the European integration process (1945–2009). CVCE.eu. Retrieved February 14, 2024, from https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/23bbb26c-a69c-40f1-954c-6b3cb1392b4d

- Cybersecurity Ventures. (2023). 2023 Official Cybercrime Report. eSentire. Retrieved January 22, 2024, from https://www.esentire.com/resources/library/2023-official-cybercrime-report
- De Nederlandsche Bank. (2023, October 31). DORA; tijd om uit de startblokken te komen. Retrieved January 22, 2024, from https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2023/dora-tijd-om-uit-de-startblokken-te-komen/
- Dekra. (2023, July 26). An insight overview of the NIS2 Directive. Retrieved February 26, 2024, from https://www.dekra.com/en/nis2-directive-overview/
- Deloitte. (n.d.-a). Mastering DORA: navigating regulations with 3rdRisk. Deloitte Netherlands. Retrieved March 26, 2024, from https://www2.deloitte.com/nl/nl/pages/risk/articles/mastering-dora-navigating-regulations-with-3rdRisk.html
- Deloitte. (n.d.-b). The Digital Operational Resilience Act (DORA) is here. Deloitte Belgium. Retrieved January 22, 2024, from https://www2.deloitte.com/be/en/pages/risk/articles/the-digital-operational-resilience-act-is-here.html
- Deloitte. (2019). EBA Guidelines on outsourcing arrangements. In EBA Guidelines on Outsourcing Arrangements (pp. 00–05). Retrieved July 2, 2024, from https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_EBA%20outsourcing%20guidelines.pdf
- DORA. (n.d.). Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554. Digital Operational Resilience Act (DORA). Retrieved January 22, 2024, from https://www.digital-operational-resilience-act.com/
- Eckhard, B. (2023, July 17). Revision of Directive (EU) 2015/2366 on Payment Services. Policy Commons. https://policycommons.net/artifacts/4511435/revision-of-directive-eu-20152366-on-payment-services/5321153/
- Edmond Alphandéry. (2021, May 14). The Euro Crisis. Foundation Robert Schuman. Retrieved February 15, 2024, from https://www.robert-schuman.eu/en/european-issues/240-the-euro-crisis
- Eiopa. (2023). DIGITAL OPERATIONAL RESILIENCE ACT (DORA) - REPORTING OF REGISTER OF INFORMATION, OF MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS - UPDATE. https://www.eiopa.europa.eu/document/download/2888a8e8-4a20-4e27-ad51-7ad4e5b511f7_en?filename=5_2023-10-10_EIOPA%20Reporting%20event.pdf
- EUR-Lex. (2007, November 13). Directive - 2007/64 - EN - EUR-Lex. Retrieved March 14, 2024, from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32007L0064
- EUR-Lex. (2015, November 25). Directive - 2015/2366 - EN - Payment Services Directive - EUR-Lex. Retrieved March 14, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

- EUR-Lex. (2018, March 21). Treaty of Maastricht on European Union | EUR-Lex. Retrieved February 14, 2024, from https://eur-lex.europa.eu/EN/legal-content/summary/treaty-of-maastricht-on-european-union.html
- European Banking Authority. (2019). Guidelines on outsourcing | European Banking Authority. Retrieved July 2, 2024, from https://www.eba.europa.eu/guidelines-outsourcing#:~:text=The%20Guidelines%20aim%20at%20promoting,in%20the%20field%20of%20outsourcing.
- European Banking Authority. (2024). The Single Rulebook | European Banking Authority. Retrieved April 18, 2024, from https://www.eba.europa.eu/single-rulebook
- European Central Bank. (n.d.). European System of Financial Supervision. European Central Bank - Banking Supervision. Retrieved February 20, 2024, from https://www.bankingsupervision.europa.eu/about/esfs/html/index.en.html
- European Central Bank. (2020, March). Implications of Brexit for the EU financial landscape. https://www.ecb.europa.eu/pub/fie/article/html/ecb.fieart202003_01~690a86d168.en.html
- European Commission. (n.d.). Glossary:European Monetary System (EMS) - Statistics Explained. Eurostat. Retrieved February 14, 2024, from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:European_Monetary_System_(EMS)
- European Commission. (2020a, September 24). Digital Finance Package. Retrieved January 29, 2024, from https://finance.ec.europa.eu/publications/digital-finance-package_en
- European Commission. (2020b, September 24). Digital Finance Package. European Commission - European Commission. Retrieved February 20, 2024, from https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684
- European Commission. (2020c, September 24). 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. Retrieved January 22, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN
- European Council. (2022, November 28). Digital finance: Council adopts Digital Operational Resilience Act. Retrieved January 25, 2024, from https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/
- European Council. (2023, October 27). How Maastricht changed Europe. https://www.consilium.europa.eu/en/maastricht-treaty/
- European Parliament. (2017, April 28). REPORT on FinTech: the influence of technology on the future of the financial sector | A8-0176/2017 | European Parliament. © European Union, 2017 -

Source: European Parliament. Retrieved January 20, 2024, from https://www.europarl.europa.eu/doceo/document/A-8-2017-0176_EN.html

- European Systemic Risk Board. (2020, February). Systemic cyber risk. European Systemic Risk Board. Retrieved January 20, 2024, from https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf
- European Union. (n.d.). History of the European Union – 1990-99 | European Union. Retrieved February 14, 2024, from https://european-union.europa.eu/principles-countries-history/history-eu/1990-99_en
- EY. (2023, March 15). How will DORA impact the financial sector? EY Luxembourg. Retrieved March 26, 2024, from https://www.ey.com/en_lu/wealth-asset-management/luxembourg-market-pulse/how-will-dora-impact-the-financial-sector-
- Gusiv, P. (2023). Development of a compliance gap analysis method for the Digital Operational Resilience Act (DORA). In Deloitte Oy, Knowledge Management Expertise [Thesis]. https://www.theseus.fi/bitstream/handle/10024/805417/Gusiv_Pavel.pdf?sequence=2&isAllowed=y
- Hildner, A., Ehlen, T., Utzerath, J., & Heinz, J. (2022, November 22). DORA: a cornerstone of the EU regulatory framework close to final. Lexology. https://www.lexology.com/library/detail.aspx?g=81e43410-a33e-4b9c-83fb-5b9240b70d73
- International Monetary Fund. (n.d.). Money Matters, an IMF Exhibit -- The Importance of Global Cooperation, Destruction and Reconstruction (1945-1958), Part 1 of 6. Retrieved February 14, 2024, from https://www.imf.org/external/np/exr/center/mm/eng/mm_dr_01.htm
- ISO. (2022). ISO/IEC 27001:2022. Retrieved October 8, 2024, from https://www.iso.org/standard/27001
- Karakasilioti, G. M. P. (2024). Supporting the digital operational resilience of the financial sector: the EU’s DORA Digital Operational Resilience Act. In S. Gritzalis, MSc Dissertation. https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/16273/DORA%20-%20MTE2109%20Karakasilioti.pdf?sequence=1&isAllowed=y
- KPMG. (n.d.). Cyber security for the financial sector. Retrieved January 22, 2024, from https://kpmg.com/de/en/home/services/industries-and-markets/financial-services/it-security.html
- Lukács, K., & Matek, K. (2023, April 17). Digital Operational Resilience Act. KPMG. Retrieved February 18, 2024, from https://kpmg.com/hu/en/home/insights/2023/04/digital-operational-resilience-act.html

- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. In NIST CSWP 29 [Report]. Retrieved October 8, 2024, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- NautaDutilh. (2023, December 8). Comparison - ESMA outsourcing guidelines, EBA outsourcing guidelines & DORA. Retrieved July 2, 2024, from https://www.nautadutilh.com/en/insights/comparison-esma-outsourcing-guidelines-eba-outsourcing-guidelines-dora/
- Palais, S. (2023, June 20). NIS2 vs DORA: what differences and which legislation prevails? Yogosha. Retrieved March 13, 2024, from https://yogosha.com/blog/nis2-vs-dora/
- Pinsent Masons. (2024, June 13). EBA outsourcing guidelines under DORA review. Retrieved July 2, 2024, from https://www.pinsentmasons.com/out-law/news/eba-outsourcing-guidelines-under-dora-review
- PwC. (n.d.-a). Digital Operational Resilience Act (DORA). Retrieved March 26, 2024, from https://www.pwc.nl/en/industries/financiele-sector/risk-and-regulation/digital-operational-resilience-act.html
- PwC. (n.d.-b). Introducing the Digital Operational Resilience Act. Retrieved January 22, 2024, from https://www.pwc.com/mt/en/publications/technology/dora.html
- Rohner, N. (2023, February 14). Russian Hacktivist Group KillNet Hits U.S. Hospitals with DDoS Attacks. BlackBerry. Retrieved January 20, 2024, from https://blogs.blackberry.com/en/2023/02/killnet-hits-us-hospitals-with-ddos-attacks
- Saldaña, J. (2013). The Coding Manual for Qualitative Researchers (Second Edition). SAGE Publications. https://emotrab.ufba.br/wp-content/uploads/2020/09/Saldana-2013-TheCodingManualforQualitativeResearchers.pdf
- Scheelen, Y., Machilsen, K., & Deprez, A. (2023, May 16). How to prepare for the NIS2 Directive? https://www.ey.com/en_be/cybersecurity/how-to-prepare-for-the-nis2-directive
- Secura. (n.d.). DORA Services - Gap Analysis, Training & Implementation | Secura Cybersecurity. Retrieved January 22, 2024, from https://www.secura.com/services/integrated-approach/dora
- Secura. (2023). A summary of the new DORA regulation | 9 Questions & Answers. Retrieved January 22, 2024, from https://www.secura.com/dora-summary-regulation
- Trend Micro. (2017, December 22). TRITON Wielding Its Trident – New Malware Tampering with Industrial Safety Systems - Wiadomości bezpieczeństwa. Retrieved January 19, 2024, from https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems
- Trend Micro. (2019, April 11). New Critical Infrastructure Facility Hit by Group Behind TRITON - Wiadomości bezpieczeństwa. Retrieved January 19, 2024, from

https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton

- Tsanakas, E. (2023). Open Banking: Application difficulties & API security, under PSD2 [Thesis, Luleå University of Technology]. In Department of Computer Science, Electrical and Space Engineering. https://www.diva-portal.org/smash/get/diva2:1793048/FULLTEXT01.pdf
- Tweede Kamer. (2024, January 31). Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie. Tweede Kamer Der Staten-Generaal. Retrieved March 13, 2024, from https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2024Z01452&did=2024D03298
- UCP Knowledge Network. (2023, August 20). Disruption to Critical Infrastructure. Retrieved January 19, 2024, from https://civil-protection-knowledge-network.europa.eu/eu-overview-risks/human-induced-risks/disruption-critical-infrastructure
- usd AG. (2023, September 15). NIS-2 and DORA: Why Two Pieces of EU Cybersecurity Legislation? | more security. usd AG. More Security. Usd AG. Retrieved March 13, 2024, from https://www.usd.de/en/nis-2-and-dora-why-two-pieces-of-eu-legislation/

Appendix

Appendix I: Interview protocol

English

Name of interviewer: N. Kos
Interviewee:
Date:
Location:

Introduction:
In the context of privacy, I want to ask you how I can place you in this study.

- Can I put your position and company in the study?
- Are you OK with me including the results of this interview in my study?

Introduction about the study and the purpose of the study

Start recording

Introduction of the interviewee:

- Could you introduce yourself?
- How much experience do you have with digital regulation and with DORA in particular?
- Can you describe your current role and responsibilities?

Q1: How do you define readiness when it comes to providing services related to digital regulations like DORA?
Answer:

Q2: What criteria your organization use to assess its readiness to offer services for a new regulation like DORA?
Answer:

Q3: How does your organization differentiate the services for DORA from other service providers?
Answer:

Q4: Which service that your organization offers do you consider the most important for financial organizations?
Answer:

Q5: What service is most frequently requested by financial organizations?
Answer:

Q6: What are the main reasons why financial organizations opt to use service providers instead of addressing regulations like DORA internally?
Answer:

Q7: In your experience, do financial organizations prioritize cost-effectiveness or quality of service when choosing a service provider for (DORA) compliance support?
Answer:

Q8: Are there any other concerns or requirements that financial organizations have when considering potential service providers for the (DORA) compliance support?
Answer:

Q9: What specific expertise or knowledge areas do you believe consultants must possess to assist financial organizations with DORA compliance?
Answer:

Q10: Are there any specific certifications or training programs your organization considers important for DORA readiness?
Answer:

Q11: Can you discuss any specific capabilities or skill sets that were beneficial in the past when supporting financial organizations with DORA compliance?
Answer:

Q12a: Which specific regulations (NIS2 for example) have provided the most valuable lessons that could be applicable to assisting with DORA compliance?
Answer:

Q12b: What knowledge and lessons learned are specifically applicable?
Answer:

Provide some context about the checklist that will be drafted so that the next question can be answered more easily

Q13: Can you describe the components or criteria that you believe should be included in a checklist for assessing readiness for DORA compliance support?
Answer:

Q14: Are there any additional insights or perspectives you believe are important to this research that we have not covered yet?
Answer:

Dutch

Interviewer: N. Kos
Geïnterviewde:
Datum:
Locatie:

Introductie:
In het kader van privacy wil ik u vragen hoe ik u in dit onderzoek kan plaatsen.

- Mag ik uw functie en bedrijf in het onderzoek vermelden?
- Vind je het goed als ik de resultaten van dit interview opneem in mijn onderzoek?

Introductie over de scriptie en het doel van het onderzoek

Opname starten

Introductie van de geïnterviewde:

- Kunt u zichzelf voorstellen?
- Hoeveel ervaring heeft u met digitale regelgeving en met DORA in het bijzonder?
- Kunt u uw huidige rol en verantwoordelijkheden beschrijven?

Vraag 1: Hoe zou u 'readiness' omschrijven als het gaat om het leveren van diensten met betrekking tot digitale regelgeving zoals de DORA?
Antwoord:

Vraag 2: Zijn er specifieke criteria, of tools, welke uw organisatie gebruikt om haar 'readiness' voor een nieuwe regelgeving zoals de DORA te beoordelen?
Antwoord:

Vraag 3: Hoe probeert uw organisatie zich te onderscheiden van andere DORA-dienstverleners?
Antwoord:

Vraag 4: Welke dienst die uw organisatie aanbiedt, beschouwt u als de belangrijkste voor financiële organisaties?
Antwoord:

Vraag 5: Welke dienst wordt het vaakst aangevraagd door financiële organisaties?
Antwoord:

Vraag 6: Wat zijn de belangrijkste redenen waarom financiële organisaties kiezen voor dienstverleners in plaats van regelgeving zoals DORA intern aan te pakken?
Antwoord:

Vraag 7: Vinden financiële organisaties, naar uw ervaring, de kosten of de kwaliteit van dienstverlening belangrijker bij het kiezen van een dienstverlener voor ondersteuning bij de naleving van (de DORA)?
Antwoord:

Vraag 8: Zijn er nog andere specifieke zaken of vereisten waar financiële organisaties rekening mee houden bij het overwegen van dienstverleners voor ondersteuning bij de naleving van de DORA?
Antwoord:

Vraag 9: Welke specifieke expertise of kennisgebieden moeten volgens u dienstverleners bezitten om financiële organisaties te kunnen helpen bij de naleving van DORA?
Antwoord:

Vraag 10: Zijn er certificeringen of trainingsprogramma's die uw organisatie belangrijk vindt om klaar te zijn voor DORA?
Antwoord:

Vraag 11: Kunt u specifieke vaardigheden bespreken die in het verleden nuttig zijn geweest bij het ondersteunen van financiële organisaties bij de naleving van DORA?
Antwoord:

Vraag 12a: Welke specifieke regelgeving (bijvoorbeeld NIS2) heeft de meest waardevolle lessen opgeleverd die van toepassing kunnen zijn op het helpen bij de naleving van de DORA?
Antwoord:

Vraag 12b: Welke kennis en geleerde lessen zijn specifiek van toepassing?
Antwoord:

Geef wat achtergrondinformatie over de checklist die wordt opgesteld, zodat de volgende vraag makkelijker te beantwoorden is

Vraag 13: Kunt u de componenten of criteria beschrijven die volgens u moeten worden opgenomen in een checklist voor het beoordelen van de organisatie’s readiness voor DORA-assistentie?
Antwoord:

Vraag 14: Zijn er nog andere inzichten of perspectieven die u belangrijk acht voor dit onderzoek die we nog niet hebben behandeld?
Antwoord:

Appendix II: Codebook

Code	Gr	Co
Definition of service readiness		
DORA readiness definition	15	13
Consultant readiness		
Internal training programs	13	7
Mentoring by experienced colleagues	6	4
Learning while doing	2	2
No mandatory trainings and certifications	16	12
IT/Cloud training	1	1
External trainings programs	5	5
No readiness criteria	1	1
Most Demanded DORA Services		
Third party risk management	10	6
Disaster recovery	1	1
Gap analysis	7	7
The need of benchmarking	4	3
Validation by third party	7	6
Program management	2	2
Policy drafting	2	2
Boardroom training	3	
Implement DORA requirements	4	3
Supplier register and contract drafting	7	5
Financial Organizations' Needs		
Lack of knowledge	12	10
Lack of resources	12	10

Code	Gr	Co
Lessons learned		
Example of lessons learned from NIS2	1	1
Examples of the lessons learned from the DNB good practice	1	1
Examples of the lessons learned from the PRA SS2-21	1	1
Examples of the lessons learned of GDPR	1	1
Facilitating discussions between different organizational levels	2	2
Lessons learned from AVG	1	1
Lessons learned of DNB Good Practice	2	1
Lessons learned of Double Diamond Innovation Model	1	1
Lessons learned of EBA Outsourcing Guidelines	4	4
Lessons learned of EIOPA	2	
Lessons learned of ESMA	1	1
Lessons learned of Expectations for Banks of the EU Single Resolution Board	1	1
Lessons learned of GDPR	4	4
Lessons learned of GRC Practices	2	2
Lessons learned of ISO27001	4	3
Lessons learned of KRITIS	1	1
Lessons learned of MiCA	2	2
Lessons learned of NIS2	3	3
Lessons learned of NIST Cybersecurity Framework	1	1
Lessons learned of Pensions act	1	1
Lessons learned of PRA SS2/21	4	3
Readiness criteria		
Bring lessons learned from other regulations to DORA	4	4
Employee training	1	1
Experience in the relevant industry or sector	1	1
Experience with proven services	2	2

Important factors for clients		
Importance of offering end-to-end solutions	5	
Importance of costs	7	6
Varying importance of cost and quality	5	5
Importance of quality	7	
Existing relationship with client is valued	5	5
Use-cases	2	2
Importance of timelines	5	
The extent the service provider uses technologies	1	1
References	3	
Experience with similar projects	1	1
Importance of international/local knowledge	7	6
Consultant requirements		
Analytical skills	4	4
Being a problem solver	1	1
Communication skills	2	2
Knowledge of (operational) resilience	8	5
Knowledge of cybersecurity	5	5
Knowledge of IT in general	5	4
Knowledge of IT risk management	8	7
Knowledge of supply chain management	1	1

External audits of DORA-proposition	1	1
Internal audits of DORA-proposition	2	2
New services should go through a testing phase	1	1
Peer reviews	2	2
Quality of service	1	1
Service providers must be able to make agreements with third-party service providers	1	1
Statements		
An assessment tool to evaluate the client	1	1
Becoming a business partner rather than just a service provider	1	1
Difficulties to pinpoint the most important service	1	1
DNB has indicated that it will be strictly enforced as of Jan. 17, 2025	1	1
DORA is an integral process	1	1
DORA more stringent than previous regulations	1	1
DORA remains unclear in terms of proportionality	1	1
Drafting contracts is the entry service for legal firms	1	1
Financial organizations value predictability of costs and quality of service	1	1
For larger financial organizations already under DNB supervision, the focus is on fine-tuning compliance	1	1
Gap analysis as entry to client	1	1
Helping service providers beyond implementation date	1	1
Implementing DORA can also be interesting for upcoming regulations	1	1
Legal firms unsure where their added value lays	1	1

Readiness criteria		
Access to decision-makers	2	2
Bring lessons learned from other regulations to DORA	7	4
Collaborate with external parties	5	4
Experience in the relevant industry or sector	17	10
Experience with proven services	2	2
Having a go-to-market strategy	6	5
Having a set of tools	12	8
Having domain-specific knowledge	3	2
Having governance knowledge	12	7
Having knowledgeable consultants	9	9
Having legal knowledge	23	13
Having technical knowledge	19	10
Importance of service scoping	2	2
Internal audits of the DORA-proposition	2	2
Knowledge sharing	2	2
Multi-disciplinary teams	13	9
New services should go through a testing phase	1	1
Peer reviews	3	3
Service providers must be able to make agreements with third-party service providers	2	1
Most important service depends on the phase the client is in	1	1
Not thought of how to differentiate	1	1
Organizations are waiting until the legislation becomes effective	1	1
Overloaded with new regulations	1	1
References play less prominent role with new regulations	1	1
Smaller organizations clearly have less budget to spend	1	1
The focus is shifting	1	1
While doing DORA-projects, requirements of other regulations can also be met	1	1

Gr = Groundedness (the total number of times the code has been applied)
Co = Coverage (the number of participants who referenced the code)