UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS
Postgraduate Programme "Digital Systems Security"

MSc Dissertation

Supporting the Digital Operational Resilience of the Financial Sector: The EU's DORA Digital Operational Resilience Act

Georgia Maria P. Karakasilioti

Supervising Professor: Stefanos Gritzalis, Professor

PIRAEUS

FEBRUARY 2024

MSc DISSERTATION

Supporting the Digital Operational Resilience of the Financial Sector: The EU's DORA Digital Operational Resilience Act

Georgia Maria Karakasilioti

A.M.: MTE2109

Abstract

This dissertation examines the effects and execution of the Digital Operational Resilience Act (DORA) in the financial sector of the European Union. DORA is a substantial legislative initiative aimed at harmonising the handling of Information and Communication Technology (ICT) risks among EU financial institutions to enhance the sector's resilience against ICT-related disruptions and threats.

The analysis outlines DORA's goals, highlighting its function in ICT risk management, incident reporting, digital operational resilience testing, third-party risk management, and information sharing within financial institutions. It emphasises the reasoning behind DORA, regarding the growing interconnectedness of financial services and the increasing frequency of cyber threats.

The following chapters analyse the framework in depth, from its historical background, legal structure, and its essential elements. An analysis of ICT risk management strategies highlights DORA's criteria for financial institutions, exploring the development of strong ICT risk management frameworks, incident reporting procedures, resilience testing, and oversight of third-party ICT service providers.

An analysis of "Bank X" showcases the practical use of the DORA Assessment Tool, highlighting how financial institutions can assess and improve their adherence to DORA regulations. This segment highlights the significance of preparation, teamwork, and a structured evaluation process in pinpointing compliance deficiencies and opportunities for enhancement.

The dissertation discusses the ongoing development of DORA, highlighting recent updates and improvements designed to enhance the digital operational resilience of the financial sector. These modifications demonstrate the evolving nature of digital finance, integrating the most recent technological innovations and emerging obstacles.

Ultimately, it is suggested that financial institutions should prioritise continuous compliance monitoring, improve risk management practices, invest in incident response capabilities, and strengthen third-party risk management to adhere to DORA guidelines. Financial entities can enhance their resilience against digital risks and ensure operational stability and continuity by following these recommendations to comply with regulatory requirements.

This thorough examination of DORA and its execution offers valuable insights for policymakers, financial institutions, and academics, aiding in a better comprehension of the framework's impact on improving the digital operational resilience of the EU's financial sector.

Table of Contents

1. Introduction

1.1 Background and Context

The introduction of digital technologies has significantly transformed the structure of the financial sector, ushering in a new era characterised by exceptional efficiency, innovation, and improvements in customer service. This transformation not only demonstrates the sector's ability to adjust, but also highlights the increasing reliance on information and communication technology (ICT) to provide financial services. Nevertheless, the dependence on digital solutions has made financial institutions vulnerable to a wide range of ICT risks, including cyber threats, data breaches, system failures, and operational disruptions. These vulnerabilities present substantial obstacles to the stability and integrity of the financial system, requiring a strong regulatory response to protect digital operational resilience.

In response to the importance of maintaining digital operational resilience in the financial sector, the European Union (EU) has adopted a proactive approach by implementing the Digital Operational Resilience Act (DORA).[2] DORA is a significant regulatory framework created to strengthen the financial sector against the various ICT threats it encounters. DORA seeks to establish consistent ICT risk management standards among all EU member states to ensure that financial institutions have the requisite abilities to effectively endure, respond to, and recover from disruptions and threats related to ICT.[8] The EU's commitment to improving the digital operational resilience of its financial sector is highlighted by this initiative, which is in line with the broader goals of financial stability and consumer protection.[12]

1.1.1. The imperative of Digital Operational Resilience

The importance of digital operational resilience in maintaining financial stability is becoming more widely acknowledged. In a time when digital transactions are everywhere and financial services are more and more provided through digital means, the possibility for disruptions caused by information and communication technology to cause financial instability is considerable.[12] These disruptions have the potential to impact both individual financial institutions and the entire financial system, leading to a loss of public trust and confidence. Thus, improving the digital operational resilience goes beyond the operational concerns of individual entities; it is a matter of significant importance for the entire system.

The changing landscape of cyber threats makes the need for DORA even greater. Cyber-attacks targeting financial institutions have increased, presenting a constant risk to financial stability. The potential ramifications of such attacks, including monetary loss, erosion of customer confidence, and harm to reputation, emphasise the crucial necessity for a comprehensive strategy in handling ICT risks.

1.1.2. Overview of the Digital Operational Resilience Act (DORA)

The framework will establish a standardised regulatory framework in order to ensure digital operational resilience throughout the financial sector of the European Union. It includes a wide range of financial institutions, such as banks, insurance companies, investment firms, and payment service providers. DORA covers multiple sectors and guarantees that the

framework is implemented consistently throughout the financial industry, so as it can deal with the interrelated nature of digital operational risks. [15][18]

DORA delineates precise criteria that financial institutions must adhere to in various crucial domains:

- **ICT Risk Management:** Institutions have to establish comprehensive ICT risk management frameworks in order identify, detect, responding, and recover from risks. This includes the creation of well-defined governance frameworks and procedures to effectively manage information and communication technology (ICT) risks.[18]
- **Incident Reporting:** DORA requires the implementation of systems to promptly report notable ICT-related incidents to authorities. This enables a synchronised reaction of evolving risks and contributes to a shared comprehension of the ICT risk environment. [18]
- **Digital Operational Resilience Testing:** The testing domain refers to the utilisation of penetration testing and threat-based exercises to evaluate the institution's ability to efficiently manage and respond to disruptions of information, communication technology.[18]
- **Third-party Risk Management:** Acknowledging the growing dependence on third-party service providers, DORA highlights the necessity of implementing rigorous management strategies to address information and communication technology (ICT) risks that arise from outsourcing agreements.[18]
- **Information Sharing:** DORA promotes the exchange of information among financial institutions regarding ICT risks and incidents within a secure and safeguarded framework. The objective is to cultivate a culture of collaboration and collective intelligence, thereby strengthening the sector's overall ability to withstand ICT threats.[18]

1.1.3. Implications for the Financial Sector

The implementation of DORA has substantial ramifications for the financial industry. Firstly, it requires a thorough evaluation of current ICT risk management practices, ensuring they are in line with the stringent standards established by DORA. Financial institutions should consider allocating resources towards adopting innovative technologies, bolstering their cybersecurity defences, and fortifying their incident response and recovery protocols. [8]

Moreover, DORA's focus on managing risks associated with third parties underscores the necessity for conducting thorough investigations and continuously monitoring service providers.[8] This requires a comprehensive approach to risk management that goes beyond the confines of individual institutions and includes their operational ecosystem.

1.2 Objectives

This essay thoroughly examines the Digital Operational Resilience Act (DORA), a significant legislative framework implemented by the European Union to enhance the digital operational resilience of its financial sector. The implementation of DORA represents a notable advancement in aligning the methods of handling information and communication technology (ICT) risks among financial institutions within the European Union (EU). This study is driven by the pressing necessity to comprehend the complexities of DORA and its consequences for financial institutions. It aims to achieve multiple crucial objectives that

collectively seek to improve the resilience and stability of the financial system in the digital era. [8]

1.2.1 Analysing the DORA Framework

The primary aim of this essay is to meticulously analyse the DORA framework, examining its fundamental elements and prerequisites. DORA implements a comprehensive set of regulations aimed at ensuring that financial institutions have strong mechanisms in place to efficiently handle and reduce ICT risks. This analysis seeks to elucidate the legislative text by providing a comprehensive scrutiny of the provisions in DORA pertaining to ICT risk management, incident reporting, digital operational resilience testing, third-party risk management, and information sharing among financial entities. The essay aims to analyse the potential effects of DORA on financial institutions, emphasising the operational, technological, and governance modifications required to ensure compliance and improve resilience.

1.2.2 Developing the Assessment Tool

The second objective focuses on creating and explaining a novel Excel-based tool that evaluates the level of operational resilience practices in a financial institution, in accordance with DORA's criteria. This tool aims to offer a practical solution for self-assessment, acknowledging the difficulties that financial institutions encounter when dealing with the intricacies of compliance and operational resilience improvement. The development process entails converting DORA's regulatory demands into a methodical questionnaire, integrating a scoring mechanism that enables institutions to assess their resilience practices across multiple dimensions. This tool is designed to serve not only as a means of ensuring compliance, but also as a strategic tool for ongoing improvement. It allows financial institutions to identify both their strengths and areas that need improvement in their operational resilience frameworks.

1.2.3 Offering Insights and Recommendations

Ultimately, the essay seeks to provide practical and effective suggestions for financial institutions looking to enhance their operational resilience within the framework of DORA. This includes combining the analysis of the DORA framework with the implementation of the assessment tool to develop practical strategies for the entities in scope. The recommendations will prioritise the resolution of the identified deficiencies, leveraging on technological progress, and promoting a mindset of resilience and ongoing adjustment. The essay aims to offer recommendations on optimal strategies for managing ICT risks, responding to incidents, conducting resilience testing, and managing risks associated with third-party involvement, among other topics. Furthermore, it seeks to make a valuable contribution to the wider discussion on maintaining strong and reliable digital systems, by providing insights into how regulatory frameworks such as DORA can adapt to address the difficulties posed by the swiftly evolving digital environment.

1.3 Research Questions

The study is carefully organised around a set of crucial research inquiries, each intended to analyze the framework’s characteristics and its significant consequences for the financial industry. These inquiries seek to analyse the fundamental nature of DORA and place it within the larger context of regulatory initiatives aimed at strengthening digital operational resilience.

1. **Main Components and Requirements of DORA:** The primary research question aims to address the fundamental components that comprise the DORA framework. This involves a thorough examination of the precise criteria established by DORA for financial institutions, encompassing risk management strategies, mechanisms for reporting incidents, protocols for testing resilience, and the handling of risks associated with third-party entities. The analysis aims to to provide a detailed understanding of the specific requirements set by the framework and to possibly clarify the operational, technological, and governance changes that are necessary in order to comply with these requirements.
2. **Comparative Analysis with Other Regulatory Standards:** The second question expands the analysis by placing DORA within the context of global regulatory standards. The goal is to establish connections with other standards and frameworks designed to improve digital operational resilience, such as the NIS 2 Directive and the Cybersecurity Framework created by the National Institute of Standards and Technology (NIST). This comparative analysis aims to identify similarities and differences, providing insights into the extent to which DORA conforms to or diverges from other regulatory approaches, and the consequences of these variations for financial institutions.
3. **Challenges and Opportunities Presented by DORA/ DORA's Updates:** The third question examines the tangible effects of DORA on financial institutions, investigating both the difficulties and possibilities it presents. This examines the operational, strategic, and compliance challenges that financial institutions may encounter in complying with DORA's requirements. Simultaneously, it examines the potential advantages that DORA provides in terms of improving digital resilience, gaining a competitive edge, and promoting stability across the entire sector. This inquiry seeks to address the balance of the discussion by emphasising that, despite the difficulties, DORA offers opportunities for innovation, enhancement, and strategic differentiation in the financial industry.
4. **Assessing Maturity of Digital Operational Resilience:** The objective is to examine techniques and resources that can accurately assess the preparedness and adherence of financial institutions to DORA's regulations. This entails the formulation of evaluation standards and benchmarks, as well as the investigation of optimal methods for ongoing monitoring and enhancement of digital resilience. The question highlights the significance of taking a proactive and adaptable approach to resilience, promoting the use of regular assessments as a means of guaranteeing that financial institutions maintain their strength in response to changing digital threats.

2. Literature Review

2.1. The Evolution of Digital Operational Resilience

2.1.1. Historical Context

The historical background of digital operational resilience in the financial sector is a story of gradual adjustment and regulatory development, influenced by the sector's increasing dependence on digital technologies and the simultaneous increase in cyber threats. This expedition has revolutionised the field of risk management, shifting from a limited emphasis on cybersecurity to a comprehensive approach that encompasses all aspects of digital operational risks. [21]

During the initial phases of digital implementation, financial institutions focused primarily on protecting themselves against external cyber threats. This period was defined by endeavours to strengthen digital infrastructures against hackers and malicious assaults, primarily focusing on perimeter defence mechanisms like firewalls and antivirus software. The objective was to safeguard delicate information and uphold the privacy and reliability of monetary transactions. During this period, cybersecurity emerged as a nascent field, as financial institutions started acknowledging the crucial significance of safeguarding their digital resources. [20]

As digital technologies became increasingly integrated into the operational structure of financial institutions, the range of resilience strategies started to broaden. The emergence of internet banking, mobile financial services, and subsequently, cloud computing, artificial intelligence (AI), and blockchain technology brought about new intricacies and susceptibilities. The financial sector's infrastructure has become increasingly interconnected and dependent on a network of third-party service providers, thereby magnifying the potential consequences of any individual point of failure. The interconnectedness of various components, although promoting efficiency and creativity, also implies that any disturbances can rapidly spread throughout the system, impacting a broad spectrum of activities and potentially destabilising the financial system.

In response to these changing difficulties, regulatory bodies and financial institutions adopted a comprehensive perspective on operational resilience. This comprehensive viewpoint included not just cyber threats, but also other types of IT-related disruptions, such as system outages, data corruption, and the breakdown of essential infrastructure. [8] The emphasis shifted from solely protecting against external assaults to constructing resilient systems capable of enduring various disturbances, guaranteeing uninterrupted operations and the capacity to swiftly bounce back from interruptions. This transition represented a notable advancement in the understanding of operational resilience, highlighting the importance of holistic risk management approaches that incorporate cybersecurity, IT governance, and operational risk management.

The regulatory response to these challenges has been increasingly flexible and responsive. Initially, the regulations were fragmented, with a narrow focus on specific facets of digital risk. Gradually, there has been a shift towards implementing regulatory frameworks that are more interconnected and capable of effectively managing the intricate nature of digital operational resilience. The Digital Operational Resilience Act (DORA) of the European Union exemplifies this regulatory progression. DORA aims to establish a uniform method for handling ICT risks in the financial sector of the European Union, taking into account the

significant role of digital operational resilience at a systemic level. DORA represents the culmination of years of regulatory adaptation and learning by requiring a comprehensive set of measures that address ICT risk management, incident reporting, resilience testing, third-party risk management, and information sharing. [17]

To summarise, the historical background of digital operational resilience in the financial industry demonstrates how the sector has effectively adapted to the challenges brought about by digitalization. The text describes the progression from initial cybersecurity measures to the creation of comprehensive frameworks such as DORA, which aim to protect the financial system from various digital disruptions. This development highlights the significance of flexible regulatory approaches and the necessity for financial institutions to consistently update their resilience measures in accordance with the evolving digital environment.

2.2. Overview of the DORA Framework

The Digital Operational Resilience Act (DORA) represents a significant advancement in the financial regulatory framework of the European Union. It aims to address the increasing intricacies and weaknesses arising from the digitalization of financial services. This legislative initiative was developed in response to the growing number of cyber threats, highlighting the urgent need for a comprehensive and strong strategy to protect the operational stability of the financial sector. The establishment of DORA was driven by various significant policy factors, particularly the need to strengthen the financial system's ability to withstand digital disruptions and to standardise regulations across EU member states.

2.2.1. Legislative Background

The Digital Operational Resilience Act (DORA) reflects a strategic change in the European Union's financial regulation approach, driven by legislative background and policy considerations. It aims to tackle the challenges arising from the digital era. The shift was prompted by the growing digital interconnectedness of financial entities, which, although promoting innovation and efficiency, also brought about new vulnerabilities in the financial system. [8] Prior to the implementation of DORA, the regulatory framework was fragmented, posing challenges for financial institutions in managing the intricacies of digital operations and cybersecurity. Every individual state possessed its own distinct set of regulations and principles, leading to a diverse collection of regulatory standards that made the handling of digital risks more complex and hindered the consistent implementation of cybersecurity measures across national boundaries. [18]

The advocacy for DORA intensified as the financial industry experienced a succession of prominent cyber events that underscored the concrete hazards linked to digital operations. These occurrences acted as a catalyst, exposing the potential for digital weaknesses to result in substantial monetary damages, erode consumer trust, and, in certain instances, jeopardise the overall stability of the financial system. The incidents served as catalysts, prompting the European Commission to conduct a thorough assessment of the effectiveness of the current regulatory framework in protecting against ICT risks. [8]

The European Commission aimed to achieve regulatory harmonisation and address the inconsistencies that were present in the previous regime through the development of DORA. The legislation was intended to be all-encompassing, encompassing all financial institutions

within its jurisdiction, thus guaranteeing fair competition and promoting a stronger and more robust financial industry. The development of DORA involved comprehensive consultations with various stakeholders, including financial institutions, regulatory bodies, and cybersecurity experts. This comprehensive approach facilitated the identification of crucial areas of concentration and the development of regulations that were both efficient and practical. [18]

The introduction of DORA represents a major achievement in the development of financial regulation in the EU. It demonstrates a proactive approach to dealing with the challenges of ensuring the robustness of digital operations. The purpose of the act is to not only reduce the risks related to disruptions in ICT, but also to encourage financial entities to continuously improve and adapt. DORA sets forth explicit protocols for managing ICT risks, reporting incidents, testing resilience, managing risks associated with third-party involvement, and sharing information. These guidelines establish a strong and resilient financial sector that can effectively address the challenges of the digital age. The primary objective of DORA is to augment the operational resilience of the financial sector, guaranteeing its security, stability, and reliability during a constantly changing digital environment.

2.2.2. Key Components of DORA

The Digital Operational Resilience Act (DORA) is a significant initiative undertaken by the European Union to protect the financial sector from the increasing range of digital risks. DORA's objective is to establish a comprehensive framework that not only standardises practices in the financial industry but also promotes a proactive culture of resilience and preparedness among financial entities. The components of DORA are carefully crafted to tackle the complex nature of digital operational resilience, guaranteeing that financial entities are well-prepared to effectively handle and reduce ICT risks.

- **ICT Risk Management:** The emphasis placed by DORA on ICT risk management highlights the crucial requirement for financial institutions to implement a comprehensive strategy for recognising and reducing digital threats. This component goes beyond conventional cybersecurity measures, promoting an integrated risk management strategy that encompasses the creation of resilient business continuity plans and advanced incident response mechanisms. Implementing such measures is essential to ensure that financial institutions can sustain vital operations in the event of digital disruptions, thus reducing the potential consequences on financial stability and consumer confidence. [18]
- **Incident Reporting:** The purpose of implementing systematic incident reporting under DORA is to promote transparency and collective vigilance in the financial sector. DORA mandates the prompt reporting of significant ICT-related incidents to relevant authorities. This facilitates a more coordinated approach to managing cyber threats, enabling timely interventions and the dissemination of critical threat intelligence across the sector. This provision not only strengthens the ability of financial entities to withstand and recover from challenges, but also enhances the overall stability and protection of the entire financial system. [17] [18]
- **Digital Operational Resilience Testing:** The requirement for regular digital operational resilience testing under DORA demonstrates the ever-changing and dynamic nature of the digital threat landscape. Financial institutions must conduct thorough testing of their digital security measures, utilising techniques such as penetration testing and scenario-based simulations. The purpose of these testing

protocols is to replicate actual cyberattacks and operational disruptions, in order to gain valuable insights into how well an organization's resilience measures work. The iterative process of testing and refining digital defences is crucial for staying ahead of emerging threats and vulnerabilities. [18]

- **Third-party Risk Management:** DORA focuses on the crucial element of managing third-party risks, recognising the interdependent nature of the modern financial ecosystem. The dependence of financial institutions on external service providers for various operational functions has led to an increased risk of ICT issues arising from these third-party engagements. The DORA regulation requires financial institutions to enforce stringent supervision and risk management protocols for their third-party vendors, guaranteeing that these external collaborators comply with equivalent levels of digital resilience. The DORA framework emphasises the significance of adopting a comprehensive strategy for managing risks, by applying the principles of operational resilience across the entire supply chain. [17] [18]
- **Information Sharing:** Ultimately, DORA's promotion of information exchange among financial entities signifies a deliberate step towards constructing a stronger and more robust financial ecosystem. DORA's objective is to foster a collaborative and supportive culture among financial institutions by facilitating the exchange of information on ICT risks and incidents. The utilisation of this collective intelligence methodology allows entities to acquire knowledge from the experiences of others, exchange optimal methods, and formulate more efficient strategies for the management of digital risks. The collaborative spirit exemplified in this aspect of DORA is essential for improving the industry's capacity to adjust to and alleviate the intricate challenges presented by the digital era. [17] [18]

2.3. Comparative Analysis with Other Regulatory Frameworks

As we begin to study digital operational resilience in the financial sector, it is important to consider the Digital Operational Resilience Act (DORA) in relation to global initiatives that aim to improve cybersecurity and operational strength. This investigation examines the comparative analysis of DORA in relation to other significant frameworks and standards that have emerged as fundamental elements in combating digital vulnerabilities and cyber threats. The frameworks mentioned, such as ISO 27001, the NIS 2 Directive, and the NIST Cybersecurity Framework, represent the global dedication to protecting digital infrastructures in different sectors. They particularly prioritise the financial industry due to its crucial importance and vulnerability to advanced cyberattacks. [7] [12] [14]

ISO 27001 is a recognised standard for managing information security. It offers organisations a clear framework for safeguarding their information assets. While DORA focuses specifically on the European Union's financial sector, ISO 27001 has a wider scope that extends across industries and geographies. It provides a universal standard for the establishment, implementation, and ongoing enhancement of information security management systems (ISMS).[12] The global standard emphasises the significance of thorough security practices that go beyond regional or sector-specific factors, emphasising the universal difficulties and strategies involved in information security.

The NIS 2 Directive is the European Union's enhanced effort to strengthen network and information systems in important sectors, going beyond finance to include various critical industries. This directive not only supports and enhances DORA's objectives in the financial domain, but also expands the reach of cybersecurity improvement throughout the

infrastructure of the European Union. The NIS 2 Directive enhances the cybersecurity ecosystem in Europe by imposing strict cybersecurity practices, incident reporting, and risk management procedures. This strengthens the interconnected resilience of Europe's digital landscape. [7]

The NIST Cybersecurity Framework, which originates from the United States, serves as a versatile tool for effectively managing cybersecurity risks. Its voluntary adoption and adaptability make it a widely acknowledged tool for organisations aiming to effectively navigate the complexities of cyber risk management. The framework's focus on fundamental functions—Identify, Protect, Detect, Respond, and Recover—provides a strategic approach to cybersecurity that appeals to both financial institutions and other sectors. It goes beyond regulatory boundaries to promote a universal methodology for operational resilience. [15]

The aim of this chapter is to provide a detailed examination of the subtle differences and collaborative aspects between DORA, ISO 27001, the NIS 2 Directive, and the NIST Cybersecurity Framework. Each framework plays a distinct role in achieving the overall objective of digital operational resilience. DORA concentrates on the financial sector in the EU, ISO 27001 sets a worldwide standard for information security, the NIS 2 Directive covers various sectors across the EU, and the NIST Cybersecurity Framework provides flexible guidelines for managing cybersecurity risks. These frameworks demonstrate the comprehensive approach needed to strengthen the financial sector, as well as other sectors, in the face of a growing and ever-changing digital threat landscape. This investigation not only emphasises the distinct characteristics and objectives of each framework but also showcases the joint effort towards establishing a secure, durable, and reliable digital economy worldwide.

3. Theoretical Framework

3.1. Introduction

Within the domain of financial services, where the digital environment is continuously changing, the notions of digital operational resilience and cybersecurity have gained significant prominence. An understanding of these subjects not only helps in understanding the intricate nature of digital dangers but also offers a systematic approach to handling and reducing these risks.

This chapter explores the theoretical foundations that shape our comprehension of digital operational resilience and cybersecurity. It establishes the basis for a detailed examination of regulatory frameworks such as the Digital Operational Resilience Act (DORA), ISO 27001, the NIS 2 Directive, and the NIST Cybersecurity Framework. Through an examination of the definition, historical development, and fundamental principles of digital operational resilience, we establish a conceptual framework that will guide the subsequent analysis of these regulations and standards.

3.2 Theories of Risk Management

To comprehend the theories of risk management in the realm of digital operational resilience, specifically in the financial industry, one must thoroughly examine the principles that govern the identification, assessment, mitigation, and monitoring of risks. These principles, which are fundamental to cybersecurity and operational resilience, play a crucial role in helping financial institutions navigate the complexities of the current digital threat landscape. This discussion seeks to shed light on the comprehensive approach required to protect digital financial operations by analysing specific risk management theories and their application in real-world situations.

The management of risks in the digital realm is based on various fundamental theories and principles, all of which contribute to a comprehensive approach in dealing with cybersecurity threats. The following items are included:

- The Risk Management Framework (RMF) is a structured approach used to identify, assess, and mitigate risks in a systematic manner. The National Institute of Standards and Technology (NIST) has introduced the Risk Management Framework (RMF), which provides a systematic approach to incorporating security and risk management tasks into the system development life cycle. The process highlights six key steps: categorization, selection, implementation, assessment, authorization, and monitoring of security controls. [15]
- The ISO 31000 Risk Management standard offers comprehensive guidance for organisations in effectively managing the risks they encounter. The framework promotes the implementation of a methodical, clear, and dependable procedure that is customised to the specific circumstances of the organisation. [29]

3.2.1 Application of Risk Management Theories in Financial Sector

- **Risk Identification:** Financial institutions utilise sophisticated cybersecurity tools and threat intelligence platforms to detect potential risks. As an illustration, banks employ machine learning algorithms to examine patterns and identify irregularities that suggest phishing, malware, or unauthorised transactions. An exemplary instance occurred when a European bank successfully foiled a highly advanced cyber-

espionage endeavour by promptly detecting and identifying malicious software implants within its network during the initial stages of the attack. [29]

- **Risk Analysis and Evaluation:** Financial institutions employ both quantitative and qualitative methods to assess risks, enabling them to prioritise risks based on their potential impact and likelihood. For example, a comprehensive risk assessment carried out by a prominent insurance firm may indicate that data breaches involving customer financial data present the greatest risk due to the possibility of substantial financial harm and damage to reputation. [29]
- **Risk Mitigation:** After identifying and assessing risks, financial institutions employ a range of measures to reduce these risks. This may involve utilising sophisticated encryption methods to protect data when it is stored and transmitted, implementing strong measures to control access, and adopting secure practices for developing software. An illustrative instance is the implementation of blockchain technology by various fintech startups to ensure secure and transparent transactions, thereby reducing the potential for fraud and unauthorised modifications. [29]
- **Risk Monitoring and Review:** Continuous monitoring and regular reviews are essential for adapting to the ever-changing cyber threat landscape, ensuring effective risk management. Financial institutions frequently utilise Security Operations Centres (SOC) that are equipped with Security Information and Event Management (SIEM) systems to actively monitor network traffic and user behaviour. This allows for swift identification and response to potential security risks. A prominent example involved a multinational bank effectively thwarting a specific cyber attack by promptly receiving notifications from its Security Operations Centre (SOC), thereby averting a potential compromise of sensitive information. [29]

Incorporating these risk management theories into the day-to-day operations of financial institutions promotes a culture of being able to withstand and adjust to challenges. Aligning with the RMF and ISO 31000 standards can improve an organization's capacity to withstand cyber threats and effectively respond to changes in the risk environment. Financial institutions are adopting a proactive approach to risk management in response to the growing complexity of cyber threats, including targeted ransomware attacks. Through the implementation of these risk management principles, a multinational bank successfully identified and contained a ransomware infection, effectively reducing harm and swiftly restoring essential operations within a few hours. [29]

3.3 Regulatory Compliance Theory

The complex connection between adhering to regulations and the behaviour of an organisation, particularly in the realm of cybersecurity practices and strategies for resilience, is a crucial aspect of contemporary risk management frameworks. The theory of regulatory compliance examines how legal frameworks and models for compliance not only require specific security measures, but also fundamentally shape the strategic direction and behaviour of organisations in the financial sector. This section explores the influence of regulatory frameworks on organisational behaviour, analyses different compliance models, and evaluates their effects on cybersecurity practices in the financial sector.

3.3.1 Regulatory Frameworks on Organisational Behaviour

Regulatory frameworks are essential for setting the basic requirements of cybersecurity and operational resilience that organisations are obligated to fulfil. These frameworks often

design organizations' strategies so they can implement and safeguard crucial digital assets as well an ensure business continuity in operations. For example, implementation of the General Data Protection Regulation (GDPR) in the European Union, which has had a substantial influence on how organisations manage personal data. This has led to a transition towards more rigorous data protection and privacy protocols. [28]

Following this example, the financial sector is required to adhere to regulations that enforce robust cybersecurity and resilience practices such as, the Digital Operational Resilience Act (DORA) in the European Union and the Gramm-Leach-Bliley Act (GLBA) in the United States. Financial institutions are required to take a proactive approach to cybersecurity by incorporating risk management directly into their operational and strategic planning. The regulatory nature of such rules guarantees that organisations not only comply with the most effective methods in cybersecurity but also cultivate a culture of ongoing enhancement and adjustment to emerging threats.

3.3.2. Compliance Models on Cybersecurity Practices

Compliance models differ in terms of methodology and complexity, spanning from strict regulations that specify precise security measures to adaptable frameworks that enable organisations to customise their cybersecurity practices according to their individual risk profiles. The influence of these models on organisational cybersecurity practices can be significant, affecting various aspects such as policy development and resource allocation for security initiatives.

Prescriptive compliance models necessitate organisations to adopt a predetermined set of security controls and measures. An illustration of this methodology is evident in the Payment Card Industry Data Security Standard (PCI DSS), which delineates an all-encompassing array of technical and operational prerequisites for safeguarding cardholder data. [27] Financial institutions that handle credit card information are obligated to comply with these requirements, guaranteeing a consistent level of security throughout the industry. Compliant organisations have made substantial investments in encryption, access control, and network security technologies due to the prescriptive nature of PCI DSS. [27]

Risk-based compliance models, such as the NIST Cybersecurity Framework, enable organisations to prioritise their cybersecurity initiatives according to their unique risk profile, in contrast to prescriptive models.[15] This model promotes the evaluation of an organization's vulnerabilities and exposure to threats, and the implementation of controls that are highly effective for their specific circumstances. Financial institutions may need to prioritise safeguarding systems that are essential for financial transactions and customer data. The risk-based model's flexibility promotes innovation in cybersecurity practices, allowing organisations to adjust their strategies in accordance with the changing threat landscape. [15]

3.3.3. Regulatory Compliance on Cybersecurity Practices

The impact of regulatory compliance on cybersecurity practices is complex and has multiple aspects. Compliance compels organisations to implement strong cybersecurity measures, guaranteeing the safeguarding of sensitive information and critical infrastructure. Conversely, the process of compliance can also prompt a strategic reassessment of cybersecurity priorities, prompting organisations to embrace comprehensive and robust cybersecurity approaches.

For example, a prominent financial institution may adopt sophisticated measures to identify and address potential security risks in order to meet regulatory mandates for continuous surveillance and prompt reporting of security incidents. By adhering to legal requirements, the bank not only ensures compliance but also strengthens its overall security stance, facilitating prompt detection and resolution of cyber risks. Likewise, adhering to frameworks that promote the management of risks associated with third-party involvement requires organisations to carefully examine and protect their supply chains, which is a critical aspect that is frequently disregarded in cybersecurity strategies.

The theory of regulatory compliance emphasises the important role that legal frameworks and compliance models have in influencing the cybersecurity practices and resilience strategies of organisations, especially in the financial sector. Regulatory frameworks enforce particular security measures and promote a culture of ongoing improvement, compelling organisations to strengthen their cybersecurity positions. This, in turn, enhances the overall resilience of the financial ecosystem. By analysing different compliance models, it becomes clear that regulatory compliance has a broader impact than just following the law. It also affects strategic decision-making and operational behaviour in the effort to achieve cybersecurity excellence.

3.4. Frameworks and Standards in Operational Resilience

Frameworks and standards are essential foundations for organisations aiming to strengthen their cybersecurity defences. The blueprint provided offers guidance on how to effectively implement security measures that guarantee the confidentiality, integrity, and availability of information systems and data. Organisations can systematically tackle cybersecurity threats, bolster their resilience against digital disruptions, and uphold trust with stakeholders by following these established guidelines.

- **DORA** is a regulatory framework designed specifically for the financial sector in the European Union. It imposes a set of requirements on financial entities to ensure they attain a strong level of digital operational resilience. These activities encompass ICT risk management, the reporting of incidents, testing the resilience of digital operations, and managing risks associated with third-party involvement. The prescriptive nature of DORA guarantees that financial institutions implement strong measures to endure and bounce back from disruptions related to information and communication technology (ICT). [8]
- **ISO 27001** is an internationally recognised standard for managing information security risks. It offers organisations a comprehensive framework for implementing and maintaining effective information security management systems (ISMS). The approach emphasises the use of risk assessment to customise security measures according to the specific risk profile of organisations. The widespread applicability of ISO 27001 makes it a versatile instrument for organisations in diverse sectors to accomplish and exhibit their dedication to information security. [12]
- **NIS 2 Directive:** The NIS 2 Directive seeks to enhance the cybersecurity of vital and significant organisations throughout the EU, encompassing various sectors beyond finance, building upon its predecessor. It emphasises the significance of implementing risk management measures, reporting incidents, and ensuring system resilience. The comprehensive nature of NIS 2 guarantees a consistent level of cybersecurity across vital industries, thereby strengthening the overall digital operational resilience of the European Union's domestic market. [7]

- **The NIST Cybersecurity Framework**, created by the National Institute of Standards and Technology, provides a versatile and optional collection of principles for enhancing cybersecurity and resilience. The text delineates five fundamental functions—Identify, Protect, Detect, Respond, and Recover—that organisations can adopt to effectively handle cybersecurity risk. The NIST Framework's versatility enables its application in various organisational contexts, rendering it a valuable asset for improving operational resilience. [15]

4. Methodology

The approach is described in order to investigate the complexities of digital operational resilience in the financial sector. The focus falls on how an institution can be assessed with the DORA Assessment tool as well as how the Digital Operational Resilience Act (DORA) compares with other significant cybersecurity frameworks such as ISO 27001, NIS 2 Directive, and the NIST Cybersecurity Framework.

4.1 Research Design

The research design is based on a mixed-methods approach, deliberately selected to analyse DORA's complex environment. This approach enables a thorough analysis of the framework in conjunction with the abovementioned cyber security frameworks. The inherent complexity of operational resilience and the varied regulatory environments across jurisdictions require a systematic approach that can encompass both the quantitative measures of framework adoption and the qualitative observations regarding their implementation and impact.

4.1.1 Mixed-Methods Approach

The research design includes the use of a custom assessment tool for quantitative analysis as well as thorough analysis of the framework. This tool is specifically designed to assess the maturity levels of financial institutions' operational resilience practices in accordance with the specific requirements of EU's DORA. The assessment tool's criteria are based on a thorough examination of the literature and the fundamental principles specified in the regulation. This guarantees that the evaluation is comprehensive and targeted designed to address the distinct elements of digital operational resilience.

4.2 Development of the Assessment Tool

4.2.1 Introduction &Scoping

The scoping section serves as the initial step of the assessment tool, aiming to establish if an entity is within the scope of the Digital Operational Resilience Act (DORA). The initial filtering stage is crucial in determining the direction of the organization's compliance journey before the comprehensive assessment. This tool section is meticulously designed to align with the legislative intricacies of DORA, guaranteeing accuracy in capturing the entity's regulatory scope. The scoping methodology in the tool is a structured process that conforms to the specifications of DORA. The initial checkpoint determines the necessity and scope of compliance measures that an organisation must implement.

- **Establishing Personal Scope:** The scoping section begins by closely examining the entity's classification according to DORA's definitions. Each question is related to a specific financial institution or service provider outlined in the regulatory framework, focusing on individual scope. It is crucial that this section is comprehensive and includes all categories outlined in DORA to prevent misclassification and guarantee complete regulatory adherence.
- **Assessing Organisational Measures:** Once the entity's type is determined, the evaluation moves on to organisational measures. This involves assessing the number of employees and the company's net worth, which are factors that impact the strictness of compliance requirements. The assessment tool inquiries about whether the entity has over 10 individuals or a net worth exceeding €2 million to determine if

it meets the criteria for a microenterprise, potentially changing its compliance responsibilities under DORA.

- **Exclusion criteria and material scope:** Essential in defining the entity's operations that could fall outside the material scope of DORA. Entities that only serve as particular payment systems, card payment schemes, or system operators might not be subject to DORA regulations. This distinction is crucial to prevent entities from being subjected to excessive regulatory examination or burdened with irrelevant compliance responsibilities.

Entities that meet the criteria outlined in DORA for regulated financial institutions or service providers are classified as **Fully in Scope**, moving on the complete range of the assessment tool's features. This classification requires a thorough compliance strategy that conforms to all DORA mandates.

Entities that do not completely meet these criteria or only participate in specific activities regulated by DORA are categorised as **Partially in Scope**. This intermediate classification prompts a customised evaluation that concentrates on DORA obligations that are pertinent to the entity's operations.

Entities that do not comply with DORA regulations due to their activities or operations are categorised as **Not in Scope**. The tool simplifies the process for these entities by skipping sections of the questionnaire that do not apply to their operational context.

Definitions and terms are taken directly from DORA and displayed with each question to help users correctly determine their status. Tooltips and additional information are included to clarify legal terminology and complex regulatory concepts, making it easier for users with different organisational backgrounds to navigate the section without needing specialised knowledge.

Consistent monitoring of legislative changes ensures that the questions stay up-to-date and reflect the most recent regulatory advancements. The tool is regularly updated to incorporate changes in DORA or the financial sector's regulatory landscape, ensuring its long-term usefulness and applicability.

The scoping section is a crucial part of the assessment tool, establishing the basis for a thorough and pertinent evaluation of an entity's adherence to DORA. The tool enables organisations to confidently navigate the complexities of digital operational resilience by offering a clear and structured pathway to determine the entity's regulatory scope. This chapter has outlined the thorough and important role of the scoping section in the assessment tool, highlighting its significance in achieving regulatory alignment and promoting operational resilience in the financial sector.

4.2.2 Questionnaire & Scoring

The core of the DORA assessment tool lies in its questionnaire and scoring system, which is created to methodically assess an organization's compliance to the Digital Operational Resilience Act.

Questionnaire Development

The questionnaire is carefully organised to depict the detailed requirements of DORA's directives. The document is divided into sections that align with the different chapters and

articles of the regulation, guaranteeing comprehensive coverage of the act's scope. The sections contains questions related to specific areas of compliance, such as ICT risk management, incident reporting, and business continuity planning, which are then divided into sub-requirements according to DORA.

Each item in the questionnaire, referred to as a 'sub-requirement number', is accompanied by 'Guideline Text' that clearly references the specific DORA provision it refers to. This method guarantees that participants can easily connect the question with the relevant regulatory text, which helps in providing precise and well-informed answers.

Questions are designed to inquire about the organization's methods for demonstrating compliance, encouraging entities to self-report on how they implement DORA's requirements. Respondents indicate their Response', showing the extent to which they have implemented the necessary measures.

The tool outlines the evidence that entities need to provide to support their compliance claims, in addition to the questionnaire items. By utilising an evidence-based approach, the self-reported data is grounded in verifiable information, which boosts the credibility and usefulness of the assessment.

Scoring System

The scoring system is a crucial aspect of the questionnaire, converting qualitative answers into a measurable range of compliance. This system utilises a maturity scale ranging from '1 (Best controls in place)' to '4 (No controls in place)', with intermediate scores indicating different levels of control effectiveness and implementation.

Interpretation of Maturity Scale:

- A score of 1 signifies that the entity has completely implemented best practice controls according to DORA's requirements, demonstrating perfect level of compliance.
- A score of 2 indicates that the entity is functioning effectively overall, with some minor areas for improvement or isolated instances of non-compliance.
- A score of 3 indicates that there are controls in place, but there are also notable gaps or deficiencies that must be resolved to attain complete compliance.
- A score of 4 indicates complete lack of controls, showing that the entity is not compliant with the DORA framework in that specific domain.

The tool combines scores of individual items to compute a 'Chapter Maturity Score', offering a comprehensive assessment of the entity's compliance maturity for each section of DORA. This comprehensive scoring system allows organisations to identify specific areas of excellence and weakness at detailed and broader levels.

The questionnaire's design enables a continuous feedback loop by using scoring outcomes to inform entities of their compliance status and direct them towards specific improvements. It serves as both a diagnostic tool and a guide for improving digital operational resilience in accordance with regulatory standards.

4.2.3 Dashboard

The dashboard is a compilation of data gathered from the questionnaire of the tool. It is designed to provide a quick and clear visualisation of how well an organisation follows

framework. The analytical feature of the tool is created to convert unprocessed data into practical insights, enabling organisations to promptly evaluate their compliance status in different areas of DORA.

Dashboard Structure

The dashboard consists of multiple columns that align with DORA's categories, each representing a distinct domain within the framework. The layout is organised in the following manner:
Domain: The domain column displays DORA's categories, including ICT Risk Management Framework, ICT-related Incident Reporting, Digital Operational Resilience Testing, and ICT Third-Party Risk Management.

Assessment: These assessment columns represent each rating level on the maturity scale.

- N/A: Not applicable or not assessed.
- 1 (Exemplary controls): Indicates outstanding compliance with DORA's requirements.
- 2: Showing overall effective controls with slight room for enhancement.
- 3:Demonstrating incomplete compliance with substantial opportunity for enhancement.
- 4 (Poor controls): Indicates absence of control implementation or major deficiencies.

The Total Rating per Domain is an aggregated score representing the overall rating for each domain. It is computed by averaging the scores of the sub-requirements within that domain.

Domain weight: Indicates the significance or influence of each domain on the operational resilience of the organisation. The Weighted Score is calculated by multiplying the Total Rating per Domain by the Weight per Domain, which helps determine the organization's compliance posture. The Total Weighted Score combines the Weighted Scores from all domains to create a comprehensive compliance score.

Total Questions Answered: Shows the number of questions answered in each domain, giving context to the ratings and weights.

Visual depiction: The dashboard includes graphical elements to visually represent the score for each domain, in addition to numerical data. Graphical elements like bar graphs and spider charts visually represent the compliance status, aiding stakeholders in understanding the organization's performance in different areas of DORA.

Bar graphs display the total rating for each domain, providing a visual representation of the organization's strengths and areas needing improvement. Spider charts are beneficial for evaluating an organization's maturity in various areas and showing the distribution of compliance efforts.

Analytical Capability: The dashboard functions as a tool for making decisions, providing various analytical features.

Comparative Analysis: Organisations can assess their performance by comparing it to industry benchmarks or predetermined compliance standards. Organisations can utilise the dashboard for trend analysis to monitor their advancements and enhancements in various areas over time. The dashboard identifies areas with lower scores, indicating where the organisation should concentrate its efforts to improve compliance and resilience.

The dashboard is a crucial component of the assessment tool, offering a comprehensive summary and detailed analytical information on an organization's compliance with DORA. The dashboard uses detailed scoring, weighted analyses, and visual graphs to transform intricate data into a coherent story about the organization's cybersecurity status. This narrative provides information on the current compliance status and offers a roadmap for continuous improvement, directing organisations towards achieving the highest standards of digital operational resilience.

The meticulous design of the dashboard guarantees that it is more than just a storage of scores, but a dynamic and interactive tool. It emphasises strengths, reveals weaknesses, and encourages a proactive stance towards regulatory compliance and cybersecurity advancement.

Customisation involves adjusting the weight assigned to each domain to match the organization's unique risk profile and operational priorities. Scalability refers to the capability to incorporate new domains or sub-requirements as DORA progresses or as the organisation broadens its scope.

Interactivity is majorly highlighted by the dashboard; offering drill-down features for users to explore each domain more thoroughly for a detailed analysis of compliance. The dashboard's design is expected to change as the regulatory environment and the organization's digital resilience progress. The document evolves into a dynamic central component of the compliance narrative, guiding strategic decision-making and operational changes.

Within the dissertation, the dashboard is used as a case study to demonstrate effective data visualisation and compliance management. It shows how intricate regulatory requirements can be simplified into practical, actionable insights that promote organisational change. The dashboard serves as a vital communication tool that connects the complexities of regulatory frameworks with the practical aspects of organisational implementation.

Ultimately, the dashboard in the assessment tool serves to clarify the path to compliance, streamline the intricacies of DORA's requirements, and offer a foundation for ongoing enhancement. It represents the organization's dedication to operational resilience, demonstrates its level of cybersecurity maturity, and serves as a roadmap for achieving excellence in the digital operational environment.

4.2.4 Reliability & Validity

The effectiveness of an assessment tool depends greatly on its reliability and validity. The metrics guarantee the tool's reliability for strategic decision-making and establish its credibility as a reliable tool for measuring compliance with the Digital Operational Resilience Act (DORA). This part of the dissertation explains the detailed processes and methodological foundations that strengthen the reliability and validity of the DORA assessment tool.

Consistency Over Time: The assessment tool is designed to ensure consistent results over time by being calibrated for temporal stability. Stringent version control mechanisms are implemented, which involve documenting all changes and revisions made to the tool. The tool's criteria and benchmarks are kept current and relevant by synchronising updates with the latest developments in the DORA framework and industry best practices. Periodic

validation exercises are performed, and the tool's algorithm is tested against historical data to ensure that results remain stable over time, regardless of changes in regulations.

Inter-rater Reliability: The tool includes a comprehensive set of guidelines and definitions to reduce variability in results caused by subjective interpretations, ensuring clarity on the purpose and extent of each questionnaire item. Standardised training modules and user manuals are given to ensure that all users have a consistent comprehension of the assessment criteria. A standardised feedback system gathers user interpretations and modifies the guidance text to reduce ambiguities, improving the consistency of results among various assessors.

Test-retest Protocol: The tool includes a protocol that prompts entities to regularly review their compliance. This feature serves as both a consistency check and a real-time monitor of an entity's progress and its reaction to corrective measures. It is recommended that organisations record alterations in operational procedures during assessments to explain any discrepancies in scores.

Content Validity: The tool's content validity was ensured by directly extracting compliance criteria from the DORA legislation and meticulously translating them into questionnaire items during the development process. Every item was compared with the legislative text to guarantee thorough coverage of all compliance aspects. EU financial regulation legal experts were consulted to confirm that the tool accurately reflects and measures the intended content domains of DORA. The assessment tool was rigorously validated against external compliance measures, such as third-party audits and regulatory reports, to establish criterion validity.

Criterion Validity: To determine its criterion validity. By correlating the tool's scoring with outcomes from established compliance measures, we guaranteed that the tool's evaluations are predictive and in line with industry standards. The tool's scores and outcomes were frequently evaluated by regulatory experts to ensure their precision and dependability in indicating actual compliance status. The assessment tool is based on theoretical frameworks relevant to digital operational resilience, ensuring construct validity. The tool assesses constructs like ICT risk management, incident reporting, and third-party risk management based on the DORA framework. Industry experts were involved to confirm that the tool's content matches the theoretical and practical aspects of operational resilience as defined in the regulatory framework.

Benchmarking Against Industry Standards: The tool's scoring system was created by analysing industry standards and regulatory guidelines to set benchmarks. This guarantees that the tool evaluates adherence to DORA standards and assesses the entity's level of development within the wider financial sector. The tool uses industry benchmarks to offer comparative insights, enabling entities to assess their resilience posture in relation to sector-wide best practices.

Chapter 5: Analysis of the DORA Framework

5.1 Introduction

Overview of the DORA Framework's Objectives

The Digital Operational Resilience Act (DORA) represents a significant legislative milestone in the European Union's efforts to fortify the digital operational resilience of its financial sector. Instituted against a backdrop of escalating cyber threats and the increasing digitalization of financial services, DORA aims to establish a comprehensive regulatory framework that standardizes the approach to managing information and communication technology (ICT) risks across financial entities. Its primary objectives are to ensure that the financial sector can withstand, respond to, and recover from all types of ICT-related disruptions and threats, thereby safeguarding the sector's integrity, continuity, and stability. [8]

DORA encompasses several key domains, including ICT risk management, incident reporting, digital operational resilience testing, third-party risk management, and information sharing. Through these domains, the framework seeks to elevate the cybersecurity posture of financial institutions, enforce rigorous oversight of third-party ICT service providers, and enhance collaboration among financial entities and authorities. This holistic approach underscores the recognition that operational resilience is not merely a matter of individual institution's strength but also a function of the collective security and resilience of the financial ecosystem. [8]

Rationale for the Analysis

The analysis of the DORA framework, as delineated in this chapter, is motivated by the pressing need to understand the intricacies and implications of this comprehensive legislation for the financial sector. Given the pivotal role of digital technologies in today's financial services landscape, the ability of financial institutions to manage and mitigate ICT risks is of paramount importance. As such, DORA represents both a challenge and an opportunity for the sector - a challenge in terms of compliance with its extensive requirements, and an opportunity to achieve a higher standard of operational resilience. [8]

This analysis is significant within the context of this dissertation as it provides a detailed examination of how DORA is poised to reshape the cybersecurity and operational resilience strategies of financial institutions. [8] By dissecting the framework's objectives, requirements, and potential impacts, this chapter aims to contribute to a deeper understanding of DORA's role in enhancing the digital operational resilience of the financial sector. Furthermore, it endeavours to offer valuable insights for financial institutions navigating the compliance landscape, policymakers evaluating the framework's effectiveness, and academics researching the intersection of cybersecurity, operational resilience, and financial regulation.

In essence, the analysis of the DORA framework encapsulated in this chapter is a foundational element of the dissertation, setting the stage for subsequent discussions on compliance challenges, implementation strategies, and the broader implications of DORA for the financial sector's resilience in the digital age.

5.2 Understanding the DORA Framework

The key components of DORA can be summarized in the following points:

- **ICT Risk Management Framework**: DORA's core refers to the need for financial institutions to create a thorough ICT risk management framework. This includes strategies, protocols, and measures created to recognise, safeguard against, notice, react to, and recuperate from ICT hazards. The framework requires a proactive risk management approach, highlighting the significance of resilience in ensuring continuous financial services. [16]
- **Incident Reporting**: DORA mandates strict incident reporting requirements for financial entities, necessitating prompt notification to authorities of significant ICT-related incidents. This guarantees prompt detection and reaction to new threats, enabling a unified strategy for handling cybersecurity issues throughout the sector.
- **Digital Operational and Resilience Testing**: The framework requires routine testing of digital operational resilience, which includes vulnerability assessments, penetration testing, and threat-led penetration testing. These testing requirements are crucial for verifying the effectiveness and resilience of financial entities' cybersecurity measures against sophisticated cyberattacks. [16]
- **Third-party Risk Management**: DORA establishes stringent requirements for managing third-party risks due to the growing dependence of financial institutions on third-party ICT service providers. Financial institutions must perform due diligence, oversee third-party providers' performance, and include provisions in contracts to comply with DORA requirements. [5]
- **Information Sharing**: DORA promotes the exchange of information among financial institutions, regulatory bodies, and other involved parties. This provision is intended to promote a collaborative environment for sharing information on cyber threats, vulnerabilities, and best practices to improve the overall resilience of the financial sector. [8][17]

5.3 ICT Risk Management

The Digital Operational Resilience Act (DORA) focuses on creating a strong ICT risk management framework in financial institutions. This framework aims to help organisations recognise, evaluate, reduce, and oversee ICT risks that may affect their operational resilience. DORA requires financial institutions to incorporate risk management practices into their business strategies and decision-making processes in a comprehensive manner.

5.3.1 Risk Identification and Assessment

Financial institutions must create and uphold procedures for ongoing identification and evaluation of ICT risks that may affect their services and operations.

1. **Comprehensive Risk Mapping:** Developing a thorough risk map by cataloguing ICT assets and their vulnerabilities, considering the intricate nature of digital operations and connections with third-party service providers. This entails:
    - **Asset Inventory**: Financial institutions must create a comprehensive list of all ICT assets, encompassing hardware, software, data, and network resources. This inventory is essential for risk mapping, allowing organisations to identify the location of crucial data and understand the interactions of ICT systems internally and externally. [28]

- **Vulnerability Identification**: Entities must systematically identify vulnerabilities associated with each asset, in addition to maintaining an asset inventory. This encompasses identified security flaws in software, potential points of exploitation in hardware, and vulnerabilities related to human behaviour. [28]
- **Coordinated Analysis**: Entities need to assess the risk landscape beyond their own ICT environment due to their dependence on third-party service providers and the interconnected nature of digital financial services. This includes evaluating the security status of partners and suppliers and comprehending how external vulnerabilities could affect their operations.
- **Risk Prioritization**: After identifying assets and vulnerabilities, financial institutions need to prioritise risks by considering their potential impact and probability. This prioritisation assists in concentrating efforts and resources on reducing risks that present the most significant danger to operational resilience. [28]

2. **Emerging Threat Analysis**: Conducting ongoing surveillance and assessment of new cyber threats and vulnerabilities, such as those associated with software updates, hardware security, and external threat intelligence reports, to maintain up-to-date and forward-looking risk evaluations.
    - **Continuous Monitoring:** Continuous monitoring is essential due to the rapidly evolving cyber threat landscape, allowing for the prompt identification and evaluation of new risks. Financial institutions should utilise sophisticated monitoring tools and methods to identify irregularities and indications of possible security breaches.
    - **External Intelligence Gathering:** Utilising external intelligence sources like cybersecurity agencies, industry consortiums, and private threat intelligence services is essential for keeping up to date with emerging threats. This involves signing up for notifications regarding new malware, ransomware, phishing strategies, and software weaknesses.
    - **Predictive Analysis:** Entities are advised to use predictive analysis methods that utilise historical data, threat intelligence, and trend analysis to anticipate potential threats before they occur, moving beyond reactive monitoring. Being proactive allows for improving risk assessments and strengthening defences before any potential threats arise.
    - **Collaborative Threat Assessment:** Engaging in industry-wide and cross-sector threat assessment initiatives enables financial institutions to understand systemic risks and emerging threat vectors. Collaboration helps to achieve a thorough comprehension of the threat environment, improving both individual and collective ability to withstand challenges.

5.3.2 Protective and Preventive Measures

The crucial defense layer is essential for preserving the integrity, availability, and confidentiality of financial services against cyber threats. These measures are implemented through various key strategies.

1. **Deployment of Cybersecurity Solutions**
    - **Security Software**: Institutions need to implement advanced cybersecurity solutions such as firewalls, antivirus programmes, anti-malware tools, and

intrusion prevention systems. These tools act as the primary defence against external threats by preventing unauthorised access and identifying malicious activities.

- **Security Information and Event Management (SIEM)**: Implementing SIEM technology allows for the immediate analysis of security alerts produced by applications and network hardware. Centralising the monitoring of security events enables institutions to promptly detect and address potential threats.
- **Threat Intelligence Platforms**: Leveraging machine learning and artificial intelligence, anomaly detection systems can identify unusual patterns of behavior that may indicate a cybersecurity threat, allowing for early intervention before a breach occurs.

2. **Access Control Mechanisms**
   - **User Authentication:** Strong access control policies guarantee that only approved users can access sensitive information and crucial ICT systems. This involves enforcing robust password policies, utilising multi-factor authentication (MFA), and implementing role-based access controls (RBAC) to reduce the likelihood of unauthorised access.
   - **Identity & Access Management (IAM) / Privileged Access Management (PAM):** Institutions need to meticulously oversee and control privileged accounts, which have heightened access to systems and data. IAM and PAM solutions assist in managing, securing, and monitoring access to important resources, ultimately lowering the chances of insider threats and data breaches.
3. **Data Encryption Practices**
   - **Encryption of Data at Rest and in Transit:** It is crucial to encrypt sensitive data when it is stored or being transmitted to prevent unauthorised access and data leaks. This involves implementing robust encryption standards and protocols for storing data, sending emails, and communicating through various channels.
   - **Key Management Systems:** Secure key management practices are essential for effective encryption. Financial institutions need to establish systems for securely storing, rotating, and managing cryptographic keys to maintain the strength and effectiveness of encryption mechanisms.
4. **Implementation Challenges and Best Practices**
   - **Regular Security Assessments:** To ensure the effectiveness of protective and preventive measures, institutions should conduct regular security assessments, including vulnerability scans and penetration testing. These assessments help in identifying potential weaknesses in security controls and inform necessary adjustments.
   - **Employee Training and Awareness:** Human error continues to be a major weakness in cybersecurity. Institutions should allocate resources to consistent employee training programmes to enhance understanding of cyber threats and advocate for optimal information security practices.
   - **Continuous Improvement:** Cybersecurity requires ongoing improvement rather than being a one-time endeavour. Financial institutions need to stay updated on current cyber threats and emerging technologies, adapting their security measures to ensure a strong defense.

5.3.3 Detection Mechanisms

The Digital Operational Resilience Act (DORA) requires financial institutions to have strong systems in place to quickly detect incidents related to information and communication technology (ICT). Being proactive is essential for reducing the potential impact of cyber threats on the continuity and integrity of financial services. DORA emphasises the significance of incorporating Security Information and Event Management (SIEM) systems and Intrusion Detection Systems (IDS) into a holistic cybersecurity approach. These technologies are crucial for detecting suspicious activities and potential breaches immediately, allowing for quick response and mitigation.

1. **Utilization of SIEM Systems**
   - **Real-time Monitoring and Analysis:** SIEM systems collect and examine log data from different sources in an organization's IT environment, such as servers, network devices, and applications. SIEM systems centralise log data collection to offer a comprehensive view of security status, allowing for real-time monitoring and analysis of events that may signal a security breach.
   - **Correlation and Alerting:** SIEM systems excel at correlating diverse events and recognising patterns that could indicate a cyber threat. SIEM systems utilise advanced correlation rules and algorithms to identify anomalies and suspicious activities that might otherwise be overlooked. When the system identifies these patterns, it creates alerts, initiating an immediate investigation by cybersecurity staff.
   - **Compliance Reporting:** SIEM systems provide valuable capabilities for compliance reporting, going beyond mere detection. They are able to create reports that detail incident response actions and audit trails, helping financial institutions show compliance with DORA's requirements and other regulatory duties.
2. **Intrusion Detection Systems**
   - **Network-based and Host-based IDS:** IDS can be classified as network-based (NIDS) and host-based (HIDS) systems. NIDS monitor network traffic for potentially malicious behaviour, whereas HIDS concentrate on specific devices or hosts by scrutinising system logs and identifying unauthorised alterations. Both Intrusion Detection Systems (IDS) are necessary for a layered defence strategy, providing complementary detection abilities.
   - **Signature-based and Anomaly-based Detection:** Intrusion Detection Systems (IDS) use different detection methods such as signature-based detection, which compares network traffic with a database of known threat signatures, and anomaly-based detection, which detects deviations from established normal activity baselines. Using these methodologies improves the capability to identify both familiar and novel cyber threats.
   - **Integration with Incident Response:** Integrating IDS with incident response protocols significantly boosts an entity's cybersecurity resilience. When a potential threat is detected, the Intrusion Detection System (IDS) should automatically activate predefined incident response protocols to swiftly and efficiently address the threat.
3. **Best Practices**
   - **Tuning and Optimization:** Both SIEM and IDS need frequent tuning and optimisation to reduce false positives and ensure accurate identification and

prioritisation of real threats. This includes modifying correlation rules, updating signatures, and adjusting anomaly detection thresholds in response to changing threat environments and organisational adjustments.

- **Skilled Personnel:** Skilled cybersecurity personnel are required to effectively implement and operate detection mechanisms by interpreting alerts, conducting investigations, and taking necessary actions. Continuous training and development are essential for establishing and preserving the necessary expertise to efficiently oversee these systems.

Financial entities can greatly improve their ability to detect and address ICT-related incidents promptly by using SIEM systems and IDS effectively. Being proactive in cybersecurity not only meets regulatory standards but is also a crucial part of a financial institution's strategy to protect its operations and services from cyber threats.

5.3.4 Response and Recovery Plans

The Digital Operational Resilience Act (DORA) requires financial institutions to create thorough incident response and recovery strategies. These plans are essential for institutions to promptly and efficiently handle cybersecurity incidents, thus reducing their impact on operational capabilities and financial stability.

1. **Incident Response Team**
   - **Team Formation and Structure:** A core requirement under DORA is the formation of a dedicated incident response team. This team is composed of individuals with specific expertise in cybersecurity, risk management, and operational functions. The structure of the team often reflects the complexity and scale of the financial entity's operations, ensuring that all critical areas are represented.
   - **Roles and Responsibilities:** The incident response team has specific roles and responsibilities that encompass the entire incident lifecycle, including detection, analysis, containment, eradication, and recovery. Key roles may involve an Incident Manager responsible for coordinating response efforts, technical experts tasked with analysing and mitigating threats, and communication specialists in charge of managing internal and external communications.
   - **Training and Exercises:** Consistent training activities, like tabletop simulations and live drills, are crucial to ensure the incident response team is ready to respond quickly and efficiently. The exercises aid in pinpointing deficiencies in the response plan and offer team members hands-on experience in handling various cybersecurity situations.
2. **Business Continuity Planning**
   - **Integration with ICT Risk Management:** DORA focuses on integrating business continuity planning (BCP) and disaster recovery (DR) within the larger ICT risk management framework. This guarantees that the actions taken to respond and recover are in accordance with the organization's risk profile and resilience goals.
   - **Critical Functions Identification:** An essential part of Business Continuity Planning (BCP) involves identifying critical business functions and the Information and Communication Technology (ICT) systems that underpin them. Identifying crucial functions of the organisation enables prioritisation during the recovery phase, ensuring that the most vital services are restored promptly.

- **Recovery Strategies:** Financial institutions must create recovery strategies detailing the procedures to reinstate essential operations after an event. This involves predetermined recovery time objectives (RTOs) and recovery point objectives (RPOs), which establish specific expectations for the duration to restart operations and the permissible amount of data loss.
- **Testing and Review:** Regular testing is required to ensure the effectiveness of Business Continuity Planning (BCP) and Disaster Recovery (DR) plans. These assessments, which include desktop reviews and full-scale recovery exercises, enable organisations to evaluate their readiness and pinpoint areas that need enhancement. Plans should be regularly reviewed and updated to incorporate changes in the operational environment, technological advancements, or shifts in the entity's risk landscape.

3. **Best Practices**
   - **Scalability and Flexibility:** Response and recovery plans need to be adaptable and adjustable to different types and levels of incidents. Financial institutions should develop modular strategies that can be customised for particular situations to guarantee a suitable and efficient reaction.
   - **Communication Protocols:** Establishing precise communication protocols is crucial. This involves communication within the response team and with regulators, customers, and partners. Clear and prompt communication can greatly reduce the damage to a reputation caused by an incident.
   - **Post-Incident Review:** After resolving an incident, it is essential to conduct a post-incident review to capture lessons learned and incorporate them into future planning. This ongoing improvement process improves the organization's ability to withstand challenges and be ready for what lies ahead.

DORA's requirements for incident response and recovery plans emphasise the significance of readiness and flexibility when dealing with ICT incidents. Financial entities can ensure the resilience of their operations by creating specialised response teams, merging business continuity with ICT risk management, and consistently testing and improving response and recovery strategies. This comprehensive strategy not only complies with regulatory requirements but also safeguards the organisation and its stakeholders from the potentially significant consequences of cybersecurity breaches.

5.3.5 Testing and Situational Awareness

The Digital Operational Resilience Act (DORA) highlights the importance for financial institutions to create a thorough ICT risk management framework, conduct rigorous effectiveness tests, and stay highly aware of cyber threats. These components are crucial for financial institutions to quickly adjust to and reduce changing cyber risks, thus protecting their operational integrity.

1. **Resilience Testing**: Financial entities are required by DORA to conduct periodic testing on their cybersecurity measures to assess their effectiveness. Being proactive is crucial for detecting vulnerabilities that may be targeted in a cyberattack.
   - **Penetration Testing**: This form of testing involves simulating cyberattacks on an institution's networks, systems, and applications to identify vulnerabilities and security gaps. Penetration testing is conducted from the perspective of an external attacker attempting to breach the entity's defenses.

- **Threat-Led Penetration Testing**: An advanced testing method that replicates intricate and focused cyberattacks using up-to-date threat intelligence. TLPT assesses an organization's ability to defend against advanced persistent threats (APTs) by testing the strength of its cybersecurity measures in realistic attack situations.
- **Red Teaming**: Red Teaming is an advanced attack simulation that evaluates an organization's ability to withstand real-life threats by testing its people, networks, applications, and physical security controls. Red Teaming offers a thorough evaluation of an organization's overall security stance, encompassing more than just its digital protections.

2. **Threat Intelligence Sharing**: DORA promotes engaging in threat intelligence sharing initiatives. These platforms enable the sharing of information on new cyber threats, weaknesses, and hostile strategies among financial institutions, regulatory bodies, and cybersecurity communities. Having access to shared, timely, and actionable threat intelligence allows organisations to proactively adapt their cybersecurity strategies, improving their readiness for potential cyber incidents.
   Using up-to-date threat intelligence enables financial institutions to continuously adjust their risk management frameworks, ensuring that their cybersecurity defences stay in line with the current threat environment.

   Integrating threat intelligence into the ICT risk management framework is crucial to ensure that risk assessments accurately reflect current cybersecurity threats and trends. By adopting a proactive approach, financial entities can consistently improve their risk mitigation strategies, guaranteeing a strong level of operational resilience.
3. **Best Practices**
   - **Implementing Comprehensive Testing Strategies**: Penetration Testing, TLPT, and Red Teaming exercises require specialised skills and resources due to their complexity. Financial institutions must have the required expertise to conduct and interpret these tests effectively.
   - **Trusted Network for Intelligence Sharing**: Building and sustaining reliable relationships is crucial for successful sharing of threat intelligence. Organisations must find a way to prioritise information security while also reaping the advantages of sharing intelligence collaboratively. They must address concerns regarding data privacy and confidentiality in order to establish a unified security environment.
   - **Operationalizing Threat Intelligence**: Simply gathering threat intelligence is inadequate; financial institutions need strong procedures for analysing, incorporating, and responding to the intelligence they receive. This involves revising security protocols, improving detection methods, and optimising response tactics using practical information.

Resilience testing and situational awareness are crucial components of the ICT risk management framework promoted by DORA. By actively participating in Penetration Testing, TLPT, Red Teaming, and sharing threat intelligence, financial institutions can guarantee that their cybersecurity defences are proactive and effective. These practices not only meet regulatory requirements but also greatly enhance the operational resilience and security of the financial sector in the face of advancing digital threats.

5.3.6 Use Cases

5.4 Incident Reporting

Incident reporting is a vital component of the Digital Operational Resilience Act (DORA), highlighting the significance of transparency and accountability in handling ICT-related incidents in the financial sector. This section delves into DORA's thorough method for incident reporting, outlining the obligations it imposes on financial institutions to guarantee prompt notification and thorough documentation of cybersecurity incidents. [8]

5.4.1 The Role of Incident Reporting in DORA

DORA aims to improve the financial sector's overall ability to handle risks by requiring incident reporting, in order to oversee and manage systemic risks. Aggregated incident data assists in recognising patterns, weaknesses, and possible regulatory deficiencies. [8]

It enables the exchange of best practices and insights between financial institutions and regulatory authorities. This cooperative method promotes a culture of ongoing enhancement and contributes to elevating the general level of cybersecurity and operational resilience within the sector.

Incident reporting is a tool used for regulatory compliance and oversight to verify that financial institutions are following DORA's regulations and implementing necessary actions to handle and reduce ICT risks. [8]

5.4.2 Mandatory Reporting

Mandatory reporting in the Digital Operational Resilience Act (DORA) is crucial for enhancing cybersecurity and operational resilience in the financial sector. Financial entities must promptly inform relevant supervisory authorities of significant ICT-related incidents as required. This mandate aims to improve transparency in the cyber threat landscape and facilitate a coordinated response to reduce potential systemic risks.

1. **Purpose, Impact & Challenges**
   - **Transparency**: Compulsory reporting guarantees that regulatory bodies have a current and thorough understanding of the cyber threat environment affecting the financial industry. Regulators need clear visibility to comprehend the frequency, severity, and characteristics of ICT-related incidents, enabling a data-driven approach to cybersecurity supervision.
   - **Systemic Risk Mitigation**: Involves regulatory bodies collecting incident data from various parts of the financial system to detect patterns, vulnerabilities, and trends that could indicate systemic risks. This collective intelligence enables the creation of specific regulatory interventions, guidelines, and best practices aimed at enhancing the overall resilience of the sector.
   - **Regulatory Response**: Timely incident reporting allows regulatory authorities to promptly allocate resources, offer guidance, and collaborate with other organisations to manage and mitigate the effects of major cyber incidents. Having a quick response capability is essential for reducing the possible disturbance to financial services and protecting market stability.
   - **Defining Significance**: An important operational element of mandatory reporting under DORA is setting clear criteria to determine what qualifies as a 'significant' ICT-related incident. Financial institutions must assess these criteria, which take

into account the effects on operations, data accuracy, financial damages, and customer consequences, in order to ascertain the reportability of an incident.

- **Reporting Timelines**: The requirement for immediate reporting presents the difficulty of swiftly evaluating incidents and collecting the essential information to meet reporting requirements. Financial institutions need to have effective procedures for detecting and evaluating incidents in a timely manner.
- **Cross-border Considerations**: Financial institutions operating in different countries must ensure that their mandatory reporting under DORA complies with incident reporting requirements in other regulatory systems. Entities need to maintain consistency in their reporting procedures while dealing with variations in definitions, thresholds, and reporting methods in different jurisdictions.
- **Strategic Importance**: Mandatory reporting is essential for creating a culture of resilience in financial institutions by promoting transparency, preparedness, and ongoing enhancement. Institutions can improve their resilience and support the overall security of the financial ecosystem by incorporating incident reporting into their risk management and governance frameworks.
- **Stakeholders**: Enhancing stakeholder confidence can be achieved by showing a dedication to complying with mandatory reporting requirements outlined in DORA. Stakeholders perceive strong incident reporting and management procedures as signs of an organization's commitment to protecting its operations and their interests.

5.4.3 Thresholds for Reporting

The Digital Operational Resilience Act (DORA) establishes detailed guidelines for incident reporting in the financial sector, requiring specific criteria and thresholds to assess the importance of ICT-related incidents. This methodical approach guarantees that regulatory bodies are informed about incidents that may affect the stability and integrity of the financial system, while also avoiding an excessive number of reports on trivial or insignificant matters. It is essential for financial entities to comprehend and implement these thresholds so as to effectively meet DORA's reporting requirements.

While evaluating the importance of an incident one should identify how it affects the organization's activities. This encompasses interruptions to vital business operations, decline in services, or any hindrance to the organization's capacity to sustain operations at acceptable risk thresholds. Factors like the length of the disruption and how well backup systems or contingency plans reduced the impact are considered.

The financial consequences of an ICT-related incident are crucial in deciding whether it needs to be reported. This includes tangible financial losses from fraud, theft, or data breaches, along with additional expenses related to responding to incidents, restoring systems, and damage to reputation. The threshold for financial losses is adjusted to match the size and operational range of the entity, guaranteeing relevance and proportionality.

The risk of harm to clients, such as personal data breach, unauthorised account access, and service disruption, is a crucial consideration in the decision-making process for reporting. The framework also considers the incident's effect on other stakeholders, including third-party service providers, market participants, and the wider financial ecosystem, especially if it erodes trust or presents systemic risks.

1. **Challenges**

- Assessing incidents against DORA's multifaceted criteria can be a complex task for financial entities, especially when time is limited. This necessitates a robust incident evaluation process capable of swiftly collecting pertinent information, applying reporting criteria, and deciding on the need for notification.
- Due to the changing financial operations and the evolving cyber threat environment, the reporting thresholds may require frequent evaluation and modification. Entities need to keep up-to-date with regulatory guidance and best practices to ensure that their assessment criteria are in line with current expectations.
- Entities must thoroughly document their assessment procedures and the reasoning behind their reporting choices. This helps with regulatory compliance and readies the organisation for potential audits or inquiries from supervisory authorities concerning their incident reporting procedures.

2. **Best Practices**
   - Automated assessment tools utilise technology to streamline the initial evaluation of incidents, aiding entities in consistently and efficiently applying reporting thresholds. These tools can identify incidents that may qualify for reporting, making the decision-making process more efficient.
   - Consistent training and simulations for staff engaged in incident management can improve the entity's ability to implement reporting thresholds effectively in real-world scenarios.
   - Proactively interacting with regulatory authorities to clarify reporting thresholds and criteria can offer valuable insights and guidance, ensuring that the entity's practices align with regulatory expectations.

Setting precise criteria and thresholds for incident reporting under DORA is a well-balanced strategy to regulate notifications. This ensures that authorities are notified of important events without being overwhelmed by reports of minor incidents. To successfully navigate these thresholds, financial entities must incorporate a thorough assessment process into their incident response protocols. This will help cultivate a culture of diligence and transparency, ultimately strengthening the resilience of both the institution and the financial sector as a whole.

5.4.4 Detailed Incident Documentation

The Digital Operational Resilience Act (DORA) expands the incident reporting obligations to include providing comprehensive documentation of the incident, going beyond simple notification. This thorough documentation approach aims to give supervisory authorities a profound insight into each incident, enabling a more knowledgeable and efficient regulatory reaction. This section details the essential components of incident documentation mandated by DORA and explains their significance within the broader framework of operational resilience and regulatory adherence. [8]

The components of a detailed incident communication are outlined as the following:

- **Nature of the Incident**: Financial institutions must offer a detailed account of the incident, specifying the type of incident (such as data breach, malware attack, system outage). Comprehending the incident's nature aids authorities in assessing its potential consequences and recognising any developing patterns or trends in the financial sector. [8]

- **Affected Data and Systems**: Documentation should clearly outline the data and systems that were compromised or impacted by the incident. This involves recognising sensitive or personal information that may have been revealed and describing the essential operations or services affected. This level of detail allows for a thorough evaluation of the incident's impact on data security, customer confidentiality, and operational stability. [8]
- **Timeline of the Event**: A timeline of the event is essential, detailing the incident from detection to resolution in chronological order. The timeline should consist of significant events, such as the initial detection of the incident, the notification of authorities and affected parties, and the restoration of normal operations. Presenting a timeline aids in assessing the effectiveness and punctuality of the entity's response. [8]
- **Mitigation and Resolution**: Entities must detail the actions taken to address and resolve the incident, including immediate containment measures, long-term prevention strategies, and data recovery or system restoration efforts. This information is crucial for evaluating the entity's incident management abilities and for disseminating insights to the wider financial community. [8]
- **Impact Assessment**: In-depth documentation should incorporate an evaluation of the incident's effect on the entity's operations, financial performance, and clients. This assessment aids in determining the seriousness of the incident and directs the regulatory reaction, which may involve implementing consumer protection measures or increased supervision. [8]

Challenges and Best Practices

1. **Challenges**

- **Time & Comprehensiveness:** Striking a balance between timely reporting and comprehensive documentation presents a challenge. Financial institutions need to establish streamlined procedures to promptly collect, organise, and report comprehensive incident data.
- **Data Sensitivity:** Maintaining the confidentiality of sensitive information in incident reports necessitates thorough consideration, especially when recording impacted data and systems. Entities must comply with data protection laws and set up secure reporting channels to protect this information.
- **Dynamic Incident Environments:** The changing conditions of an incident can create difficulties in making initial evaluations and recording information. Entities are advised to submit preliminary reports, as additional documentation may be required as more information is gathered or the circumstances evolve.

2. **Best Practices**

- **Automated Documentation Tools:** Automated Documentation Tools Integrating automated tools for incident tracking and documentation can optimise the process, guaranteeing precise and efficient capture of all necessary information.
- **Pre-defined Templates:** Creating predefined templates for incident documentation according to DORA's specifications can guarantee uniformity and thoroughness in reporting.
- **Regular Training:** Training incident response teams on documentation requirements and best practices ensures that all personnel involved in incident management understand their roles in compiling and submitting detailed reports.

5.4.5 Follow-Up Reports

The Digital Operational Resilience Act (DORA) creates a detailed structure for financial institutions to report important ICT-related incidents and maintain communication with supervisory authorities by submitting follow-up reports. The reports are essential for updating the resolution of the incident, assessing the effectiveness of the response, and outlining the lessons learned and modifications made to improve future resilience. This section explores the prerequisites, objectives, and strategic consequences of follow-up reports according to DORA. [8]

- **Timely Updates**: Under DORA regulations, financial institutions must provide additional reports following the initial notification of an incident involving information and communication technology within a specified period. The reports should provide updates on current resolution efforts, modifications in impact assessment, and any new information discovered since the initial report. [8]
- **Resolution Details**: Entities are required to give a detailed report on how the incident was resolved. This encompasses the technical and operational actions implemented to rectify the underlying vulnerabilities, reinstate affected services, and fortify the systems against potential breaches. [8]
- **Effectiveness of Response**: An essential aspect of the follow-up report involves assessing the entity's effectiveness in responding to incidents. Entities need to evaluate their actions based on their timeliness, adequacy, and overall effectiveness in reducing the consequences of the incident. [8]
- **Lessons Learned**: Examining past events to learn important lessons is a crucial part of DORA's follow-up reporting mandate. Financial institutions should detail any knowledge acquired from handling the incident, such as deficiencies in current protocols, unexpected obstacles, and areas of proficiency. [8]
- **Preventive Measures**: In addition to reviewing past events, follow-up reports should include specific information about the actions taken and modifications made to avoid similar incidents in the future. This could require modifications to ICT risk management frameworks, improvements to cybersecurity defences, or revisions to business continuity plans. [8]

Challenges and Best Practices

1. **Challenges**

- Regulatory compliance reports offer supervisory authorities' important information about how well an organization's risk management and incident response practices are working. This continuous supervision guarantees that financial institutions comply with DORA's regulations and implement proactive measures to improve their ability to withstand challenges.
- Openly discussing incident resolution and post-incident improvements fosters trust with clients, investors, and regulatory bodies. It shows the entity's dedication to protecting its operations and customers from ICT risks.

2. **Best Practices**

- Conducting a comprehensive incident analysis can be challenging, especially in complex or ongoing incidents, to inform the follow-up report. Financial institutions should utilise organised incident review procedures to guarantee thorough and precise reporting.

- Establishing and maintaining open and effective communication channels with regulatory authorities is essential for submitting follow-up reports. Entities should strive to comprehend regulatory expectations thoroughly and communicate to resolve any uncertainties in reporting requirements.
- The real benefit of follow-up reports is the organization's capacity to incorporate insights and feedback from regulators into operational procedures. Organisations should create systems to turn report findings into practical enhancements.

Follow-up reports, required by DORA, are essential for completing the process of managing ICT-related incidents. They ensure financial entities are held accountable for resolving incidents and improving their defences, while also helping to strengthen the operational resilience of the financial sector. Financial entities can show their dedication to ongoing improvement and resilience against changing cyber threats by following the reporting requirements.

5.4.6 Incident Reporting Challenges and Considerations

Financial institutions must balance the need for detailed incident reports with the protection of sensitive information and confidentiality. This necessitates thoughtful evaluation of the disclosed information and the establishment of secure reporting channels. Creating streamlined reporting procedures is crucial to meet DORA's deadlines. Organisations need to allocate resources towards training, technology, and procedures to guarantee timely identification, assessment, and reporting of incidents.

International coordination of incident reporting for financial entities operating in multiple jurisdictions adds complexity due to compliance with DORA and other global regulations. Global entities must align reporting standards and practices to effectively handle their regulatory obligations.

5.5 Digital Operational Resilience Testing

The Digital Operational Resilience Act (DORA) is a significant regulatory framework designed to enhance the cybersecurity and operational reliability of the European Union's financial industry. DORA's main focus is on strict testing requirements to help financial entities identify vulnerabilities, evaluate the strength of their cyber defences, and improve their ability to withstand disruptions related to information and communication technology. The importance of a proactive cybersecurity approach is highlighted by these requirements, which necessitate a thorough set of testing exercises such as penetration testing, threat-led penetration testing (TLPT), and red teaming.

Penetration testing is mandated by DORA for financial institutions. It entails systematically simulating cyberattacks on their systems to identify vulnerabilities. This testing is crucial for identifying and resolving security vulnerabilities before they can be taken advantage of.

Threat-led Penetration Testing (TLPT) surpasses traditional penetration testing by utilising up-to-date cyber threat intelligence to replicate focused attacks. This approach aims to assess the entity's readiness and response strategies against advanced and emerging threats by replicating the methods and tactics used by real adversaries.

Red Teaming is a sophisticated method of resilience testing that includes a thorough and multi-faceted attack simulation designed to evaluate the ability of an organization's personnel, procedures, and technology to endure an attack from a genuine adversary. Red

teaming exercises aim to be highly realistic and are typically carried out covertly within an organisation to evaluate the actual preparedness of the financial entity.

5.6 Third-Party Risk Management

The Digital Operational Resilience Act (DORA) has introduced an innovative method for handling the risks related to third-party ICT service providers, acknowledging the growing reliance of financial institutions on external services for crucial operations. DORA's guidelines emphasise the need for a strong framework for third-party risk management (TPRM) to safeguard the operational resilience of financial institutions from vulnerabilities in their supply chain. [5]

5.6.1 Risk Assessment & Due Diligence

The Digital Operational Resilience Act (DORA) highlights the importance of conducting risk assessment and due diligence processes before working with third-party ICT service providers. This mandate acknowledges the increasing dependence of financial institutions on external services for crucial operations and the potential risks this dependence presents to the institution's operational resilience. DORA's requirements are designed to ensure that financial institutions consistently assess and reduce risks linked to third-party relationships. [28]

DORA’s requirements for risk assessment and due diligence are outlined as follows.

1. **Comprehensive Evaluation**: DORA requires financial institutions to conduct a thorough assessment of potential third-party service providers. This assessment covers multiple crucial areas:

- **Security Policies:** Financial institutions need to evaluate the cybersecurity policies and practices of third-party providers to ensure they match the institution's security standards and the regulatory requirements set by DORA. This involves reviewing the provider's policies regarding data protection, incident response, access controls, and encryption practices.
- **Regulatory Compliance:** Due diligence involves confirming that the third-party provider complies with relevant regulations, including DORA and other applicable laws like GDPR.[28] This guarantees that the provider complies with the most rigorous data protection and operational resilience standards.
- **Service Continuity:** Financial institutions need to assess the provider's capacity to uphold service continuity during challenging circumstances. This entails evaluating the provider's business continuity and disaster recovery strategies to verify their strength and effectiveness in reducing service interruptions during ICT-related incidents.

2. **Documented Assessments**: DORA requires that these risk assessments and due diligence processes be thoroughly documented. Financial entities must maintain records of their evaluations, including the criteria used for assessment, the findings, and the rationale for selecting a particular third-party provider. This documentation is essential for demonstrating compliance with DORA's requirements and for supporting ongoing monitoring and oversight of third-party relationships.
3. **Challenges**

- **Complexity and Resource Constraints:** Conducting thorough risk assessments and due diligence on third-party providers can be complex and resource-intensive,

necessitating specialised knowledge and expertise. Smaller financial institutions may struggle to allocate sufficient resources to conduct thorough assessments.

- **Dynamic Risk Landscape:** The fast-paced development of cyber threats and the evolving regulatory environment create difficulties in maintaining current risk assessments and due diligence procedures. Financial institutions need to regularly revise their assessment standards and procedures to incorporate emerging risks and regulatory modifications.
- **Limited Visibility:** Obtaining information about the internal workings and security measures of third-party providers can be difficult due to limited visibility. Providers may hesitate to disclose detailed information, which hinders the financial entity's capacity to perform a comprehensive risk assessment.

4. Best Practices

- Utilising External Expertise: Financial institutions can gain advantages by collaborating with cybersecurity and legal professionals who offer specialised knowledge and assistance in performing risk assessments and due diligence procedures.
- Creating standardised templates and checklists for risk assessment and due diligence can guarantee a uniform and thorough evaluation of third-party providers.
- Establishing transparency and collaboration with third-party providers can help in sharing essential information for conducting thorough risk assessments.

Under DORA, risk assessment and due diligence are essential aspects of third-party risk management for financial institutions. They aim to help identify and reduce risks linked to third-party ICT service providers through a proactive approach. Financial entities can enhance their operational resilience by carefully assessing providers' security policies, regulatory compliance, and service continuity capabilities. Overcoming obstacles by implementing best practices and utilising external expertise can improve the efficiency of these processes, in line with DORA's main goals to protect the operational integrity of the financial sector.

5.6.2 Contractual Agreements

The Digital Operational Resilience Act (DORA) emphasises the crucial need to formalise the connection between financial institutions and third-party ICT service providers through contractual agreements. These agreements are crucial for creating a precise structure for cybersecurity and operational resilience, outlining the duties and roles of both parties. DORA's provisions require contracts to adhere to high standards of data protection and system security, while also promoting a collaborative approach to managing and reducing ICT risks. [8] The key provisions in contractual agreements can be summarized as follows:

- Detailed Cybersecurity Requirements: DORA requires that contracts with third-party providers clearly outline the cybersecurity protocols that must be put in place. This involves implementing particular technologies, following cybersecurity guidelines, and meeting industry standards. The goal is to make sure that the security position of the service provider matches the requirements of the financial entity and the overall regulatory environment.
- Operational Resilience Obligations: Operational resilience obligations require contracts to specify the service provider's responsibilities in enhancing the operational resilience of the financial entity. This involves ensuring the upkeep of essential operations during challenging circumstances, establishing strong business

continuity and disaster recovery strategies, and being able to promptly and efficiently address ICT incidents.

- Data Protection and Confidentiality: DORA stresses the importance of incorporating stringent clauses regarding data protection and confidentiality in contractual agreements due to the sensitive nature of financial data. Service providers must enforce measures to guarantee the confidentiality, integrity, and availability of the financial entity's data, in accordance with relevant data protection laws.
- Incident Reporting and Communication: Contracts should outline the procedures for reporting incidents, including the deadlines for informing the financial entity about any ICT-related incidents that may affect its operations. The contracts should specify the methods for continuous communication and information exchange between the service provider and the financial entity to ensure transparency and collaboration in handling cyber risks.
- Audit and Compliance: Contractual agreements should include provisions for regular audits and assessments to allow financial entities to verify compliance with contractual obligations. This may require providing the financial entity or a designated third-party auditor with access to pertinent documentation, systems, and facilities.

1. **Challenges**

- **Flexibility**: Creating contractual agreements that are thorough yet flexible can be difficult. Financial institutions must ensure that contracts are comprehensive enough to address all essential cybersecurity and resilience needs, while also being flexible to accommodate changing threats and technological progress.
- **Negotiating**: When negotiating with third-party providers, the process can be intricate, particularly when enforcing strict cybersecurity and operational resilience requirements. Financial institutions may encounter opposition from providers who are hesitant to accept burdensome responsibilities or who have their own customary contract terms.
- **Compliance**: Ensuring that contractual agreements comply with all relevant local and international regulations can be complex for financial entities and third-party providers operating in multiple jurisdictions.

2. Best Practices

- Utilising established cybersecurity and operational resilience standards in contractual agreements can establish clear requirements and expectations.
- Engaging in open and collaborative negotiations with third-party providers can help develop mutually acceptable agreements that effectively address cybersecurity and resilience concerns.
- Regularly review and update contractual agreements to align with regulatory changes, technological advancements, and evolving cyber threats.

5.6.3 Ongoing Monitoring and Oversight

The Digital Operational Resilience Act (DORA) requires financial institutions to assess third-party ICT service providers initially and then continuously monitor and oversee them in the changing digital operational resilience environment. This dynamic approach recognises that third-party risks are subject to change due to factors such as new cyber threats, alterations in service provision, or shifts in the regulatory environment. Continuous monitoring and

supervision are essential for upholding the confidentiality, integrity, and availability of the financial entity's data and systems. [8]

1. **Mechanisms For Continuous Monitoring**: DORA mandates the establishment of systematic mechanisms to continuously monitor the performance and compliance of third-party service providers. These are:

a. **Performance against Service Levels**: Financial institutions need to consistently assess the service provider's performance in comparison to established service level agreements (SLAs). This guarantees that the provider complies with the operational and resilience standards necessary for the efficient operation of the financial entity.

b. **Compliance with Security Standards**: Continual monitoring should involve evaluating the service provider's compliance with established cybersecurity and resilience standards. This entails assessing the provider's procedures and measures to safeguard against emerging cyber threats.

2. **Adaptability & Responsiveness**: Monitoring and oversight mechanisms should be flexible to enable financial entities to promptly address any shifts in the risk profile of their third-party providers. This involves the capacity to raise concerns, review the provider's risk assessment, and, if needed, implement corrective measures or modifications to the contractual agreement.

3. **Challenges**

a. **Resource Intensity**: Consistently monitoring and supervising third-party providers can be resource-intensive, necessitating dedicated personnel, technology, and procedures. Smaller financial institutions may find it challenging to allocate enough resources to effectively meet these requirements.

b. **Information Access**: Accessing information from third-party providers to support continuous oversight can be difficult. Providers may be hesitant due to confidentiality issues or other priorities, which can obstruct the necessary information flow for effective monitoring.

c. **Third-Party Ecosystems**: Third-party ecosystems can be complex for financial entities as they interact with various providers, each offering different roles, services, and risk profiles. To manage and supervise such a varied ecosystem effectively, advanced processes and tools are necessary to guarantee thorough coverage.

4. Best Practices

a. **Leveraging Technology**: Implementing technology solutions, like third-party risk management platforms, can simplify the monitoring and oversight process. These solutions offer immediate insight into the performance and adherence to regulations of service providers, making it easier to manage third-party risks efficiently.

b. **Clear Communication Channels**: Creating clear communication channels: Establishing structured communication channels and protocols with third-party providers allows financial entities to promptly receive updates and alerts regarding any potential issues or changes in the provider's operations.

c. **Reviewing and Updating Oversight Practices**: Financial institutions should consistently review and update their monitoring and oversight practices to align with operational changes, emerging risks, and regulatory demands. This involves reviewing SLAs and contracts to guarantee their continued relevance and efficiency.

5.6.4 Incident Reporting and Information Sharing

The Digital Operational Resilience Act (DORA) emphasises the crucial need for prompt incident reporting and efficient information exchange between third-party ICT service

providers and financial entities. ICT-related incidents are essential for reducing the potential impact on financial services and operations. DORA mandates service providers to promptly notify financial entities of any events that may jeopardise the security, availability, or integrity of their services. [8]

DORA's components on third-party risk management for incident reporting includes:

- **Notification Requirement**: Third-party service providers are required by DORA to promptly notify financial entities of any ICT-related incidents that could negatively impact their services. This requirement aims to ensure that financial institutions are knowledgeable and ready to implement measures to reduce the effects of such incidents on their operations and, consequently, on their clients. [8]
- **Reportable Incidents Scope**: The reportable incidents under DORA encompass a wide variety of ICT-related events, such as cybersecurity breaches, data leaks, system outages, and service disruptions. The goal is to address any event that may affect the operational resilience of financial institutions. [8]
- **Information Sharing Protocols**: DORA promotes the creation of standardised protocols for incident reporting and sharing information. The protocols aim to simplify the communication process, guaranteeing that financial entities receive prompt and pertinent information regarding incidents. Standardisation promotes a uniform method for incident management throughout the financial sector. [8]

Incident reporting and information sharing are crucial aspects of third-party risk management according to DORA, significantly improving the operational resilience of the financial sector. DORA ensures that financial institutions are prepared to quickly respond to ICT-related incidents and reduce their impact on operations by requiring immediate notification and promoting the use of standardised reporting procedures. To address the difficulties related to incident reporting, financial institutions and third-party providers must work together, following clear guidelines, secure communication methods, and a dedication to ongoing enhancement.

1. **Challenges**

- **Reporting Threshold**: One of the challenges in implementing DORA's incident reporting requirements is establishing the threshold for defining a reportable incident. Third-party providers and financial entities must work together to define clear criteria that balance the need for prompt notification with the avoidance of unnecessary alerts that could lead to alert fatigue.
- **Confidentiality and Security**: Ensuring the confidentiality and security of shared information during incident reporting is crucial. Financial institutions and external service providers need to create secure communication channels and protocols to safeguard sensitive data while enabling the efficient transfer of incident-related information.
- **Coordination and Collaboration**: Effective incident reporting and information sharing necessitate a high level of coordination and collaboration between financial institutions and their third-party service providers. Building robust working relationships and fostering mutual trust are essential for optimising the efficiency and effectiveness of information flow.

2. **Best Practices**

- Establish precise reporting protocols: Financial institutions and third-party vendors should create explicit guidelines and contracts outlining the procedures for reporting

incidents, specifying the types of incidents to report, reporting deadlines, and report formats.
- Invest in secure communication platforms to protect sensitive information and ensure timely incident notifications for financial entities.
- Periodically review and update reporting protocols to align with changes in the threat landscape, regulatory requirements, and operational environment. This involves performing routine drills and exercises to assess the efficiency of reporting mechanisms and protocols.

5.6.5 Challenges in Implementing TPRM Strategies

Financial entities face distinct challenges when implementing Third-Party Risk Management (TPRM) strategies to comply with the Digital Operational Resilience Act (DORA). The challenges arise from the complexities of contemporary financial ecosystems, the variety of service providers, the strict regulatory compliance requirements, and the complexities of incident response coordination. It is essential for financial institutions to tackle these challenges in order to protect their operations and strengthen their ability to withstand changes in the digital environment. [5]

Complex Supply Chains

Financial institutions frequently depend on a network of third-party vendors for crucial services, such as cloud computing, data storage, payment processing, and customer support. This interdependence results in an intricate supply chain that may be challenging to control and supervise.

- **Visibility and Transparency**: Attaining complete visibility throughout the entire supply chain can be difficult, especially when subcontractors and fourth-party providers are part of the process. Insufficient transparency can conceal possible weaknesses and exposure to risks.
- **Resource Allocation**: Resource allocation involves mapping and evaluating the risk linked to each connection in the supply chain, requiring substantial resources and specialised knowledge. Financial institutions need to invest in advanced tools and highly skilled staff to efficiently handle these intricacies.

Diversity of Service Providers

Customising risk assessments to consider the distinct characteristics of each service provider necessitates a subtle strategy that harmonises comprehensiveness with feasibility.

- **Customized Risk Assessments**: Personalised risk assessments involve a detailed approach that considers the specific characteristics of each service provider, striking a balance between comprehensiveness and feasibility. [28]
- **Adaptable Contractual Agreements**: Creating flexible contractual agreements that consider the unique risks and needs of various services requires a comprehensive understanding of legal and technical aspects. [28]

Regulatory Compliance

The regulatory environment is resistant to change, necessitating continual monitoring and adjustment. Consistently monitoring the compliance status of multiple third-party providers is resource-intensive and requiresa structured approach.

Financial institutions must ensure that their third-party providers adhere to DORA and other relevant regulations, requiring a comprehensive compliance framework.

Incident Response Coordination

Efficiently coordinating incident response activities with various third-party providers is important for reducing the impact of ICT-related incidents on financial institutions. Establishing dependable and secure communication channels with third-party providers ensures prompt and efficient sharing of incident-related information as well as establishing predefined incident response protocols with third-party providers that simplify the response process and decrease the time needed to address and recover from incidents. [8]

5.7 Information Sharing and Collaboration

The Digital Operational Resilience Act (DORA) acknowledges the important role of information sharing and collaboration among financial entities in improving cybersecurity and operational resilience in the financial sector. DORA aims to create a collaborative environment where entities can enhance their defence mechanisms against ICT-related incidents by sharing insights on cyber threats, vulnerabilities, and best practices. This chapter examines the particular regulations set by DORA for sharing information and analyses how they affect the overall resilience of the sector. [28]

5.7.1 Structured Information Sharing

The Digital Operational Resilience Act (DORA) mandates the creation of structured information sharing frameworks to improve cybersecurity and operational resilience in the financial sector. The frameworks are designed as fundamental elements that facilitate the exchange of vital cybersecurity information among financial entities in an effective, standardised, and secure way. DORA aims to democratise access to crucial cybersecurity insights by facilitating this exchange, enabling entities in the financial sector to collectively strengthen their defences.

Structured frameworks streamline the sharing of cybersecurity information, reducing delays and enabling entities to promptly access and utilise relevant data. Efficiency is vital in the fast-moving field of cyber threat management, as the quickness of response can greatly affect the seriousness of an incident's result. One of the main advantages of these frameworks is the standardisation of the information exchange process. Standardisation guarantees that data exchanged between different parties follows a uniform structure, simplifying its analysis and utilisation. This consistency also enables the automation of data processing and integration into current risk management systems.

DORA prioritises structured information sharing frameworks to promote inclusivity, enabling financial entities of varying sizes and operational scopes to engage. Ensuring inclusivity is essential for creating a fair competition, particularly for smaller organisations that may not have the means to collect thorough threat intelligence on their own.

Implementation considerations should be around the development of shared platforms. Structured information sharing frameworks rely on the creation of accessible, secure, and user-friendly shared platforms for success. The platforms should be tailored to meet the requirements of the financial sector, offering features that enable information sharing, collaboration, and discussion.

It is crucial to prioritise data security and privacy when promoting the open exchange of information. Frameworks need to include strong data protection measures to protect sensitive information and adhere to regulations like the General Data Protection Regulation (GDPR).[28]

Finally, establishing precise governance structures and oversight mechanisms is also essential for effectively managing these frameworks. This involves delineating roles and duties, establishing guidelines for data sharing and utilisation, and executing procedures for overseeing and assessing the framework's influence on sector-wide resilience.

1. **Challenges**

- Balancing openness and security is crucial for effective information sharing while safeguarding sensitive data. Measures such as encryption, access controls, and anonymization techniques can be used to safeguard data integrity and enable beneficial transactions.
- Encouraging broad participation in the financial sector can be difficult, especially when it comes to involving smaller entities. Possible solutions involve providing incentives for participation, lowering entry barriers, and showcasing the concrete advantages of engaging in these systems.
- Adapting to changing cyber threats requires information sharing frameworks to be flexible and evolve continuously. Regular evaluations, revisions, and integration of input from participants are crucial to ensure the pertinence and efficiency of these frameworks.

2. **Best Practices**

- Financial institutions should cooperate to establish detailed guidelines outlining the specific information to be exchanged, the method of sharing, and procedures for addressing shared intelligence. Precise guidelines maintain uniformity and pertinence in the information shared.
- Implement secure sharing platforms using advanced technology to share information securely. The platforms should provide strong encryption, access controls, and real-time information sharing capabilities.
- Automating the process of collecting and sharing threat intelligence can enable organisations to react more quickly to new threats. Automated systems can help filter and prioritise information, making it more actionable for participants.
- Periodically review and update frameworks to ensure they reflect changes in the threat landscape, technological advancements, and regulatory requirements. This guarantees that the frameworks stay pertinent and efficient.
- Implement feedback mechanisms to allow participants to evaluate the effectiveness of the information sharing framework. Feedback can pinpoint areas needing improvement, showcase successful instances, and guarantee that the framework aligns with the changing requirements of its participants.
- Host regular training sessions and workshops to improve participants' proficiency in utilising the information sharing framework. Training will include guidelines for analysing and utilising shared intelligence, as well as procedures for sharing information.
- Emphasise the concrete advantages of actively engaging in information sharing frameworks by showcasing case studies and examples of how shared intelligence has helped prevent cyber threats. Showing successful examples can inspire individuals to participate more actively in the system.

5.7.2 Confidentiality and Data Protection

The Digital Operational Resilience Act (DORA) focuses on ensuring confidentiality and data protection when financial entities share information. The act recognises the fine line between the necessity for sharing cybersecurity information openly and the importance of safeguarding sensitive data. This chapter examines DORA's regulations that focus on maintaining the confidentiality and integrity of shared cybersecurity information, emphasising their significance in promoting a secure and trustworthy atmosphere for cooperation. [8]

Provisions for Confidentiality and Data Protection

- **Robust Data Handling Protocol**: DORA requires the enforcement of strict data handling protocols that detail the procedures for collecting, storing, processing, and sharing cybersecurity information among financial institutions. The protocols are created to safeguard sensitive information from unauthorised access, disclosure, or alteration.
- **Encryption and Anonymization**: DORA promotes the utilisation of encryption and anonymization methods to enhance the security and privacy of shared data. By obfuscating the data to unauthorised parties and eliminating personally identifiable information, these methods reduce the likelihood of data breaches and privacy infringements.
- **Access Controls**: DORA requires strict access controls to ensure that only authorised individuals within participating entities can access shared cybersecurity information. This measure is essential for preventing unintentional or intentional exposure of sensitive data.
- **Compliance with Data Protection Regulations**: The confidentiality and data protection regulations in DORA comply with broader data protection regulations like the General Data Protection Regulation (GDPR). Financial institutions must ensure that their information-sharing procedures adhere to these regulations, strengthening the safeguarding of personal data and privacy. [8] [28]

Importance of Confidentiality and Data Protection

- **Maintaining Trust**: Ensuring confidentiality and data protection is crucial for maintaining trust between financial institutions involved in sharing information. Trust is essential for successful collaboration, allowing parties to exchange important information without worrying about jeopardising their competitive advantage or revealing confidential data.
- **Preventing Additional Risks**: DORA's provisions help prevent participants from being exposed to additional cybersecurity risks by ensuring the confidentiality and integrity of shared information. This pertains to the possibility of data breaches caused by mishandling or unauthorised access to shared cybersecurity information.
- **Fostering Sector-wide Resilience**: Promoting across the entire sector Resilience is enhanced in the face of cyber threats when financial institutions can securely and confidently share information. Preserving confidentiality and data security allows for the sharing of important information about new risks, weaknesses, and effective strategies within the industry, ultimately improving its ability to withstand challenges.

Challenges and Best Practices

- Ensuring sufficient protection is a key challenge, as confidentiality and data protection measures need to continuously adapt to keep up with changing cyber threats and technological progress. Financial institutions need to regularly assess and enhance their data protection protocols to tackle emerging vulnerabilities.
- Finding the optimal equilibrium between promoting information sharing and protecting sensitive data necessitates thoughtful deliberation. Entities should adopt a tiered strategy for sharing information, adjusting the level of data security according to the sensitivity of the information.
- Encouraging a culture of security awareness and compliance among all participants is crucial for the success of confidentiality and data protection efforts. Consistent training, transparent policy communication, and implementing accountability measures can improve compliance with data protection protocols.

The confidentiality and data protection rules in DORA are crucial for facilitating secure and efficient information exchange among financial institutions. DORA enhances trust and collaboration in the financial sector by implementing strong measures to protect the confidentiality and integrity of shared cybersecurity information, thus aiding in the collective endeavour to improve digital operational resilience. By addressing data protection challenges and following best practices, financial entities can benefit from information sharing while reducing the risks of data exposure.

5.7.3 Sector-wide Collaboration

The Digital Operational Resilience Act (DORA) broadens its focus on cybersecurity and operational resilience in the financial sector to include collaboration across the entire sector, going beyond individual entities and regulatory requirements. DORA advocates for active collaboration among financial entities, regulatory bodies, and cybersecurity experts to enhance the financial system's resilience against cyber threats. This chapter examines the different ways in which this collaboration could manifest and its importance in developing a stronger financial ecosystem.

Forms of Sector-wide Collaboration

- **Joint Exercises:** DORA promotes the organisation of collaborative cybersecurity drills that replicate genuine cyber threats. These exercises aim to assess the financial sector's ability to respond collectively, pinpoint any preparedness deficiencies, and enhance coordination mechanisms by involving various financial entities and regulatory bodies.
- **Workshops and Training Programs:** Workshops and training programs facilitate the exchange of knowledge and the development of skills among financial institutions and cybersecurity experts. These initiatives will concentrate on new cyber threats, effective practices in cyber cleanliness, and the most recent advancements in cybersecurity technologies and methodologies.
- **Development of Collective Response Strategies:** DORA encourages the creation of collective response strategies to cyber threats by acknowledging the interconnectedness of the financial sector. This involves creating standardised procedures for responding to incidents, sharing information, and recovering from them, to guarantee a unified and effective response across the entire sector.
- **Public-Private Partnerships:** DORA emphasises fostering collaborations between the public sector (regulatory bodies and government agencies) and private sector

(financial entities and cybersecurity firms) through Public-Private Partnerships. These collaborations can utilise the strengths and resources of both sectors to improve the financial system's overall resilience.

Significance of Sector-wide Collaboration

- **Enhanced Collective Intelligence:** Collaboration enables the sharing of knowledge and resources, resulting in a better understanding of cyber threats and defence strategies. Having a common understanding is essential for outsmarting cyber enemies and safeguarding the critical infrastructure of the sector.
- **Strengthened Incident Response:** Financial entities and their partners can collaborate to create stronger incident response procedures, decreasing the time needed to address and bounce back from cyber incidents. This collaborative method of incident management greatly reduces the potential impact on the financial system.
- **Trust and Confidence:** Collaboration fosters trust among financial institutions, regulatory authorities, and the general public. The financial sector can enhance consumer confidence in its ability to protect financial stability by presenting a unified stance against cyber threats.

Challenges & Best Practices

- **Ensuring Participation:** Encouraging active involvement from all pertinent stakeholders, particularly smaller financial entities, can be difficult. To tackle this challenge, strategies involve providing incentives for participation and emphasising the advantages of collaboration.
- **Maintaining Security and Confidentiality:** Ensuring security and confidentiality is crucial while promoting collaboration in an open environment. By implementing secure communication channels and establishing clear guidelines for information sharing, these risks can be reduced.
- **Effectiveness:** To ensure that collaborative efforts are producing tangible improvements in resilience, it is crucial to set metrics and benchmarks to measure the effectiveness of these initiatives. Periodic evaluations and feedback systems can improve and strengthen cooperative projects.

5.7.4 Significance of Information Sharing and Collaboration

Information sharing and collaboration are crucial in the digital operational resilience landscape. The Digital Operational Resilience Act (DORA) promotes a culture of open communication between financial entities, regulatory bodies, and cybersecurity experts. This chapter explores how information sharing and collaboration through DORA improve situational awareness, speed up incident response, and encourage best practices in the financial sector.

Financial entities share information to combine their understanding of cyber threats, creating a collective intelligence. This intelligence is crucial for comprehending the characteristics, strategies, methods, and protocols of possible opponents. By gaining a deeper understanding of potential risks and weaknesses, financial institutions can proactively approach cybersecurity. This involves proactive preparation for potential attacks to enhance preventative measures and decrease the chances of successful breaches, rather than just reacting to incidents as they happen.

By sharing information, aggregated data can improve the accuracy and dynamism of sector-wide risk assessments. This assessment helps identify systemic vulnerabilities and prioritise efforts to address them, thus enhancing the sector's overall resilience. Collaboration promotes a synchronised strategy for addressing ICT-related incidents. Financial entities can enhance their incident response strategies and recovery techniques by exchanging insights and expertise, leading to a more cohesive and efficient sector-wide response.

Furthermore, swift communication of information about current or developing situations enables organisations to react promptly. This can greatly decrease the time needed to control and lessen the effects of cyberattacks, thus reducing operational interruptions and financial damages.

Collective defence mechanisms can be established through information sharing and collaboration, resulting in shared threat intelligence platforms and joint cybersecurity task forces. These mechanisms improve the sector's capacity to identify, react to, and recover from cyber incidents.

Best Practices

- **Repository of Knowledge**: Information sharing platforms store accumulated knowledge, including valuable insights on effective cybersecurity measures, incident management strategies, and recovery processes. This knowledge base is a valuable resource for financial institutions looking to improve their ability to withstand cyber threats.
- **Continuous Improvement Cycle**: Access to shared best practices and lessons learned allows financial entities to participate in a continuous improvement cycle. Entities can compare their practices with those of their peers, pinpoint areas for improvement, and make changes to enhance their cybersecurity and operational resilience.
- **Standardization**: Standardisation of cybersecurity practices in the financial sector can be achieved through the exchange of best practices and collaboration over time. Standardisation enhances the sector's security by increasing the complexity for cyber adversaries to exploit vulnerabilities.

Information sharing and collaboration, as emphasised in DORA, play a crucial role in enhancing the digital operational resilience of the financial sector. These initiatives aim to improve situational awareness, speed up incident response, and encourage the implementation of best practices to establish a more secure, resilient, and collaborative financial ecosystem. The combined knowledge and organised actions of the sector help reduce the effects of cyber threats and enhance the stability and integrity of the financial system.

5.8 Comparative Analysis with Other Frameworks

The Digital Operational Resilience Act (DORA) is a major regulatory measure aimed at improving the cybersecurity and operational resilience of the financial sector in the European Union. Nevertheless, DORA is not the sole framework created to tackle these crucial areas. This chapter compares DORA with two other well-known frameworks: the Network and Information Systems (NIS) Directive and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The analysis will compare and contrast the frameworks, emphasising their distinct characteristics and implications for financial institutions.

5.8.1 DORA and NIS2 Directive

Within the European Union's legislative framework focused on strengthening digital operational resilience and cybersecurity, two prominent frameworks are the Digital Operational Resilience Act (DORA) and the revised Network and Information Systems (NIS2) Directive. Each framework aims to improve cybersecurity and resilience but targets different audiences with unique requirements and enforcement mechanisms. This study compares DORA and the NIS2 Directive, examining their implications for the financial sector and other areas. [7][8]

DORA is a regulation tailored for the financial sector in the European Union. It aims to ensure that financial entities such as banks, insurance companies, and investment firms are prepared to handle, endure, and bounce back from ICT-related disruptions. The act clearly defines requirements for ICT risk management, resilience testing (including penetration testing and threat-led penetration testing), third-party risk management, and thorough incident reporting. This focused strategy aims to strengthen the cybersecurity stance and operational resilience of financial institutions, ensuring they are ready to effectively address ICT risks. [7][8]

The NIS2 Directive expands cybersecurity and resilience efforts to include a broader range of essential sectors such as energy, transport, health, and digital infrastructure. NIS2 aims to enhance cybersecurity standards in critical sectors by mandating entities to implement suitable technical and organisational measures for risk management and to report significant cybersecurity incidents. The NIS2 Directive stands out for its flexibility, permitting member states to adjust the implementation specifics and enforcement methods to align with the distinct requirements and cybersecurity maturity levels of each sector and state. [7][8]

DORA creates a consistent regulatory structure for the financial industry in the EU, including detailed compliance requirements and consequences for failing to comply. This standardised method guarantees a uniform level of cybersecurity and resilience among European financial institutions. The enforcement mechanism of the NIS2 Directive provides member states with greater autonomy, recognising the varied cybersecurity environments within the EU. The flexibility in the NIS2 Directive is intended to cater to the diverse sectors it encompasses, enabling a customised strategy to improve resilience. [7][8]

While DORA and the NIS2 Directive share the goal of strengthening cybersecurity and operational resilience, they differ significantly in their scopes, focus areas, and enforcement approaches. DORA provides a tailored, directive structure specifically designed for the financial industry, guaranteeing that these organisations possess the necessary resources and directives to effectively manage ICT risks. The NIS2 Directive offers a comprehensive and flexible framework to enhance cybersecurity standards in various critical sectors, focusing on adaptability and customised implementation by individual states. It is crucial for organisations in the EU to comprehend these differences as they deal with the challenges of compliance and work to improve their cybersecurity and operational resilience in a more digital environment. [7][8]

5.8.2 DORA and NIST Cybersecurity Framework

Digital Operational Resilience Act (DORA) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework refer to managing cybersecurity risks and improving operational resilience, especially in the financial industry. DORA provides

regulations for financial entities in the EU, while the NIST Cybersecurity Framework offers voluntary standards, guidelines, and best practices for organisations worldwide. [8][15]

DORA takes a prescriptive approach by requiring financial entities to implement specific actions and controls to ensure a high level of regulatory compliance. The directive mandates that all financial institutions under its jurisdiction comply with a standardised level of cybersecurity and operational resilience, specifically targeting the distinct risks and obstacles encountered by the industry. NIST Cybersecurity Framework is voluntary and offers adaptable guidelines for organisations to customise to their specific situations. This flexibility permits a broad spectrum of customisation, allowing organisations to adapt their cybersecurity practices to their specific needs and risk profiles, promoting a risk-based approach to cybersecurity management. [8][15]

When compared to the NIST Cybersecurity Framework, DORA's requirements may be viewed as complementary due to the framework's flexibility and wide relevance. Institutions can use the flexibility of the NIST Framework to enhance their cybersecurity and resilience practices by addressing areas not explicitly covered by DORA and incorporating globally recognised best practices. [8][15]

Financial entities must consider strategic factors beyond just complying with DORA regulations, like evaluating how DORA's requirements align or differ from other cybersecurity frameworks, such as the NIST Framework. This strategic approach allows financial institutions to meet regulatory requirements and establish a strong cybersecurity framework based on international best practices and standards. [8][15]

A comparison of DORA and NIST Cybersecurity shows the different strategies they use to improve cybersecurity and operational resilience in the financial industry. DORA establishes strict regulations for EU financial entities, while the NIST Framework provides adaptable guidelines that are voluntary and applicable worldwide. Financial institutions must comprehend the relationship between DORA and the NIST Framework to effectively navigate the intricate cybersecurity environment, maintain regulatory adherence, and implement a comprehensive strategy for managing cybersecurity risks. [8][15]

5.8.3 Comparative Overview of the Frameworks

This analysis compares the distinct focus, prerequisites, and relevance of DORA, the NIS2 Directive, and the NIST Cybersecurity Framework. DORA provides specific requirements for the EU financial sector, while the NIS2 Directive takes a more comprehensive approach to improving cybersecurity in essential services within the EU. The NIST Cybersecurity Framework is globally applicable, flexible, and voluntary, complementing regulatory frameworks such as DORA and sector-specific directives like NIS2. Comprehending the intricacies of these frameworks enables financial institutions and other organisations to better manage their cybersecurity and resilience efforts by utilising the strengths of each framework to improve their overall cybersecurity position.

Feature	DORA	NIS2 Directive	NIST Cybersecurity Framework
Scope & Target Audience	Focuses on the financial sector of the EU, such as banks, insurance companies, and other financial entities.	Encompasses a wide variety of crucial and digital service providers in various sectors within the EU.	Voluntary and universally applicable to all industries, providing recommendations for enhancing cybersecurity risk management.
Risk Management	Demands specialised ICT risk management strategies designed for the financial industry, including precise measures for evaluating and reducing risks.	Requires specific technical and organisational strategies for managing risks in different sectors, allowing for some adaptability in how they are put into practice.	Offers a collection of optimal methods and principles for recognising, evaluating, and handling cybersecurity threats, which can be customised to suit an organization's requirements.
Testing & Audits	Requires regular resilience testing, such as penetration and threat-based penetration testing, tailored to financial institutions.	Advocates for security audits and testing to establish a foundational level of security without specifying particular types.	Suggests regular evaluations and audits as part of its ongoing enhancement process, without requiring particular types of testing.
Incident Reporting	Enforces specific mandatory reporting rules for significant ICT-related incidents in the financial sector.	Requires the reporting of important cyber incidents, with the criteria for importance differing among member states.	Encourages the sharing of information regarding cybersecurity incidents and vulnerabilities but does not have compulsory reporting obligations.
Third-Party Risk Management	Outlines requirements for financial institutions to oversee risks associated with third-party ICT service providers, involving thorough investigation and ongoing supervision.	Offers broad advice on handling third-party risks and ensuring supply chain security, with less specific instructions compared to DORA.	Provides direction on recognising and handling third-party risks within a comprehensive risk management structure that can be customised by organisations.
Regulatory Compliance & Oversight	Imposes particular regulatory measures to ensure compliance in the EU financial sector, with explicit penalties for non-compliance.	Comprehensive structure for security and resilience, where member states establish specific requirements and mechanisms for enforcement.	Primarily utilised as a best practice framework, compliance is driven by organisational policy or sector-specific regulations rather than direct enforcement.
Global vs. EU-centric approach	EU-centric, with a focus on standardising regulations within the EU's financial industry.	EU-focused, with the goal of raising cybersecurity standards in key sectors within the EU.	Universally applicable, utilised by organisations globally to direct cybersecurity risk management endeavours in different sectors.

Table 1 Comparison of Frameworks

6. Development and Explanation of the Assessment Tool

The DORA Assessment Tool has been created to assist financial institutions in understanding and adhering to these extensive regulations. It is designed to offer an organised way to evaluate financial entities' compliance to the extensive requirements established by DORA. It is flexible to accommodate the specific operational contexts and risk profiles of various entities in the financial sector, such as banks, investment firms, insurance companies, and other financial services providers.

The tool is designed to be user-friendly, making it accessible to individuals with different levels of expertise in compliance and digital operational resilience. It offers clear instructions, an intuitive design, and a logical flow that systematically leads users through the assessment process.

The tool covers various domains such as ICT risk management, incident reporting, digital operational resilience testing, and third-party risk management to meet all of DORA's requirements. The questionnaire is comprehensive and examines each area to ensure a thorough evaluation of all relevant aspects of DORA compliance. The usage of the tool is crucial in helping financial entities prepare to meet and surpass the digital operational resilience standards outlined by DORA by aiding in a thorough comprehension of its requirements and offering a structured assessment framework.

Overall, its user-friendly, comprehensive, and adaptable design shapes an asset for financial institutions to effectively manage digital risks and enhance the resilience of the financial sector.

6.1 Objective and Scope

The DORA Assessment Tool is carefully designed to improve digital operational resilience in the financial sector. Financial entities can assess their compliance with the Digital Operational Resilience Act (DORA) principles by using a standardised format. The tool helps organisations identify strengths and weaknesses in their digital operations, enabling them to make specific improvements and meet regulatory standards.

6.1.1 Tool Composition

The tool consists of multiple separate sheets, each intended to serve specific functions during the assessment process.

- **Instructions & Scope**: This section is a detailed guide for users on how to effectively use the tool. The instructions provide guidance on navigating the tool's various sections, enabling users to effectively utilise its features for precise assessment of their compliance status. The Scoping part is crucial for assessing whether DORA is relevant to the specific entity. It aids in determining if the entity complies entirely, partially, or not at all with DORA regulations. This initial stage is essential for customising the evaluation process to the particular requirements and legal responsibilities of the organisation.
- **Questionnaire & Scoring**: The central component of the tool is the Questionnaire & Scoring sheet, which includes a set of questions that correspond to DORA's compliance standards. This section assesses the entity's adherence to different areas including ICT risk management, incident reporting, and third-party risk management.

The scoring mechanism enables a detailed evaluation, emphasising areas of adherence and areas needing improvement.

- **Dashboard**: The Dashboard visually summarises the assessment outcomes, showing the entity's maturity levels in various DORA domains. The tool combines the scores from the Questionnaire & Scoring section to provide a quick overview of the organization's digital operational resilience status.

6.1.2 Appendices

Aside from the primary sections, the tool also contains appendices that offer additional context and assistance for the assessment process.

- Appendix – Score: The appendix provides definitions and explanations for terms and concepts used in the tool to ensure a shared understanding of the criteria and methodology used in the assessment.

6.1.3 Guidelines

The tool is designed for a wide variety of stakeholders in financial institutions, such as compliance officers, risk managers, and IT security professionals. Users are advised to participate in a collaborative assessment process by consulting with appropriate internal stakeholders to accurately establish the weightings in the Dashboard. They should then fill out the response section of the Questionnaire & Scoring tab based on interviews and material review.

6.2 Instructions and Scoping

This chapter explores the first steps in using the DORA Assessment Tool, crucial for financial institutions seeking to comply with the Digital Operational Resilience Act (DORA). The approach involves guiding users on how to effectively use the tool and outlining the scoping process to determine the entity's compliance requirements under DORA.

The tool comes with a detailed instruction sheet that is carefully crafted to familiarise users with its features and proper use. These instructions are crucial for users to effectively use the tool and promote a standardised approach to DORA compliance evaluation in different financial entities. The instructions cover key aspects.

An overview is given to introduce users to the tool's objectives, particularly its role in aiding a structured evaluation against DORA's principles for ensuring digital operational resilience in the financial sector.

Detailed navigational tips are provided to assist users in smoothly moving between various sections of the tool. This involves instructions for accessing and interpreting various sheets like the Questionnaire & Scoring and Dashboard, improving the user's capacity to effectively oversee the assessment process. The tool provides explicit instructions for inputting data, responding to questionnaire items, and comprehending the scoring system. This guarantees uniformity in data input, facilitating precise evaluation results.

The scoping section is crucial for assessing the pertinence and suitability of DORA for the financial entity being considered. It is crucial to customise the assessment to the entity's specific context, following DORA's personal scope criteria. The process includes:

Organisations follow a detailed checklist to determine their responsibilities and tasks as outlined in DORA. This assessment is essential for classifying entities based on the regulation's scope, helping to identify relevant DORA requirements. Entities are categorised as fully in scope, partially in scope, or not in scope of DORA based on the results of the personal scope assessment.

This classification determines the level of compliance requirements that apply to the entity.

- **Fully in scope**: Entities that are required to comply with all of DORA's regulations.
- **Partially in scope**: Entities that must adhere to DORA's regulations, but with some exceptions from particular requirements.
- **Out of Scope**: Entities that are not subject to DORA's regulations and are therefore not required to comply with its provisions.

The tool offers crucial guidance to help entities interpret their scope classification. This involves taking into account complex operational situations that could impact the organization's compliance path under DORA, to ensure a clear grasp of regulatory responsibilities.

6.3 Questionnaire and Scoring

The Questionnaire & Scoring section is the focal point of the DORA Assessment Tool, designed with great care to assess a financial entity's compliance with the detailed regulations of the Digital Operational Resilience Act (DORA). This crucial part of the tool consists of a wide range of questions carefully spread out throughout different DORA chapters. Each question is designed to assess the thoroughness and effectiveness of the entity's compliance strategies in specific areas of digital operational resilience.

Structure and Content

The questionnaire is designed to encompass various essential areas for digital operational resilience, such as governance, ICT risk management frameworks, systems, protocols, tools, and incident management processes. The questions in each category are designed to closely reflect the specific requirements outlined in DORA, guaranteeing that the assessment thoroughly evaluates the entity's compliance status.

- **Governance and Organization:** Questions in this area evaluate the internal governance structures of the entity and how well they manage ICT risks.
- **ICT Risk Management Framework:** This area evaluates the organization's structures for overseeing ICT risks, encompassing policies, protocols, and the comprehensive risk management approach.
- **ICT Systems, Protocols, and Tools:** This section assesses the dependability, capability, and robustness of the organization's ICT systems and the protocols that regulate their operation.
- **Identification and Protection:** This section explores the entity's ability to identify ICT-related business functions, assets, and the measures in place to protect them.
- **Detection, Response, and Recovery:** The questions centre on the entity's methods for identifying ICT-related incidents, as well as its strategies for responding to and recovering from them.

- **Backup Policies and Recovery Methods:** Assessment of backup policies and recovery methods evaluates the organization's procedures for data backup and system recovery.

Scoring Mechanism

The scoring system, in accordance with the European Banking Authority (EBA) guidelines on scoring for SREP IT, provides a detailed method for assessing the entity's maturity level in the evaluated areas. The scoring scale ranges from 1 to 4.

1 (Best Controls in Place): Signifies a highly developed level of control, with risks effectively reduced and no expected need for additional investment.

2 (Generally Operating Effectively): Indicates that controls are mostly effective throughout the organisation, with potential for further improvement.

3 (Some Controls in Place but Not Fully): Indicates that controls are not consistently implemented throughout the entity, indicating areas that require enhancement.

4 (No Controls in Place): Indicates an absence of efficient controls and an urgent requirement for implementing mitigation measures.

Evaluation and Reporting

The questionnaire responses are recorded and evaluated based on the maturity scale to enable a detailed analysis of the organization's operational resilience. The scoring results help create a comprehensive evaluation, offering a complete perspective on the entity's adherence to DORA's requirements. This thorough assessment identifies strengths and critical gaps, helping organisations prioritise improvements to strengthen their digital operational resilience.

The Questionnaire & Scoring section plays a crucial role in offering a strict, standardised approach to evaluating financial entities based on DORA requirements. By using thorough inquiries and a systematic evaluation system, it provides valuable information about the organization's adherence status, which helps enhance digital operational resilience practices. Conducting a thorough assessment is crucial for organisations to comply with DORA regulations and maintain operational integrity in the digital era.

6.4 Dashboard

The Dashboard section of the DORA Assessment Tool provides a visually appealing and easy-to-understand overview of a financial entity's compliance maturity with the Digital Operational Resilience Act (DORA). This section acts as a crucial analytical tool, offering entities a thorough overview of their performance in key domains necessary for maintaining digital operational resilience.

The Dashboard contains carefully designed graphs and charts that visually compare the entity's performance scores with the maximum potential scores in each assessed domain. This comparison is crucial for clearly identifying the entity's strengths and areas that need improvement. The domains encompass Governance and Organisation, ICT Risk Management Framework, ICT Systems, Protocols, and Tools, among others, demonstrating the tool's thorough approach to evaluating digital operational resilience.

- **Graphical Representations:** Graphical representations such as bar graphs or pie charts are used to compare the current compliance level of each domain with the ideal state specified by DORA's requirements.
- **Performance Analysis:** Color-coded indicators offer instant visual signals regarding compliance levels, where green represents strong compliance, yellow signifies moderate compliance, and red points out areas requiring substantial improvement.
- **Weighted Scores:** The Dashboard displays both raw scores and the weighted scores for each domain, providing a detailed view of the entity's overall compliance status. This scoring system assigns different weights to domains based on their importance within the entity's operational and risk management framework.

The Dashboard goes beyond basic compliance tracking; it serves as a strategic tool that guides decision-making processes. Providing a clear visualisation of compliance maturity allows senior management and compliance officers to make informed decisions on resource allocation to improve digital operational resilience.

Identifying Compliance Gaps: The Dashboard's visual design facilitates the identification of compliance gaps in domains where the entity does not meet DORA's requirements, allowing for focused interventions.

Improvements: The Dashboard helps prioritise improvement efforts by identifying areas of weak compliance, ensuring resources are directed towards areas with the highest potential impact on the entity's operational resilience.

Progress Over Time: The Dashboard serves as both a current status overview and a tool for monitoring progress over time. Organisations can utilise it to assess the efficiency of their compliance initiatives and adapt strategies in accordance with changing regulatory requirements and cyber threat environments.

The Dashboard in the DORA Assessment Tool is crucial for financial institutions as it provides a dynamic and insightful summary of their digital operational resilience. By providing visual representations, it simplifies the complex DORA compliance landscape and empowers entities with actionable insights for strategic planning and decision-making in maintaining digital operational resilience in the financial sector.

6.5 Appendix: Maturity Rating Definition

The Appendix of the DORA Assessment Tool is crucial for standardising the evaluation process by clearly defining the maturity ratings used in the assessment. This section ensures that assessors possess a uniform comprehension of how to interpret and implement the maturity levels to the entity's IT risk controls, which greatly enhances the tool's overall consistency and reliability.

The appendix presents a structured framework for maturity ratings, dividing them into four distinct levels. The description of each level provides explicit criteria to assist assessors in evaluating the efficacy of an IT risk controls within a financial entity. The levels vary from the highest maturity, signifying well-established and mature controls, to the lowest maturity, where controls are either absent or ineffective.

Level 1 (Best Controls in Place): Indicates a high level of control maturity, with well-established controls that require only regular maintenance, and no additional investment is

anticipated or planned. This level indicates that the entity has surpassed standard compliance requirements, showing outstanding operational resilience.

Level 2 (Generally Operating Effectively): Level 2 signifies that controls are generally functioning effectively and consistently throughout the organisation. Risks are mostly reduced, with room for additional enhancement or optimisation.

Level 3 (Some Controls in Place): Indicates a situation where some controls exist, but they are not uniformly implemented throughout the entire organisation. There is an acknowledged necessity for enhancement, and despite ongoing mitigation projects, risks have not been completely reduced.

Level 4 (No Controls in Place): Indicates a situation where controls are absent or ineffective in reducing risks. Identified mitigation activities have not yet started and require immediate attention.

The appendix provides detailed criteria for determining a maturity level, such as the thoroughness of controls, their incorporation into the organization's risk management system, uniformity of implementation across various areas and sites, and the organization's preparedness to respond to new threats and regulatory modifications.

Criteria A to J: Criteria A to J each address a distinct aspect of IT risk control, ranging from the organization's governance structure and policy compliance to the efficiency of incident response procedures and the strength of IT infrastructure.

Concluding, the appendix improves the tool's effectiveness in evaluating compliance with DORA's requirements by offering a standardised rating system, which promotes consistent interpretation of maturity levels in various assessments. It helps in understanding a financial entity's operational resilience by defining maturity levels and criteria. This guidance assists in making targeted improvements and strategic decisions to enhance digital resilience in the financial sector.

6.6 Usage and Implementation

The last section of the DORA Assessment Tool documentation offers a comprehensive manual on how to practically apply and implement the tool in financial institutions. It covers the process from first using the tool to fully understanding and implementing its results.

1. **Preliminary Journey:** The assessment process starts by comprehensively understanding the Instructions and Scoping sheets, which establish the basis for a methodical assessment process. Organisations are instructed on how to precisely define their scope under DORA, ensuring that the evaluation is customised to their particular regulatory requirements and operational circumstances.
2. **Conducting the Assessment:** The central focus of the implementation process is the comprehensive Questionnaire & Scoring sheet. Organisations should approach this stage with careful attention to detail, making sure that each question is answered with honesty and backed up by documentary evidence whenever feasible. This stage is crucial for pinpointing strengths and possible weaknesses in the entity's operational resilience framework.
3. **Scoring and Evaluation:** After finishing the questionnaire, entities receive guidance on accurately applying the scoring mechanism. The scoring, in accordance with the European Banking Authority's guidelines, offers a detailed comprehension of the

entity's maturity levels in different areas. This process is crucial for pinpointing areas that need to be improved and invested in.

4. **Dashboard Analysis:** The Dashboard provides a visual and quantitative analysis of the entity's operational resilience posture, summarising the assessment process. Entities are instructed on how to analyse the dashboard metrics, specifically comparing scores to maximum potential scores, in order to obtain practical insights into their operational resilience status.
5. **Flexibility and Adaptability:** The tool's implementation guidance stands out for its focus on flexibility and adaptability. The tool is created to cater to the varied terrain of the financial sector, ranging from large multinational corporations to smaller, specialised entities. This adaptability ensures that the tool stays relevant and useful in various sectors, offering value regardless of the entity's size or complexity.

The tool is highlighted as more than just a compliance task, but as a strategic tool for improving digital operational resilience. By following the tool's guidelines diligently, financial institutions can comply with regulations and enhance their operational resilience in the face of growing digital risks.

7. Application of the Tool

This exemplary application of the tool aims to show how financial institutions can use this tool in order to align their digital operational resilience practices with the guidelines of the framework. It is demonstrated how entities can evaluate their compliance status, pinpoint areas for enhancement, and strengthen their resilience against ICT risks through a step-by-step analysis of a hypothetical scenario using the tool.

The case study focuses on "Bank X," a fictional financial institution operating in the European Union. This organisation provides various digital financial services such as online banking, mobile payments, and digital asset management. Bank X heavily depends on Information and Communication Technologies (ICT) to provide its services. Bank X must prioritize ensuring digital operational resilience due to the critical role of ICT in its business model and the rising frequency and complexity of cyber threats.

Bank X faces distinctive challenges and opportunities in achieving DORA compliance within its operational context. This case study will examine how Bank X uses the DORA Assessment Tool to assess its practices against DORA's requirements and make essential enhancements to strengthen its digital resilience.

7.1 Preparation Phase

Bank X considers the preparation phase crucial for successfully implementing the DORA Assessment Tool in its operations. This phase prepares the entity for a thorough assessment of its digital operational resilience practices according to DORA requirements. Bank X's approach during the preparation phase is outlined in the following steps:

1. **Team Formation:** Bank X began by forming a specialised assessment team made up of individuals from key departments essential to the bank's ICT and digital operational resilience strategies. The team consisted of members from various fields such as IT, cybersecurity, risk management, compliance, and business operations. The goal was to guarantee that the assessment encompassed all pertinent aspects of the bank's operations, utilising the knowledge of specialists from various domains.
2. **Tool Customization:** Bank X customised the DORA Assessment Tool to suit its specific needs, considering the unique aspects of its operational environment. This required modifying the tool's settings to align with the bank's organisational hierarchy, complexity of its ICT infrastructure, and the characteristics of its digital financial services. The tool's flexible design guided the customisation process, enabling the assessment team to tailor the questionnaire and scoring metrics to accurately reflect the bank's operational realities.
3. **Preliminary Data Collection:** Bank X conducted a preliminary data collection exercise before starting the assessment to gather all necessary information for the tool. This step entailed gathering information on the bank's ICT systems, cybersecurity protocols, third-party service provider agreements, and current risk management strategies. The objective was to provide the assessment team with thorough and current information to enable a precise evaluation based on DORA's criteria.
4. **Initial Scoping:** During the preparation phase, a vital step was the initial scoping exercise to assess how various DORA requirements applied to Bank X's operations. The team utilised the Scoping section of the tool to evaluate the pertinent aspects of DORA for the bank, taking into account its size, operational complexity, and exposure

to ICT risks. This step assisted in concentrating the assessment on the most relevant and impactful areas, guaranteeing an effective and focused evaluation process.

Bank X established a strong groundwork for effectively implementing the DORA Assessment Tool through these preparatory measures. The bank prepared itself to thoroughly assess its digital operational resilience by assembling a skilled team, customising the tool, collecting necessary data, and conducting initial scoping.

7.2 Conducting the Assessment

Bank X conducted a comprehensive evaluation of its compliance with the Digital Operational Resilience Act (DORA) using a structured Questionnaire & Scoring sheet from the DORA Assessment Tool. This chapter outlines the procedures for conducting the assessment, highlighting the collaborative approach used to guarantee thoroughness and precision in the evaluation.

7.2.1 Utilizing the Questionnaire & Scoring Sheet

The use of the Questionnaire & Scoring Sheet was crucial for Bank X's evaluation process to assess its digital operational resilience in compliance with the Digital Operational Resilience Act (DORA) requirements. This thorough part of the tool included a variety of questions carefully crafted to evaluate the organization's readiness and ability to handle ICT-related risks and to measure the strength of its digital operational infrastructure.

The questions covered important topics like governance structures, risk management policies, ICT system integrity and security, and the efficiency of incident detection, response, and recovery strategies. We examined each domain to assess how Bank X's practices conformed to industry best practices and regulatory requirements. For example, in the governance sector, inquiries were made to ascertain the extent of senior management's participation in supervising ICT risks. In the ICT systems field, questions were focused on evaluating the robustness and dependability of the technological infrastructure that sustains the bank's activities.

The Bank X team interacted with various departments and teams throughout the organisation to conduct a thorough assessment. This interdisciplinary cooperation was crucial for collecting precise information and providing the necessary evidence to respond thoroughly to the questionnaire. IT departments offered expertise on the technical components of ICT systems and security protocols. On the other hand, the risk management team provided information about the frameworks and processes used to recognise and reduce ICT risks.

This collaborative method not only helped gather pertinent data but also enhanced comprehension of digital operational resilience throughout the organisation. The assessment identified strengths in areas with effective controls and practices and identified areas needing improvement to enhance the entity's resilience.

The scoring system was vital in this assessment process. The assessment team could quantitatively measure Bank X's operational resilience capabilities by assigning maturity ratings according to the European Banking Authority's guidelines. The objective scoring system offered a precise and actionable analysis of the bank's current situation, facilitating the pinpointing of particular areas in need of focus and funding.

Furthermore, this thorough assessment emphasised the significance of a comprehensive and unified strategy for overseeing digital operational resilience. Bank X developed a thorough understanding of its resilience posture by methodically addressing each question and interacting with various parts of the organisation. This enabled the bank to lay the foundation for specific improvements and strategic enhancements in its operational resilience framework.

7.2.2 Engagement with Department and Teams

Interacting with departments and teams was a fundamental aspect of the assessment process at Bank X, highlighting the complex nature of digital operational resilience. This project required a collaborative approach involving various departments such as IT, cybersecurity, risk management, compliance, business continuity planning, and third-party vendor management. The wide-ranging collaboration was based on two critical objectives.

Gathering Necessary Information and Evidence: Collating detailed information and evidence from the various departments involved was crucial to ensure the accuracy and reliability of the assessment. The data needed was comprehensive, covering cybersecurity measures, risk management policies, compliance records, business continuity and disaster recovery plans, third-party service agreements, and audits of ICT systems and controls. Every department provided distinct perspectives and information, creating a thorough overview of the bank's digital resilience framework. This thorough collection process was essential for comprehensively addressing all aspects of the bank's digital operational environment, including technical safeguards, procedural frameworks, governance structures, and external partnerships.

Validation of Responses: The engagement process went beyond just collecting data, providing a strong validation mechanism for the gathered information. The assessment team verified the accuracy and completeness of the responses by directly interacting and collaborating with the respective departments. This phase included examining written evidence, interviewing important staff members, and comparing information from various sources. This thorough validation process guaranteed that the assessment's conclusions were grounded in accurate and current information, and accurately represented the real practices and controls at Bank X.

These interactions were a valuable opportunity for sharing knowledge and raising awareness within the bank. Departments developed a better understanding of the significance of digital operational resilience and the contribution of their functions through participation in the assessment process. This promoted a culture of resilience, emphasising interconnections and promoting a more cohesive strategy for handling digital risks.

The assessment's collaborative process revealed gaps and inconsistencies in the bank's resilience framework that may not have been obvious in a more isolated approach. Bank X improved its digital operational resilience by combining various viewpoints and expertise, leading to a more detailed understanding. This enabled the bank to make specific enhancements and strategic improvements to strengthen its resilience against cyber threats.

7.3 Scoring & Analysis

Scoring and Analysis played a crucial role in implementing the DORA Assessment Tool at Bank X, involving the detailed process of scoring each domain according to the

questionnaire responses. This chapter explores the intricacies of the scoring system and the following analysis of the results, providing insight into the bank's operational resilience environment.

7.3.1 Scoring Mechanism

The scoring system, closely following the European Banking Authority's guidelines, provided a systematic approach to assess Bank X's practices in various areas including governance, ICT risk management, identification, protection, detection, response, and recovery. Each questionnaire response was rated for maturity on a scale from "1" (best controls) to "4" (lack of controls) based on the effectiveness and comprehensiveness of the controls and practices.

Score 1: Bank X was found to have highly developed, established controls that did not necessitate immediate investment or major alterations.

Score 2: Proposed mostly efficient measures with slight room for enhancement or fine-tuning.

Score 3: Indicates inconsistent controls throughout the organisation, indicating a requirement for substantial improvement or continuous mitigation efforts.

Score 4: Identified areas lacking controls, labelled them as critical gaps needing immediate attention and action.

7.3.2 Analysis of Results

The analysis phase extracted detailed insights from the scoring, providing a thorough view of Bank X's digital operational resilience. The dashboard, a crucial element of the tool, displayed the scores from various domains visually, making it simple to compare them with the maximum possible scores. This highlighted Bank X's strengths and identified areas that require immediate enhancement.

Bank X showed exceptional controls in various areas, particularly in governance and identification, aligning closely with DORA's rigorous standards. The areas were characterised by established policies, clearly defined roles and responsibilities, and strong mechanisms for identifying ICT-related risks.

On the other hand, the evaluation revealed areas that require substantial improvement. The areas of response and recovery, as well as protection and prevention measures, received lower scores, suggesting a requirement for a more organised strategy and the adoption of stronger controls to effectively reduce ICT risks.

Bank X found the scoring and analysis phase to be essential for gaining a precise, data-based insight into its digital operational resilience status. Bank X could enhance its resilience in the digital financial landscape by identifying strengths, areas for improvement, prioritising actions, allocating resources effectively, and charting a strategic path. This focused analysis created a plan for ongoing enhancement, guaranteeing that Bank X stays adaptable and quick to respond to the changing digital operational resilience needs.

7.4 Dashboard Review

The Dashboard Review section in the DORA Assessment Tool application at Bank X is a crucial element that converts raw data collected during the assessment phase into practical

insights. This chapter thoroughly examines the dashboard's output, explaining the visual representations and scores, and clarifying how these insights inform decisions about operational resilience strategies.

7.4.1 Interpreting Dashboard Outputs

The dashboard visually displays Bank X's performance in key areas crucial to digital operational resilience, with a focus on clarity and impact. The dashboard uses graphs and charts to compare actual scores with maximum potential scores for various domains, including governance, ICT risk management framework, and response and recovery strategies.

Visual Representations: The colour of each domain corresponds to its score: green for excellent performance (score of 1), yellow for areas needing attention (scores of 2 and 3), and red for critical improvement required (score of 4). This color-coding system highlights areas of concern and excellence, making it easier to interpret and act upon quickly.

Score Interpretation: The dashboard provides a numerical and graphical representation of Bank X's operational resilience posture by quantifying the maturity levels across different domains. Domains with lower scores are identified for immediate attention, while higher-scoring areas are acknowledged as strengths. This scoring system also enables trend analysis over time, enabling Bank X to monitor its advancements in improving digital operational resilience.

7.4.2 Utilizing Dashboard Insights

The information obtained from the dashboard plays a crucial role in guiding Bank X's strategic decisions regarding operational resilience. The dashboard offers a detailed yet easily understandable summary of the bank's resilience landscape, acting as a basis for discussions among senior management and different departments.

The dashboard insights inform strategic planning, prioritise investments, and allocate resources to areas needing immediate attention. If the response and recovery domain scores low, Bank X may choose to allocate additional resources to enhance the development of strong incident response plans.

The dashboard provides visual and numerical data that support the improvement of Bank X's operational resilience strategies. The bank can utilise best practices in other areas by recognising strengths. On the other hand, pinpointing areas that need improvement allows for specific action plans to be implemented, such as training, policy revisions, and infrastructure upgrades, in order to strengthen weaker areas.

Finally, the dashboard enables a process of ongoing enhancement. Bank X can monitor the effectiveness of implemented measures, adapt strategies to emerging threats, and ensure resilience measures evolve by reviewing dashboard outputs regularly to keep up with the changing digital landscape of the financial sector. For Bank X, these insights are not just reflective but also serve as a catalyst for developing and implementing proactive strategies, ensuring that the bank not only meets but surpasses the standards established by DORA for digital operational resilience.

7.5 Action Plan Development

After conducting a thorough evaluation of Bank X's digital operational resilience with the DORA Assessment Tool, the subsequent crucial step was to create a focused action plan. This chapter outlines the systematic approach taken by Bank X to develop an action plan, highlighting the importance of prioritising actions according to risk, impact, and regulatory urgency identified in the assessment.

7.5.1 Formulating the Action Plan

The action plan was initiated by conducting a thorough analysis of the assessment results, specifically targeting domains and areas that required improvement or showed a risk of non-compliance with DORA regulations. The process was comprehensive, engaging essential stakeholders from IT, risk management, compliance, and business units to guarantee a well-rounded approach to resolving the identified deficiencies.

The initial step required creating a list of all actions needed to rectify the identified weaknesses or non-compliance issues. This encompassed both short-term solutions for pressing issues and long-term strategies to improve resilience. Specific tasks were defined for each identified action, such as developing or revising policies, enhancing controls, implementing new technologies, or providing additional training for staff. Every action was clearly described, including objectives, anticipated results, and the departments or teams in charge of carrying it out.

7.5.2 Prioritizing Actions

Due to the extensive range of digital operational resilience and limited resources, it became crucial to prioritise actions. Bank X utilised a risk-based strategy to prioritise initiatives based on their potential impact on the bank's operations and the urgency imposed by regulatory requirements.

Risk and Impact Assessment: Actions were assessed according to the potential risk they pose to Bank X's operations and their impact on the bank's ability to sustain operational continuity. Actions that focused on critical vulnerabilities or directly impacted customer services and compliance with DORA mandates were given greater priority.

Regulatory: Compliance requirements outlined in DORA influenced the prioritisation, with a primary focus on areas that have a direct impact on regulatory compliance. Actions that filled regulatory gaps or were essential for meeting DORA's strict requirements were prioritised in the action plan.

7.5.3 Action Plan Implementation

Bank X began implementing the action plan with a structured and phased approach to ensure efficient execution and minimal disruption to ongoing operations.

Timeline and Milestones: A timeline with specific milestones and deadlines was created to guide the implementation of the action plan. This aided in monitoring advancement and guaranteeing responsibility.

Resource Allocation: Resource allocation involved distributing resources such as budget, personnel, and technology according to the prioritisation of tasks. This guaranteed that crucial areas obtained the required assistance for prompt and efficient correction.

Monitoring and Reporting: A system for ongoing monitoring of the action plan's execution was established, enabling frequent reporting to senior management and modifications as required in response to emerging risks or challenges.

Implementing the action plan at Bank X was crucial for improving its digital operational resilience in compliance with DORA regulations. Bank X strengthened its defences against digital operational threats by prioritising actions according to risk, impact, and regulatory urgency, ensuring a focused and efficient approach. This helped safeguard its operations and maintain trust with customers and stakeholders.

7.6 Future Perspectives

Implementing the DORA Assessment Tool at Bank X improved the institution's compliance with the Digital Operational Resilience Act and established a stronger digital operational framework. The DORA Assessment Tool is expected to experience increased utilisation and incorporation in the future as the financial sector adapts to technological advancements and regulatory changes. This chapter delves into the future possibilities of the tool, taking into account potential updates to regulations, shifts in the operational landscape, and the incorporation of other risk management frameworks or technologies.

7.6.1 Adapting to Regulatory Updates

In the rapidly changing realm of digital finance, regulatory frameworks are dynamic and regularly revised to adapt to new risks and technological progress. The Digital Operational Resilience Act (DORA) is a framework created to enhance the digital resilience of the financial sector in response to growing cyber threats and IT difficulties. Regulatory bodies must update and refine their guidelines and requirements to ensure they are effective and relevant as threats evolve and new technologies emerge.

The DORA Assessment Tool is designed with flexibility and adaptability to ensure alignment with regulatory changes. This design philosophy guarantees that financial institutions can quickly adapt to new regulatory requirements or interpretations upon their introduction. The developers of the tool promise to consistently update its content and features by utilising regulatory change logs, industry feedback, and firsthand experiences from its use in different financial institutions.

These updates not only respond to regulatory changes but also integrate enhancements from user feedback to improve the tool's usability and effectiveness. The tool's developers can improve it by interacting with a community of users, such as compliance officers, risk managers, and IT security professionals. This helps identify areas for enhancement, simplification, or expansion to ensure the tool complies with current regulations and prepares for future needs.

Furthermore, the tool's adaptability goes beyond regulatory compliance. It is created to smoothly blend with current risk management frameworks and operational resilience strategies in financial institutions. This integration capability enables a comprehensive approach to operational resilience, ensuring that regulatory compliance is integrated into the broader operational and risk management practices of the entity, rather than being isolated.

The DORA Assessment Tool will adapt in parallel with the changing digital finance landscape, incorporating new technologies, services, and operational models. The ongoing development of the instrument will be guided by a proactive approach to regulatory

monitoring, user feedback, and technological trends to ensure it remains essential for financial entities aiming to achieve and maintain digital operational resilience in a complex and interconnected financial ecosystem.

7.6.2 Operational Environment Changes

Financial institutions' digital operational environment is rapidly changing due to technological advancements, complex cyber threats, and shifts in business practices. The DORA Assessment Tool must be dynamic and adaptable to remain effective and relevant. This requires a proactive approach to tool development that foresees upcoming challenges and includes mechanisms to tackle them.

Future improvements to the tool could involve creating specific modules designed to assess the entity's ability to withstand emerging threats. The emergence of quantum computing brings about opportunities and challenges, which could make current encryption methods outdated. The tool could also be enhanced to evaluate vulnerabilities to advanced persistent threats that utilise various methods to secretly penetrate financial systems.

Furthermore, the incorporation of advanced technologies like artificial intelligence and blockchain into financial processes is quickly revolutionising the industry. These technologies provide substantial advantages such as increased efficiency, enhanced security, and new opportunities for innovation in products and services. Nevertheless, they also bring about new hazards and intricacies. Future versions of the DORA Assessment Tool could incorporate criteria to evaluate the adoption and management of technologies, ensuring that their implementation enhances operational resilience and strengthens defence against digital threats.

Adapting the tool to match alterations in the operational environment is essential for preserving its effectiveness. It ensures that financial institutions can comply with existing regulations and effectively manage risks related to new technologies and changing cyber threats to protect their operations and the overall financial system.

7.6.3 Integration with Other Risk Management Framework

Integrating digital operational resilience tools with comprehensive risk management frameworks and technologies significantly boosts their effectiveness. This method offers a more thorough understanding of an organization's risk environment and ability to recover from challenges. It is increasingly acknowledged that aligning tools like the DORA Assessment Tool with established risk management standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the ISO/IEC 27000 series for information security management, or sector-specific guidelines, is valuable. This integration enables a comprehensive risk management approach that covers digital operational resilience and broader organisational risks.

This integration has the potential to combine the strengths of each framework to create a strong, multi-layered defence against various threats. The NIST Framework's emphasis on identifying, protecting, detecting, responding, and recovering from cybersecurity risks aligns well with the DORA Assessment Tool's thorough assessment of financial institutions' digital resilience. The ISO/IEC 27000 standards focus on information security management systems, offering a systematic method for securing and overseeing digital assets, in line with the goals of digital operational resilience.

Future versions of the DORA Assessment Tool could be created to easily combine with these frameworks by providing templates or modules that align directly with their controls and best practices. This would not only simplify compliance efforts but also improve strategic risk management planning. Financial entities can optimise their investments in cybersecurity and resilience by gaining a comprehensive understanding of risks and controls. This approach helps ensure compliance with regulations and prepares them to address the changing digital threat environment.

7.6.4 Leveraging New Technologies

Incorporating new technologies into assessment tools is a frontier for innovation and improvement. Applying machine learning algorithms is a revolutionary method for handling and examining the large datasets found in digital operations. The algorithms can quickly analyse data to identify patterns that may suggest emerging vulnerabilities or areas needing attention. This predictive ability enables organisations to address potential vulnerabilities before they are taken advantage of.

Moreover, implementing blockchain technology offers a new approach for securely storing and sharing assessment results. Utilising blockchain's decentralised, immutable, and transparent characteristics, assessment outcomes can be distributed to pertinent parties in a way that promotes trust and collaboration. This technology improves data security and enables a clear audit trail of actions taken in response to assessment findings.

Integrating these technologies into the DORA Assessment Tool or comparable platforms can greatly enhance the efficiency and effectiveness of digital operational resilience assessments. Machine learning can expedite assessments by reducing time and resources, while blockchain can simplify reporting and compliance processes by accurately recording and making all actions accessible.

As these technologies advance, incorporating them into digital operational resilience frameworks has the potential to transform how organisations evaluate and control their digital risks. This proactive strategy will not only stay up-to-date with the fast evolution of digital risks but also utilise the most recent technological progress to protect financial transactions.

7.6.5 Latest Updates and Framework Improvements

The ongoing development of the Digital Operational Resilience Act (DORA) demonstrates the European Union's proactive approach to protecting its financial sector from various digital risks. The recent updates to DORA demonstrate a keen awareness of the evolving cyber threats, growing reliance on digital technologies, and the interconnectivity of global financial markets. The updates aim to strengthen the resilience of financial entities and keep the regulatory framework up-to-date with technological advancements and emerging challenges.

DORA is increasing its scrutiny on third-party service providers in the financial ecosystem due to their expanding role in providing crucial IT services and infrastructure. Recent updates have aimed to fix possible weaknesses caused by these providers, acknowledging that a single point of failure could have extensive consequences throughout the financial sector. Future revisions will further explore the governance, risk management practices, and operational resilience of these providers. This may require establishing more detailed criteria for risk assessments, improving oversight mechanisms, and setting clearer guidelines for

operational and contractual relationships between financial entities and their service providers.

DORA's framework has made a notable progress by incorporating environmental factors into the operational resilience strategy. This reflects the EU's comprehensive sustainable finance agenda, acknowledging that digital operations are also vulnerable to environmental risks. In the future, updates may mandate financial entities to assess and reduce the environmental effects of their digital activities. This involves ensuring data centres are energy-efficient, advocating for the use of renewable energy sources, and creating disaster recovery plans that take into account environmental disasters. DORA aims to integrate sustainability into the foundation of digital operational resilience to promote a financial sector that is strong, prepared for the future, and in line with the EU's environmental goals.

The recent updates to DORA emphasise the significance of cross-border and cross-sector collaboration in effectively addressing cyber threats. The framework promotes the exchange of threat intelligence, optimal practices, and resilience strategies among EU member states, financial institutions, and other involved parties. This collaborative strategy is crucial for establishing a cohesive defence system against cyber threats that transcend national or sectoral borders. In the future, DORA may enhance collaboration by creating shared platforms for information exchange, conducting joint resilience testing exercises, and establishing coordinated response protocols.

DORA's updates demonstrate a forward-thinking approach that anticipates future challenges in the rapidly changing digital environment. The framework is expected to adapt to address advanced threats, such as those posed by emerging technologies like quantum computing, on encryption and cybersecurity. DORA's adaptability allows it to stay relevant and effective amidst rapid changes in digital operations and cyber threats.

The recent enhancements and expected future advancements to DORA showcase the EU's dedication to upholding a robust, environmentally friendly, and cooperative financial sector in the era of digitalization. DORA ensures that the European financial sector can confidently and securely navigate the complexities of the digital world by keeping up with technological advancements and adhering to broader EU policies on sustainability and cooperation.

8. DORA Updates

In 2023, the European Supervisory Authorities (EBA, EIOPA, and ESMA) took a major step towards implementing the Digital Operational Resilience Act (DORA) by starting a public consultation on the initial set of policy products. This initiative comprises four draft Regulatory Technical Standards (RTS) and one set of draft Implementing Technical Standards (ITS). The standards aim to establish a unified legal framework that emphasises ICT risk management, reporting of significant ICT-related incidents, and management of ICT third-party risks. The consultation period will end on September 11, 2023, and a public hearing will be held via webinar on July 13, 2023. [25]

DORA, which became effective on January 16, 2023, with an application starting on January 17, 2025, aims to enhance the digital operational resilience of organisations in the EU financial industry. The legislation requires the ESAs to create a total of 13 policy tools in two groups to guarantee a uniform and unified strategy throughout the EU. [25]

The initial set of technical standards was submitted on January 17, 2024 [25], and consists of:

- Comparing an RTS on ICT risk management framework with a simplified ICT risk management framework.
- RTS on criteria for categorising ICT-related incidents.
- ITS is to create the templates for the information registry.
- RTS to define the policy regarding ICT services carried out by third-party ICT providers.

This update is a crucial advancement in regulations, designed to ensure that financial institutions have strong systems in place to handle and reduce ICT risks efficiently. Implementing these standards is a crucial advancement in strengthening the EU's financial sector's resilience in the face of changing digital risks and challenges. [25]

8.1 Regulatory Framework Enhancements

The 2023 revisions to the Digital Operational Resilience Act (DORA) represent a notable progression in the European Union's strategy to safeguard the resilience of its financial sector from ICT risks. The European Supervisory Authorities (ESAs), including the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA), have introduced updates through public consultations to establish the framework for digital operational resilience in the financial sector. [8][25]

The initial set of policy products within DORA comprises draft regulatory technical standards (RTS) and implementing technical standards (ITS). The documents concentrate on critical elements like ICT risk management, significant ICT-related incident reporting, and ICT third-party risk management. The ESAs aim to standardise requirements throughout the EU to ensure that financial entities have a clear and consistent set of guidelines for improving their digital operational resilience. [8][25]

The second set of policy mandates expands the scope of DORA to include incident reporting, guidelines on aggregated costs and losses from major incidents, and details on subcontracting critical or important functions. This batch also deals with the necessity for harmonisation in oversight practices and collaboration between national competent

authorities and the ESAs. The Regulatory Technical Standards on Threat-Led Penetration Testing (TLPT) emphasise the significance of actively and dynamically testing financial institutions' ICT systems against real cyber threats. [8][25]

The updates demonstrate the EU's proactive approach to dealing with the changing landscape of ICT risks, such as cyber threats, system failures, and third-party dependencies. The EU is continuously improving and expanding the DORA framework to safeguard the financial sector from disruptions and boost its competitiveness and innovation capacity. By prioritising a harmonised approach, financial entities of all sizes and operational scopes in the EU can benefit from a fair and equal competitive environment, which helps strengthen and fortify the financial ecosystem. [8][25]

Updating the DORA Assessment Tool requires a thorough examination of new requirements and standards to maintain its relevance and compliance with current regulations. This iterative process helps financial institutions evaluate their compliance with DORA and enhance their digital operational resilience practices. [8][25]

8.2 Revised Requirements for DORA

Financial entities must comprehend and adjust to these revisions as they directly affect risk management practices and operational strategies.

The most recent updates to DORA, as of late 2022 and continuing into 2023, have focused on enhancing a thorough framework designed to strengthen the ICT security of financial institutions throughout the EU. DORA aims to guarantee that financial institutions are capable of enduring, reacting to, and recovering from ICT-related disruptions and threats. This goal is accomplished by establishing consistent standards for the security of network and information systems that underpin the business operations of these entities. [8][25]

Key aspects covered by the revised requirements include:

- ICT Risk Management: Enhancements in ICT risk management involve assigning new duties to the board of directors to create and authorise the Digital Operational Resilience Strategy (DORS), establishing specific data protection policies, and implementing an ICT governance framework for communication, collaboration, and coordination. [8][25]
- ICT-Related Incident Reporting: Updates to ICT-related Incident Reporting streamline the reporting process, with a focus on major ICT incidents. This shift aims to lessen the reporting workload for financial entities while ensuring that important cyber threats and operational disruptions are effectively communicated to regulatory authorities. [8][25]
- Digital Operational Resilience Testing: ICT Management The amendments highlight the significance of evaluating and controlling risks linked to third-party ICT service providers. Financial institutions must perform concentration risk evaluations for outsourcing agreements, especially those involving crucial or significant operations. [8][25]

DORA is applicable to various financial entities and also covers regulations that apply to third-party ICT service providers, showing a significant impact on the operational resilience of the financial sector. The changes to DORA highlight the changing digital finance environment and the growing focus on cybersecurity and operational resilience. [8][25]

Financial institutions need to carefully track these changes and incorporate the updated requirements into their risk management frameworks and operational strategies to comply with regulations and protect against ICT-related risks.

8.3 Changes to ICT Risk Management Obligations

The Digital Operational Resilience Act (DORA) implemented various improvements to the regulatory structure for financial institutions in the European Union in 2023, with a specific emphasis on bolstering digital operational resilience. Financial entities must meet specific obligations regarding Information and Communications Technology (ICT) risk management to ensure they can successfully endure, address, and bounce back from ICT-related disruptions and threats. [8][25]

Key Updates to ICT Risk Management Obligations:

- **Governance and Organization**: Financial institutions must create a strong internal governance and control system to efficiently handle ICT risks. Management body is to oversee ICT risk, emphasising the crucial role of leadership in promoting digital operational resilience.
- **ICT Risk Management Framework**: Entities are required to create a thorough ICT risk management framework that includes identifying all ICT risk sources, safeguarding ICT systems, detecting abnormal activities, and establishing response and recovery plans and procedures. This framework is essential for the ongoing learning and development of the organization's digital operational resilience capabilities. [8][25]
- **Incident Management, Classification, and Reporting**: A formalised process for managing and reporting significant ICT-related incidents is required, necessitating entities to monitor, manage, and report such incidents to the relevant authorities. DORA outlines specific criteria that should be met, which include evaluating incident's geographical impact, criticality of the affected services, and the duration of the incident. [8][25]
- **Digital Operational Resilience Testing**: The DORA requires the establishment of a digital operational resilience testing programme that encompasses various tests like vulnerability assessments, gap analyses, and network security assessments. The programme needs to be balanced and based on risk, with critical ICT systems being tested annually. Furthermore, specific financial institutions are mandated to conduct advanced threat-focused penetration testing at least once every three years. [8][25]
- **Managing ICT Third-Party Risk**: The act stresses the significance of managing ICT third-party risk as a fundamental element of the overall ICT risk management framework. Financial institutions must create a risk management strategy, keep a record of all contracts with ICT third-party service providers, and perform thorough pre-contracting analyses. [8][25]

8.3.1 Strategies for Alignment

Financial entities should adhere to these revised obligations by reinforcing the governance frameworks related to ICT risk management by establishing clear lines of responsibility and accountability as well as by revising ICT risk management frameworks to encompass all elements specified by DORA, incorporating advanced testing methodologies. [6][10]

Furthermore, entities should be establish or enhance ICT-related incident management procedures to facilitate prompt identification, categorization, and reporting of incidents. Entities should perform comprehensive evaluations of third-party service providers, emphasising their importance and the related risks, and revise contractual agreements as necessary. [6][10]

Financial entities can greatly enhance their resilience against ICT risks by following these increased obligations, which will help ensure stability and continuity in their operations. [6][10]

8.4 Updates on Incident Reporting Mechanisms

In 2023, DORA implemented enhancements to its incident reporting systems that focus on a systematic and stringent method for financial institutions to handle, categorise, and report ICT-related incidents. The changes are intended to improve digital operational resilience in the financial sector by ensuring that financial entities have strong mechanisms to detect, manage, notify, and reduce the effects of ICT-related incidents. [8][25]

The updated framework mandates financial entities to create and execute thorough ICT-related incident management processes. This involves documenting all ICT-related incidents and important cyber threats, creating protocols for continuous and unified monitoring, managing responses to incidents, and performing root cause analyses to avoid future occurrences. The emphasis is on encouraging companies to actively participate in change programmes in order to effectively manage and reduce risks. [8][25]

The updates also establish specific classification systems for ICT-related incidents, mandating financial institutions to evaluate incidents according to criteria such as the number of affected transactions, clients, financial counterparts, reputational impact, duration, geographical reach, data losses, and economic consequences. This classification system enables a detailed comprehension of the severity and potential consequences of incidents. [8][25]

Financial entities must now report significant ICT-related incidents to the appropriate competent authorities using designated templates and within specified deadlines. This involves submitting initial notifications, interim reports, and final reports that outline the impact of the incident and the actions taken to resolve it. The reporting requirements aim to enhance transparency and facilitate prompt responses to significant incidents. [8][25]

For more information about incident management, classification, and reporting requirements under DORA, consult the detailed articles by Fieldfisher and Pinsent Masons. The sources offer detailed information on the regulatory framework, emphasising the practical consequences for financial institutions and third-party ICT service providers. [8][25]

8.5 Enhanced Focus on Third-Party ICT Service Providers

The 2023 updates to the Digital Operational Resilience Act (DORA) have brought important improvements, particularly in the areas of ICT and third-party risk management, as well as the categorization of ICT-related incidents. The ESAs, which consist of EBA, EIOPA, and ESMA, have released the initial final draft technical standards to enhance the digital operational resilience of the EU financial sector. These updates are essential for financial institutions and third-party ICT service providers as they specify the necessary measures for enhancing ICT risk management frameworks, incident reporting frameworks, and policies

for ICT services offered by third parties. In 2023, DORA implemented enhancements to its incident reporting systems that focus on a systematic and stringent method for financial institutions to handle, categorise, and report ICT-related incidents. The changes are intended to improve digital operational resilience in the financial sector by ensuring that financial entities have strong mechanisms to detect, manage, notify, and reduce the effects of ICT-related incidents. [8][25]

The updated framework mandates financial entities to create and execute thorough ICT-related incident management processes. This involves documenting all ICT-related incidents and important cyber threats, creating protocols for continuous and unified monitoring, managing responses to incidents, and performing root cause analyses to avoid future occurrences. The emphasis is on encouraging companies to actively participate in change programmes in order to effectively manage and reduce risks. [8][25]

The updates also establish specific classification systems for ICT-related incidents, mandating financial institutions to evaluate incidents according to criteria such as the number of affected transactions, clients, financial counterparts, reputational impact, duration, geographical reach, data losses, and economic consequences. This classification system enables a detailed comprehension of the severity and potential consequences of incidents. [8][25]

Financial entities must now report significant ICT-related incidents to the appropriate competent authorities using designated templates and within specified deadlines. This involves submitting initial notifications, interim reports, and final reports that outline the impact of the incident and the actions taken to resolve it. The reporting requirements aim to enhance transparency and facilitate prompt responses to significant incidents. [8][25]

For more information about incident management, classification, and reporting requirements under DORA, consult the detailed articles by Fieldfisher and Pinsent Masons. The sources offer detailed information on the regulatory framework, emphasising the practical consequences for financial institutions and third-party ICT service providers. [8][25]

Key components of the updates include:

- Regulatory Technical Standards (RTS) provide a standardised approach to tools, methods, processes, and policies for managing ICT risks across financial sectors. This involves a streamlined ICT risk management framework designed for smaller entities with lower risk, size, and complexity. [8][25]
- Requesting the criteria for classifying ICT-related incidents, particularly focusing on the method for categorising major incidents, such as materiality thresholds and criteria for evaluating significant cyber threats. [8][25]
- RTS on Information and Communication Technology third-party provider policy emphasises governance arrangements, risk management, and internal control frameworks that financial entities must uphold during contractual arrangements with ICT third-party providers. [8][25]
- Developing Technical Standards (ITS) to create templates for the information register, crucial for overseeing ICT third-party risk in financial entities and ensuring compliance with DORA by competent authorities and ESAs. [8][25]

The updates aim to help financial entities maintain control over their operational risks, information security, and business continuity while working with ICT third-party service

providers. For additional information regarding these updates, please refer to the European Banking Authority's announcement.

8.6 Adjustments to Digital Operational Resilience Testing

The modifications highlight a more organised and strict method for testing the resilience of ICT systems in financial institutions. The main highlights from the most recent updates and insights on DORA's testing requirements are as follows:

- The updates require microenterprises to conduct security tests in a way that is proportionate to their resources and level of risk. This suggests a flexible strategy that takes into account the size of operations and the importance of the information assets and services offered.
- Annual testing is mandatory for financial institutions to assess all Information and Communication Technology (ICT) systems and applications that are essential for critical or important operations. This requirement highlights the significance of frequent evaluations to guarantee the strength of systems crucial to the financial sector's operation.
- DORA requires conducting advanced threat-led penetration testing (TLPT) every three years on critical infrastructure and services. Financial entities must involve certified and experienced testers, both internal and external. The advanced testing is designed to reveal vulnerabilities that could be targeted by sophisticated cyber threats.
- The updates mandate the inclusion of third-party ICT service providers in the scope of TLPT, acknowledging their important role in the financial ecosystem. This guarantees that the resilience testing encompasses all essential services, including those that are delegated to third parties.
- DORA introduces pooled testing, which enables a single TLPT to cover services offered by a third-party to multiple financial entities. This provision aims to simplify the testing process and ensure a thorough evaluation of services crucial to multiple entities.

The modifications made to digital operational resilience testing under DORA demonstrate a dedication to upholding elevated levels of cyber resilience in the financial industry. The updates aim to strengthen the financial sector against evolving cyber threats by focusing on regular, advanced testing, utilising third-party services, and incorporating external threat intelligence.

9. Conclusion and Recommendations

9.1 Conclusion

The enactment of the Digital Operational Resilience Act (DORA) is a major step in improving the digital operational resilience of financial institutions in the European Union. DORA aims to reduce ICT risks, enhance incident management and reporting, and bolster the financial sector's resilience to digital threats through robust regulatory frameworks and technical standards.

The continuous updates and improvements to DORA demonstrate how digital risks are constantly changing and how regulatory authorities are dedicated to adjusting to new challenges. DORA offers financial institutions a systematic method for handling ICT risks, ensuring adherence to regulations, and improving operational resilience through well-defined guidelines and responsibilities.

Financial institutions need to adopt these changes and adjust their risk management practices, incident response protocols, and third-party oversight mechanisms to comply with DORA's requirements. By doing this, they can promote a culture that emphasises resilience, adaptability, and proactive risk management, ensuring the security of their operations and preserving trust with stakeholders.

9.2 Recommendations

Following the DORA analysis, the following recommendations are suggested:

1. **Continuous Compliance Monitoring:** Implement strong systems to monitor regulatory changes and maintain compliance with evolving DORA standards. This involves keeping up-to-date with new policy products, technical standards, and guidelines released by the European Supervisory Authorities (ESAs).
2. **Enhanced Risk Management Practices:** Improve ICT risk management by integrating best practices for DORA compliance, performing frequent risk assessments, and investing in cybersecurity capabilities. Involve management and supervisors in the risk handling procedure.
3. **Investment in Incident Response Capabilities:** Invest in incident response capabilities to improve incident management and reporting for quick identification, evaluation, and mitigation of ICT-related incidents. Create thorough incident response plans, perform frequent drills and simulations, and set up transparent communication channels with regulatory authorities.
4. **Third-Party Risk Management:** Establish strong oversight measures for third-party ICT service providers, such as conducting due diligence assessments, creating contractual agreements, and continuously monitoring performance and compliance. Ensure that third-party risk management strategies comply with DORA requirements.
5. **Adoption of Advanced Testing practices:** Implement advanced testing methodologies like threat-led penetration testing (TLPT) to evaluate the robustness of crucial ICT systems and applications. Work with certified testers and utilise external threat intelligence to detect and resolve vulnerabilities in a proactive manner.
6. **Cross-Sector Collaboration:** Promote collaboration and information exchange between financial institutions, regulatory authorities, and industry stakeholders to tackle shared challenges and new risks. Engage in industry forums, working groups,

and initiatives focused on enhancing cyber resilience and implementing best practices.

7. **Investment in Training and Awareness:** Implement continuous training and awareness programmes to educate employees on cybersecurity risks, incident response procedures, and compliance obligations under DORA. Promote a culture that prioritises security awareness and accountability throughout the organisation.
8. **Continuous Improvement:** Embrace a culture of continuous improvement and adaptability to effectively address evolving digital threats and regulatory requirements. Periodically assess and revise policies, procedures, and controls in response to insights gained, industry advancements, and regulatory modifications.

Financial institutions can enhance their digital operational resilience, reduce risks, and comply with DORA regulations by implementing these suggestions. Financial entities can protect their operations, customer data, and maintain trust in the financial system by addressing digital risks and improving resilience capabilities.

Appendix

Abbreviation	Definition
DORA	Digital Operational Resilience Act
EU	European Union
ICT	Information and Communication Technology
ESAs	European Supervisory Authorities
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ESMA	European Securities and Markets Authority
RTS	Regulatory Technical Standards
ITS	Implementing Technical Standards
TPRM	Third-Party Risk Management
TLPT	Threat-Led Penetration Testing
NIST	National Institute of Standards and Technology
GDPR	General Data Protection Regulation
PCI DSS	Payment Card Industry Data Security Standard
DORS	Digital Operational Resilience Strategy
Global vs. EU-centric approach	Universally applicable, utilised by organisations globally to direct cybersecurity risk management endeavours in different sectors.

References

[1] AIMA (n.d.). *Digital Operational Resilience Act ('DORA')*. [online] www.aima.org. Available at: https://www.aima.org/regulation/keytopics/digital-operational-resilience-act.html.

[2] Anon, (n.d.). *European Parliament, & Council of the European Union. (2022). Regulation (EU) 2022/2024 of the European Parliament and of the Council on Digital Operational Resilience for the Financial Sector (Digital Operational Resilience Act)* .

[3] Atzema, H. (n.d.). *What can we expect from the Digital Operational Resilience Act*. [online] Deloitte Netherlands. Available at: https://www2.deloitte.com/nl/nl/pages/risk/articles/digital-operational-resilience-act.html.

[4] Clifford Chance. (2022). *DORA: Exploring what the new European Framework for Digital Operational Resilience means for your business*. [online] Available at: https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/11/dora-exploring-european-framework-for-digital-operational-resilience.html [Accessed 25 Feb. 2024].

[5] Downes, S.F.T. reporter S. (2023). *DORA to drive significant change to TPRM, says Acuiti*. [online] www.securitiesfinancetimes.com. Available at: https://www.securitiesfinancetimes.com/securitieslendingnews/regulationarticle.php?article_id=226662&navigationaction=regulationnews&newssection=regulation [Accessed 25 Feb. 2024].

[6] EY Luxemburg (n.d.). *Digital Operational Resilience Act (DORA)* | *EY Luxembourg*. [online] Available at: https://www.ey.com/en_lu/digital/digital-operational-resilience-act--dora- [Accessed 25 Feb. 2024].

[7]European Parliament and Council of the European Union, 2022. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148*. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.337.01.0001.01.ENG [Accessed 25 Feb. 2024].

[8] European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/2024 on Digital Operational Resilience for the Financial Sector (Digital Operational Resilience Act), Regulation 2022/2024*.

[9] Guagliano, C. and Harris, A. (2022) *'Data risks and security in the financial sector: Adapting to a new* environment', Journal of Financial Compliance, 6(1), pp. 49–56. Available at: https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=bsu&AN=159998853&site=ehost-live&scope=site (Accessed: 25 February 2024).

[10] IBM. (n.d.). *What is the Digital Operational Resilience Act (DORA)?* | *IBM*. [online] Available at: https://www.ibm.com/topics/digital-operational-resilience-act#:~:text=The%20Digital%20Operational%20Resilience%20Act%2C%20or%20DORA%2C%20is%20a%20European.

[11] IT Governance Europe Belgium. (n.d.). *DORA (Digital Operational Resilience Act) compliance* | *IT Governance Europe Belgium*. [online] Available at: https://www.itgovernance.eu/nl-be/eu-digital-operations-resilience-act-dora-regulation-be [Accessed 25 Feb. 2024].

[12] International Organization for Standardization, 2013. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Geneva: International Organization for Standardization.

[13] Lang, S. (2022). *Meeting DORA Third-Party Risk Requirements*. [online] Prevalent. Available at: https://www.prevalent.net/blog/dora-digital-operational-resilience-act/.

[14] Maples. (2023). *DORA: New EU Operational Resilience Regime for the Financial Sector*. [online] Available at: https://maples.com/en/knowledge-centre/2023/1/dora-new-eu-operational-resilience-regime-for-the-financial-sector [Accessed 25 Feb. 2024].

[15] National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. U.S. Department of Commerce. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 25 Feb. 2024].

[16] Ozdemir, O. (2023). *DORA regulation: all your questions answered*. [online] KPMG. Available at: https://kpmg.com/lu/en/blogs/home/posts/2023/04/dora-regulation-all-your-questions-answered.html [Accessed 25 Feb. 2024].

[17] Palais, S. (2023). *DORA and the Digital Operational Resilience Testing Program*. [online] Yogosha. Available at: https://yogosha.com/blog/dora-digital-operational-resilience-testing/ [Accessed 25 Feb. 2024].

[18] PECB (n.d.). *What is the Digital Operational Resilience Act (DORA)?* [online] pecb.com. Available at: https://pecb.com/article/what-is-the-digital-operational-resilience-act-dora [Accessed 25 Feb. 2024].

[19] Pillay, K. (n.d.). *The EU's DORA has been agreed: implications for the financial services sector*. [online] Deloitte Suomi. Available at: https://www2.deloitte.com/fi/fi/pages/risk/articles/eu-dora-implications-for-financial-services-sector.html [Accessed 25 Feb. 2024].

[20] Portnoy, A. and Nauwelaerts, W. (2023). *What You Should Know About the EU Digital Operational Resilience Act* | *News & Insights* | *Alston & Bird*. [online] www.alston.com. Available at: https://www.alston.com/en/insights/publications/2023/11/eu-digital-operational-resilience-act [Accessed 25 Feb. 2024].

[21] PricewaterhouseCoopers (n.d.). *DORA: What you should know about the latest changes*. [online] PwC. Available at: https://www.pwc.com/mt/en/publications/technology/dora-latest-changes.html [Accessed 25 Feb. 2024].

[22] Šehomerović, F.N. (NL), Ademir (2023). *AFM – Getting ready for DORA: Managing ICT risk for third-party providers*. [online] Regulation Tomorrow. Available at: https://www.regulationtomorrow.com/the-netherlands/regulation-and-compliance-the-netherlands/afm-getting-ready-for-dora-managing-ict-risk-for-third-party-providers/ [Accessed 25 Feb. 2024].

[23] Shah, N. (2023). *ICT incident management, classification and reporting under DORA*. [online] Fieldfisher. Available at: https://www.fieldfisher.com/en/insights/ict-incident-management-classification-and-reporting-under-dora [Accessed 25 Feb. 2024].

[24] www.consilium.europa.eu. (2022). *Digital finance: Council adopts Digital Operational Resilience Act.* [online] Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/.

[25] www.digital-operational-resilience-act.com. (n.d.). *Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554*. [online] Available at: https://www.digital-operational-resilience-act.com/#:~:text=Before%20DORA%2C%20financial%20institutions%20managed [Accessed 25 Feb. 2024].

[26] www.eiopa.europa.eu. (n.d.). *Digital Operational Resilience Act (DORA)*. [online] Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

[27] Payment Card Industry Security Standards Council, 2018. *Payment Card Industry (PCI) Data Security Standard (DSS), Version 3.2.1*.

[28] European Parliament and Council of the European Union, 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L119, pp.1-88.

[29] International Organization for Standardization (ISO), 2018. *ISO 31000:2018 Risk management - Guidelines*. Geneva: International Organization for Standardization.