Benchmarking on digital operational resilience activities of financial entities

With focus on Digital Operational Resilience Act (DORA)

Master Thesis

For attainment of the academic degree of
Master of Science in Engineering (MSc)

in the Master Programme Cyber Security and Resilience
at St. Pölten University of Applied Sciences

by
Milyan Mikich
01577034

First advisor: Dr. Simon Tjoa

St. Pölten, 20.09.2023

Declaration

I hereby affirm that

- I have written this thesis independently, that I have not used any sources or aids other than those indicated, and that I have not made use of any unauthorised assistance.
- I have not previously submitted this thesis topic to an assessor, either in Austria or abroad, for evaluation or as an examination paper in any form.
- This thesis corresponds to the thesis assessed by the assessor.

....

St. Pölten, 20.09.2023 Signature

Preface

Hereby I would firstly like to express gratitude to my supervisor FH-Prof. Mag. Dr. Tjoa Simon of the University of applied Sciences St. Pölten for his expertise, support and guidance provided during the work on my master thesis. Also, I would like to express my sincere thanks to colleagues of mine from the “Group Security” of Erste Group Bank AG, for their support in providing various industry-driven inputs for creation of this thesis. Lastly, I would also like to express my sincere appreciation to all participants who have taken a part in conducted interviews.

Thank you.

Abstract

This thesis examines the observation, benchmarking and analysis on digital operational resilience related activities with a major focus on Digital Operational Resilience Act (DORA)[1].

The aim of the thesis is to observe and analyze the impact of DORA on financial entities as well as the current maturity level in accordance with DORA requirements, self-assessed by representatives of various financial organizations.

For the purpose of the questionnaire used for interview conductions, the methodology established in the Building Security in Maturity Level (BSIMM)[2] has been considered, but adapted according to the subject and goal of this thesis.

The model used is observational and real data-driven which provides an in-depth analysis of gathered information from conducted interviews including various different observational conclusions stipulated per each interview question at the end of the thesis, in the chapter dedicated for interview result analysis.

As a conclusion, the thesis emphasizes what was determined, in terms of activities, as the major impact of DORA as well as what a maturity level of financial entities is based on the self-conducted assessment, taken by representatives of organizations in scope of the carried out interviews.

Lastly, upon consented by the respective interview participants, the achieved results may serve as an input for other financial organizations on preparing themselves to be compliant against DORA and may be shared among participating firms in an aggregated and anonymized way only, with a goal that all participating firms may benefit from using the same measuring stick established as well as considering how mature/"prepared" on a certain activity other financial entities are (at this point in time) in respect to DORA.

Used but adapted BSIMM assessment empowers financial entities to analyze and benchmark their current ICT risk management program against other organizations across financial industry. As an objective analysis financial entities may base decisions of resources, time, budget, and priorities as seek to improve their security and digital operational resilience posture. [1]

[1] EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu)

[2] Building Security Maturity Model (BSIMM) Consulting Services | Synopsys

Table of Content

1 Introduction

The operational resilience may be defined as “the ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions”. [2]

Digital operational resilience has gained increasing importance in the European Union (EU) in recent years, among other, due to general growth of digital technologies and the recognition of the eventual risks and vulnerabilities associated with them.

Historically seen, there have been several developments and events that have contributed to the prominence of digital operational resilience in the EU. Thus, the regulatory landscape may be highlighted in the following way:

- The EU has actively been working on strengthening cybersecurity measures and incident response capabilities. Initiatives such as the Network and Information Security Directive (NIS Directive) and the establishment of the EU Agency for Cybersecurity (ENISA) have focused on enhancing the resilience of critical infrastructure, including digital systems, against cyber threats.
- The “EU's Digital Single Market Strategy” aimed to harmonize digital regulations across member states and promote a seamless digital environment. In addition, this strategy emphasized the importance of robust digital infrastructure and operational resilience to support the digital economy and society. [3]
- The publishment of the “Guidance on cyber resilience for financial market infrastructures” by the joint Committee on Payments and Market Infrastructures (CPMI) and the Board of the International Organization of Securities Commissions (IOSCO) [4]
- The publication of “Guidelines ICT and Security Risk Management” by the European Banking Authority (EBA) on Information and Communication Technology (ICT) and security risk management for the banking sector. These guidelines provided recommendations on governance, risk

assessment, incident management, and business continuity planning to ensure the operational resilience of banks. [5]

- The enforcement of the “General Data Protection Regulation” (GDPR) played a significant role in driving organizations to strengthen their digital operational resilience by enhancing data protection and privacy requirements and practices. Among other, the GDPR emphasized the necessity for organizations to implement appropriate technical and organizational measures (TOMs) to ensure the security and integrity of personal data. [6]
- “The Cybersecurity Strategy for the Digital Decade”, which outlines the EU's vision and objectives for cybersecurity. The strategy highlights the importance of operational resilience and sets forth initiatives to enhance cyber incident response capabilities, strengthen critical infrastructure protection, and promote cybersecurity standards and certification. [7]
- The release of the “Cross Industry Guidance on Operational Resilience” by the Central Bank of Ireland (CBI) [8]
- The publication of the “Joint Policy Statement on Operational Resilience” by the Prudential Regulatory Authority (PRA), Financial Conduct Authority (FCA) and Bank of England [9]
- Finally, in 2021 the European Commission proposed the Digital Operational Resilience Act (DORA) as part of the broader Digital Finance Package. DORA aims to establish a comprehensive framework for ensuring the operational resilience of digital services in the financial sector. It introduces requirements for incident reporting, risk management, testing, and oversight to enhance the resilience of financial institutions and digital service providers. [10]
- The proposed NIS2 Directive which aims to set the common security level across the EU, by ensuring adequate preparedness and cooperation across all Member States. [11]

Simultaneously with implementing DORA, the co-legislators have adopted two directives, the Directive on Network and Information Security (Directive (EU) 2022/2555, NIS 2) and the Directive on the Resilience of Critical Entities (Directive (EU) 2022/2557, CER). Whereas NIS 2 and CER are not specific to the financial sector they do apply to certain financial-sector entities, as well as to providers of digital infrastructure and ICT services who serve the financial sector. Although DORA has been designated explicitly as a sectoral ‘lex specialis’ for the purposes of Art. 4 NIS 2 and Art. 1(3) CER, and hence takes precedence, there are still significant overlaps between these legislative frameworks, which could dilute their effectiveness unless their respective scopes of application are clearly delineated

and criteria and definitions aligned as closely as practicable, as observed by the Securities and Markets Stakeholder Group (SMSG) of European Securities and Markets Authority (ESMA). [12]

These developments reflect the EU's increasing recognition of the need to address the risks and challenges associated with digital operational resilience. Also, they demonstrate the EU's commitment to promoting a secure and resilient digital environment to protect critical systems, services, and data.

All above listed regulatory papers laid the groundwork and highlight the importance of a robust risk management, incident response, digital operational resilience testing, ICT third-party risk management and business continuity planning, which is an essential element to consider in establishing a comprehensive and harmonized framework specifically for digital operational resilience in the financial sector, as according to DORA.

1.1 Aims and Objectives

The primary aim of this thesis is to conduct a comprehensive observation and analysis on digital operational resilience related activities, with a particular focus on DORA, carried out by representatives of various financial institutions based in the EU, by benchmarking on DORA impact as well as on self-assessed maturity level of financial entities in accordance with DORA requirements. To achieve this aim the following objectives must be followed and achieved, too:

Objective 1: Analyze the implementation and adaption of the BSIMM framework as the methodology followed to formulate DORA specific questions for the conducted interviews

Objective 2: Study the DORA, its core requirements and formulate a set of questions/activities which is to be used for conduction of interviews

Objective 3: Carry out in-depth interviews with representatives of participating financial entities

Objective 4: Observe, compare, analyze, evaluate and report results on what the major impact of DORA has been ranked as well as what a maturity level of each participated party is, in accordance with DORA

1.2 Research Questions

The following are the research questions relevant to be taken into account for the aim and objective of this thesis and which during the research have been attempted to be answered:

1. What are the main requirements of DORA?
2. What are the main benefits and strains of DORA?
3. What actions have participated financial entities taken so far to familiarize and prepare themselves for DORA compliance?
4. What DORA requirement poses the biggest impact on operations of participating financial entities?
5. What is the current maturity level of participating financial entity for DORA compliance, in accordance with their self-assessment conduction?
6. What challenges may be identified as a conclusion out of interview result evaluations?

1.3 Hypothesis

Mentioned below are some of the hypotheses for the master thesis that can hold to prove a point of study:

1. Operational resilience is an evolving area which will be more and more regulated and further developed in the EU
2. DORA is a “milestone” in financial sector of the EU, when it comes to digital operational resilience
3. Financial entities are well informed about DORA importance and its requirements
4. Financial entities are mature enough to be well prepared for an adequate DORA implementation

1.4 Outline of the thesis

Master thesis is outlined in five different chapters

Chapter 1 - Introduction

This chapter presents the general introduction to the topic of the master's thesis, including the aims, objectives, research questions, and hypotheses relevant to the

study. The focus of the thesis is to observe and analyze the impact of DORA on operations of participated financial entities as well as to conduct a self-assessment on their current maturity level per activities defined throughout the thesis.

Chapter 2 - Background and related works

This chapter is entitled with a section "Background Research - Problem," which focuses on various regulatory and legislative considerations as relevant background information for DORA enforcement at the EU level, with the main goal to make sure the financial sector in the European Union is able to maintain resilient operations through severe operational disruptions.

Chapter 3 - Requirements / Methods

This chapter provides a detailed explanation of the experimental design and methodology employed in the study. The requirements and steps of the experiment are outlined, with a particular focus on the specific methods and processes involved. The goal of this chapter is to provide a clear and concise description of the experimental approach taken.

Chapter 4 - Implementation / Testing / Evaluation results

This chapter presents the results of the experimental study analyzing and evaluating assessment results observed out of conducted interviews. This chapter is divided into 2 sub-chapters, general management summary of result evaluation and detailed result evaluation per interview questions following two established self-assessments.

Chapter 5 - Conclusion

This final chapter of the thesis provides an evaluative summary of the study's findings and conclusions. It presents a brief overview of the experimental results and discussions as an outcome from the carried out interviews, outline limitations and poses questions for future research. Also, this chapter highlights general challenges identified out of all final result analysis and it offers suggestions for any further development in researching the area of digital operational resilience.

2 Background and Related Work

2.1 Background Research – Problem Statement

In the digital age, information and communication technology (ICT) supports complex systems used for everyday societal activities. It keeps our economies running in key sectors, including finance, and enhances the functioning of the single market. Increased digitalization and interconnectedness also amplify ICT risks making society as a whole - and the financial system in particular - more vulnerable to cyber threats or ICT disruptions. While high digitalization and connectivity are nowadays core features of all activities of Union financial entities, digital resilience is not yet sufficiently built in their operational frameworks. [10]

The finance sector is subject to both EU and national legislations. This sector, which stands as a crucial backbone of the European economy, is among others extremely dependent on ICT infrastructures, providers, and their supply chain. [13]

However, digitalization and finance have become increasingly interconnected in today's time, including but not limited to, digital payments and transactions, online banking and digital services and many other finance services which have majorly/largely become digital. With this growth of digitalization the dependencies between financial sector and its ICT systems and third-party service providers has also drastically increased. Therefore and consequently, many ICT risks, which pose a challenge for operational resilience, may not be taken isolated any longer and will rather have a broader impact across the entire financial sector at the EU level.

Among other, due to all of above stated, there was a clear need identified to make the Union financial system more resilient and stabile, proposing and introducing a respective legislation regulating the digital operational resilience at the EU level, which led into implementation of DORA. Its timeline may be presented as follows:

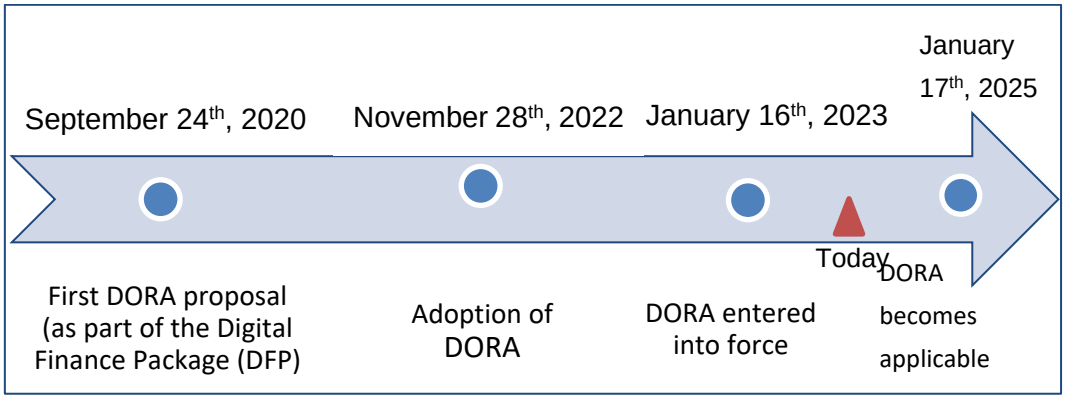


Figure 1: DORA timeline

As illustrated in the Figure 1, DORA shall apply from 17th of January 2025 whereas the EC and ESAs have foreseen a period of two years (2023 & 2024) for companies to prepare for DORA and implement it. This is a crucial time for financial entities to align their governance and practices to DORA's resilience pillars and to identify a roadmap with key deliverables to materialize their digital resilience strategy. Also, by beginning of 2025 ESAs will expect the mandatory reports outlined by DORA to be available upon their request, and will use them to assess any gaps in the market. By then, financial entities should also be prepared to perform the mentioned annual evaluations, testing and reports. By the end of 2025, mandatory penetration testing will come into force, and certification by ESAs will have to be obtained. [14]

DORA is the first piece of legislation at the European level addressing the topic of digital operational resilience for financial services. It represents the EU's most important regulatory initiative on operational resilience and cyber security in the financial services (FS) sector. Lastly, the DORA also establishes the world's first framework that allows FS supervisors to oversee Critical ICT Third Party Providers (CTPPs) including Cloud Service Providers (CSPs). [15]

DORA as a new regulation introduced aims to harmonize existing legislation, supplement existing gaps and establish a unified digital framework whereby financial entities ensure they can adapt and endure all types of ICT-related disruptions and threats, in order to prevent and mitigate cyber threats. Thus in a nutshell, DORA sets out the following objectives: [16]

- Increase the collective digital resilience of the financial sector
- Harmony across and access to ICT incident reporting information
- Identify ICT vulnerabilities and analyze the efficacy of resilience measures against these vulnerabilities

- Streamline the existing inconsistent regulatory approach across member states
- Increase the contractual safeguards in the use of ICT services
- Oversee the activities of critical ICT third-party service providers
- Encourage the exchange of intelligence regarding ICT threat

According to the above outlined objectives, it may be concluded that DORA will drastically strengthen the digital resilience of financial sector in the EU, by safeguarding essential digital services and providing the regulatory ground for creating a more secure and resilient digital environment.

Important to note is that this thesis has been examined before publication of any respective DORA Regulatory Technical Standards (RTSs) prepared by the European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs), which mostly get published 2023-2024, hence does not cover further specifications and guidance laid down in those and which will be provided to financial firms.

However, DORA has mandated the ESAs to jointly develop altogether 13 policy instruments in two batches. At the time of this thesis ESAs consulted on the first batch of DORA policy products which includes 4 draft RTSs and one set of draft implementing technical standards (ITS): [17]

- RTS on ICT risk management framework and RTS on simplified ICT risk management framework
- RTS on criteria for the classification of ICT-related incidents
- ITS to establish the templates for the register of information
- RTS to specify the policy on ICT services performed by ICT third-party providers

In addition to above listed, DORA introduces a Union Oversight Framework for ICT third-party providers (ICT TPPs) deemed critical (CTPPs) and sets out 4 high-level criteria to assess criticality of ICT TPPs and thus according to the Article 31(6) it empowers the Commission to adopt a delegated act to further specify criticality criteria by July 2024. [18]

Whereas, the overall timeline table for DORA's level 2 mandates mapped with respective DORA article and including due dates for public consultation and submission to European Commission may be presented as follows: [19]

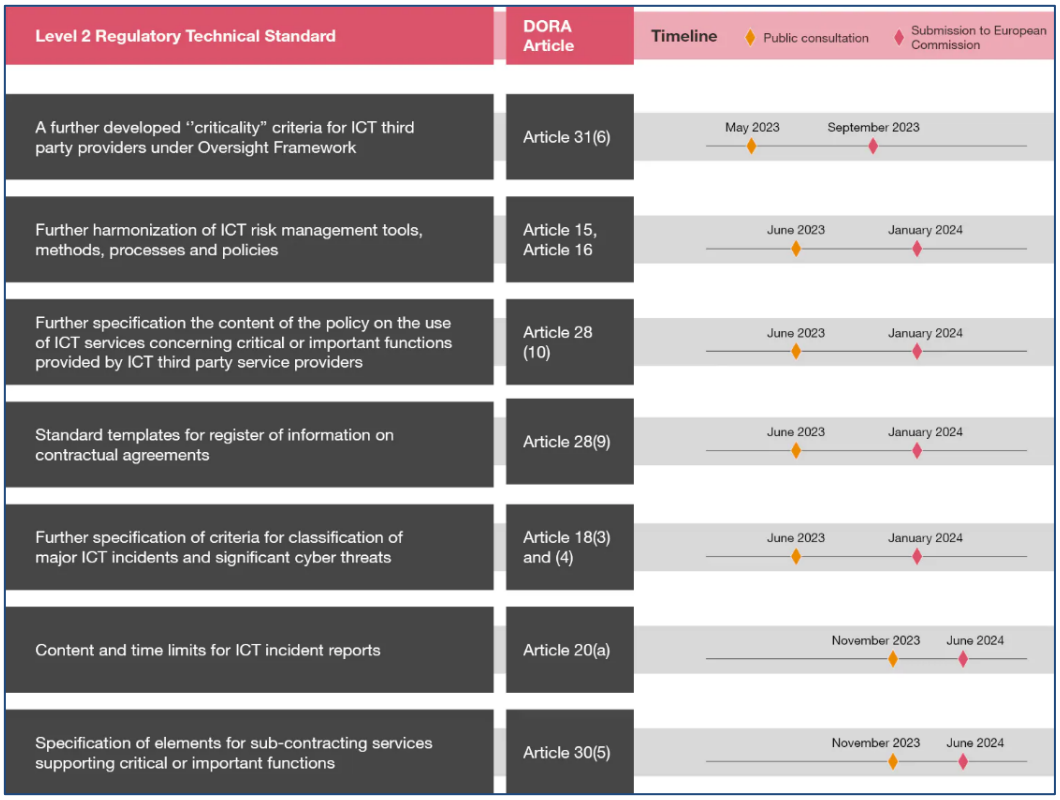


Figure 2: Level 2 Regulatory Technical Standards

As empathized on the technical discussion of the joint ESAs public event on DORA [18], the aim is a comprehensive, strong and effective ICT risk management by:

- Tackling fragmentation of ICT requirements laid down in the current Union financial services law
- Upgrading ICT risk requirements
- Achieving consistency in rules
- Promoting risk-based implementation and supervision
- Covering explicitly cyber hygiene
- Introducing key principles for financial entities' management of ICT third-party risk
- Complementing existing requirements on ICT outsourcing
- Enabling monitoring of the ICT third party contractual arrangement (not anchored fully into Union law before DORA)
- Achieving homogeneity and convergence on the monitoring of ICT third-party risk and ICT third-party dependencies
- Considering size, the overall risk profile of the financial entity, the nature, scale and complexity of its services, activities and operations.

3 Requirements / Methods

The previous chapter discussed the background including the history of digital operational resilience in the EU as well as about the background of DORA as a regulation, whereas this chapter covers in depth the method and methodology used for the research as well as the respective framework used for the purpose of the research.

In order to achieve the ultimate goal of this thesis which is to observe, benchmark and analyze the on digital operational resilience related activities conducted by participating financial entity, with a major focus on Digital Operational Resilience Act (DORA).

For this research purpose, respective interviews with relevant stakeholders dealing with DORA, in different participating firms, have been conducted by filling out an MS Form.

The interview questionnaire serves as a basis for further analysis in accordance with the objective of the master thesis. It is divided into 6 sections and consists of 34 questions/activities in total:
- One general, no DORA specific focused, with single and multiple-choose questions
- Five specific ones, following five main DORA pillars

Within the general, no DORA specific section of the questionnaire, the goal is to gain an overview on how familiar and aware a participated financial entity with DORA is, whether any actions in respect to DORA have taken place as well as acquire basic information on estimated impact of DORA, according to each participated financial entity.

Whereas questions in five DORA specific sections are based on 2 self-assessments where interview participants have been asked to:

- Rank defined activities according to higher/lower impact they may generate in respect to DORA preparation

- Assess their current maturity level per activity defined, from 1-5 (lower to higher; Initial to Optimized)

3.1 Implementation of BSIMM framework

Building Security in Maturity Model (BSIMM) [3] framework/methodology has been used to formulate a questionnaire which served as a basis of carried out interviews.

In particular, for the purpose of formulating the 5 DORA specific questions, the methodology established BSIMM framework has been used to a certain extend.

BSIMM is a unique program which examines the strategies organizations employ to build security into software development. It includes participants from various industries like cloud, financial services, financial technology (FinTech), independent software vendor (ISV), insurance, Internet of Things (IoT), healthcare, and technology verticals. Furthermore, It is a descriptive model that provides a baseline of observed activities (i.e., controls) for software security initiatives (SSIs) to build security in to software and software development. [1]

In fact, the BSIMM is a set of facts, a measurement tool for software security initiatives based on actual, real data gathered. The base for measuring is in-person interviews conducted in order to determine whether or not a firm that is a subject of measurement is carrying out each of those activities. The pre-built set of activities do not indicate how software security should be done, but instead the idea is to gather as much relevant data as possible. Therefore, the model is very much observational and linked to real data from the real world. [20]

Finally, as a descriptive model, the only goal of the BSIMM is to observe and report. [21]

In accordance to the BSIMM terminology the set of questions has been structured in the following way:

BSIMM Terminology	Description and adaption	Amount of
Domains	Domains are: - Governance & ICT Risk Management - ICT Incident Reporting - Resilience Testing - ICT Third Party Risk - Information Sharing	5
Practices	Not defined	n/a

[3] Building Security Maturity Model (BSIMM) Consulting Services | Synopsys

Activities	Actions carried out. Activities are divided into three levels in the BSIMM.	23

Table 1: BSIMM Framework Adaption

All participants fall under the financial industry.

Please note that the methodology for determining the levels per each practice (1-3) according to BSIMM has not been used in the thesis due to the fact that there was no focus on how frequent (e.g. commonly or rare) a particular activity has been observed/performed by a participating firm.

Besides considering BSIMM, for various questions e.g. 11th, 15th, 21st, 27th and 34th, the report on "*Position of the European Financial Congress with regard to the European Commission's consultation document on Digital Operational Resilience framework for financial services"*, based on expert responses in a group expertise of EKF" [22] has been referred, too.

3.2 Carried out interviews

The “Interview” has been the used method for conducting the research.

In particular, for the purpose and goal of this thesis, the in-person interview technique has been used to conduct analysis and assessment with 9 participating financial entities which are all based within the European Union (EU):

- Austria (78%; 7 out of 9)
- Romania (11%; 1 out of 9)
- Croatia (11%; 1 out of 9)

Due to confidentiality reasons, names of participated financial entities will not be disclosed throughout this thesis.

Time for providing answers was unlimited. However, estimated time for filling out the form was 30 minutes whereas the average time to complete the survey/interview was 45 minutes. All questions are required and preparation was not needed.

The interview might have either be conducted online, using MS Teams or in person, which was a preferable option.

In any case, for the purpose of evaluating the interview results using a thematic analysis, if consented by interviewees, the interview was recorded, and records have been deleted after the analysis has been completed.

The answers, experiences and comments shared in the interview have been treated confidentially by me and analyzed and used for the master's thesis purposes only.

Finally, if consented by interviewees, too, the result of this thesis will be shared with them as well as with other participating firms in an aggregated and anonymized way only, with a goal that all participating firms may benefit from using the same measuring tool/stick established as well as considering how mature/”prepared” on a certain activity other financial entities are (at this point in time) in respect to DORA.

Link to the summary of interview responses:
https://forms.office.com/Pages/AnalysisPage.aspx?AnalyzerToken=pKGt5h1TfW1V2fq7OGVnAruzNkInKVkX&id=DQSIkWdsW0yxEjajBLZtrQAAAAAAAAAAAAMAAC4cWiFUQjlJWUExMjQ4UzEzSjFZRFJCUjExNllQRi4u

3.3 Interview Questionnaire Structure

The interview has been structured in predetermined set of questions/the interview questionnaire which consists of 2 major sections:

- General, no DORA domain specific
- DORA pillar specific

In total, 34 defined questions/activities may be shown in the following way:

DORA Questionnaire	
General (no domain specific)	
Have you taken any internal action so far to prepare for DORA?	○ Yes (please list 3 major ones) ○ No
How familiar are you with DORA?	○ Very well ○ Know a fair amount ○ Know something/a little ○ Heard of it ○ Never/barely heard of it
Did you perform any high-level analysis on DORA requirements?	○ Yes ○ No
How aware are you of the current digital operational resilience capability of your organization?	○ Extremely aware ○ Very aware ○ Moderaly aware ○ Slightly aware ○ Not at all aware
Did you conduct a mapping between requirements of DORA and of other relevant regulations/directives?	○ Yes, with GDPR ○ Yes, with NIS2 ○ Yes, with PSD2 ○ Yes, with SWIFT ○ No, with none of above listed
Have you engaged any external support e.g. consultancy firm so far to support with DORA preparation?	○ Yes ○ No
Have you consulted with any other financial institution?	○ Yes ○ No
Do you consider DORA as a priority for your organization for 2023 or upcoming year(s)?	○ Yes ○ No
Is the Management Board of your organization aware of DORA importance and did you take any awareness measures to educate employees about DORA requirements?	○ Yes ○ No

Is the Management Board of your organization involved in effective management of security risks and incidents?	○ Extreme involvement ○ High involvement ○ Moderate involvement ○ Slight involvement ○ No involvement
What division in your organization is accountable to ensure the adequate preparation for DORA compliance?	○ CRO ○ COO ○ CFO ○ Other (free text box)
What do you think is the main benefit(s) of DORA?	(Free text box)
What do you think is the main strain of DORA?	(Free text box)
Where in the context of the risk management cycle has your organization until now faced most difficulties, gaps and flows in relation to its ICT resilience? (1 - Not problematic, 5 - High problematic)	○ Identification ○ Detection ○ Ability to protect ○ Respond ○ Recovery ○ Learning and evolving ○ Information sharing with other financial actors on treat intelligence ○ Internal coordination (within the organization)
Which DORA pillar may cause the biggest implementation difficulties/obstacles for your organization and would be seen as the main strain(s)/challenge(s) for its implementation?	○ ICT Risk Management ○ ICT Incident Reporting ○ Digital Operational Resilience Testing ○ Third-party Risk Management ○ Treat Intelligence Sharing
What in your view are possible causes/difficulties in handling ICT operational resilience incidents? (1 - Not problematic, 5 - Highly problematic)[4]	○ ICT environmental complexity ○ Issues with legacy systems ○ Lack of analysis tools ○ Lack of staff support
How good was the digital operational resilience of Austrian companies (e.g. banks) prior to DORA?	○ Excellent ○ Good ○ Fair ○ Poor ○ Very poor
How do you assess the impact of DORA on Austrian companies (e.g. banks)?	○ Sever ○ Major ○ Moderate ○ Minor

[4] This question has been answered under the section 3/Pillar 2 in the questionnaire

	○ Insignificant
How do you assess your current readiness to be DORA compliant?	On the scale from 1-5
What is/would be the impact on your budget allocation for DORA preparedness and compliance?	On the scale from 1-10
Which DORA specific measure is completely new for your organization?	(Free text box)
Do you think that DORA will support the financial sector in the EU to become more resilient or would you find it more as an additional administrative document enforced?	○ Yes, it will majorly support the EU financial sector to be more resilient ○ Yes, it will minorly support the EU financial sector to be more resilient ○ Yes, it will support to a certain extend but it's more an additional administrative paper ○ It's more an additional administrative paper than the actual operative support for resilience
Domain specific	
ICT Risk Management ***(Chapter II, Article 5-14)***	***RM1.1*** Establish internal governance and control framework ***RM1.2*** Develop the comprehensive and well-documented ICT risk management framework ***RM1.3*** Establish digital resilience strategy ***RM1.4*** Maintain updated ICT systems, protocols and tools ***RM1.5*** Identify, classify and document all ICT related business functions, roles, processes or assets ***RM1.6*** Continuously monitor and control the security and functioning of the ICT systems ***RM1.7*** Enforce mechanism to properly detect anomalous activities ***RM1.8*** Ensure a dedicated and comprehensive ICT business continuity policy and develop response and recovery plans/methods, including the backup policies and their review ***RM 1.9*** Ensure capabilities and staff for information gathering and adequate communication

ICT Incident Reporting ***(Chapter III, Article 17-23)***	***IR 1.1*** Define, establish and implement an ICT-related incident management process, enforcing early warning indicators ***IR 1.2*** Classify ICT-related incidents and determine their impact following required criteria ***IR 1.3*** Report major ICT-related incidents to the competent authority including the incident report ***IR 1.4*** Establish process for handling a supervisory feedback/guidelines
Resilience Testing ***(Chapter IV, Article 24-27)***	***DORT 1.1*** Establish, maintain and review a comprehensive digital operational resilience testing program as an integral part of the ICT risk management framework ***DORT 1.2*** Ensure a full range of appropriate tests before any deployment/redeployment of new or existing services supporting the critical functions ***DORT 1.3*** Perform advanced testing of ICT tools, systems and processes based on threat led penetration testing ***DORT 1.4*** Ensure that tests are undertaken internally/externally by independent parties and that testers are used for the deployment of threat led penetration testing
ICT Third Party Risk ***(Chapter V, Article 28-44)***	***TPRM 1.1*** Ensure that managing of third party risk management is as an integral component of ICT risk management framework in accordance with key principles of ICT third party risk management ***TPRM 1.2*** Ensure a termination of contractual clauses and enforcement of exit strategies ***TPRM 1.3*** Ensure a preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements ***TPRM 1.4*** Weight the benefits and costs of alternative solutions, including possible sub-contracting ***TPRM 1.5*** Enforce key contractual provisions
Information Sharing ***(Chapter VI, Article 45)***	***IS 1.1*** Exchange on cyber threat information and intelligence among relevant stakeholders

Figure 3: Interview Questionnaire

Section 1 presents the general, no DORA specific questions, as shown above. The goal of this section is to gain a basic understanding whether participating firms perform comparable activities as preparation and consideration of being compliant with DORA.

Sections 2-6 in the questionnaire cover DORA specific questions, following 5 identified DORA pillars. For each of these sections 2 standardized “questions” have been formulated in which a participated firm has been asked to:

1. **rank** the activities from higher to lower, which in their opinion will generate the biggest impact on DORA preparation
2. perform a **self-assessment on maturity level** of defined DORA activities. (from lowest to highest, 1 - Initial, 5 - Optimized)

Section 2 has a limitation for ranking the top 5 activities only due to pragmatic and result evaluation reasons, as this is the section with the most activities defined.

Section 3 (Pillar 2) has an additional question to the two standardized one, as explained above, which focuses on possible causes/difficulties in handling ICT operational resilience incidents.

Section 6 which focuses on DORA Pillar 5 (Threat Intelligence Sharing) is an exception to the stated above, as it consists of a single activity defined hence no ranking has been required. Instead, a participating firm has been asked whether any activities are being performed in respect to exchanging on cyber threat information and intelligence among relevant stakeholders. Also, this section contains an additional question which focuses on whether the EU should have a role in supporting and promoting the voluntary exchange of the tactics, techniques, and procedures (TTPs) and Indicator of Compromises (IoCs) between financial institutions.

3.4 "Activities" mapped with DORA requirements

As stated in the Section 3.1, the BSIMM framework has been followed to define activities. Activities are defined at the high level hence an activity may include several corresponding requirements stipulated in DORA.

Below is the mapping performed between each activity defined and its associated requirement(s) from DORA. [23] As part of the interview, interview participants may also consider the mapping conducted prior to provide their answers and inputs:

Activity vs DORA requirement(s)			
Activity ID	**Activity**	**DORA requirement(s)**	
RM 1.1	Establish internal governance and control framework	*The management body shall define, approve, oversee and be accountable for the implementation of all arrangements related to the ICT risk management framework. The **management body** shall:* - *bear the final responsibility for managing the financial entity's ICT risks* - *set clear roles and responsibilities for all ICT-related functions* - *determine the appropriate risk tolerance level of ICT risk of the financial entity,* - *approve, oversee and periodically review the implementation of the financial entity's ICT Business Continuity Policy and ICT Disaster Recovery Plan* - *approve and periodically review the ICT audit plans, ICT audits and material modifications thereto* - *allocate and periodically review appropriate budget of all types of resources, including training on ICT risks and skills for all relevant staff* - *approve and periodically review the policy on arrangements regarding the use of ICT services*	***Pillar 1***

		provided by ICT third-party service providers - *be duly informed, of the arrangements concluded with ICT third-party service providers on the use of ICT services, of any relevant planned material changes regarding the ICT third-party service providers, and on the potential impact of such changes on the critical or important functions subject to those arrangements, including receiving a summary of the risk analysis to assess the impact of these changes* - *be duly informed about ICT-related incidents and their impact and about response, recovery and corrective measures.* *Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date sufficient knowledge and skills to understand and assess ICT risks and their impact on the operations of the financial entity* *Establish a role to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation*	
RM 1.2	Develop the comprehensive and well-documented ICT risk management framework	*ICT risk management framework enables an financial entity to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.* ***ICT risk management framework** shall include at minimum the following:* - *strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets* - *assign the responsibility for managing and overseeing ICT risk and ensure the independence and*	

		segregation of ICT mgmt.. functions *The ICT risk management framework shall be a subject to an internal audit on a regular basis and shall also be documented and reviewed at least once a year.*	
RM 1.3	Establish digital resilience strategy	*A **digital resilience strategy** shall stipulate how the framework shall be implemented:* - *explaining how the ICT risk management framework supports the financial entity's business strategy and objectives* - *establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analyzing the impact tolerance of ICT disruptions* - *setting out clear information security objectives* - *explaining the ICT reference architecture and any changes needed to reach specific business objectives* - *outlining the different mechanisms put in place to detect, protect and prevent impacts of ICT-related incidents* - *evidencing the number of reported major ICT-related incidents and the effectiveness of preventive measures* - *defining a holistic ICT multi-vendor strategy at entity level showing key dependencies on ICT third-party service providers and explaining the rationale behind the* - *implementing digital operational resilience testing* - *Outlining a communication strategy in case of ICT-related incidents.*	
RM 1.4	Maintain updated ICT systems, protocols and tools	*This applies to the following **ICT systems, protocols and tools**:* - *appropriate to the magnitude of operations supporting the conduct*	

		of their activities, in accordance with the proportionality principle - *reliable* - *equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak orders, message or transaction volumes, as needed, including where new technology is introduced* - *technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions*	
RM 1.5	Identify, classify and document all ICT related business functions, roles, processes or assets	*This includes the following:* - *review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation* - *identification on a continuous basis of all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets incl. the review on a regular basis, and at least yearly, the risk scenarios impacting them* - *perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets* - *identification of all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and their mapping with considered critical incl mapping the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets* - *identification and document of all processes that are dependent on*	

		ICT third-party service providers, and of their interconnections with ICT third-party service providers - *Maintenance of relevant inventories and update them periodically and every time any major change occurs* - *Conduction of a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems, on a regular basis, and at least yearly*	
RM 1.6	Continuously monitor and control the security and functioning of the ICT systems	*This includes the following:* - ***ICT tools** which should:* - *ensure the security of the means of transfer of data* - *minimize the risk of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity* - *prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data* - *ensure that data is protected from risks arising from data management, including poor administration, processingrelated risks and human error* *Enforcement of **Information security policy** which:* - *defines rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers* - *following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks* - *limits the physical or logical access to information assets and ICT assets to what is required for*	***Pillar 1***

		legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereo - *enforces a strong authentication mechanisms and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes* - *covers the changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner* - *documents patches and updates*	
RM 1.7	Enforce mechanism to properly detect anomalous activities	*This includes the following:* - *ICT network performance issues and ICT-related incidents, and identification of potential material single points of failure* - *regular testing* - *enabling multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response* - *Devoting of sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.*	
RM 1.8		*This refers to* ***ICT business continuity policy*** *which should:* - *ensuring the continuity of the financial entity's critical or important functions*	

	Ensure a dedicated and comprehensive ICT business continuity policy and develop response and recovery plans/methods, including the backup policies and their review	- *quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritizes the resumption of activities and recovery actions* - *activation, without delay, of dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures* - *estimation of preliminary impacts, damages and losses* - *communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders* ***ICT response and recovery plans*** *which:* - *are subject to independent internal audit reviews* - *with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers are maintained, reviewed and periodically tested including the the crisis communication plans* ***Business impact analysis (BIA)*** *which should:* - *assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate* - *consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies* - *be used in designed in full alignment with ICT assets and ICT services in particular with regard to adequately ensuring the redundancy of all critical components*	
	Ensuring a dedicated and comprehensive ICT business continuity policy and develop response and recovery plans/methods, including the backup policies and their review		

	Ensure a dedicated and comprehensive ICT business continuity policy and develop response and recovery plans/methods, including the backup policies and their review	***In addition:*** - *Testing plans scenarios should include the cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities* - *Determine a crisis management function, which, in the event of activation of their ICT business continuity plans or ICT response and recovery plans, shall, inter alia, set out clear procedures to manage internal and external crisis communications* - *Keeping readily accessible records of activities before and during disruption events when their ICT business continuity plans and ICT response and recovery plans are activated* - *Central securities depositories shall provide the competent authorities with copies of the results of the ICT business continuity tests, or of similar exercises.* - *Reporting to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents* *To ensure the restoration of ICT systems and data with minimum downtime, limited disruption and loss, a* ***backup policy and recovery procedures and methods*** *shall be developed to ensure:* - *the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data* - *the periodically testing* - *A backup systems that:* - *Can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods.*	

		- *By activation, it shall not jeopardize the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data.* ***In addition:*** - *When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorized access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary* - *For central counterparties, the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date* - *Maintenance of redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs* - *Central securities depositories shall maintain at least one secondary processing site endowed with adequate resources, capabilities, functions and staffing arrangements to ensure business needs.* *The **secondary processing site** shall be:* - *Located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site* - *capable of ensuring the continuity of critical or important functions identically to the primary site, or providing the level of services necessary to ensure that the*	

		financial entity performs its critical operations within the recovery objectives - *immediately accessible to the financial entity's staff to ensure continuity of critical or important functions in the event that the primary processing site has become unavailable* *In determining the recovery time and recovery point objectives for each function, it shall be taken into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.* *When recovering from an ICT-related incident, necessary checks shall be performed, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.*	

RM 1.9	Ensure capabilities and staff for information gathering and adequate communication	***Information gathering*** *on:*
		
		- *on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyze their likely impacts on their digital operational resilience*
		
		- *Carry out* ***post ICT-related incident reviews:***
		  - *To ensure after significant ICT disruptions of their core activities, analyzing the causes of disruption and identifying required improvements to the ICT operations or within the ICT Business Continuity Policy. It should include:*
		  - *the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity*	

		- *the quality and speed in performing forensic analysis* - *the effectiveness of incident escalation within the financial entity* - *the effectiveness of internal and external communication* *Communication to competent authorities when implementing changes* *Lessons derived from the digital operation resilience testing carried out from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of business continuity or recovery plans, together with relevant information exchanged with counterparties and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. These findings shall translate into appropriate reviews of relevant components of the ICT risk management framework* *Monitor the effectiveness of the implementation of their digital resilience strategy, including the mapping the evolution of ICT risks over time, analyze the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understand the level of ICT risk exposure and enhance the cyber maturity and preparedness of the financial entity.* *Ensure at least yearly report to the management body on the findings by the Senior ICT staff* *Develop ICT security awareness programs and digital operational resilience trainings as compulsory modules in their staff training schemes, applicable to all employees and to senior management staff.*	

		Monitor relevant technological developments on a continuous basis, also with a view to understand possible impacts of deployment of such new technologies upon the ICT security requirements and digital operational resilience ***Communication plans/policies:*** - *to enable a responsible disclosure of ICT-related incidents or major vulnerabilities to clients and counterparts as well as to the public, as appropriate* - *for staff and for external stakeholders taking into account the need to differentiate between staff involved in the ICT risk management, in particular response and recovery, and staff that needs to be informed.* - *Ensuring that at least one person in the entity shall be tasked with implementing the communication strategy for ICT-related incidents and fulfil the role of public and media spokesperson for that purpose*	
IR 1.1	Define, establish and implement an ICT-related incident management process, enforcing early warning indicators	*Establish appropriate processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to make sure that root causes are identified and eradicated to prevent the occurrence of such incidents.* *The **ICT-related incident management** process shall:* - *establish procedures to identify, track, log, categories and classify ICT-related incidents according to their priority and to the severity and criticality of the services impacted* - *assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios* - *set out plans for communication to staff, external stakeholders and media and for notification to clients, internal escalation procedures, including ICT-related customer complaints, as well as*	***Pillar 2***

		for the provision of information to financial entities that act as counterparts, as appropriate - *ensure that major ICT-related incidents are reported to relevant senior management and inform the management body on major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of ICT-related incidents* - *Establish ICT-related incident response procedures to mitigate impacts and ensure that services becomes operational and secure in a timely manner*	
IR 1.2	Classify ICT-related incidents and determine their impact following required criteria	***ICT-related incidents** shall be classified and their impact shall be determined based on the following criteria:* - *the number of users or financial counterparts affected by the disruption* - *the duration of the ICT-related incident, including service downtime* - *the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member State* - *the data losses that the ICT-related incident entails, such as integrity loss, confidentiality loss or availability loss* - *the severity of the impact of the ICT-related incident on the financial entity's ICT systems* - *the criticality of the services affected* - *the economic impact of the ICT-related incident*	
IR 1.3	Report major ICT-related incidents to the competent authority including the incident report	*For the purpose of reporting, an incident report shall be produced, after collecting and analyzing all relevant information, and submitted to the competent authority* *Where a major ICT-related incident has or may have an impact on the financial interests of service users and clients, without undue delay,*	

		inform their service users and clients about the major ICT-related incident and inform as soon as possible them of all measures which have been taken to mitigate the adverse effects of such incident. *The following to be **submitted to the competent authority**:* - *an initial notification, without delay, but no later than the end of the business day, or, in case of a major ICT-related incident that took place later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day, or, where reporting channels are not available, as soon as they become available* - *an intermediate report, no later than 1 week after the initial notification, followed as appropriate by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority* - *a final report, when the root cause analysis has been completed, regardless of whether or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates, but not later than one month from the moment of sending the initial report.* *Any delegation of the reporting obligations to a third-party service provider, in case of, it shall be approved by the relevant competent authority*	
IR 1.4	Establish process for handling a supervisory feedback/guidelines	*Upon receipt of a report, the competent authority shall acknowledge receipt of notification and shall as quickly as possible provide all necessary feedback or guidance to the financial entity, in particular to discuss remedies at the level of the entity or ways to minimize adverse impact across sectors.*	

DORT 1.1	Establish, maintain and review a comprehensive digital operational resilience testing program as an integral part of the ICT risk management framework	*The **digital operational resilience testing program** shall include a range of assessments, tests, methodologies, practices and tools:* - *A risk-based approach shall be followed taking into account the evolving landscape of ICT risks, any specific risks to which the financial entity is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.* - *It shall be ensured that tests are undertaken by independent parties, whether internal or external.* - *Procedures and policies to prioritize, classify and remedy all issues acknowledged throughout the performance of the tests shall be established as well as internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.* - *All critical ICT systems and applications shall be tested at least yearly.*	***Pillar 3***
DORT 1.2	Ensure a full range of appropriate tests before any deployment/redeployment of new or existing services supporting the critical functions	*A **full range of appropriate tests** including:* - *vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing or penetration testing.* *Vulnerability assessments shall be performed before any deployment or redeployment of new or existing services supporting the critical functions, applications and infrastructure components of the financial entity.*	

DORT 1.3	Perform advanced testing of ICT tools, systems and processes based on threat led penetration testing	***Threat led penetration testing*** *shall:* - *cover at least the critical functions and services and shall be performed on live production systems supporting such functions.* - *be carrying out at least every 3 years* - *the precise scope of threat led penetration testing, based on the assessment of critical functions and services, shall be determined by financial entities and shall be validated by the competent authorities.* - *all relevant underlying ICT processes, systems and technologies supporting critical functions and services, including functions and services outsourced or contracted to ICT third-party service providers shall be identified* - *where ICT third-party service providers are included in the remit of the threat led penetration testing, the necessary measures to ensure the participation of these providers shall be taken.* - *Effective risk management controls to reduce the risks of any potential impact to data, damage to assets and disruption to critical services or operations at the financial entity itself, its counterparties or to the financial sector shall be applied* - *at the end of the test, after reports and remediation plans have been agreed, the financial entity and the external testers shall provide to the competent authority the documentation confirming that the threat led penetration testing has been conducted in accordance with the requirements.* - *Competent authorities shall validate the documentation and issue an attestation.*	
DORT 1.4	Ensure that tests are undertaken internally/externally by independent parties and	*Only* ***testers*** *for the deployment of threat led penetration testing shall be used, which:*	

	that testers are used for the deployment of threat led penetration testing	- *are of the highest suitability and reputability* - *possess technical and organizational capabilities and demonstrate specific expertise in threat intelligence, penetration testing or red team testing* - *are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks* - *in case of external testers, provide an independent assurance or an audit report in relation to the sound management of risks associated with the execution of threat led penetration testing* - *In case of external testers, are dully and fully covered by relevant professional indemnity insurances*	
TPRM 1.1	Ensure that managing of third party risk management is as an integral component of ICT risk management framework in accordance with key principles of ICT third party risk management	***Key ICT third-party risk management principles:*** - *Financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall at all times remain fully responsible for complying with, and the discharge of, all obligations under this Regulation* - *Of proportionality, taking into account:* - *the scale, complexity and importance of ICT-related dependencies* - *the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers* *As part of the **ICT risk management framework:*** - *a strategy on ICT third-party risk shall be adopted and regularly reviewed.* - *that strategy shall include a policy on the use of ICT services provided by ICT third-party service providers and shall apply on an individual and, as relevant, on a sub-consolidated and consolidated basis.*	***Pillar 4***

		- *the management body shall regularly review the risks identified in respect of outsourcing of critical or important functions* - *a Register of Information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers shall be maintained and updated at entity level and, at sub-consolidated and consolidated levels* - *the contractual arrangements shall be appropriately documented, distinguishing between those that cover critical or important functions and those that do not.* - *information on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the services and functions which are being provided shall be reported at least yearly to the competent authorities* - *the full Register of Information shall be made available to the competent authority, upon request, or as requested* - *the competent authority shall be informed in a timely manner about planned contracting of critical or important functions and when a function has become critical or important.* ***Before entering into a contractual arrangement*** *on the use of ICT services, it shall be ensured to:* - *assess whether the contractual arrangement covers a critical or important function* - *assess if supervisory conditions for contracting are met* - *identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangements may contribute to reinforcing ICT concentration risk* - *undertake all due diligence on prospective ICT third-party service providers and ensure*	

		throughout the selection and assessment processes that the ICT third-party service provider is suitable - *identify and assess conflicts of interest that the contractual arrangement may cause.* *In exercising access, inspection and audit rights over the ICT third-party service provider, it shall be pre-determined on a risk-based approach the frequency of audits and inspections and the areas to be audited* *For contractual arrangements that entail a high level of technological complexity it shall be verified that auditors, whether internal, pools of auditors or external auditors possess appropriate skills and knowledge to effectively perform relevant audits and assessments.*	
TPRM 1.2	Ensure a termination of contractual clauses and enforcement of exit strategies	***Termination of contractual arrangements*** *on the use of ICT services shall be ensured at least under the following circumstances:* - *breach by the ICT third-party service provider of applicable laws, regulations or contractual terms* - *circumstances identified throughout the monitoring of ICT third-party risk which are deemed capable of altering the performance of the functions provided through the contractual arrangement* - *ICT third-party service provider's evidenced weaknesses in its overall ICT risk management and in particular in the way it ensures the security and integrity of confidential, personal or otherwise sensitive data or non-personal information* - *circumstances where the competent authority can no longer effectively supervise the financial entity as a result of the respective contractual arrangement.*	

		Exit strategies/plans *shall be put in place in order to take into account risks that may emerge at the level of ICT third-party service provider, in particular a possible failure of the latter, a deterioration of the quality of the functions provided, any business disruption due to inappropriate or failed provision of services or material risk arising in relation to the appropriate and continuous deployment of the function.* *It shall be ensured to* ***exit contractual arrangements*** *without:* - *disruption to their business activities* - *limiting compliance with regulatory requirements* - *detriment to the continuity and quality of their provision of services to clients.* ***Alternative solutions*** *and develop* ***transition plans*** *shall be identified to enable to remove the contracted functions and the relevant data from the ICT third-party service provider and securely and integrally transfer them to alternative providers or reincorporate them in-house.* *Appropriate contingency measures to maintain business continuity under all of the circumstances shall also be taken.*	
TPRM 1.3	Ensure a preliminary assessment of ICT concentration risk and further sub-outsourcing arrangements	*When performing the* ***identification and assessment of ICT concentration risk*** *it shall be taken into account whether the conclusion of a contractual arrangement in relation to the ICT services would lead to any of the following:* - *contracting with an ICT third-party service provider that is not easily sustainable or* - *having in place multiple contractual arrangements in relation to the provision of ICT service with the same ICT third-party service provider or with*	

		closely connected ICT third-party service providers	
TPRM 1.4	Weight the benefits and costs of alternative solutions, including possible sub-contracting	***Benefits and costs of alternative solutions*** *shall be weighed, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strategy. This shall also be weighed where the contractual arrangement on the use of ICT services may include the possibility of further* ***sub-contracting*** *in particular in the case of an ICT sub-contractor established in a third-country.* *It shall also be assessed whether and how potentially long or complex chains of sub-contracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively provide a supervision.* *Where contractual arrangements on the use of ICT services are concluded with an ICT third-party service provider established in* ***a third-country****, the following factors shall be considered* - *the respect of data protection* - *the effective enforcement of the law* - *insolvency law provisions that would apply in the event of the ICT-third party service provider's bankruptcy* - *any constraints that may arise in respect to the urgent recovery of the financial entity's data.*	
TPRM 1.5	Enforce key contractual provisions	*The rights and obligations of the financial entity and of the ICT third-party service provider shall be* ***clearly allocated and set out in a writing.*** *The* ***full contract****, which includes the services level agreements, shall be documented in one written document available to the parties on paper or in a downloadable and accessible format which includes at least the following:*	

		- *a clear and complete description of all functions and services to be provided by the ICT third-party service provider,* - *the locations where the contracted or sub-contracted functions and services are to be provided and where data is to be processed,* - *provisions on accessibility, availability, integrity, security and protection of personal data and on ensuring access, recover and return in an easily accessible format of personal and non-personal data processed by the financial entity in the case of insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider;* - *full service level descriptions, including updates and revisions thereof, and precise quantitative and qualitative performance targets within the agreed service levels* - *notice periods and reporting obligations of the ICT third-party service provider to the financial entity* - *the obligation of the ICT third-party service provider to provide assistance in case of an ICT incident at no additional cost or at a cost that is determined ex-ante* - *requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies which adequately guarantee a secure provision of services by the financial entity in line with its regulatory framework* - *the right to monitor on an ongoing basis the ICT third-party service provider's performance, which includes:* - *rights of access, inspection and audit by the financial entity or by an appointed third-party, and the right to take copies of relevant documentation, the effective exercise of which is not*	

		impeded or limited by other contractual arrangements or implementation policies; - *the right to agree alternative assurance levels if other clients' rights are affected* - *the commitment to fully cooperate during the onsite inspections performed by the financial entity and details on the scope, modalities and frequency of remote audits* - *the obligation of the ICT-third party service provider to fully cooperate with the competent authorities and resolution authorities of the financial entity, including persons appointed by them* - *termination rights and related minimum notices period for the termination of the contract, in accordance with competent authorities' expectations* - *exit strategies, in particular the establishment of a mandatory adequate transition period* - *during which the ICT third-party service provider will continue providing the respective functions or services with a view to reduce the risk of disruptions at the financial entity which allows the financial entity to switch to another ICT third-party service provider or change to on-premises solutions consistent with the complexity of the provided service.*	

IS 1.1	Exchange on cyber threat information and intelligence among relevant stakeholders	*Financial entities **may** exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing* - *aims at enhancing the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting financial entities' range of defensive capabilities, threat detection techniques, mitigation strategies or response and recovery stages* - *takes places within trusted communities of financial entities* - *is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data48 and guidelines on competition policy.* *The information sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which the latter may be associated to the information-sharing arrangements, as well as on operational elements, including the use of dedicated IT platforms.* *Financial entities shall notify competent authorities of their participation in the information-sharing arrangements, upon validation of their membership, or, as applicable, of the cessation of their membership, once the latter takes effect.*	***Pillar 5***

Table 2: Activities mapped with DORA requirements

Legend:
Majority – more than 60%
Middle – 30% - 60%
Minority – less than 30%

4 Evaluation Results

4.1 – Summary

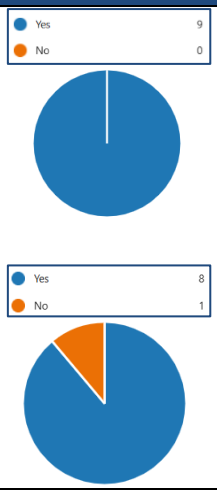
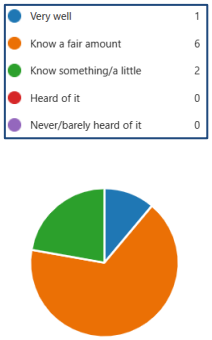
The below summary of result evaluation may also serve as "One-pager" which may be provided back to all financial firms who participated in interviews.

Area	Conclusion	Status
Internal actions	All financial entities have performed certain internal actions towards DORA preparation so far, whereas majority performed high level analysis	
Familiarity with DORA	Majority knows a fair amount of DORA requirements	
Digital operational resilience capability	Financial entities are fairly aware of their current digital operational resilience capability	
Mapping with other regulations	Half of financial entities haven't performed any mapping against any of other relevant regulations/directives, whereas a third did so against NIS2	
External support	Majority engaged an external consultancy	
Consultancy with other financial entities	The half consulted with other financial institutions, whereas the half has not.	
DORA as priority	Almost all financial entities consider DORA as priority for 2023/upcoming years	
Management board (MB) and DORA	• In almost all financial entities the MB is aware of DORA importance and have taken internal actions to educate relevant employees • In majority of financial entities the MB is moderately to highly involved in managing security risks and incidents	
Division responsible for DORA	No common approach identified, in majority COO and/or CRO	
"Most difficult" DORA pillar for implementation	No common consideration identified. As first, Third-party Risk Mgmt, then Digital Operational Resilience Testing and lastly ICT Risk Mgmt.	
DORA impact	DORA impact has been assessed between major and severe	
DORA readiness	Overall average rating is 3 out of 5	
Budget allocation	On average, the medium budget allocation is/will be allocated	
DORA and EU	All financial entities consider DORA as EU regulation which supports (majorly or minorly) the overall EU resilience	
Pillar I	Biggest impact assessed on "Identifying, documenting and classifying ICT business functions, roles, processes, assets". Lowest maturity assessed on "Establishing digital resilience strategy"	
Pillar II	Biggest impact and lowest maturity assessed on "Defining, establishing and implementing ICT Mgmt. process"	
Pillar III	Biggest impact assessed on "Ensuring a full range of tests before deployment of new/existing services supporting critical functions"; Lowest maturity assess on performing advanced testing based on TLPT	
Pillar IV	Biggest impact assessed on "Ensuring preliminary assessment on ICT concentration risk and sub-outsourcing arrangements"; Lowest maturity assessed on "Weighting benefits and costs on alternative solutions, inc. possible sub-contracting"	
Pillar V	Majority assessed the maturity between 2-3 (managed-defined), out of 5	

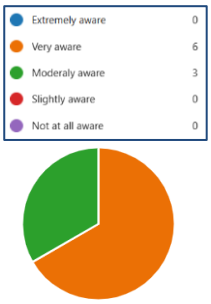
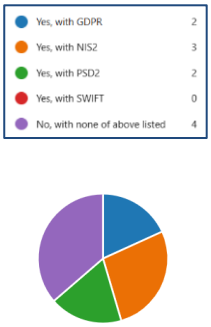
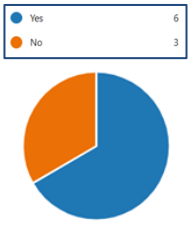
Table 3: Summary of evaluation results

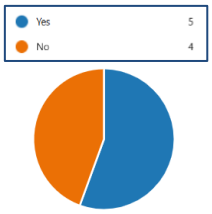
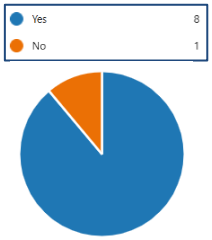
4.2 – Detailed Result Observation (*per questions/activities*)

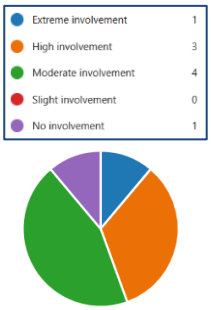
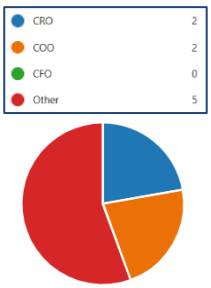
4.2.1 General Part

Question	Graphic	Result observation			Consistent Trend[5]
		% per response	In-depth result analysis	Observational conclusion	
1,2 and 3		*100% - taken internal actions* *89% - Yes, perform high level gap analysis* *11% - No*	*All participated financial entities have taken some internal actions to prepare for DORA.* *Frequent examples:* - *Gap Analysis (89%)* - *Roadmap/project plan* - *Task assignment to experts*	*This indicates that financial entities are well aware of DORA importance and early perform various internal actions towards preparation for its compliance.*	✓
3		*67% - A fair amount* *22% - Know something/a little* *11% - Very well*	*All participated financial entities have taken some internal actions to prepare for DORA compliance.* *Frequent examples:* - *High level Gap Analysis* - *Roadmap/project plan* - *Task assignment to experts*	*This indicates that all interviewed financial entities identified an essential DORA importance, thus majority familiarized themselves on DORA requirements in time.*	✓

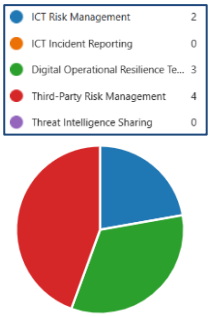
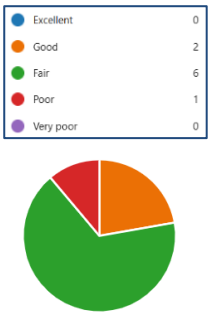
[5] Consistent trend means that major (more than 60%) of participated financial entities perform or consider a certain activity identically, whereas the inconsistent trend means the opposite i.e. that a certain activity has been performed/considered differently/unequally by minority of participated financial entities (less than 60%)

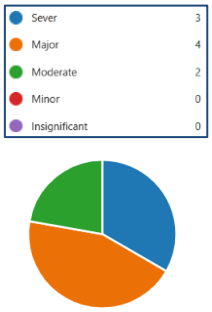
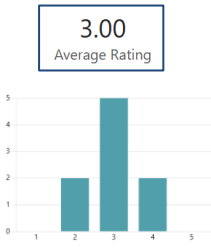
5		*67% - Very aware* *33% - Moderaly aware*	*All entities are aware, to a certain degree, of their current digital operational resilience capability. Major is very aware.*	*This provides financial entities a strategic advantage and it may significantly support the preparation for DORA compliance since awareness on current resilience capabilities may be considered as a pre-condition for an adequate DORA preparation. It enables them to proactively identify and mitigate risks and optimize resource allocation.*	✓
6		*36% - No, with none of listed* *27% - Yes, with NIS2* *18% - Yes, with GDPR* *18% - Yes, with PSD2*	*Financial entities have performed the mapping with differently relevant regulations, directives and/or standards e.g. in addition to available options against the ISO 27000.*	*This may indicate that now financial entities have majorly been focused on requirements set out in DORA itself rather than in any other relevant regulations. However, this does not exclude that mapping may be performed at the later stage as all financial entities agreed that mapping will minimize the compliance gaps, streamline compliance efforts by identifying overlaps and reduce duplication of work, operational efforts and risks.*	✗
7		*67% - Yes* *33% - No*	*Major financial entities did involve an external support/consultancy.*	*This may indicate several assumptions:* *- DORA importance has been identified* *- Ensuring independency, specialized expertise and*	✓

				fresh perspective in early gap analysis/assessments as preparation for DORA	
8		*56% - Yes* *44% - No*	*More than half of financial entities have officially consulted and exchanged information with other financial institution*	*No officially/clearly established communication and cooperation among financial entities; Potential lack of information sharing, industry-wide collaboration, collective learning and knowledge sharing*	✓
9		*89% - Yes* *11 – No*	*Almost all financial entities consider DORA as priority, except 1*	*This shows that DORA presents a strategic imperative and a major regulatory document which generates a major impact on organizational operations and awareness of top management that in case of not prioritizing it may lead to severe financial penalties, reputational damage and eventual business disruptions*	✓
10		*89% - Yes* *11% - No*	*Consistent trend identified i.e. that in almost all entities (except in 1) there is a management commitment achieved.*	*This may be analyzed together with the question 9.* *However, this indicates a clear management commitment which is a precondition to adequately prepare for DORA compliance. Furthermore, in most cases this also mean a readiness for ensuring a necessary budget, operational efforts and resources. This also*	✓

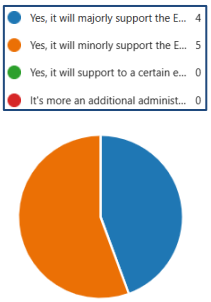
				fosters the cultural changes across the organizations and demonstrates to relevant stakeholders that organization is dedicated to DORA requirements.	
11		*44% - Moderate involvement* *33% - High involvement* *11% - Extreme involvement* *11% - No involvement*	*In most cases the management board is involved to a certain degree (moderate-high) in effective management of security risks and incidents rather than being not involved at all, which was the rare case observed*	*This may indicate the maturity level of financial entities i.e. that MB is not only aware but also actively involved in managing security incidents and risks which may furthermore significantly impact the preparation for DORA compliance. From the observation, it may also be concluded that the MB involvement does not relate to the entity size.*	✗
12		*56% - Other* *22% - COO* *22% - CRO*	*In major cases this was assigned to COO or CRO or defined like a shared responsibility between these two divisions.*	*There is no "rule" or a common practice identified but this varies from entity to entity e.g. depending on their own organizational structure like where the cyber security or cyber risk is allocated. Also, in some cases this was undefined. Interests in sharing the best/common practices on this subject have been raised by many financial entities.*	✗
13	-	*- (Open question)*	*No commonly stated benefits identified. Some of mentioned ones are:* *- Security awareness*	*Many various benefits have been identified which indicates additional values this regulation introduces which will ultimately support the adequate*	✗

			- *Having a concrete regulation which provides more details for implementation but also harmonizes relevant requirements e.g. on incident reporting obligations* - *Requirements for critical service providers* - *Extension of third-party risk management* - *Enforcing the adherence to the same testing standards* - *Impact on digital trust towards customers*	*implementation of digital resilience across the EU, as it has also been assessed so within the question 22. Ultimately, this also motivates other financial entities to prioritize and position themselves towards the compliance with DORA.*	
14	-	*- (Open question)*	*There are numerous examples mentioned:* *- More regulatory demands e.g. on reporting, risk mgmt.* *- No official/unclear mapping or interconnection with other relevant information security regulations/standards* *- Requirements on IT resilience testing* *- To many detailed requirements*	*This indicates that besides many benefits there are still many reasonable "concerns" and expected operational burdens in respect to operational impact of DORA and its adequate implementation. However, based on observations it may be concluded that many identified stains will be addressed/specified and resolved within respective RTSs and ITSs.*	✗

15	*This question has not been formualted on percentage basis hence it has been analysed separately. (please see below, at the end of this Table)*				
16		*44% - Third-party risk management* *33% - Digital Operational Resilience Testing* *22% - ICT Risk Management*	*Almost half of participated firms declared that this is the pillar 4, Third-party risk management. However, there was a common view that requirements in all pillars will create operational impact to a certain extend.*	*Assuming that answers have been provided in accordance with the current maturity and readiness status of organizations, this indicates that financial firms are differently mature in different areas/pillars. Also, this result may indicate that more and more services are being outsourced hence enforcement of an adequate third-party risk mgmt. (incl. coordinating and standardizing risk management) becomes more important but more difficult, too due to its complexity. Also, some of reasons for this identification may be more reliability on diverse service providers outside the EU which complicates the compliance even more.*	✗
17		*67% - Fair* *22% - Good* *11% - Poor*	*Most answers have been in the range between Fair-Good.*	*This indicates that generally the situation in respect to digital operational resilience, prior to DORA, has been fairly mature. Moreover, this may mean that there is a certain basis achieved which may support the compliance with DORA. Nevertheless, based on observations there are many areas*	✓

				identified where financial entities face a complete lack of compliance.	
18		*44% - Major* *33% - Severe* *22% - Moderate*	*Most answers have been in the range between Moderate-Sever.*	*This indicates that is evident that DORA has a potential to reshape how financial institutions will operate in evolving threat landscape. In combination with consideration of Question 17, this may also indicate that this impact was not assessed so because digital resilience was at poor level so far, but because DORA does address critical aspects of digital operational resilience and request completely different and/or new requirements. Substantial penalties for non-compliance have been considered, too.*	✗
19		*56% - 3* *22% - 4* *22% - 2*	*The average rating has been 3, out of 5.*	*Despite the significance of DORA, this shows that there is no financial firm who declared itself as fully ready to be compliant with DORA. On another side, minority of firms consider themselves as "confident" with DORA compliance, whereas majority is the opinion that they are somewhere in between/in the middle i.e. aware of what is still lacking to be enforced for insurance of DORA compliance. There*	✓

				was no relation between readiness rate and size of the entity identified. As a conclusion, based on all observations and taking DORA requirements into account, it may be agreed that DORA requires a cultural shift and lastly that this result seems to be reasonable realistic.	
20	-	*33% - 5* *22% - 3* *22% - 2* *11% - 4* *11% - 7*	*Out of the offered range between 1-10, the average value for budget allocation is set at 3.6, which would mean "Medium".*	*Considering the Question 9, i.e. that DORA is seen as a priority for most of the firms, this relatively low budget allocation does not follow this trend i.e. is not assessed as High. However, this may change over time especially at the later stage when requirements will be specified hence organizations may more preciously know what is to be enforced. Therefore, change (decrease/increase) of a budget allocation may follow. Lastly, with more specifications on requirements through RTSs and ITSs, the understanding may be increased which may also impact a potential re-allocation of budget.*	✗
21	-	*- (Open question)*	*This was an open question hence no statists is provided.*	*Answers to this question which also include declaring that there are*	✗

			Therefore, some of examples given have been the following: *- Incident communication e.g. SPOCs assignments* *- Treat Led Penetration Testing (TLPT) and interconnections with TIBER-EU framework* *- Introducing "Loss of Authenticity" as a separate protection class/level* *- Requirements on contraction and sub-contracting* *- Detailed third-party risk register* *"None" has also been one of answers.*	*"none" completely new requirements stipulated in DORA, indicate that financial firms may either understand DORA requirements differently or that they are at different maturity levels and therefore some requirements may be considered as "completely" new whereas for others not. In case 1, this furthermore clearly shows a need for RTSs which will provide further specifications in order to reduce potential misunderstanding/misleading as much as possible i.e. to make all stakeholders as equally to understand the requirements as possible.*	
22 and 34		*55% - Will minorly support the EU* *44% - Will majorly support the EU* *100% - Agree on the EU role*	*Results exhibit that all financial entities consider DORA as a regulation which supports (minorly or majorly) the overall EU resilience rather than an additional administrative document which would not generate an actual impact on EU resilience.* *Furthermore, all financial entities identify the essential role of the EU in*	*This indicates that the pivotal role of the EU in strengthening the cyber security of financial entities as well as in supporting financial sector in Europe to stay resilient is recognized by all financial entities.*	✓

			*supporting and promoting digital operational resilience across the EU.*		

Table 4: Detailed result evaluation and observation

Question 15:

Where in the context of the risk management cycle has your organization until now faced most difficulties, gaps and flows in relation to its ICT resilience? (1 - Not problematic, 5 - High problematic)

Legend: 1 - Not problematic, 5 - High problematic

Figure 4: ICT risk mgmt. cycle assessment

Result analysis: "*Detection*" and "*Internal coordination*" as one of areas of ICT resilience process resulted do be assessed as the highest problematic areas, reported by 1/3 of participated entities. On another side, the area of "*Information sharing with other financial actors on treat intelligence*" appeared to be the least problematic ICT area.

Observational conclusion: This indicates that many organizations have difficulties in the very early stage of detecting incidents/risks rather than protecting against

them once identified, respond and recover from them. Also, it may be challenging to establish comprehensive and real-time monitoring systems that can detect emerging threats and vulnerabilities effectively. Moreover, the scope of such monitoring mechanisms may cause difficulties as many financial entities struggle with setting up and maintaining robust detection mechanisms that cover a wide range of potential risks, from cyberattacks to operational disruptions.

The constantly evolving nature of cyber threats and the increasing sophistication of attacks make it difficult to keep detection mechanisms up-to-date. This may also refer to new attack vectors and techniques which rapidly emerge, requiring continuous adaptation and refinement of detection tools, policies and strategies.

Overall, the problematic nature of the detection phase in ICT risk management may be taken as an indication which highlights the need for ongoing investment, expertise, and adaptability in detective mechanisms to effectively identify and respond to emerging threats and vulnerabilities.

The table below displays the summary on where a consistent/inconsistent trend per questions has been identified. In addition to definition of consistent/inconsistent trend, "n/a" means that there was no possibility to identify a trend due to formulation of a question.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22
Consistent trend	x	x	x	x	x		x	x	x	x							x		x			x
Inconsistent trend						x					x	x	x	x		x		x		x	x	
n/a															x							

Figure 5: Summary of trend consistency

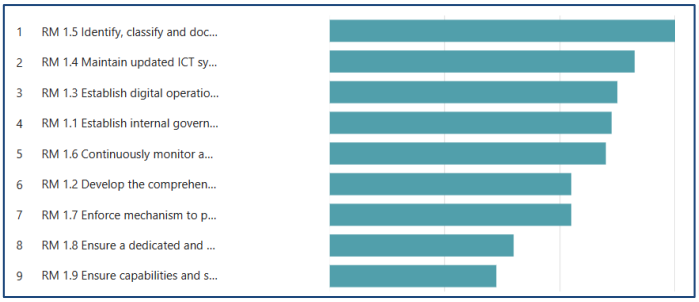
4.2.2 DORA specific

Pillar 1 - ICT Risk Management

Self-assessment I (Question 23)

*Ranking **top 5** activities in accordance to their impact on DORA preparation:*

General overview:



Analysis in more detail:

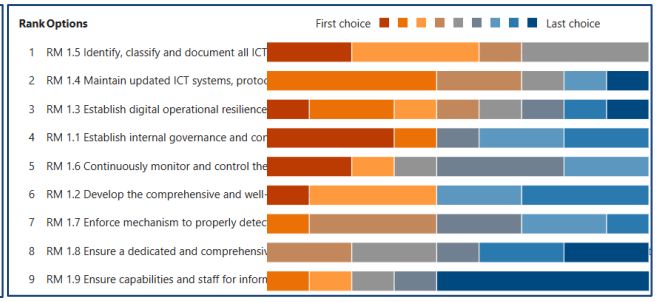


Figure 6: Pillar I – Ranking assessment

RM 1.5	RM 1.4	RM 1.3	RM 1.1	RM 1.6
1st choice: 2 (22%) 3rd choice: 3 (33%) 4th choice: 1 (11%) 5th choice: 3 (33%)	2nd choice: 4 (44%) 4th choice: 2 (22%) 5th choice: 1 (11%) 7th choice: 1 (11%) 9th choice: 1 (11%)	1st choice: 1 (11%) 2nd choice: 2 (22%) 3rd choice: 1 (11%) 4th choice: 1 (11%) 5th choice: 1 (11%) 6th choice: 1 (11%) 8th choice: 1 (11%) 9th choice: 1 (11%)	1st choice: 3 (33%) 2nd choice: 1 (11%) 6th choice: 1 (11%) 7th choice: 2 (22%) 8th choice: 2 (22%)	1st choice: 2 (22%) 3rd choice: 1 (11%) 5th choice: 1 (11%) 6th choice: 3 (33%) 7th choice: 2 (22%)

Figure 7: Pillar I - Percentage view per top 5 activity (left to right)

Result analysis:

Note: Due to complexity and many activities defined in this pillar, only top 5 activities have been taken into account for the performed result analysis.

Activity to "*Identify, classify and document all ICT related functions, roles, processes or assets*" (addressed in Article 8) has been assessed as top 1 activity that will generate the biggest impact to ensure compliance with requirements laid down hereunder. This indicates that majority of financial entities may have operational difficulties within the "Identification" as one of preconditions for enforcement of an adequate and comprehensive ICT risk management framework, which in this case addresses 2 aspects, identification of ICT risks and mapping of

processed, infrastructure that may be exposed to such risks. Complexity of ICT ecosystems and environments consisting of numerous systems, applications and networks may cause difficulties in identifying all respective components, assets and vulnerabilities.

Furthermore, this may also show that financial entities may currently not be aware enough or may not have adequately established inventory of their own hardware/software/applications/systems interconnections and/or interdependencies (internal and external) with ICT service providers that support critical or important functions.

Financial entities may struggle to maintain a complete and accurate asset inventory, making it difficult to assess the full scope of potential risks. However, this will form an essential basis for adequate conduction of vulnerabilities scanning to identify and assess cyber threats and ICT vulnerabilities as well as for compliance with chapter 5, ICT third-party risk management.

The activity to "*Maintain updated ICT systems, protocols and tools*" (addressed in Article 7) has been assessed as the 2nd one in accordance with the impact that will generate, which shows that a lot of financial entities may still have legacy systems in place which may not provide a sufficient capacity to properly and accurately process the data and may therefore not be considered as technologically resilient. Also, ensuring the compatibility of updated systems with any legacy solutions, applications or databases can be a time-consuming and resource-intensive process. The results under the question 27, where the "*Issues with legacy systems*" has been examined, confirms this indication since 45% of financial entities declared this area as highly problematic in handling ICT operational resilience incidents.

These challenges highlight the importance of strategic planning, investment, and risk management in maintaining the resilience and security of ICT systems in the financial sector and DORA therefore sets out a necessity to focus on new technology and use and maintain updated ICT systems, protocols and tools.

Self-assessment II (Question 24)

Focus on maturity levels per defined activities

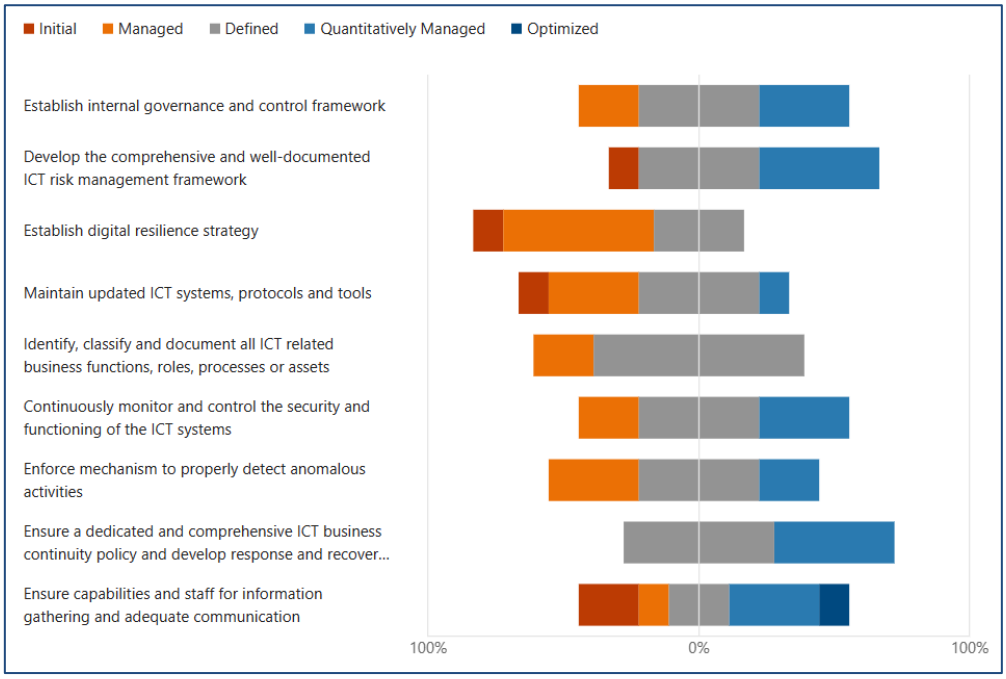


Figure 8: Pillar I – Maturity level assessment

Result analysis:

The lowest maturity level of financial entities has been assessed on the activity to "*Establish digital resilience strategy*" where more than half of financial entities, 56% self-assessed their maturity at "Managed" i.e. at 2 at the scale from 1-5.

This may indicate that financial entities may not have at all or may not have a dedicated/separately established and approved digital resilience strategy so far. Preparation activities towards compliance with these requirements (addressed in Article 6, paragraph 8) may be essential as elements which shall be addressed by the strategy concern information security area itself e.g. by setting out clear information security objectives, including KPIs and KRIs as well as concerning other areas set out in other DORA pillars like handling ICT related incidents by outlining different mechanisms to detect them, implementing digital operational resilience testing (Chapter IV) and lastly defining a holistic ICT multi-vendor strategy which concerns ICT third-party risk management.

Furthermore, in general establishing a strategy, in this case for digital resilience, shall consider the cyber threat landscape as well as the interconnectedness of the financial institutions. This means that such strategy shall address emerging risks,

following on evolving and dynamic nature of cyber threats and continuously adapting the strategies.

On the other side, the resilience of one entity is closely tied to the resilience of another/its counterparts. Thus, establishing a collective and encompassed resilience strategy request coordination and cooperation among financial entities. All of this presents an ongoing challenge.

The highest maturity level has been determined on the activity to "*Ensure a dedicated and comprehensive business continuity policy and develop response and recovery plans/methods including the backup policies and their review*" where none of financial entities have self-evaluated themselves below "Managed" (2 out of 5), but 56% have been determined at "Defined", whereas the rest 44% has even been at "Quantitatively managed" which is 4 out of 5, or in other words at one level before the highest one, "Optimized". This activity has also been determined within the question 23 as the one with low expected impact to prepare for, being ranked at 8th place out of 9 as a total number of defined activities.

Question 15, assessing on various risk management cycle, including recovery, has also shown the identical trend that the area of respond and recovery is not self-evaluated as highly problematic to cause difficulties, gaps and flows in relation to ICT resilience.

On average the maturity level of financial entities for this pillar is medium i.e. at the value "Defined" which is 3 out of 5, according to the used values in the assessment.

Pillar 2 – ICT Incident Reporting

Self-assessment I (Question 25)

Ranking activities in accordance to their impact on DORA preparation:

General overview:

Analysis in more detail:

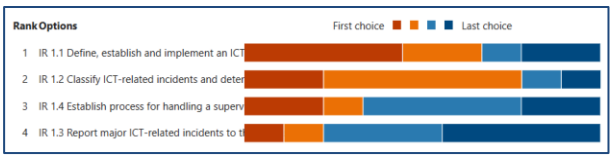


Figure 9: Pillar II – Ranking assessment

IR 1.1	IR 1.2	IR 1.4	IR 1.3
1st choice: 4 (44%) 2nd choice: 2 (22%) 3rd choice: 1 (11%) 4th choice: 2 (22%)	1st choice: 2 (22%) 2nd choice: 5 (56%) 3rd choice: 1 (11%) 4th choice: 1 (11%)	1st choice: 2 (22%) 2nd choice: 1 (11%) 3rd choice: 4 (44%) 4th choice: 2 (22%)	1st choice: 1 (11%) 2nd choice: 1 (11%) 3rd choice: 3 (33%) 4th choice: 4 (44%)

Figure 10: Pillar II - Percentage view per activity (left to right)

Result analysis:

The activity to "*Define, establish and implement an ICT related incident management process, enforcing early warning indicators*" has been self-assessed by financial entities as the activity which will generate the biggest impact to ensure and prepare for its compliance. With the same expected impact, but which less financial entities determined as their first choice, is the activity to "*Classify ICT related incidents and determine their impact following required criteria".*

In general, incident management and reporting has become an important and hot topic across financial industry due to other relevant EU regulations which regulate this area, too. This also includes potential multiple overlapping obligations to report incidents to competent authorities, eventually in different timeframes and/or with different information required.

Furthermore, the ICT-related incident reporting management process under DORA includes many elements and not only procedures for identification but e.g. for continuous tracking, logging and classification, defining roles and responsibilities as well as plans for communication on incident responding etc.

Therefore, the result above may indicate that many financial entities expect a need to re-review and revise their existing and established regimes, policies and processes in order to adapt them in accordance with requirements laid down in

DORA, which among other refer to all ICT related incidents and not to major incidents only.

On the other side, reporting of major ICT related incidents to the competent authorities has been assessed as the one for which the minimum impact for its preparation and compliance is expected, which may also indicate that financial entities may already have established mechanisms for reporting of major ICT incidents in order to comply with other EU regulations addressing the same subject, which may ultimately serve as a basis for particular DORA requirements on reporting of major ICT incidents, too.

Self-assessment II (Question 26)

Focus on maturity levels per defined activities

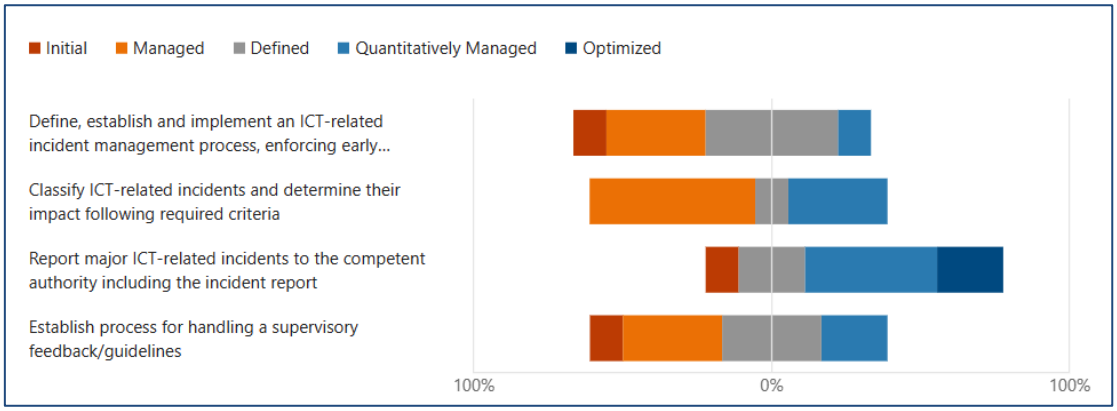


Figure 11: Pillar II – Maturity level assessment

Result analysis:

All financial entities consider their lowest maturity level on all evaluated activities almost equally with slight differences. The lowest maturity level has been assessed at the same activity which was evaluated within the question 25, as the one which will generate the biggest impact to prepare for/comply with, according to answers provided by participating financial entities.

Also, almost equal low maturity level has been determined at the activity to "*Classify ICT related incidents and determine their impact following required criteria"* which confirms the trend identified within the previous question 25, where the same activity has also been defined as the one which may pose the same expected high impact on operations to prepare for its adequate implementation.

On the other side, the highest maturity level has by far been determined at the activity to "*Report major ICT-related incidents to the competent authorities including incident report*" which also follows the trend and matches with results identified within the previous self- assessment (Question 25) since the same conclusion has also been made there.

There may be several reasons why the reporting of major ICT incidents is not generally recognized as a significant issue for financial entities. One of them may be a good and transparent criteria provided by DORA on what falls under category of a major ICT-related incident. Furthermore, many financial institutions may already have incident reporting mechanisms and protocols in place, aligned with industry best practices and regulatory requirements. Therefore, the transition to

DORA's reporting framework may be considered as an extension of existing incident management processes rather than a novel burden.

Finally, financial entities understand the importance of timely and transparent reporting in mitigating the impact of cyber incidents but also its connection to their commitment to maintaining trust with customers, regulators, and stakeholders.

On average the maturity level of financial entities for this pillar is medium i.e. between the values of "Managed" and "Defined" which is in the range from 2-3 out of 5, according to the used values in the assessment.

Self-assessment III (Question 27)

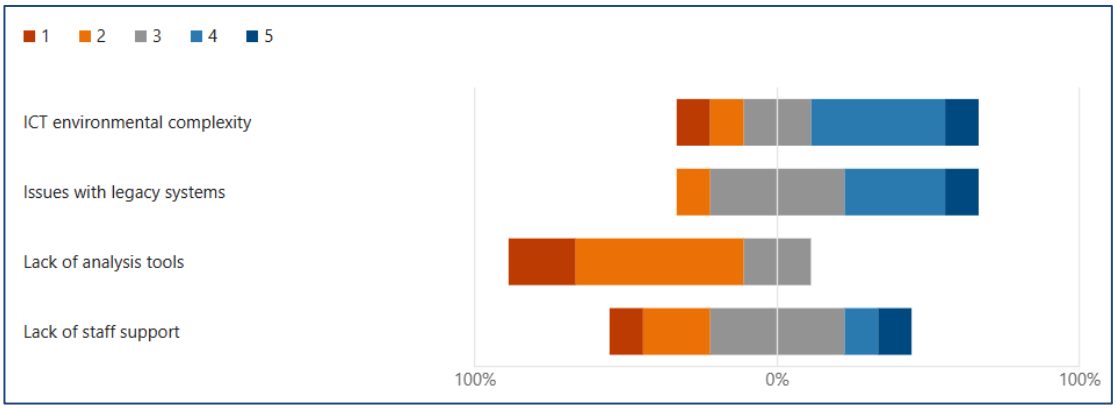


Figure 12: Assessment on handling ICT incidents

Result analysis:

The answers to this question clearly illustrates the high significance of problems or possible causes and difficulties with complexity of ICT environment as well as with legacy systems which may still be in use and have not been replaced with new, more resilient and secure ones. This shows that modernization of legacy systems in the banking industry still presents an operational challenge not only from technical but also from business and regulatory perspective.

However, modernizing legacy systems should still be seen as one of priorities in order to improve operational efficiency, customer experience, reduce costs and enhance security, as such systems are tend to be more vulnerable to cyber threats due to inadequate/outdated security measures.

On the other side, it seems that least possible operational difficulties in an organization may relate to the lack/low availability of analysis tools. One of potential reasons for assessing this area as not that problematic is the fact that cybersecurity market has witnessed substantial growth, leading to a wide array of available incident management specialized tools and solutions on the market which

significantly support throughout the entire incident management cycle and in particular in resolving incidents faster and more efficiently. Also, increased awareness of cybersecurity challenges has prompted innovation, resulting in the development of sophisticated incident detection and response tools, too.

Finally, despite the increasing importance of ICT incident management as well as availability of various analytical tools, certain difficulties persist in securing adequate staff support, as according to the results.

The lack of staff support has been assessed as neither not completely problematic nor highly problematic but in the middle i.e. “medium problematic”. This may be interpreted that there may be a fair availability of various analytical tools but there may still be a global shortage of cybersecurity professionals, making it challenging to recruit and retain skilled incident response personnel.

Pillar 3 – ICT Resilience Testing

Self-assessment I (Question 28)

Ranking activities in accordance to their impact on DORA preparation:

General overview:

Analysis in more detail:

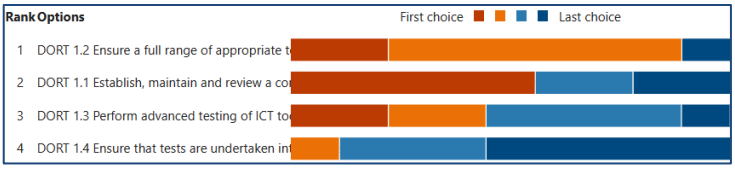


Figure 13: Pillar III - Ranking assessment

DORT 1.2	DORT 1.1	DORT 1.3	DORT 1.4
1st choice: 2 (22%) 2nd choice: 6 (67%) 4th choice: 1 (11%)	1st choice: 5 (56%) 3rd choice: 2 (22%) 4th choice: 2 (22%)	1st choice: 2 (22%) 2nd choice: 2 (22%) 3rd choice: 4 (44%) 4th choice: 1 (11%)	2nd choice: 1 (11%) 3rd choice: 3 (33%) 4th choice: 5 (56%)

Figure 14: Pillar III - Percentage view per activity (left to right)

Result analysis:

Testing is certainly one of the crucial point for which the increased requirements are addressed by DORA by requiring an establishment of a digital operational resilience testing program which shall consist of a wide range of tests.

As according to the self-assessment performed, the activity which will lead to the biggest impact to prepare for is "*To ensure a full range of appropriate tests before any deployment/re-deployment of new or existing services supporting the critical functions*".

Taking into account that this activity refers to a wide variety of tests like vulnerability assessments and scans, open source analyses, network security assessments, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing, but moreover extending to processes and people, too, this may demonstrates that many financial entities may not have an established testing program adequately covering the complete range of tests or a major adaption of an existing program is necessary.

Furthermore, following the risk based approach when conducting the digital operational resilience testing program may also be considered as a potential challenge for many financial entities.

Lastly, when it comes to activities in respect to conduction of a treat-led penetration testing (TLPT), these have not been ranked high i.e. no major impact has been identified in order to prepare for their compliance even though according to many available articles regarding DORA, this subject area has been determined as the one which may require major operational adaptions and preparations by financial entities in order to comply with all requirements regulating how to organize and carry out a TLPT.

On the other side, this may also indicate that technical standards to apply for TLPT are likely to be aligned with the Threat Intelligence-based Ethical Red Teaming (TIBER)-EU framework introduced by the EU and developed by ECB[6], which is described as a common framework that delivers a controlled, intelligence-led red team test of entities' critical live production systems, which tests mimic the tactics, techniques and procedures (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to entities. It helps an entity to assess its protection, detection and response capabilities. [24] Many EU member states might have issued the framework nationally which enabled financial entities to participate in.

The lowest expected impact for its preparation and compliance has been determined on the activity to "*Ensure that tests are undertaken (internally/externally) by independent parties and that the testers are used for deployment of TLPT*".

[6] TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming (europa.eu)

Self-assessment II (Question 29)

Focus on maturity levels per defined activities

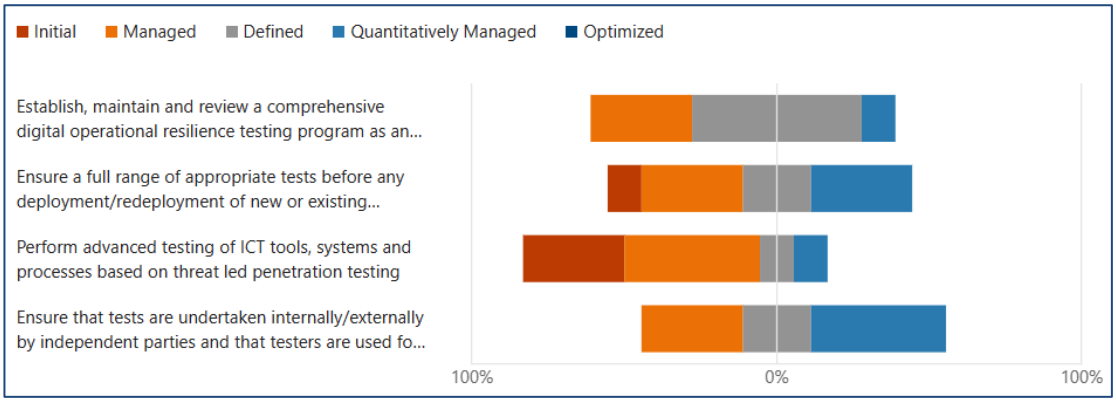


Figure 15: Pillar III – Maturity level assessment

Result analysis:

In comparison to self-assessment evaluation shown above, within the previous question 28, the evaluation results and analysis here look differently. In other words, the lowest maturity level of financial entities has been assessed at the activity on "*Performing advanced testing on ICT tools, system and processed based on TLPT*" which on another side was not recognized as an activity which will generate a major impact to prepare for its compliance, as according to the previous question.

However, this illustrates that a majority of financial entities, more preciously 77% of them would rate themselves with "Initial" or "Managed" maturity levels whereas only 11% of financial entities consider themselves "ready" for this requirement declaring their own maturity level at "Quantitatively managed".

44% of financial entities consider own maturity level as high - "Quantitatively managed" when it comes to ensuring the independence of internal/external parties of testers used for deployment of TLPT which may indicate that financial entities have already engaged (external) independent parties to conduct regular penetration tests hence this may not cause major operational efforts and/or procedure or process adaptions.

Nevertheless, the highest maturity level has been determined on the activity to ""*Ensure that tests are undertaken (internally/externally) by independent parties and that the testers are used for deployment of TLPT*" which follows the trend and matches the results analyzed under the question 28.

This illustrates that financial entities often do not encounter significant difficulties in ensuring independent ICT resilience testing due to several factors like frequent engaging of specialized third-party firms with expertise in ICT resilience testing, ensuring a high level of independence. Also, this shows that the importance of resilience testing in safeguarding financial stability is recognized and has led to investments in robust testing procedures, where independence has already been considered as one of mandatory principles.

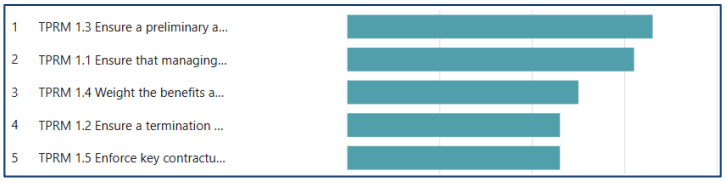
On average the maturity level of financial entities for this pillar is medium i.e. at the value “Defined” (3 out of 5), according to the used values in the assessment.

Pillar 4 – ICT Third-party Risk

Self-assessment I (Question 30)

Ranking activities in accordance to their impact on DORA preparation:

General overview:



Analysis in more detail:

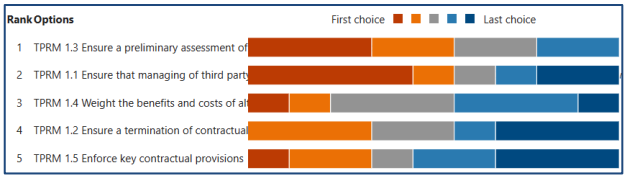


Figure 16: Pillar IV – Ranking assessment

TPRM 1.3	TPRM 1.1	TPRM 1.4	TPRM 1.2	TPRM 1.5
1st choice: 3 (33%) 2nd choice: 2 (22%) 3rd choice: 2 (22%) 4th choice: 2 (22%)	1st choice: 4 (44%) 2nd choice: 1 (11%) 3rd choice: 1 (11%) 4th choice: 1 (11%) 5th choice: 2 (22%)	1st choice: 1 (11%) 2nd choice: 1 (11%) 3rd choice: 3 (33%) 4th choice: 3 (33%) 5th choice: 1 (11%)	2nd choice: 3 (33%) 3rd choice: 2 (22%) 4th choice: 1 (11%) 5th choice: 3 (33%)	1st choice: 1 (11%) 2nd choice: 2 (22%) 3rd choice: 1 (11%) 4th choice: 2 (22%) 5th choice: 3 (33%)

Figure 17: Pillar IV - Percentage view per activity (left to right)

Result analysis:

The highest ranked activity where the biggest impact on operations is expected is "*Ensuring a preliminary assessment of ICT concentration risk and further sub-contracting arrangements*" whereas the lowest expectation to generate an impact *is "Enforcing key contractual provisions".*

One key difficulty lies in assessing whether an existing or new third-party relationship poses a concentration as well as the cybersecurity practices, maturity level and resilience of various third-party service providers, especially those offering important and critical functions. Ensuring that third parties adhere to the same rigorous cybersecurity standards and incident response protocols as the financial institution itself can be complex.

One significant challenge is the need for careful oversight, management and monitoring of subcontractors to ensure they meet the same cybersecurity standards and resilience requirements mandated by DORA. This involves additional assessment of subcontractor practices which may introduce more complexity and diversity in managing the third-party risk management process.

Therefore, financial entities must dedicate significant resources to due diligence, monitoring, and ongoing collaboration with third parties service providers.

Self-assessment II (Question 31)

Focus on maturity levels per defined activities

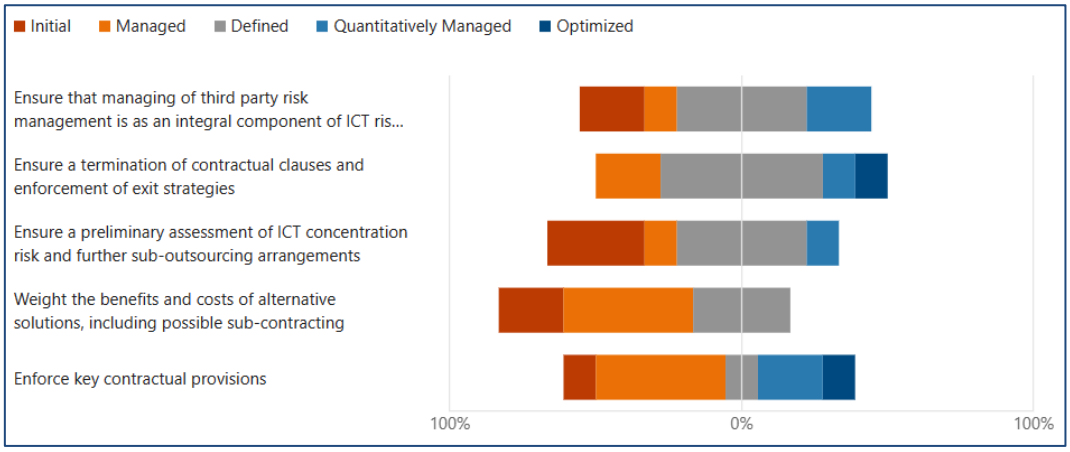


Figure 18: Pillar IV – Maturity level assessment

Result analysis:

Result of maturity level assessments do not follow the trend identified within the self-assessment on ranking activities in accordance with expected operational impact on DORA preparation.

In comparison to Question 30, the lowest maturity level has here been determined by the activity on "*Weighting the benefits and costs of alternative solutions, including possible sub-contacting"* which was the 3rd activity ranked in accordance with the expected impact.

Cost-benefit analysis may be challenging due to several factors. Evolving and dynamic nature of cyber threats may require regular assessments and adaptions of risk management strategies. Thus, inability to predict effectiveness of risk mitigation measures makes it difficult the accurately assess the long-term benefits.

On another side, the highest maturity level has been assessed on activity to "*Ensure a termination of contractual clauses and enforcement of exit strategies*". Nevertheless, the area of contact management including the enforcement of exit plans/strategies i.e. conducting required adaptions in contracts and sub-contacts, does present an area which will pose a significant resource allocation, especially in respect to monitoring performance against established contracts/key performance indicators (KPIs).

On average the maturity level of financial entities for this pillar is rather low, as it has been assessed between "Managed" and "Defined" i.e. in the range from 2-3, out of 5, according to the used values in the assessment.

Pillar 5 – Information Sharing

Self-assessment I (Question 32)

On performing any activities in respect to exchanging on cyber threat information and intelligence among relevant stakeholders

Due to the fact that there is only one activity defined for this pillar there was no ranking according to the expected impact required hence one general question has been formulated instead aiming at whether financial entities perform any activities in respect to exchange of cyber threat intelligence information.

General overview:

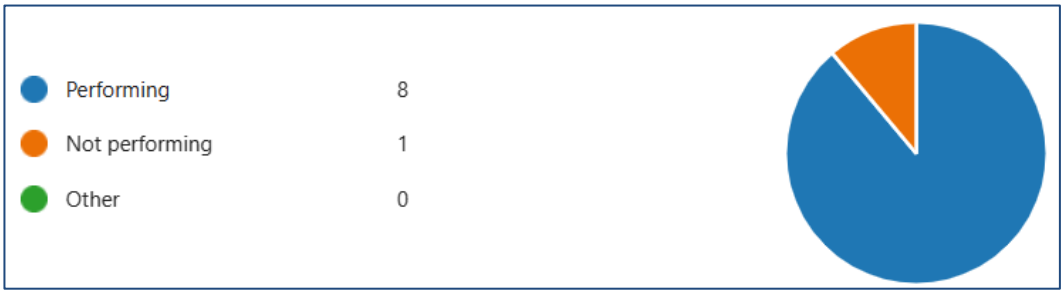


Figure 19: Pillar V – Performance assessment

Result analysis:

89% of financial entities already perform some activities in respect to exchanging on cyber threat information and intelligence among relevant stakeholders.

This shows that almost all financial institutions recognized the importance of CTI information sharing and have embraced it as an integral part of their cybersecurity strategy. Regulatory demands as well as operational demands on more effective industry collaborations are driving financial entities even more to actively engage in CTI information sharing and to enhance the joint defense mechanisms against sophisticated cyber threats.

In summary, this indicates that the area of CTI information sharing has been recognized as one of strategic imperatives for many/majority of financial entities. This also empowers financial institutions to fortify their cybersecurity defenses, detect threats as early as possible, and collaborate effectively in the fight against modern and evolving cyber threats. Ultimately, CTI information sharing is a proactive and collaborative approach that enhances the digital operational resilience of the financial sector.

Self-assessment II (Question 33)

Focus on maturity levels per defined activities

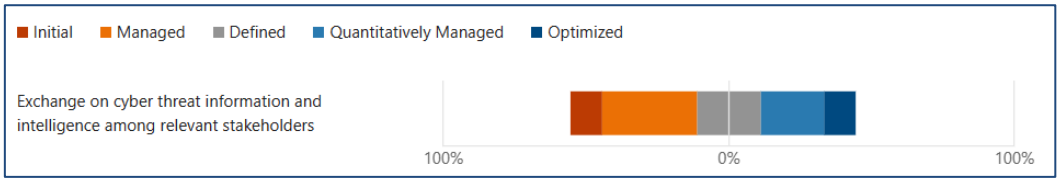


Figure 20: Pillar V – Maturity level assessment

Result analysis:

On average, the maturity level of financial entities on CTI information sharing may be assessed as medium meaning between “Managed” and “Defined”, according to the used values in the assessment.

Only 11% of financial entities identify their maturity level as “Initial” (the lowest) and on the other side the identical percentage of 11% applies for identification at “Optimized” (the highest).

This illustrates that financial entities identified a beneficial role of CTI information sharing which allows them to stay up-to-date on the latest cyber threats, vulnerabilities, and attack techniques. By receiving timely and relevant threat intelligence, as early warning signals, financial entities may proactively bolster their cybersecurity defenses, identify potential risks, and take preventative measures to timely mitigate threats. Lastly, this ultimately strength the overall security posture of the entire financial sector.

5 Conclusion

DORA represents a watershed moment in the regulation of financial entities within the EU. As this research paper has examined, DORA underscores the critical imperative of fortifying the operational resilience of financial institutions in the face of an evolving digital landscape. With its ambitious provisions, DORA has set forth a formidable framework that places cybersecurity and operational continuity at the forefront of financial services.

Throughout the course of this research, I have explored the multifaceted challenges and opportunities that financial entities encounter on their journey to comply with DORA. The findings reveal a complex tapestry of readiness factors, ranging from the resource-intensive nature of compliance to the intricacies of incident management and cross-border coordination. Financial institutions, both large and small, must navigate these challenges while striving to meet the stringent requirements of DORA.

One of the pivotal insights that emerges from this analysis is the transformative impact of DORA on the financial sector. Compliance with DORA necessitates more than just regulatory adherence, it demands a cultural shift towards digital operational resilience. Financial entities must adopt a proactive stance, investing in robust cybersecurity measures, fostering a culture of continuous improvement, and embracing the dynamic nature of digital threats.

The benefits of DORA compliance are significant, extending beyond regulatory demands. Financial entities that successfully navigate the complexities of DORA will drastically bolster their cybersecurity defenses, enhance incident response capabilities, and ultimately safeguard the digital trust of their customers and stakeholders.

However, it is essential to acknowledge that DORA readiness is not without its challenges and this has also been illustrated throughout the interview conduction process and its final results. Smaller financial entities, in particular, face resource constraints that can make compliance a daunting endeavor. The need for harmonization across borders adds another layer of complexity, requiring cross-border institutions to navigate diverse regulatory landscapes.

In particular and among other taking all interview results and their analysis into account as well as considering reports [25] and [26], there may be several potential

challenges for financial entities to be identified for each DORA pillar and those may be listed as follows:

ICT risk management:

- Senior/top management accountability for implementation of the ICT risk management framework
- Designation across the financial institutions of what the critical and important business services and their associated assets, functions and processes are
- Enforcing a digital operational resilience strategy which should be in line with the financial entity's business strategy and objectives
- Establish a role to monitor the arrangements concluded with ICT third-party service providers, with an exception of microenterprises
- Developing response and recovery strategies and plans

ICT incident management:

- Complex and evolving threat landscape which significantly impact managing and responding as well as a constant adaptation of incident management practices and processes
- Lack of resources, incident response tools and technologies, and necessary trainings
- Incident detection mechanisms and investments in advanced monitoring and detection systems
- Review of existing incident classification methodology to ensure that is in line with the requirements of the regulation and a establishment of a proper incident classification
- Cross-border operations for which incident management practices must be aligned with different international considerations and legal and regulatory frameworks
- Dependencies on third-party service providers for which an effective incident management system shall be ensured
- Data privacy as financial entities handle PII/sensitive customer data hence incident management must align with data various privacy regulations
- Incident reporting and notification where financial entities are required to comply with different timelines and requirements, particularly in the event of a significant/major incident where financial entities shall set up the adequate processes and channels

- Incident response testing where financial entities shall conduct regular testing and simulation of incident response plans

To address these challenges, financial entities should invest in robust incident management programs that include advanced detection and response capabilities, clear incident classification processes, cross-border coordination, and thorough training for incident response teams. Collaboration with industry peers and participation in information sharing initiatives may also enhance incident management practices.

ICT digital operational resilience testing:

- Testing complexity due to a demand to conduct various types of testing, including vulnerability assessments, penetration testing, and scenario-based testing. These activities can be complex, time-consuming, and may require specialized expertise.
- Testing frequency
- Third-party involvement as financial entities often rely on third-party vendors and service providers. Ensuring that third parties also adhere to robust testing practices and share the results with the entity can be challenging but is critical for overall resilience.
- Reporting and documentation where financial entities must maintain comprehensive records of testing activities and results for regulatory compliance.

To address these challenges, financial entities should establish well-defined testing programs that include a mix of automated and manual testing approaches and to adhere to regulatory testing schedules.

ICT third-party risk management:

- Complexity of third-party and supply chain ecosystem with a special focus on cloud service providers, software vendors, data processors
- Obligatory contractual provisions that have to be present in any contracts between a financial entity and an ICT third-party provider
- Defining a multi-vendor ICT third-party risk strategy
- Establishing and maintaining of a Register of Information
- Major increase on resources to establish an effective third-party risk management
- Vendor Due Diligence/assessment used for selecting and onboarding third-party vendors which more preciously and more rigorously involves assessing the vendor's security and resilience measures as well as their

maturity levels. This may also refer to vendor reliance and exit strategies in case of multiple vendor selection

- Rapid technological changes and innovations which requires a continuous monitoring on new technologies and service as well as on evolving risks associated with these technologies
- Data protection and cross-border data processing due to applicability of different regulations

To address these challenges, financial entities may need to invest in dedicated third-party risk management programs, establish clear governance structures, leverage technology solutions for risk assessment and monitoring, and prioritize ongoing training and education for their staff.

In addition, as elaborated in [27] DORA would also establish a new EU-level oversight framework for certain TSPs designated as “critical” by the ESAs. The CTPP oversight regime represents a novel regime in comparison to the current regulatory framework for technology outsourcing by financial institutions in Europe—EU financial regulators currently supervise and impose outsourcing requirements on financial institutions, but do not directly supervise TSPs.

Information and Intelligence sharing:

- Determination of what information to be shared and how to be shared
- Regulatory compliance on information confidentiality while CTI information sharing financial institutions may process sensitive customer data which shall be properly safeguarded
- Hand-in-hand the adequate security of shared information shall be ensured
- Compatibility on used tools and platforms
- Timeliness and relevance of shared information is a pre-condition for an effective CTI sharing mechanism/concept as it significantly relies on the timely and relevant exchange of threat information.
- Resource allocation may be at high demand due to amount of information to be processed and analyzed.
- Cross-border collaboration where various obstacles may appear like legal/regulatory demands, language barriers, legal differences etc.
- Legal concerns and liability that may be associated with sharing CTI

A general challenge applicable for all DORA pillars is enforcement of a continuous improvement which DORA encourages by persistent investments in awareness measures, training, assessments, and updates to their ICT related processes to remain effective in the face of evolving threats.

This research on preparedness and current maturity level of participated financial entities with DORA is confronted with several limitations. The major limitations may be listed as follows:

- Novelty of DORA and difficulties to assess its long-term impacts
- Availability of research papers at the moment of the research conduction
- Limited public information on cyber security/digital operational resilience practices
- Analyzing the final text on DORA only without taking into account any further specifications laid out in respective RTSs and ITSs
- Variability in regulatory interpretations
- The rapidly evolving cybersecurity and regulatory landscape necessitates continuous updates to research findings
- Communication and cooperation between financial institutions
- Confidentiality nature of the topic and its impact on sharing relevant information

However, to overcome the limitations listed above a better and more transparent collaboration with industry stakeholders, regulatory authorities, and financial institutions should be established. This would provide access to critical data and real-world insights. Also, conducting surveys, interviews, and case studies may enable tracking of compliance trends over time. Comparisons across different financial entities may also encourage a more transparent information sharing i.e. better communication and cooperation which would enable financial entities to benefit from each other’s experiences and practices.

DORA embodies the EU's commitment to fortifying the digital foundations of its financial ecosystem. As financial entities embark on the path to DORA compliance, they must recognize that this journey extends beyond regulatory checkboxes. It represents an opportunity to elevate their digital operational resilience capabilities, ensuring that they not only meet the requirements of DORA but also stand resilient in the face of an ever-evolving digital threat landscape.

Ultimately, DORA underscores the imperative of proactively securing the digital future of financial services. By understanding the challenges, embracing the opportunities, and cultivating a culture of digital operational resilience, financial entities can navigate this transformative regulatory landscape and emerge as stewards of trust in the digital age.

In conclusion, DORA certainly represents a significant milestone for the overall operational resilience of financial sector within the European Union. This comprehensive legislation aims to strengthen the cybersecurity, incident response,

and risk management practices of financial institutions to better protect their digital services and the enhance financial stability of the EU. However, as according to the final results of interviews conducted for the purpose of this thesis, the journey towards DORA compliance is full with challenges and complexities.

Nevertheless, while the road to DORA compliance is challenging, financial entities have clear interest in meeting these requirements to enhance their operational resilience by ensuring a structured framework for improving cybersecurity measures, strengthening incident response capabilities, harmonizing and improving third party oversight which ultimately supports and contributes to the overall stability of financial services in the EU.

To bridge the gap between the requirements of DORA and current state of financial entity's readiness, financial entities must invest in dedicated risk management programs, establish clear governance structures, and leverage technology solutions to streamline risk assessment and monitoring. Collaboration with industry peers and regulatory authorities, as well as participation in various industry forums, may facilitate the sharing of best practices and support the collective problem approaching and solving.

Based on assessments of the finalized DORA text performed by Deloitte [28] the gap analysis should focus in particular on:

- ICT risk governance framework, including the identification of critical or important functions (CIFs)
- Maturity level of incident and threat data collection and analysis processes
- Level of maturity of testing scenarios and ability to construct high severity scenarios
- ICT outsourcing processes and data (including the ability of practitioners to analyze risks of concentration on third and fourth parties).

By adhering to DORA requirements and objectives financial entities will better prepare themselves for the evolving digital threats of the modern financial landscape.

Lastly, there are various further developments identified in researching readiness for compliance with DORA which may be identified as follows:

- Conduction of more extended studies
    - To track DORA compliance (readiness) over several years to assess how financial entities evolve in response to this any other changing regulation

    - To expand of comparative research by examining the readiness for DORA compliance across different geographical regions, including more financial entities.
    - To extend the scope to other types of financial entities e.g. insurance sector, investment firms etc.
- Developing industry benchmarks and key performance indicators (KPIs) specific to DORA compliance may support in facilitating standardized assessments and comparisons
- Consideration of technological innovations and researching how emerging technologies such as artificial intelligence, cloud computing, blockchain impact DORA compliance and generally the digital operational resilience.
- Integrating cyber threat intelligence (CTI) data e.g. collected by different CTI service providers, into the research to compare how financial entities have been ranked as well as to analyze how threat landscapes impacts and shapes DORA compliance.

References

[1] “Building Security Maturity Model (BSIMM) Consulting Services | Synopsys.” Accessed: May 21, 2023. [Online]. Available: https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html

[2] C. C. Editor, “operational resilience - Glossary | CSRC.” Accessed: Jun. 04, 2023. [Online]. Available: https://csrc.nist.gov/glossary/term/operational_resilience

[3] “Digital single market for Europe.” Accessed: Sep. 17, 2023. [Online]. Available: https://www.consilium.europa.eu/en/policies/digital-single-market/

[4] “Guidance on cyber resilience for financial market infrastructures,” *Bank for International Settlements and International Organization of Securities Commissions 2016*, 2016, doi: ISBN 978-92-9197-288-3.

[5] European Banking Authority, “Guidelines on ICT and security risk management,” European Banking Authority. Accessed: Sep. 17, 2023. [Online]. Available: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management and https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf

[6] “EUR-Lex - 32016R0679 - EN - EUR-Lex.” Accessed: Jun. 06, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[7] Joint Commision, “The EU’s Cybersecurity Strategy for the Digital Decade | Shaping Europe’s digital future.” Accessed: Jun. 06, 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[8] “Cross Industry Guidance on Operational Resilience,” *Central Bank of Ireland*, Accessed: Oct. 10, 2023. [Online]. Available: https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf

[9] “PS21/3 Building operational resilience,” Financial Conduct Authority - FCA. Accessed: Jun. 07, 2023. [Online]. Available:

https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience

[10] “Radley-Gardner et al. - 2016 - Fundamental Texts On European Private Law.pdf.” Accessed: Jun. 04, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

[11] “NIS 2 Directive.” Accessed: Oct. 11, 2023. [Online]. Available: https://www.nis-2-directive.com/ and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

[12] “Esma Library | European Securities and Markets Authority - SMSG advice on DORA.” Accessed: Oct. 11, 2023. [Online]. Available: https://www.esma.europa.eu/databases-library/esma-library and ESMA22-106-4405_SMSG_advice_on_DORA.pdf.

[13] “Achieving Harmonisation and Cyber Resilience in the Finance Sector,” ENISA. Accessed: Aug. 26, 2023. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/achieving-harmonisation-and-cyber-resilience-in-the-finance-sector

[14] S. Goethals and B. Bosch, “How to prepare for the Digital Operational Resilience Act?” Accessed: Aug. 26, 2023. [Online]. Available: https://www.ey.com/en_be/financial-services/how-to-prepare-for-the-digital-operational-resilience-act

[15] “Deloitte Search - DORA,” Deloitte Ireland. Accessed: Oct. 11, 2023. [Online]. Available: https://www2.deloitte.com/ie/en/misc/search.html and ie-risk-advisory-digital-operational-resilience-act-dora-05102022.pdf.

[16] “KPMG Ireland - DORA,” KPMG. Accessed: Oct. 11, 2023. [Online]. Available: https://kpmg.com/ie/en/home/misc/search.html and https://assets.kpmg.com/content/dam/kpmg/ie/pdf/2022/02/ie-digital-operational-resilience.pdf

[17] “European Securities and Markets Authority (ESMA) - ESAs consult on the first batch of DORA policy products.” Accessed: Aug. 26, 2023. [Online]. Available: https://www.esma.europa.eu/press-news/esma-news/esas-consult-first-batch-dora-policy-products

[18] B. Daskala, “RTS on ICT risk management framework RTS on simplified ICT RMF RTS to specify the policy on ICT services RTS to specify elements when sub-contracting critical or important functions”, [Online]. Available:

https://www.esma.europa.eu/sites/default/files/2023-02/Joint_ESAs_DORA_event_-_ESAs_slides.pdf

[19] PricewaterhouseCoopers, “Digital Operational Resilience Act (DORA),” PwC. Accessed: Aug. 26, 2023. [Online]. Available: https://www.pwc.at/de/dienstleistungen/wirtschaftspruefung/cybersecurity/der-digital-operational-resilience-act--dora.html

[20] J. Boote, E. Erlikhman, S. Gardner, and S. Migues., “BSIMM 13 - Trends and Insights Report 2022.” [Online]. Available: https://www.synopsys.com/software-integrity/resources/analyst-reports/bsimm.html

[21] “Building Security In Maturity Model (BSIMM) – Practices from Seventy Eight Organizations.” Carnegie Mellon University. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=450642

[22] E. Cd, “Answers of the European Financial Congress to the consultation questions,” *European Financial Congress*, [Online]. Available: http://efcongress.com/wp-content/uploads/2020/03/Position-of-the-EFC_Digital-Operational-Resilience-Framework-for-financial-services.pdf

[23] H. Snellman, “Digital Operational Resilience Act (DORA),” Digital Decade by Hannes Snellman. Accessed: Sep. 02, 2023. [Online]. Available: https://digitaldecade.hannessnellman.com/cybersecurity-strategy/digital-operational-resilience-act-dora/

[24] “TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming,” *European Central Bank*, [Online]. Available: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

[25] M. James, M. Martin, T. Ivell, and N. Nikitin, “Preparing For The New Digital Operational Resilience Rules.” Accessed: Oct. 11, 2023. [Online]. Available: https://www.oliverwyman.com/our-expertise/insights/2022/dec/preparing-for-the-new-digital-operational-resilience-rules.html and https://www.marshmclennan.com/content/dam/mmc-web/insights/publications/2023/april/digital-operational-resilience-pov(with-appendix)-final.pdf

[26] N. Ameye, “The digital operational resilience act (DORA): what you need to know about it, the requirements and challenges we see.,” NVISO Labs. Accessed: Sep. 03, 2023. [Online]. Available: https://blog.nviso.eu/2021/11/23/the-digital-

operational-resilience-act-dora-what-you-need-to-know-about-it-the-requirements-and-challenges-we-see/

[27] “Scott - The E.U.’s Digital Operational Resilience Act Clo.pdf.” Accessed: Jun. 07, 2023. [Online]. Available: https://www.pifsinternational.org/wp-content/uploads/2022/08/The-E.U.s-Digital-Operational-Act-Cloud-Services-Financial-Companies-08.06.2021.pdf

[28] A. Rigoni and G. Tessitore, “Deloitte | Audit, Consulting, Financial Advisory, Risk Management & Tax services and reports | Italy - Regulatory News Alert EU Digital Operation Resilience Act passed: implications for the financial sector,” Deloitte Italia. Accessed: Oct. 11, 2023. [Online]. Available: https://www2.deloitte.com/it/it.html and https://www2.deloitte.com/content/dam/Deloitte/it/Documents/risk/digital-operation-resilience-act-deloitte-eng.pdf

List of Figures

List of Tables