National College of Ireland

Developing a Pre-Readiness Compliance Assessment Framework for Financial Institutions under the EU's Digital Operational Resilience Act (DORA)

MSc Research Project
Masters in Cyber Security

Rishabh Sachdeva
Student ID: X21213909

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Rishabh Sachdeva
Student ID:	X21213909
Programme:	MSc Cyber Security **Year:** 2022/2023
Module:	MSc Research Project - Industry Internship
Supervisor:	Prof. Vikas Sahni
Submission Due Date:	04/09/2023
Project Title:	Developing a Pre-Readiness Compliance Assessment Framework for Financial Institutions under the EU's Digital Operational Resilience Act (DORA)
Word Count:	7870 **Page Count** 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rishabh Sachdeva

Date: 02/09/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Developing a Pre-Readiness Compliance Assessment Framework for Financial Institutions under the EU's Digital Operational Resilience Act (DORA)

Rishabh Sachdeva
X21213909
MSCCYB1- Master's in Cyber Security
National College of Ireland

Abstract

The EU Digital Operational Resilience Act (DORA) is set to become a crucial regulatory framework designed to enhance the operational resilience and cybersecurity measures within the financial services sector. By the fourth quarter of 2024, financial services regulators will require firms to fully comply with all new requirements set forth by DORA. Non-compliance will lead to substantial fines and penalties. This regulation imposes strict mandates in various areas such as ICT risk management, incident reporting, digital operational resilience testing, managing third-party risks, and information sharing. This research focuses on developing a Pre-Readiness Compliance Assessment Framework that enables financial institutions to effectively assess, quantify, and evaluate their current capabilities and potential gaps in their compliance levels in relation to the DORA requirements. Our framework primarily features a comprehensive control database aligned with DORA's requirements to conduct a gap analysis. Each control is evaluated on a compliance scale, offering a quantifiable measure of an institution's current capabilities. To facilitate this, a specialized compliance management tool is employed to generate a shareable assessment questionnaire, enabling financial institutions to easily conduct evaluations on their own. The results are then translated into intuitive visual dashboards via Power BI, offering insights into an institution's compliance level. This approach not only aids financial entities in identifying their readiness and potential gaps but also give insights for developing a roadmap for achieving full compliance with DORA's regulations.

Keywords: Digital Operational Resilience, DORA, Financial Institutions, ICT Risk Management, Third-Party Risk Management, Compliance Management, Gap Analysis, Operational Resilience

1 Introduction

The financial sector is increasingly vulnerable to sophisticated cyberattacks, making it evident that traditional cybersecurity measures are insufficient for protecting the integrity of critical computer systems (Dupont, 2019). The concept of cyber-resilience has thus emerged as a crucial supplement to the traditional framework of cybersecurity. This shift is further emphasized by the World Economic Forum's Global Risk Report, which identifies cybersecurity as a risk that has significantly worsened due to the COVID-19 pandemic.(The Global Risks Report 2022 17th Edition, 2022) The escalating costs of cybercrime is now projected to reach $10.5 trillion by 2025 which adds another layer of urgency to this issue.[1]

Financial institutions, given their size and scope, are leading the charge in adopting innovative technologies related to business process digitalization, automation, and AI.(Mavlutova & Volkova, 2019) However, this rapid digital transformation also supplements the sector's vulnerability to cyber threats. Risks associated with the use of third-party service

[1] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

providers, including cloud services, introduce additional operational challenges, such as temporary outages and data breaches.(Financial Stability Board, 2019)

To mitigate these challenges and strengthen the overall digital and operational resilience of financial institutions, European policymakers proposed the Digital Operational Resilience Act (DORA) in September 2020(European Commission 2020 -Proposal on Digital Operational Resilience, 2020). The Digital Operational Resilience Act (DORA) aims to standardize IT risk management across the financial sector, including credit institutions, banks, insurers, and pension funds etc. The regulation mandates these organizations to prove their capacity to withstand and recover from IT-related disruptions and imposes strict mandates in various areas such as ICT risk management, incident reporting, digital operational resilience testing, managing third-party risks, and information sharing .

Article 64 of DORA states that the regulation will take effect 20 days after its publication in the Official Journal of the European Union and will be applicable from January 17, 2025. (The Digital Operational Resilience Act 2022/2554, n.d.)The European Commission and European Supervisory Authorities have given companies a two-year window (2023-2024) to prepare for DORA, expecting full compliance by Q4 2024. Oversight will be provided by European Supervisory Authorities like EBA, ESMA, and EIOPA. With DORA set to become the "lex specialis," it will take precedence over other overlapping regulatory frameworks like the NIS Directive or ESA guidelines for financial entities. Therefore, financial firms are recommended to prioritize DORA as their primary point of reference for internal cyber security regulatory compliance assessments to avoid further unforeseen gaps when DORA comes into force in 2025. Entities violating the Act could be fined up to 2% of their annual global revenue or up to EUR 1 million if an individual. "Critical" third-party ICT providers may face up to EUR 5 million in fines or EUR 500,000 if an individual.

In light of the changing cybersecurity risk landscapes and the impending mandatory regulatory changes of this regulation requirements, there is an urgent need for financial institutions to reassess and realign their cybersecurity and digital operational resilience strategies. Firms are now faced with a stringent timeline to evaluate their capabilities and readiness for compliance. The immediate objective for financial entities should be to assess their current compliance levels in relation to DORA's mandates by performing a comprehensive gap analysis and identify any potential gaps. To facilitate this, firms must proactively plan to make the necessary adjustments for achieving full compliance and for it they need a well-defined set of checklists and control framework that can be rigorously tested and evaluated.

This research aims to address this critical concern by introducing a Pre-Readiness Compliance Assessment Framework tailored for financial institutions. The framework follows a gap analysis approach for firms to evaluate their current capabilities, identify any compliance gaps and evaluate their overall compliance level. At the core of this framework, is its comprehensive control database that is aligned with DORA's requirements and mandates, and for every chapter, articles and clauses, specific requirements are identified, and corresponding controls are put in place. To ensure a quantifiable assessment, each control is evaluated on a compliance maturity scale ranging from 1 to 5. And to further streamline this complex assessment process, a specialized compliance management tool OneTrust is employed to develop a customized shareable Compliance Assessment Template. The tool generates a shareable assessment template, making it easier for financial institutions to conduct evaluations independently. The collected data is processed and translated into intuitive visual dashboards using Power BI. These dashboards offer real-time insights into an institution's compliance level, both overall and broken down by individual chapters and articles etc. This multi-faceted approach not only aids financial entities in identifying their current state of readiness and their

compliance maturity level but also helps them identify actionable insights towards achieving full compliance with DORA's regulations.

1.1 Research Questions:

The primary research questions this study aims to answer are:
Q1: *How can financial institutions effectively assess their current capabilities and maturity level in relation to DORA's mandates?*
Q2: *What can financial institutions do to identify their compliance level and potential gaps in relation to DORA's mandates?*
Q3: *What methodologies can be utilized to quantify and gain insights into their compliance level with respect to DORA's mandates?*

1.2 Research Objective

The primary goal of this research is to create a Pre-Readiness Compliance Assessment Framework tailored for financial institutions to assess their compliance with the EU's Digital Operational Resilience Act (DORA). The research aims to develop a robust methodology for gap analysis, construct a detailed control database aligned with DORA's requirements, and establish a scoring mechanism for nuanced compliance evaluation. Additionally, the study seeks to develop assessment templates and integrate specialized tools and analytics platforms to generate shareable templates and visual dashboards, thereby streamlining the assessment process and offering real-time compliance insights.

1.3 Research Outline

The research paper is structured into seven sections. It starts with an "Introduction" that sets the context and objectives, followed by a "Literature Review" comparing this study to existing research on DORA and compliance frameworks. The "Methodology" outlines the methods and techniques used to achieve the objectives of this research. "Design Specifications" describes the framework's structure, while "Implementation" discusses control database, tool integration and analytics. The "Evaluation" section provides a comprehensive analysis, carried out by Waystone's cybersecurity experts, to assess the framework's efficacy Finally, the "Conclusion and Future Work" section summarizes the key findings and suggest avenues for future research and improvements.

2 Related Work

In the course of the research, existing literature was examined to identify relevant studies and methodologies that could inform the development of a DORA-specific compliance assessment framework. It was observed that research specifically focused on the DORA Act and its compliance is limited, owing to the regulation's recent introduction. While valuable insights were offered by existing literature, there were notable gaps and limitations. These observations underscore the necessity for a specialized, DORA-focused compliance assessment framework, which this research aims to provide.

2.1 Studies Specific to DORA

A significant contribution to the field of DORA compliance has been made by Pavel Gusiv, The author employs a blend of literature review and regulatory analysis to formulate a method for compliance gap analysis under DORA(Gusiv, 2023). One of the strengths of this work is its constructive research approach, which aligns closely with the methodology of the present study. This similarity in approach is advantageous as it provides a foundational understanding of DORA compliance, thereby validating the relevance and applicability of this research.

However, there are certain limitations in Gusiv's work that this research aims to address. First, Gusiv's study does not include the Regulatory Technical Standards (RTS) published that provide further technical mandates for DORA compliance. These RTS cover various aspects such as ICT risk management frameworks, criteria for ICT-related incidents, and policies on ICT services by third-party providers, all of which are incorporated into our control framework. Second, while Gusiv's study provides a method for identifying compliance gaps, it lacks a quantitative mechanism for assessing the maturity level of compliance. It categorizes requirements simply as "implemented" or "not implemented," without offering a nuanced understanding of compliance maturity. This limitation underscores the need for a more comprehensive framework, such as the one proposed in this research, which aims to not only identify but also quantitatively assess the level of compliance maturity. Pavel Gusiv himself outlined specific areas for future improvement in his work, notably the organization of DORA requirements into logical units and the inclusion of an organization's target state perspective on compliance maturity. This research directly addresses these gaps by introducing a logically structured Control Database and a quantitative scoring methodology for assessing compliance maturity. In doing so, we fulfill the future work suggested by Gusiv, offering a more comprehensive and nuanced framework for DORA compliance.

(Neumannová & Elshuber, 2022) Neumannova's study of interest focuses on the relationship between DORA and the ISO 27001:2013 standard, which has been a prevalent framework for information security governance. This study examines the alignment between DORA and ISO 27001:2013, identifying nine gaps in the latter when compared to DORA's requirements. While the paper provides useful insights into the relationship between these two frameworks, it lacks a detailed literature review and does not focus on developing a DORA-specific compliance assessment framework. This leaves room for research aimed at creating a specialized compliance framework for DORA, which is the focus of this study.

The study by (Ter Haar, 2022) offers an understanding of stakeholder perceptions within the financial sector towards DORA. While it illuminates the general acceptance and challenges of the regulation, it does not provide a methodology for compliance. This gap in the literature emphasizes the necessity for this research in developing a compliance assessment framework. (Kourmpetis, 2023) offers insights on management of ICT Third Party Risk Under the Digital Operational Resilience Act, however, it falls short in outlining methods for achieving compliance with regulations concerning third-party risk management.

2.2 Adaptation and Critique of Maturity Models in Compliance Assessment

The concept of application of maturity models, as defined by (Pullen, 2007)offers a structured approach for evaluating operational resilience and ICT risk management in financial institutions. The design science perspective, as articulated by(March & Smith, 1995), is particularly relevant, as it views maturity models as tools for problem-solving, aligning well with this project's objectives to assess and enhance compliance. The literature presents a range of frameworks for designing maturity models, with varying phase structures as outlined by(Becker et al., 2009), (De Bruin et al., 2005.) , (Maier et al., 2012), (Antonsen & Madsen, 2021)While this range of frameworks allows for adaptability, it also suggests that a one-size-fits-all approach may be ineffective for DORA compliance. Each of these works has its strengths in providing comprehensive frameworks but falls short in offering a DORA-specific model. As this research progresses in the development of a DORA-specific Compliance Maturity Model, it is planned to integrate elements from the planning, scoping, and problem-defining phases of these established frameworks. This approach aims to address the limitations

observed in the existing literature by creating a DORA-specific model to score and assess compliance maturity effectively.

2.3 Compliance Assessment Methodologies - GDPR

(Chatzipoulidis et al., 2019) introduces a readiness assessment tool aimed at evaluating GDPR compliance within businesses. The tool proposes a scoring scale that allows auditors to assess the level of conformity for each item of evidence listed. The scale includes ratings such as 'Compliant,' 'Major Nonconformity,' 'Minor Nonconformity,' 'Correction,' and 'Not Applicable,' providing a nuanced evaluation of a business's GDPR compliance status. This work provides valuable insights into structuring a compliance assessment tool but would need significant adaptation to be applied for developing a framework for DORA compliance, to give a quantifiable output that can assist to understand the maturity of the compliance level. The study by (Serrado et al., 2020) is instrumental for our DORA Compliance Assessment Framework as it employs a design science approach to identify GDPR compliance practices in banking. This aligns well with this project's focus on creating a structured, evidence-based framework for digital operational resilience. (Agarwal et al., 2018) and (Bonatti et al., 2020) both offers valuable insights into the complexities and nuances of compliance frameworks, both for GDPR and potentially for DORA. They provide various methodologies and tools that could be adapted or integrated into our DORA Compliance Assessment Framework

2.4 Existing Qualitative and Quantitative Gap Assessment Approach in Information Security Compliance

In the development of our DORA-specific compliance framework, the insights of established risk and gap assessment methodologies is crucial. The NIST Cybersecurity Framework (NIST CSF) (Institute of Standards, 2018), as developed by the National Institute of Standards and Technology, offers a qualitative, organization-wide approach risk assessment approach that aligns well with the project's objectives to identify, evaluate, and mitigate our information security requirements as per DORA. Similarly, the ISO/IEC 27001 standard provides a comprehensive risk assessment methodology and a control database, which is particularly relevant for our DORA-specific control framework. The literature also presents specialized frameworks like SOC 2 and PCI DSS, which also focus on auditing controls over information security . These frameworks offer valuable insights into the necessity of gap analysis for achieving compliance. Moreover, frameworks such as Cyber Essentials and FedRAMP offer self-assessment and third-party audit mechanisms, respectively. While these frameworks were designed for various regulatory contexts, they offer invaluable insights for constructing an effective qualitative and quantitative gap assessment strategy, a key component of our DORA compliance framework. OCTAVE published by (Alberts et al., 1999)and CORAS (Fredriksen et al., 2002), for instance, bring qualitative, asset-centric, and stakeholder-focused approaches, aligning well with our aim to develop our pre-readiness assessment tactics through tool integration, as seen in CRAMM by (Yazar, 2002)

2.5 Scoring Mechanisms

The literature on cyber risk quantification methodologies like FAIR and Monte Carlo simulations emphasizes the importance of a quantitative approach for precise risk assessment and resource allocation. Similarly, the Capability Maturity Model Integration (CMMI) framework, widely recognized for its qualitative assessment of process maturity, offers a structured path for organizational improvement (Menezes, 2002). Both approaches have their merits and limitations. While quantitative methods provide financial metrics for risk, they often require complex calculations and expert knowledge. On the other hand, CMMI's qualitative

approach is more accessible but may lack the granularity offered by quantitative metrics. Therefore, our research aims to adapt elements from these established methodologies into a DORA-specific model, focusing on the quantification of controls to gauge compliance maturity effectively.

2.6 Conclusion

The existing body of literature provides valuable insights into various methodologies for compliance assessment, risk management, and scoring mechanisms. However, it also reveals significant gaps, especially when it comes to the relatively new DORA regulations. While there are robust frameworks for assessing compliance in other domains, such as GDPR and ISO 27001, none are specifically tailored to meet the unique requirements of DORA. Existing studies, although insightful, have their limitations. For example, Gusiv's work offers a DORA-specific gap analysis but lacks a nuanced scoring system and the updates to the DORA Act. These shortcomings in the current literature highlight the need for a more comprehensive approach to DORA compliance. In summary, the current state of research underscores the need for a specialized, DORA-focused compliance assessment framework. This framework should effectively combine both qualitative and quantitative methods to provide a nuanced understanding of an institution's compliance maturity. Our research aims to fill this gap by developing a DORA-specific compliance assessment framework that addresses these needs, thereby contributing to the field of digital operational resilience in financial institutions.

3 Research Methodology

3.1 Constructive Research/Design Science Methodology

Constructive research or design science methodology serves as the backbone of this research project. This approach was utilized due to it being instrumental in identifying and resolving issues, as well as enhancing an existing system or performance, all of which contribute to the existing body of knowledge. This is particularly suited for research that aims to develop new frameworks, tools, or processes that address given challenges(Oyegoke, 2011) . It involves six key steps: problem selection, understanding the issue, designing a solution, demonstrating feasibility, linking to theory, and examining generalizability. (Pasian & Turner, 2016)

Figure 1 Key 6 steps of Constructive Research Methodology

- **Problem Selection:** The project addresses the urgent need for financial institutions to comply with the EU's Digital Operational Resilience Act (DORA).
- **Understanding:** A thorough review of DORA regulation papers, technical mandates and specifications, publications, articles and clauses.
- **Solution Design:** The research develops a Pre-Readiness Compliance Assessment Framework tailored for financial institutions.
- **Feasibility:** The framework's practicality is demonstrated through a compliance scale of 1-5 and the integration of specialized tools.
- **Theory Linkage:** The research contributes to academic discussions on cybersecurity, compliance management, digital operational resilience, third-party risk management, incident management and threat intelligence information sharing.

- **Generalizability:** The framework's approach can potentially be adapted for other similar regulations for variety of sectors, not limited to a geographical jurisdiction.

3.2 Development of Comprehensive Framework

To construct a robust Pre-Readiness Compliance Assessment Framework for financial institutions, a six-phased methodology was adopted, grounded in the principles of constructive research methodology.

Figure 2 6-Phased approach for development of the Framework

Phase 1: Literature Review and Understanding of DORA Regulation: The initial phase of the research was dedicated to a comprehensive literature review and an in-depth analysis of the Digital Operational Resilience Act (DORA). The objective was to gain a holistic understanding of the regulation, its scope, various chapters, clauses, guidelines, and their implications for financial institutions. Apart from conducting a thorough literature review on various subjects outlined in the Section 2 of this paper, various publications related to DORA were reviewed. These included white papers, reports, and guidelines primarily published by Big 4 consulting firms and other cybersecurity and compliance service providers. This helped in understanding the industry perspective on DORA compliance and identifying best practices.

During the course of this phase, the European Supervisory Authorities (ESAs) launched a public consultation on the first batch of mandatory technical standards related to DORA.[2] These standards were also reviewed and considered in the research to ensure it is up to date with the changes. By the end of Phase 1, a robust understanding of DORA and its requirements was established, setting the stage for the data collection and mapping phase that followed.

Phase 2: Data Collection and Mapping : In this phase, DORA's legal document was dissected into its constituent chapters, articles, sections, and clauses. These elements were then systematically mapped onto an Excel sheet for easier analysis and cross-referencing.

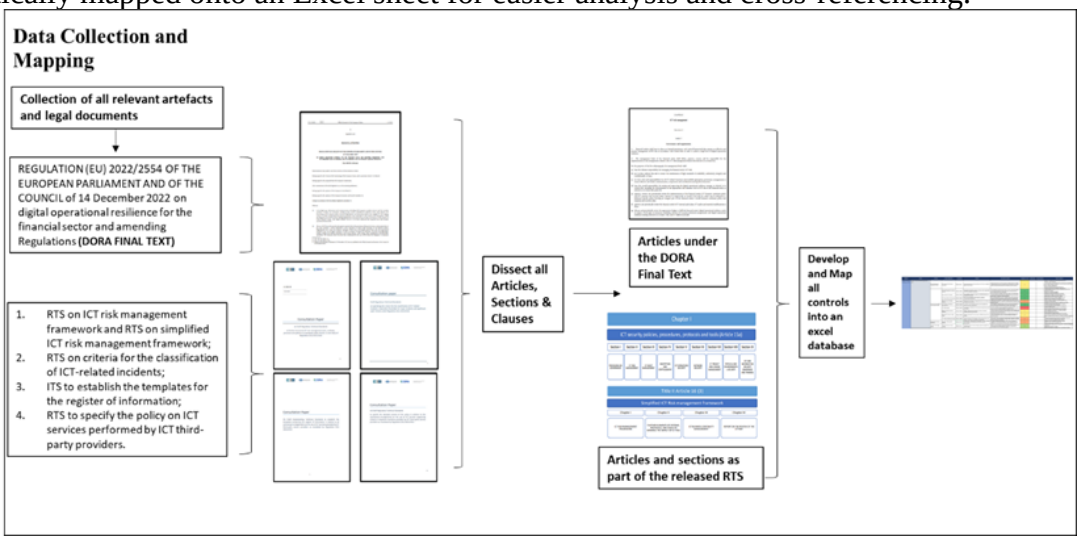

Figure 3 Data Collection and Mapping Process

[2] https://www.esma.europa.eu/press-news/esma-news/esas-consult-first-batch-dora-policy-products

Phase 3: Development of Control Framework: In this critical phase, the focus was on developing a comprehensive control framework that would serve as the backbone for assessing DORA compliance. The process began by identifying the specific requirements outlined in DORA's articles and chapters. Each requirement was then mapped to a corresponding control, which was categorized into relevant sections within an Excel matrix. The language and structure of these controls were carefully designed to align with established cybersecurity frameworks, notably the NIST Cybersecurity Framework (CSF) and ISO 27001. This alignment was crucial for ensuring that the controls were both robust and universally understood within the cybersecurity community. For each control, additional columns were added to the matrix to include control objectives, detailed descriptions, and recommendations for achieving compliance. Moreover, the controls were crafted to focus specifically on financial entities, as DORA's regulations also encompass requirements for other stakeholders like European financial supervisory agencies and third-party service providers. These were deliberately excluded to maintain the focus on financial institutions.

The end result was a comprehensive control framework that not only met the stipulations of DORA but also integrated best practices from globally recognized standards. This database serves as the foundation for the gap analysis and scoring methodology developed in subsequent phases.

Phase 4: Development of Scoring Methodology: This phase was pivotal in operationalizing the control framework into a practical tool for assessing compliance. The objective was to develop a scoring methodology that could quantify the level of compliance for each control, thereby providing a measurable metric for evaluation. Inspired by the scoring ranges used in the Capability Maturity Model Integration (CMMI) maturity levels, a 1-5 scoring range was adopted. The scoring criteria were designed to evaluate three key aspects of each control: technical implementation, operational effectiveness, and documentation quality. This multi-faceted approach was essential given DORA's comprehensive focus on these areas. For instance, a control could score low if it was well-documented but poorly implemented, or vice versa. The scoring methodology was then integrated into the existing Excel matrix developed in Phase 3. For each control, a dedicated column was added for the compliance score for facilitating the gap analysis process**.** By the end of this phase, the research project had a robust, quantifiable method for assessing DORA compliance.

Phase 5: Tool Integration: The control datasheet developed in Phase 3 served as a foundational reference for this stage. Using OneTrust, a leading compliance management platform, a template for DORA assessment was created that mirrored the structure and content of the control datasheet. This enabled a seamless transition from the theoretical framework to a practical, user-friendly tool. The OneTrust platform was configured to generate shareable assessment questionnaires based on the control framework. These questionnaires were designed to be easily distributed to key stakeholders within financial institutions, thereby facilitating independent evaluations.

Phase 6: Data Visualization and Reporting: The concluding phase of this research was centred on data visualization and comprehensive reporting. Utilizing advanced analytics tools like Power BI, the data was transformed into a series of intuitive visual dashboards. These dashboards were designed to offer multiple insights into an institution's compliance level. Various types of graphs were employed to showcase compliance metrics at different levels—ranging from an overall compliance level to chapter-wise, section-wise, and even article-wise assessments. By the end of Phase 7, the research had come full circle, providing a complete end-to-end solution for assessing and improving compliance with DORA, thereby fulfilling the objectives set out at the beginning of this study.

4 Design Specification

4.1 Overall Approach to Pre-Readiness Compliance Assessment

The overall approach to pre-readiness compliance assessment is designed to be a comprehensive, step-by-step process that leverages a gap analysis approach, the developed DORA Control Framework and associated tools developed in this research. The aim is to provide financial entities with a clear pathway to assess their current compliance levels and prepare for the upcoming DORA regulations and assist in achieving full compliance with DORA and its technical standards by January 17, 2025.

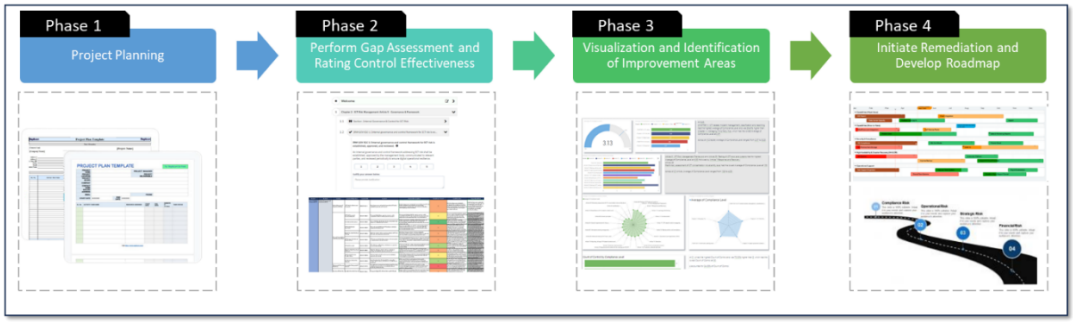

Figure 2 Four-Phased Approach to DORA Pre-Readiness Compliance Assessment

1. **Project Planning:** Financial entities are advised to initiate the compliance journey by outlining the scope of the assessment to include all relevant business functions and ICT systems. Additionally, stakeholders, both internal and external, should be identified, and a dedicated control function should be set up to oversee the activities. The outcome will be a well-defined project plan that serves as a foundational roadmap for the compliance assessment.
2. **Gap Assessment and Rating Control Effectiveness:** For this phase, it is recommended that financial entities utilize the Pre-Readiness Compliance Assessment Templates. Two options are available for this purpose: the DORA Assessment OneTrust template or Excel Bases Assessment Template, both tailored to align with DORA's requirements. Financial entities should review and rate each control based on its current level of implementation and documentation. Justifications for the scores and identified gaps should be documented. The outcome will be a quantifiable measure of the entity's current compliance level and a Gap Analysis Report.
3. **Visualization and Identification of Improvement Areas:** Financial entities should leverage the Visualization artifact for this phase. Power BI dashboards should be created to offer both a snapshot and an in-depth analysis of compliance levels. These dashboards will help in identifying and prioritizing areas that require improvement. The outcome will be an interactive visual dashboard that provides actionable insights.
4. **Remediation Phase**: In this final phase, financial entities are advised to develop their own roadmap for compliance, detailing the steps needed to achieve full compliance. Resources, both human and technological, should be allocated, and a budget should be planned. A timeline should be set, ensuring that all remediation actions are completed by the stipulated DORA deadline. The outcome will be a strategic and time-bound remediation plan.

By following this proposed approach and utilizing the associated artifacts and toolsets, financial entities can systematically assess and improve their readiness for DORA compliance, thereby mitigating risks and facilitating a seamless transition to the new regulatory landscape.

4.2 Scoring Methodology

The control scoring methodology employed in this research aims to provide a comprehensive yet straightforward way to assess compliance levels. It considers three key elements for each control: Documentation, Implementation, and Operating Effectiveness. The scoring scale of 1-5 is inspired by the Capability Maturity Model Integration (CMMI) maturity levels, which are widely recognized for assessing the maturity and capability of business processes.

Score	1	2	3	4	5
Our Scale	Not Implemented / No Documentation / Not Effective	Partially Implemented / Partial Documentation / Partially Effective	Mostly Implemented / Mostly Complete Documentation / Mostly Effective	Fully Implemented / Comprehensive Documentation / Fully Effective	Fully Implemented and Continuously Improved / Comprehensive and Continuously Updated Documentation / Continuously Effective
CMMI Scoring Interpretation	**Level 1 - Initial:** Processes are unpredictable, poorly controlled, and reactive. This corresponds to a score of 1 in our methodology, indicating that the control is not implemented, lacks documentation, and is not effective.	**Level 2 - Managed:** Processes are project-focused and often reactive. This corresponds to a score of 2, indicating that the control is partially implemented and documented but may not be fully effective.	**Level 3 - Defined:** Processes are well-characterized and understood, with proactive management. This corresponds to a score of 3, indicating that the control is mostly implemented, documented, and effective.	**Level 4 - Quantitatively Managed:** Processes are measured and controlled. This corresponds to a score of 4, indicating that the control is fully implemented, comprehensively documented, and effective.	**Level 5 - Optimizing:** Processes are stable and flexible, with a focus on continuous improvement. This corresponds to a score of 5, indicating that the control is not only fully implemented and documented but is also subject to continuous improvement.
Compliance Level Interpretation	**Non-Compliant**		**Partially Compliant**	**Fully Compliant**	

Table 1 Compliance Maturity Scoring Methodology

4.2.1 Compliance Level Calculation

Each control is scored on a scale of 1-5 based on its Documentation, Implementation, and Operating Effectiveness and the following.

1. **Section Score**: For each section within an article, calculate the average score of all controls in that section.

$$Section\ Score\ (Average\ of\ all\ controls\ in\ that\ Section) = \frac{Sum\ of\ Control\ Scores}{Number\ of\ Controls\ in\ that\ Section}$$

2. **Article Score**: For each article, calculate the average score of all sections within that article.

$$Aritcle\ Score\ (Average\ of\ all\ Sections\ in\ that\ Article) = \frac{Sum\ of\ Section\ Scores}{Number\ of\ Sections\ in\ that\ Section}$$

3. **Chapter Score**: For Each chapter, calculate the average score for the entire article.

$$Chapter\ Score\ (Average\ of\ Articles\ in\ that\ Section) = \frac{Sum\ of\ Articles\ Scores}{Number\ of\ Articles\ in\ that\ Section}$$

4. **Overall Score**: Finally, calculate the overall score.

$$Chapter\ Score\ (Average\ of\ Articles\ in\ that\ Section) = \frac{Sum\ of\ Chapter\ Scores}{Number\ of\ Chapers\ (5)}$$

5 Implementation

5.1 Pre-Readiness Compliance Framework Control Database

The Control Database is the most pivotal part of this research, serving as a structured repository for controls that are meticulously aligned with the DORA regulations. The database aims to offer a comprehensive view of the requirements landscape and the mandates required by DORA regulation, thereby enabling financial entities a one-stop solution to assess, track, and improve their compliance posture effectively.

5.1.1 Transformation of Regulatory Clauses into Actionable Controls

The transformation of regulatory clauses into actionable controls was a pivotal aspect of building the Control Database. The process ensured that the database not only captures the essence of the DORA regulation but also provides a structured and user-friendly language for financial entities to assess their compliance. A six-step process was employed to transform each clause of the DORA regulation into logical and actionable controls within the Control Database.

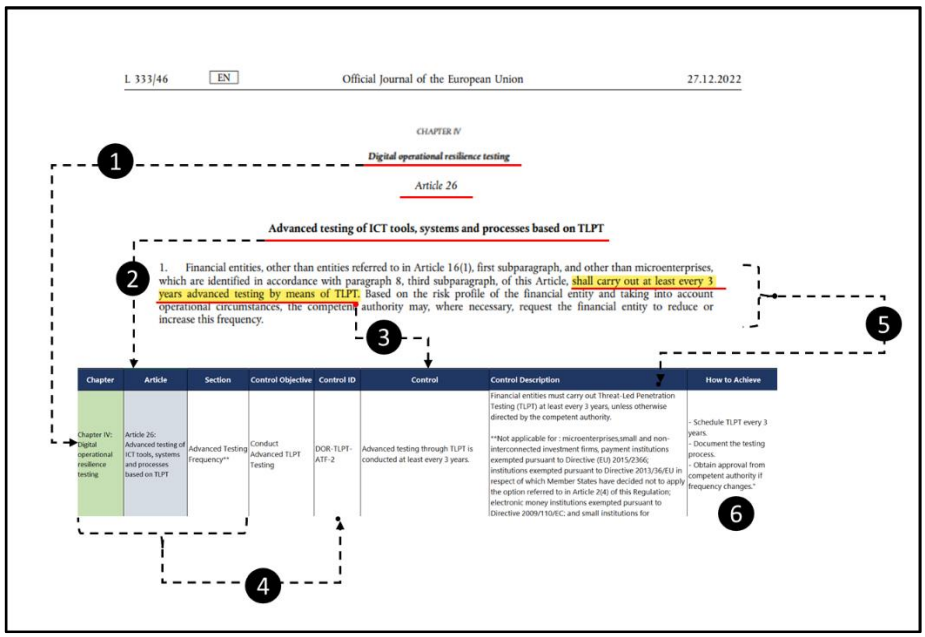

Figure 4 Process of Developing a Control

1. **Chapter Identification**: For Each Control the chapter names was extracted from the DORA regulation and placed into the 'Chapter' column of the Control Database. For example, "Chapter IV: Digital Operational Resilience Testing" is identified and recorded.
2. **Article Identification**: Subsequently, the article name was identified and inserted into the 'Article' column. In this context, "Article 26: Advanced Testing of ICT Tools, Systems, and Processes Based on TLPT" serves as the example.
3. **Control Creation**: Control were formulated based on the dissected clause and added to the 'Control field, such as " Advanced testing through TLPT is conducted at least every 3 years."
4. **Control ID Generation**: A unique Control ID is generated by combining initials from the chapter, article, and section names, along with a serial number. For instance, "DOR-TLPT-ATF-2" is created. Where, DOR represents the chapter initial, TLPT stands for the article initial, ATF denotes the section initial , and 2 is the control serial number, which increments for each new control within the same section.
5. **Control Description**: A detailed description was derived from the entire article and added to the 'Control Description' column for comprehensive insight.
6. **How to Achieve**: Finally, actionable recommendations were formulated based on industry-wide practices and added to the 'How to Achieve' column.

5.1.2 Scope and Scale of the Control Database

By following this six-step process for each regulatory clause, an expansive and comprehensive Control Database was developed. The database is expansive, covering the five main chapters

outlined in the DORA regulations. It further drills down into 21 sub-articles that are specifically tailored to the requirements of financial entities. To provide a granular level of detail, 108 sub-sections were created. In total, the database houses 212 unique controls, each designed to address a specific aspect of the DORA regulations.

Chapters	Articles	Section	Controls
5	21	108	212

Table 2 Scale of DORA Pre-Readiness Compliance Assessment Control Database

Chapter	Article	Total Controls Developed
Chapter II : ICT Risk Management (IRM)	Article 5 : Governance and organisation (GOV)	12
	Article 6 : ICT Risk Management Framework	8
	Article 7: ICT systems, protocols, and tools	4
	Article 8: Identification	7
	Article 9: Protection and prevention* *High number of controls due to inclusion of Regulatory Technical Standards (RTS)*	91
	Article 10: Detection	4
	Article 11:Response and Recovery	8
	Article 12: Backup policies and procedures, restoration and recovery procedures and methods	7
	Article 13: Learning and Evolving	7
	Article 14: Communication	3
CHAPTER III: ICT-related incident management, classification, and reporting	Article 17: ICT-related incident management process	8
	Article 18:Classification of ICT-related incidents and cyber threats	2
	Article 19: Reporting of major ICT-related incidents and voluntary notification of significant cyber threats	3
Chapter IV: Digital operational resilience testing	Article 24: General requirements for the performance of digital operational resilience testing	5
	Article 25: Testing of ICT tools and systems	3
	Article 26: Advanced testing of ICT tools, systems and processes based on TLPT	7
	Article 27 Requirements for testers for the carrying out of TLPT	9
Chapter V: Managing Third Party Risk	Article 28: General principles	9
	Article 29: Preliminary assessment of ICT concentration risk at entity level	6
	Article 30: Key contractual provisions	4
CHAPTER VI: Information-sharing arrangements	Article 45: Information-sharing arrangements on cyber threat information and intelligence	5
	Total Number of Controls	**212**

Table 3 Coverage of Articles Chapters & Articles of DORA Regulation

5.2 Assessment Templates – Excel Based & OneTrust Platform

5.2.1 Excel Based Assessment Workbook

To finally facilitate the compliance assessment and gap analysis process as per Pre-Readiness Compliance Assessment framework, the Control Database and its scoring methodologies is integrated to create an Excel-Based Assessment Workbook. This workbook serves as the one of the final outputs of this research, acting as a practical extension of the Control Database. It leverages the controls that are developed and aligned with the DORA regulations, providing a streamlined and comprehensive tool for compliance assessment. To provide a comprehensive understanding of the Excel-Based Assessment Workbook, the Figure 5 visually represents the various components or sheets within the workbook, each serving a distinct purpose in the compliance assessment process.

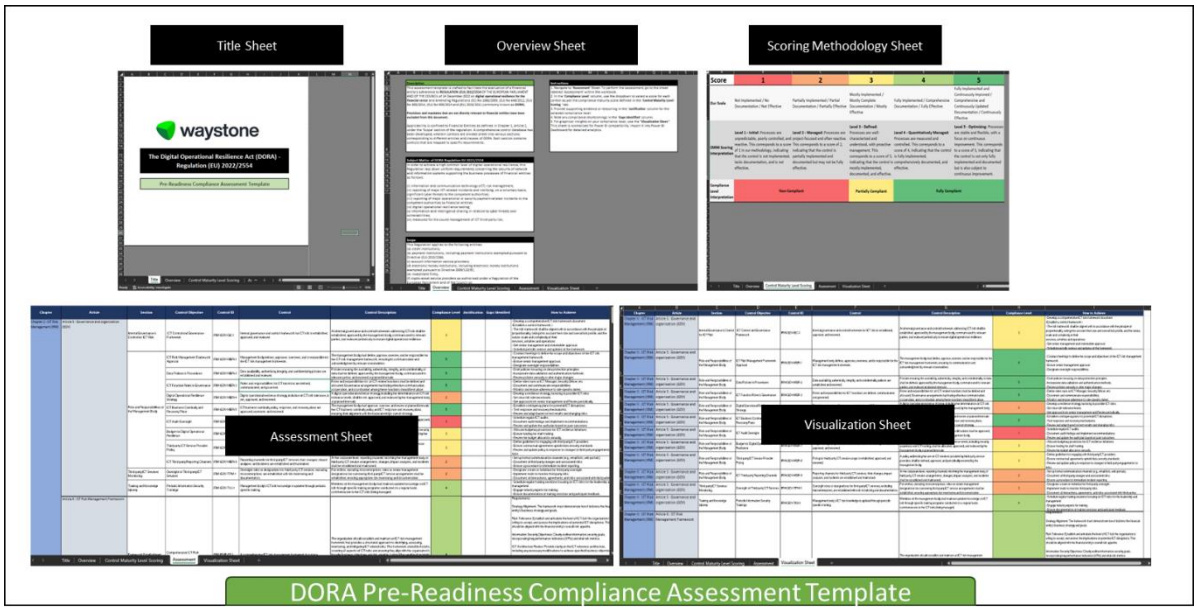

Figure 5 Excel Based Assessment Template

These components are designed to work in harmony, offering a complete solution for DORA compliance assessment. The workbook consists of the following sheets:

1. **Title Sheet**: This sheet presents the title, setting the context for the assessment.
2. **Overview Sheet**: This sheet acts as a one-stop guide, offering a comprehensive view of the DORA Act's Description, Instructions, Scope, and Subject Matter. It equips users with all the essential information needed to navigate the compliance assessment process effectively.
3. **Scoring Methodology Sheet**: This sheet explains the scoring system used in the assessment, aligning with the Capability Maturity Model Integration (CMMI) framework. It serves as the backbone for the assessment process, outlining the methodology that should be used when evaluating each control in the Assessment Sheet.
4. **Assessment Sheet**: This is the core component where the actual compliance assessment takes place. The sheet features multiple columns such as Chapter, Article, Section, Control Objective, Control ID, Control, Control Description, Compliance Level, Justification, and Gaps Identified, which is essentially the control database, but with dedicated spaces for performing the assessment. The sheet is designed to be user-friendly, featuring drop-down menus for ease of use.
5. **Visualization Sheet**: This sheet is specifically designed to work in tandem with Power BI. It contains normalized data that is structured for easy importation into Power BI for further analytics.

This workbook, therefore, serves as a practical extension of the Control Database, integrating its controls and scoring methodologies into a tool for allowing financial entities to be able to conduct a comprehensive DORA based compliance assessment and check for their readiness.

5.2.2 OneTrust Platform DORA Pre-Readiness Compliance Template

OneTrust, a platform widely recognized for its contributions to privacy, security, compliance, and governance, was employed as a foundational tool in this research. Known for its array of

templates for various types of assessments, the platform's custom template-building feature was leveraged to construct a specialized DORA Pre-Readiness Compliance Assessment Template. This cloud-based template was developed to offer an automated and interactive approach to assessing DORA compliance, thereby serving as a complementary mechanism to the Excel-Based Assessment Workbook.

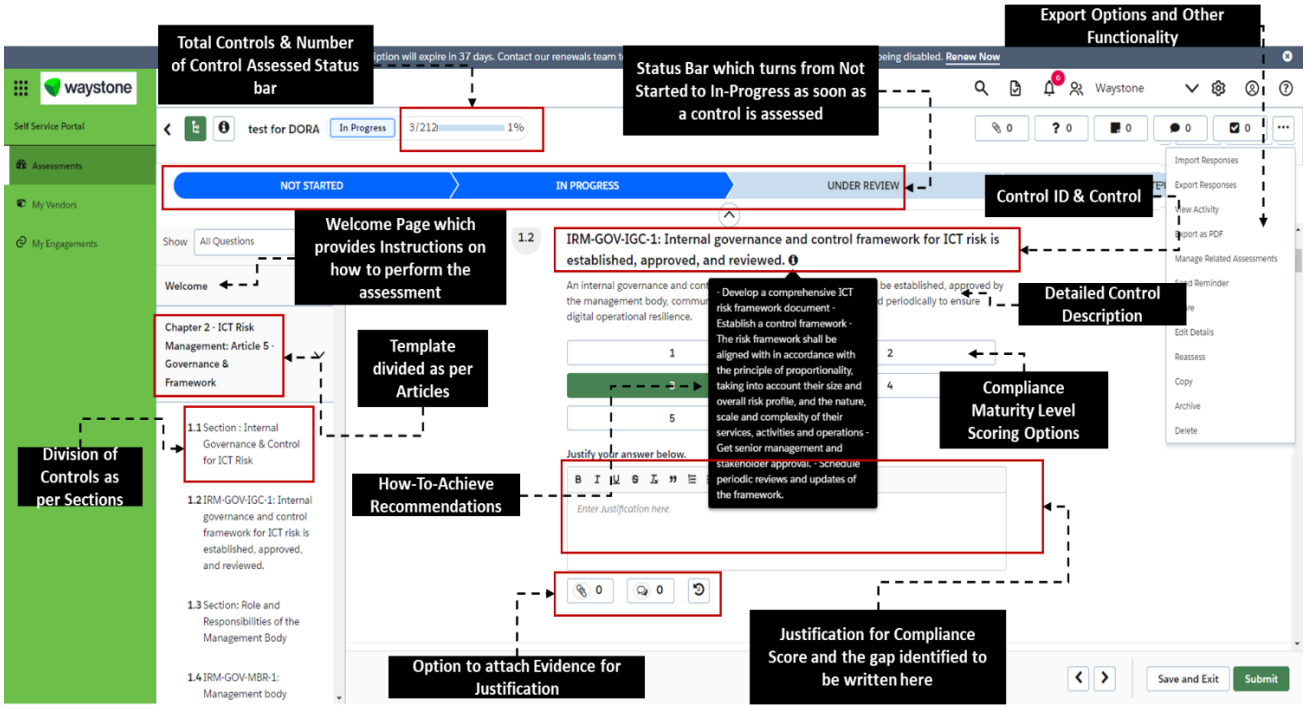

Figure 6 One Trust Platform Template – Assessment View

- **Control Mapping**: Controls from the Control Database were mapped and developed into the OneTrust platform using its question builder functionality.
- **Welcome Message and Instructions:** A preconfigured welcome message was set to appear at the start of each assessment. Instructions on how to navigate the assessment, similar to those in the Excel workbook, were appended to this welcome message for user guidance.
- **Article and Section Division:** The assessment was divided based on articles, each containing various controls and sections. This structure was designed to mirror the organization of the Control Database, thereby maintaining consistency.
- **Scoring Methodology Integration:** Options for scoring were integrated into the OneTrust template, allowing users to select scores within a range of 1-5, consistent with the Excel workbook's scoring methodology.
- **Justification and Gap Identification:** A justification box was enabled for each control, allowing users to provide evidence or reasoning for their scoring choices. This feature also enabled users to identify and document any gaps in compliance.
- **Progress Tracking and Review Phase**: Additional features like a progress bar were enabled to provide real-time tracking of the assessment's status. A review phase was also incorporated, allowing for a comprehensive review of the assessment before final submission.
- **Data Export Options:** The OneTrust template was configured to offer multiple data export options, including exporting responses and generating PDF reports.

Through execution of these steps, the Excel-Based Assessment Workbook was successfully transformed into a OneTrust Assessment Template. This transformation leveraged the advanced capabilities of the OneTrust platform while ensuring that the DORA compliance assessment process remained consistent, comprehensive, and user-friendly.

5.3 Implementation of Power BI Dashboard for Compliance Assessment Visualization

The Power BI Dashboard serves as a dynamic and interactive tool for visualizing the compliance status of financial entities with respect to DORA regulations. Designed to offer both granular and high-level insights, the dashboard is implemented to enhance decision-making processes and facilitate effective communication among team members and stakeholders. Below is a detailed outline of its implementation:

Initial Setup and Objective: Power BI Dashboard is implemented in a way, so that users are presented with an interface targeted at providing a comprehensive view of compliance levels. The primary objective is to offer a visual representation that allows both assessors and management to identify compliance gaps at various levels—from an overall perspective down to individual chapters, articles, and sections.

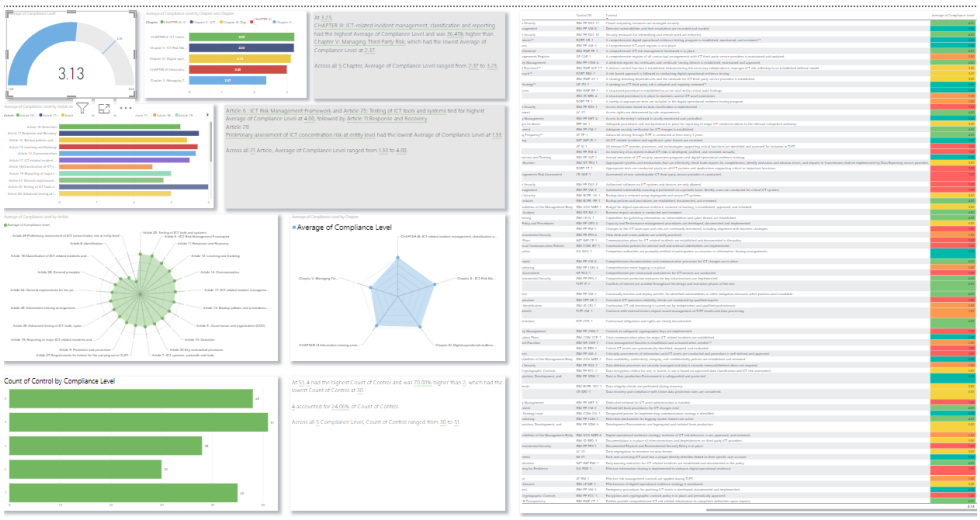

Figure 7 Power BI Dashboard

Key Visualizations and Features

- **Gauge Chart for Overall Compliance:** The dashboard kicks off with a gauge chart that displays the overall compliance level. The gauge axis is set with a target level of 4, indicating the desired compliance level to be achieved.
- **Stacked Bar Chart for Chapter-wise Compliance:** Following the gauge chart, a stacked bar chart provides a breakdown of compliance levels by chapter. This is accompanied by a dynamic summarizer that offers insights tailored to the data displayed in the chart.
- **Article-wise Compliance Visualization:** Another stacked bar chart follows, focusing on compliance levels by articles. Like its chapter-wise counterpart, this chart also features its own dynamic summarizer for in-depth analysis.
- **Radial Charts and Spider Graphs:** These are used to offer alternative visual perspectives on compliance levels, adding another layer of analytical depth.

- **Control Count by Compliance Level:** A stacked bar chart shows the count of controls based on their compliance levels. For example, it can display how many controls are rated at level 5.
- **Dynamic Matrix Table:** This feature provides a detailed view of all the metrics, offering a tabular representation that complements the graphical visualizations.

Interactivity and Dynamic Features: One of the features of this Power BI Dashboard is its interactivity. Clicking on any of the metrics or indicators refocuses the entire dashboard based on that specific metric. This dynamic functionality allows for a more focused and customized analysis, thereby supporting in more effective decision-making.

Facilitating Collaboration and Decision-Making: The visual nature of the dashboard enhances communication and collaboration among team members and stakeholders. By presenting data in a clear and concise manner, it allows for the sharing of insights and facilitates more effective decision-making, ultimately leading to higher-quality project outcomes.

In summary, the Power BI Dashboard for DORA Pre-Readiness Compliance Assessment offers a robust, interactive, and insightful tool for evaluating and improving compliance levels within financial entities.

6 Evaluation

The evaluation of the DORA-specific compliance framework was conducted by seasoned cyber security consultants from Waystone's Cyber & Data Privacy Team. These experts are acting CISOs for multiple organizations and possess between 20 to 35 years of experience in the cybersecurity domain. Their extensive experience includes advising multiple financial entities across the European Union. Given their expertise, they are well-positioned to evaluate the control framework rigorously.

Each expert independently scored past financial clients with whom they have worked closely. This scoring was based on their intimate knowledge of these organizations' capabilities in cybersecurity and compliance as per their knowledge and interaction.

6.1 Experiment/Case Study 1: ICT Risk Management for a Credit Institution (Client A)

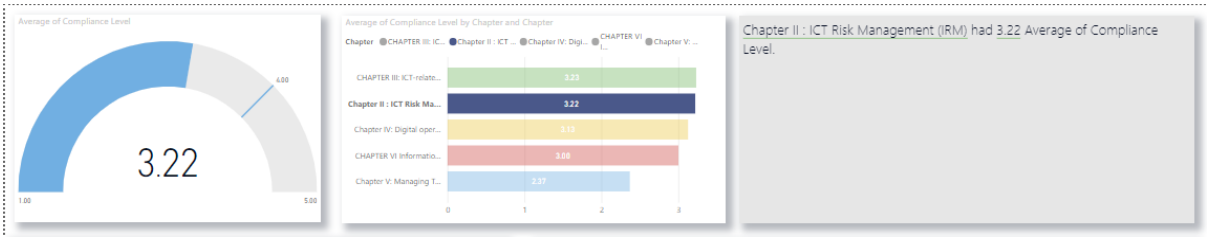

Figure 8 Chapter II Compliance Scores for Client A

Evaluator A, a seasoned cybersecurity expert with years of advisory experience with Client A (credit institution – banking sector) , focused on the ICT Risk Management chapter for this case study. The evaluation was particularly insightful given his intimate knowledge of the client's current capabilities. The compliance score for this chapter was calculated to be 3.22, which falls within the expected range of 3-4. This score range was anticipated because Client A has most of its ICT risk management controls documented and implemented, indicating a state of partial to full compliance.

To further analyze the score, Evaluator A utilized Power BI for data visualization and insights. This allowed him to pinpoint specific areas where Client A could improve. The Power BI insights also revealed that while Client A excels in areas like "Management body's role in ICT risk management" and "Data policies" with scores of 4, there is room for improvement in areas like "Oversight roles for third-party ICT services" and "Reporting channels for third-party ICT services," which scored a 2.

6.2 Experiment / Case Study 2: Evaluation of ICT-Related Incident Management in Client A

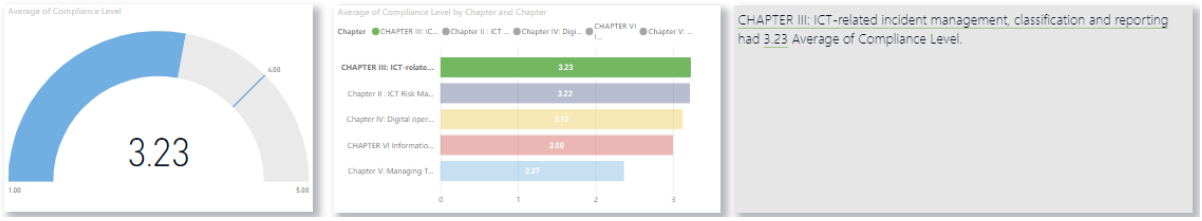

Figure 9 Chapter IV Compliance Scores for Client A

In this case study, Evaluator A turned his attention to Chapter 3, which centres on ICT-related incident management, classification, and reporting. The compliance score for this chapter was calculated to be 3.23, which is consistent with the organization's general compliance maturity. Power BI analytics revealed several key areas of strength and weakness. For instance, Client A excelled in "ICT-related incident management process" and "Roles and responsibilities for ICT-related incidents," both of which scored a 5. These high scores indicate that the organization has a robust process for managing ICT-related incidents and has clearly delineated roles and responsibilities.

However, the analysis also pinpointed areas requiring improvement. One such area is "Significant cyber threats are voluntarily reported," which scored a 1. This low score suggests that Client A has room for improvement in voluntarily reporting significant cyber threats to the relevant authorities. This is a critical area, especially considering the increasing prevalence of cyber threats in the financial sector. Overall, the evaluation confirms that Client A is generally compliant in most areas but needs to focus on enhancing its voluntary reporting mechanisms for significant cyber threats, improving its communication and response strategies for ICT-related incidents. The Power BI analysis proved invaluable in visually highlighting these areas, thereby aiding in the prioritization of improvement measures.

6.3 Experiment / Case Study 3: Evaluation of Digital Operational Resilience Testing in Client B

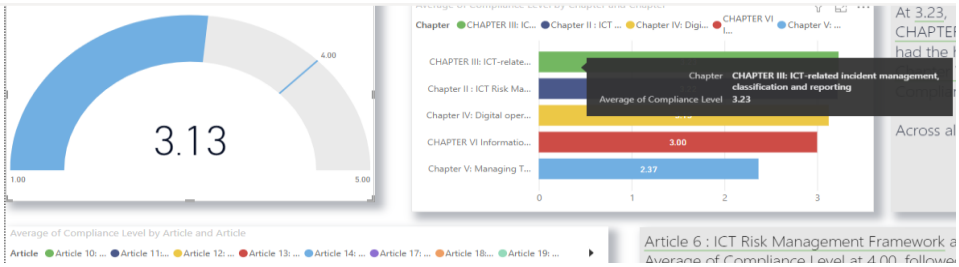

Figure 10 Chapter 3 Compliance Scores for Client B

In this case study, Evaluator B focused on Chapter 4, which centers on digital operational resilience testing for Client B, a financial services firm. The firm received an overall compliance score of 3.13 in this chapter, indicating a moderate level of compliance.

Evaluator B utilized Power BI analytics to delve into the scores, highlighting both strengths and areas needing improvement. For instance, Client B excelled in "A comprehensive digital operational resilience testing program is established, maintained, and reviewed," with a top score of 4. This suggests that the firm has successfully integrated a robust digital operational resilience testing program into their ICT risk-management framework.

However, the evaluation also pinpointed areas for improvement. One such area is "Tests are undertaken by independent parties," which scored a mere 1. This low score suggests that Client B primarily relies on internal teams for testing, potentially compromising the objectivity and effectiveness of the tests. Another area that scored low was "Appropriate tests are conducted yearly on all ICT systems and applications supporting critical or important functions," also with a score of 1. This indicates that annual testing of critical systems is not consistently carried out, posing a risk to the firm's digital resilience .The Power BI insights were particularly illuminating in identifying these areas, thereby aiding in the prioritization of remedial actions. For example, the low score in "Tests are undertaken by independent parties" could be addressed by employing external, certified testers for future resilience tests to ensure objectivity and comprehensiveness. A special focus was placed on "Advanced testing through TLPT is conducted at least every 3 years," which scored a 4. While this is a relatively high score, it suggests that while Client B does engage in Threat-Led Penetration Testing (TLPT), there may be room for improvement in the frequency or comprehensiveness of these tests.

Overall, the evaluation by Evaluator B confirms that while Client B has made commendable progress in establishing a comprehensive digital operational resilience testing program, there are key areas that require immediate attention. These insights are crucial for the firm's ongoing efforts to enhance its digital operational resilience.

6.4 Discussion

The evaluation findings were largely in alignment with the existing compliance levels of the financial institutions, validating the robustness of the compliance assessment framework in use. However, a notable area for refinement was identified in the form of redundant controls. Specifically, controls related to incident management and third-party management were found to be duplicated, appearing both in Chapter 1 and in their individual, specialized chapters. This redundancy not only complicates the assessment but also has the potential to skew the overall compliance score. To enhance the framework's efficiency and accuracy, we recommend a revision that eliminates these duplicate controls. By assessing these controls only once, their corresponding scores could be mapped across all relevant chapters, thereby streamlining the compliance assessment process and providing a more accurate representation of the institution's compliance posture.

7 Conclusion and Future Work

7.1 Conclusion

The successful implementation of the DORA Pre-Readiness Compliance Assessment framework, utilizing a multi-faceted approach that includes a Control Database, a custom OneTrust assessment template, and a Power BI Dashboard, serves as a robust toolset for financial entities navigating the complexities of DORA compliance. This comprehensive system not only ensures alignment with regulatory mandates but also empowers financial organizations with actionable insights for informed decision-making. The interactive and

visually engaging nature of these tools simplifies the compliance assessment process, making it more accessible and effective. As a result, financial entities are better equipped to identify compliance gaps, prioritize improvements, and communicate effectively with stakeholders, thereby streamlining their journey towards achieving full DORA compliance.

7.2 Future Work

1. **Incorporation of Second Batch of Mandates:** It is anticipated that a second batch of mandates will be released on 17 June 2024. These new mandates will require immediate attention to integrate them into the existing framework. The Control Database, OneTrust template, and Power BI Dashboard will need to be updated to reflect these new requirements.
2. **Compliance Matrix for Each Control**: One of the key enhancements for future work would be the development of a detailed compliance matrix for each control. This matrix would specify what each score from 1 to 5 means in the context of that particular control. By doing so, it would provide a more granular understanding of compliance levels, making the assessment process more transparent and actionable. This would also aid in standardizing the assessment across different assessors, ensuring that each score is based on a well-defined set of criteria.
3. **Removing Redundancy**: One area for improvement could be the elimination of redundant controls within the Control Database. Currently, certain controls, particularly those related to third-party risk management, appear in multiple chapters—such as Chapter 2 and Chapter V. This repetition can create confusion and inefficiencies in the assessment process. A future enhancement could involve consolidating these repeated controls and developing a mechanism that allows their scores to be reflected across all applicable chapters and articles, thereby streamlining the compliance assessment.
4. **Enhanced Analytics**: Future work could focus on incorporating more advanced analytics and machine learning algorithms to predict potential compliance risks and offer proactive solutions.
5. **Integration with Other Regulatory Frameworks:** The existing system could be expanded to include compliance checks for other financial regulations, making it a more versatile tool for regulatory compliance.

8 References

Agarwal, S., Steyskal, S., Antunovic, F., & Kirrane, S. (2018). Legislative compliance assessment: Framework, model and GDPR instantiation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11079 LNCS*, 131–149. https://doi.org/10.1007/978-3-030-02547-2_8/TABLES/2

Alberts, C. J., Behrens, S. G., Pethia, R. D., & Wilson, W. R. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE SM) Framework, Version 1.0*.

Antonsen, H. H., & Madsen, D. Ø. (2021). Developing a maturity model for the compliance function of investment firms: A preliminary case study from norway. *Administrative Sciences*, *11*(4). https://doi.org/10.3390/admsci11040109

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering 2009 1:3*, *1*(3), 213–222. https://doi.org/10.1007/S12599-009-0044-5

Bonatti, P. A., Kirrane, S., Petrova, I. M., & Sauro, L. (2020). *Machine Understandable Policies and GDPR Compliance Checking*.

Chatzipoulidis, A., Tsiakis, T., & Kargidis, T. (2019). A readiness assessment tool for GDPR compliance certification. *Computer Fraud & Security*, *2019*(8), 14–19. https://doi.org/10.1016/S1361-3723(19)30086-7

De Bruin, S., De Bruin, T., Rosemann, P. M., Freeze, R., Kulkarni, P. U., & Carey, W. P. (n.d.). 6 th Australasian Conference on Information Systems Maturity Assessment Model Understanding the Main Phases of Developing a Maturity Assessment Model. *2005*. Retrieved September 3, 2023, from http://www.efqm.org/Default

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/CYBSEC/TYZ013

European Commission 2020 -Proposal for a regulation of the European Parliament on digital operational resilience for the financial sector and Amending Regulations. (2020). https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034

Financial Stability Board. (2019). *Third-party dependencies in cloud services: Considerations on financial stability implications*. www.fsb.org/emailalert

Fredriksen, R., Kristiansen, M., Gran, B. A., Stølen, K., Opperud, T. A., & Dimitrakos, T. (2002). The CORAS framework for a model-based risk management process. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *2434*, 94–105. https://doi.org/10.1007/3-540-45732-1_11/COVER

Gusiv, P. (2023). *DEVELOPMENT OF A COMPLIANCE GAP ANALYSIS METHOD FOR THE DIGITAL OPERATIONAL RESILI-ENCE ACT (DORA)*.

Institute of Standards, N. (2018). *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. https://doi.org/10.6028/NIST.CSWP.04162018

Kourmpetis, S. (2023). *Management of ICT Third Party Risk Under the Digital Operational Resilience Act*. 211–226. https://doi.org/10.1007/978-3-031-17077-5_7

Maier, A. M., Moultrie, J., & Clarkson, P. J. (2012). Assessing organizational capabilities: Reviewing and guiding the development of maturity grids. *IEEE Transactions on Engineering Management*, *59*(1), 138–159. https://doi.org/10.1109/TEM.2010.2077289

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Mavlutova, I., & Volkova, T. (2019). *Digital Transformation Of Financial Sector And Challengies For Competencies Development*.

Menezes, W. (2002). Capability Maturity Model Integrated. *Encyclopedia of Software Engineering*. https://doi.org/10.1002/0471028959.SOF041

Neumannová, A., & Elshuber, C. (2022). *The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review*.

Oyegoke, A. (2011). The constructive research approach in project management research. *International Journal of Managing Projects in Business*, *4*(4), 573–595. https://doi.org/10.1108/17538371111164029/FULL/XML

Pasian, B., & Turner, R. (2016). Designs, Methods and Practices for Research of Project Management. *Designs, Methods and Practices for Research of Project Management*. https://doi.org/10.4324/9781315270197/DESIGN-METHODS-PRACTICES-RESEARCH-PROJECT-MANAGEMENT-BEVERLY-PASIAN-RODNEY-TURNER

Pullen, W. (2007). A public sector HPT maturity model. *Performance Improvement*, *46*(4), 9–15. https://doi.org/10.1002/PFI.119

Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin Bianchi, I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation and Governance* , *22*(3), 227–244. https://doi.org/10.1108/DPRG-02-2020-0019/FULL/PDF

Ter Haar, J. B. (2022). *DORA: Friend or Foe? A Qualitative Study into the Perceptions of the Financial Sector in the EU on the Expectation of the Digital Operational Resilience Act*. http://repository.tudelft.nl/

The Digital Operational Resilience Act 2022/2554. (n.d.). Retrieved September 3, 2023, from https://eur-lex.europa.eu/eli/reg/2022/2554/oj

The Global Risks Report 2022 17th Edition. (2022).

Yazar, Z. (2002). *A qualitative risk analysis and management tool-CRAMM*.