National College of Ireland

Development of a compliance gap analysis against Software X and DORA

MSc Research Project
MSCCYBETOP

Ruta Ramanauskaite
Student ID: 24242462

School of Computing
National College of Ireland

Supervisor: Raza Ul Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: …Ruta Ramanauskaite…

Student ID: …… 24242462……..……

Programme: …… MSCCYBETOP……**Year:** ……2025……..

Module: … MSc Practicum/Internship part 2 Info & Submission page……

Supervisor: …… Raza Ul Mustafa……

Submission Due Date: ……11th August 2025……..……

Project Title: Development of a compliance gap analysis against Software X and DORA

Word Count: ……11776…… **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: ……Ruta Ramanauskaite……

Date: ……03/08/2025……

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):	

Development of a compliance gap analysis against Software X and DORA

Ruta Ramanauskaite
24242462

Abstract

Previously, European cybersecurity regulations have been complex, fragmented and primarily made up of legislation that's relevant to the industry. The NIS[1] describes the financial sector as one of seven vital sectors, which means there is a requirement for EU Member States to implement appropriate technical and organizational protections through targeted legislative policies, as noted by Krüger and Brauchle (2021). This study aims to review the key relevant Regulatory Technical Standards (RTSs) under the novel Digital Operational Resilience Act or DORA, and to analyse potential compliance gaps in relation to Software X. Software X serves as the central control point for the document processing workflow platform. It provides comprehensive configuration, user management, and service coordination, ensuring that workflows run reliably and consistently across the distributed system. A gap analysis was conducted that included a revision of relevant documentation, software configurations, internal policies, and controls against selected articles under RTSs, which were deemed applicable to Software X. The results provide a basis for developing methods for addressing identified compliance gaps. The research embraced a case study methodology to analyse the relationship between Software X and DORA. As well as that, a constructive research approach was used to design a tailored compliance checklist for a specific third-party ICT service provider.

Keywords: Digital Operational Resilience Act (DORA), Regulatory Technical Standards (RTS), Compliance Gap Analysis, Financial Software Security, Operational Resilience

1 Introduction

As noted by the European Insurance and Occupational Pensions Authority (EIOPA) (2025), DORA, or the Digital Operational Resilience Act, is a new piece of European Union-level legislation that imposes strict responsibilities on financial institutions, regulating how to react to, document, and mitigate potential threats in order to improve their IT management systems. The financial sector is heavily reliant on digital infrastructure Leuprecht (2019), and financial institutions are increasingly dependent on third-party providers to deliver essential supporting business services to them. One of the key objectives of DORA is to ensure that third-party relationships do not weaken the operational resilience of financial institutions.

Risk management is essential to DORA compliance; it serves as a foundation for ensuring that organisations can respond well to crises and operational interruptions. DORA is focused on operational resilience and information security, so ISO/IEC 27001:2022 serves as a practical base for creating an effective risk management framework. Note, however, that ISO/IEC 27001:2022 outlines risk-based controls with certifiable implementation, whereas DORA is regulatory and prescriptive, and thus imposes direct responsibilities in the oversight of third-party ICT providers for financial institutions.

Because of this, while ISO/IEC 27001:2022 offers a good starting point, its implementation within an organisation can only partially meet the compliance demands outlined in the DORA legislation. Nonetheless, these controls and practices were reviewed as part of the assessment process, as they serve as an important baseline. Additional efforts focused on mapping the software solution of the third-party supplier's policies and

[1] Network and Information Systems Directive

practices to the articles of the relevant Regulatory Technical Standards (RTS) under DORA. The research question for this project was: How is the Digital Operational Resilience Act (DORA) influencing changes at the software level within third-party suppliers for financial institutions? Development of a compliance gap analysis between Software X and DORA for third-party suppliers in the financial services sector. This research focused on a small software supplier, in contrast to large software providers such as Microsoft or AWS, which typically have more robust security because of their large scale. Smaller providers are more likely to have compliance gaps and weaker security measures, making them a good candidate for risk assessment. Software X is a third-party workflow tool used by financial institutions to manage daily tasks.

This report examined internal and external requirements in relation to the software and the provider itself, where relevant. It evaluated the measures outlined by a third-party provider to ensure that backup policies are in place, vulnerability scanning is being conducted, staff are being educated regularly with regard to information security, and risk assessments are regularly being conducted internally. Externally, this report looked at legal and regulatory commitments; it focused on a selection of relevant articles under Regulatory Technical Standards (RTSs) outlined in the DORA legislation. Another objective in reviewing the relevant RTSs was to define the Software X system and its components that fall within the scope of analysis, as well as to clearly identify what lies outside of the scope, such as business processes and other non-technical elements. Additionally, a review of related work and literature was conducted, which revealed that some research exists in terms of analysis of financial institutions and third-party providers attempting to align with DORA; however, scope remains for more research in the area. A gap was discovered in research done on alignment by third-party providers in terms of their software proposition, which this research aims to fill.

A gap analysis was conducted as part of this research to determine potential areas of non-compliance. The focus was to examine the most relevant Regulatory Technical Standards outlined in the DORA legislation and to understand how they align with Software X. Based on this analysis, a checklist was created to point out actionable steps for addressing any identified gaps and to enhance compliance.

Limitations that were encountered for this research:

The ethical considerations are outlined in the report. These considerations include:

- ✓ Ensuring the protection of Software X and any sensitive information contained within it.
- ✓ Safeguarding proprietary information from disclosure.
- ✓ Refraining from revealing specific security vulnerabilities related to Software X.
- ✓ Upholding commercial confidentiality at all times.
- ✓ Protecting system configurations from exposure.
- ✓ Providing technical details in a manner that maintains the anonymity of Software X.
- ✓ Referring to the software under study as Software X.
- ✓ Ensuring that any collected data is anonymized to prevent the disclosure of sensitive content.
- ✓ Lastly, securing the necessary authorization letter and rules of engagement, which must be signed and issued before the research can proceed.

As well as an abstract and introduction, the report will include several sections to analyse the topic comprehensively. Those include: A literature review, research methodology and design implementation section, a discussion section which will look at both the successes and limitations of the study, and a conclusion section which will summarize the key findings and insights gained. The following section will include a literature review on the topic.

2 Literature Review

2.1 Introduction

The main objective of this research is to identify and evaluate potential compliance gaps within the software offering of a third-party provider, in light of financial institutions being regulated by the new DORA legislation. As financial institutions are required to ensure that their third-party providers are also aligned with DORA, this study aims to identify and assess such gaps, helping the provider to be more prepared for compliance requests. While third-party providers are not directly bound by DORA unless classified as critical, financial entities that engage their services are still fully responsible for managing the related risks. A third-party ICT service provider

is considered critical based on four specific criteria: the potential systemic impact their failure could have on financial services - in terms of Software X, this could indicate disturbances in time-critical processes; the level of reliance placed on them by EU financial institutions - in terms of the provider itself, such as the size of their customer base across the EU; the criticality of the functions they support - the supplier's services are varied and extensive, so it is important to identify how critical those are; and how easily they could be replaced by another provider - these legitimate alternatives are identified by the financial institutions themselves (A&L Goodbody LLP, 2014). As well as conducting a gap analysis, this research will produce a tailored DORA compliance checklist designed to assist the third-party provider in achieving regulatory alignment in terms of the software analysed. To support this objective, a constructive research method has been adopted as part of the methodology. This approach was used in similar studies, such as Gusiv (2023), which also uses constructive research to develop practical tools for compliance. This literature review aims to explore risk management frameworks relevant to the case study and provide a detailed overview of the relevant articles under the Digital Operational Resilience Act (DORA) and its implications for third-party providers. The first segment will examine existing frameworks for managing information security risks, with a focus on the Information Security Management System (ISMS) and NIST Cybersecurity Framework (CSF) 2.0. The following section will look into the DORA legislation, including the identification of Critical Third-Party Providers, the role of the Lead Overseer, and the significance of Threat-Led Penetration Testing (TLPT). This will be followed by a review of the Regulatory Technical Standards (RTS) most relevant to the subject in this research. The final sections will consider how gap analysis applies to this context, identify gaps in the existing research, and conclude with key insights collected.

2.2 The Foundation for Achieving Compliance: Implementing a Framework to Manage Information Security Risks

According to Edwards and Weaver (2024), Compliance refers to an organization's adherence to regulatory requirements and industry standards. To effectively manage information security risks, organizations require a framework that can be applied regardless of their type or size. The ISMS[2], as defined in ISO/IEC 27001:2022, provides such a flexible and structured approach. ISO/IEC 27001:2022 can differ significantly from one organization to another, depending on its specific objectives, needs, and operations. According to a report by Deloitte (2023), adapting ISMS is an effective first step toward aligning with the DORA legislation. An ISMS is composed of several key elements: Policies, which specify the organization's objectives, Procedures, which provide assurance that tasks being carried out are in alignment with those policies, Resources, such as employees and technology, which are necessary to implement the procedures, and Guidelines, which, combined, make up the best practices the organization enforces to stay resilient. To successfully implement ISMS several core principles are to be used, such as: recognizing the significance of information security and clearly assigning responsibility for it, securing management commitment and considering the interests of the stakeholders, supporting broader societal values, conducting risk assessments to better understand acceptable risk levels, preventing and detecting information security incidents, adopting a thorough approach to security management, and continuously reviewing and updating information security measures as needed as pointed out by IT Governance Publishing (2023).

The key objectives in implementing an ISMS include defining its scope and understanding the company's risk appetite. Following this, a risk assessment is conducted, a risk treatment plan is developed, security controls are designed and applied, and internal audits are then executed. To manage risks, various frameworks can be utilized, as ISO/IEC 27001:2022 allows for flexibility in this area. Some examples of such frameworks include COBIT 2019, ISO/IEC 27018:2019, The Standard of Good Practice for Information Security, ISO 27017, ISO/IEC 27001:2013, CIS[3], NIST[4], CCM[5], or even tailored controls developed by the organization itself.

[2] Information Security Management System
[3] Center for Internet Security
[4] National Institute of Standards and Technology
[5] Cloud Controls Matrix

NIST CSF[6] 2.0 was created to help organisations of all sizes and in any sector. As explained by Pattison (2025) the Cybersecurity Framework (CSF) is a voluntary set of guidelines created to help organizations manage and mitigate their cybersecurity risks. It is adaptable to any level of cybersecurity maturity or technical ability. Rather than mandating a single solution for all, the CSF acknowledges that each organization has its own mix of risk appetites, risks, strategic priorities. Pattison (2025) notes that its implementation is meant to be flexible and tailored to fit the specific needs and goals of each organization. The framework is structured around three main components: the Core, which outlines the desired cybersecurity outputs; Profiles, which help organizations in evaluating both their current and desired cybersecurity states; and Implementation Tiers, which provide a way to understand the maturity of cybersecurity practices. The tiers range from Tier 1 - indicating the least developed capabilities, to Tier 4 - representing the highest level of maturity and effectiveness. All components of the framework are interconnected - for example, identifying a profile can also reveal the organization's current implementation Tier. Even though the framework is designed to apply to organizations of any size, some may face difficulties in assessing and enforcing the tiers. These difficulties often come from obstacles such as smaller budgets and a shortage of experienced personnel. As well as that, achieving a balance between cybersecurity goals and broader business priorities can involve difficult compromises. Finally, an organization's culture and its attitudes toward security and risk play a crucial role in how successfully the tiers are adopted, as highlighted by Edwards (2024).

The ISMS framework (ISO 27001) provides a systematic, accreditable approach to information security, making it ideal for organizations looking for regulatory compliance. It focuses on continuous improvement through risk assessments, controls, audits, and policies, supporting strict security and trust. In contrast, NIST CSF 2.0 is a flexible, non-certifiable framework. It focuses on flexibility to unique risks and strategic goals, with a structure (Core, Profiles, and Tiers) that accommodates more incremental maturity improvements. While both encourage cybersecurity best practices, ISMS suits those aiming for a more formal certification, whereas CSF 2.0 offers a more customizable approach. The next section will take a look at DORA and the role of critical service providers, the role of Lead Overseer, and TLPT.

2.3 The DORA legislation, identification of the Critical Third Party Providers, the role of the Lead Overseer, and TLPT

As explained by Krüger and Brauchle (2021), the NIS (Network and Information Systems) Directive notes that the financial sector is one of seven critical infrastructure sectors that require EU Member States to implement appropriate technical and organizational security measures through tailored legislation. Legislation that utilizes this approach came into effect in January 2025. Before the DORA or Digital Operational Resilience Act was introduced, the cybersecurity landscape for financial services in the EU was very complex. Different financial entities were directed by a variety of national and sector-specific standards, missing a unified, sector-wide approach (Krüger and Brauchle, 2021). DORA was introduced to change the regulatory landscape by establishing a comprehensive framework for digital resilience across European financial institutions. As noted by the European Insurance and Occupational Pensions Authority (EIOPA) (2025), its five core pillars include: ICT risk and incident management, classification and reporting, digital operational resilience testing, managing ICT third-party risk, and information sharing arrangements. However, even with DORA in place, challenges persist - specifically in the area of communication and knowledge sharing regarding cyber threats. Maurer and Nelson (2020) note that even though there is a wealth of knowledge gathered on cybersecurity, international collaboration remains limited; this view is also supported by Saveleva Dovgal, Su, and Saalman (2024). Knowledge tends to circulate within trusted networks only, mainly to safeguard national security interests. This limited communication can impede the ability of financial organisations to fully prepare for, respond to, and recover from cyber incidents.

According to Pattison (2024) some of the biggest data breaches in history were caused by leveraging third-party vulnerabilities, with the 2013 Target breach being one of the most well-known. In that case, hackers first targeted a refrigeration contractor who had access to Target's systems, using that access to enter Target's network. They were then able to steal sensitive payment cards and customer information. The breach resulted in

[6] Cybersecurity Framework

the theft of 40 million credit and debit card records, 70 million customer records, an $18.5 million settlement, and major damage to Target's reputation. Also, important to mention the Health Service Executive (HSE) Cyberattack of May 2021. A ransomware attack that severely disrupted Ireland's entire public healthcare system, breaching patient data and critical services (Šípková, n.d.). As well as that, between 2016 and 2020, a series of cyberattacks targeted the SWIFT banking network, jeopardizing transaction security and leading to substantial financial losses. These breaches emphasized the critical need for a more secure and interconnected information-sharing protocol, a requirement that is now mandated by DORA, as explained by Ennis (2024). As noted by O'Neill (2024), a key component of DORA is ensuring that financial institutions identify their critical or important functions. This is vital to ensure that any disruption to these functions does not impact the institution's financial performance, its ability to maintain regulatory compliance, or the quality and delivery of its services on day-to-day basis. Buttigieg and Zimmermann (2024) argue that financial organisations have grown to thoroughly rely on ICT systems and thus cyber risks are now considered to be of systematic importance and are addressed by regulators worldwide.
DORA brought in a consolidated framework to strengthen digital resilience across the financial sector. However, challenges such as limited cyber threat information sharing persist (Maurer & Nelson, 2020). Real-world incidents - such as the Target data breach caused by a third-party vendor - showcase the importance of DORA's emphasis on identifying critical functions to prevent significant disruptions (Pattison, 2024).

Prior to DORA, there was no European Union-level Lead Overseer that would have been in place for critical third-party providers. National regulators and financial institutions themselves were responsible for managing risks associated with third-party providers. The EU level legal frameworks that existed were CRD[7], MiFID[8] and PSD2[9] which were then used by the EBA[10] to provide updated guidelines for financial institutions on outsourcing, European Banking Authority (2019). Under DORA, financial institutions are tasked to ensure that the third-party providers that they employ, which are deemed as Critical Third-Party Providers or CTPPs, are managed under the Lead Overseer from one of the supervisory authorities, namely EBA, ESMA, or EIOPA. According to Article 31 of the Digital Operational Resilience Act (2024), the Lead Overseer can be assigned to one of three European Supervisory Authorities, also known as ESAs. Those include: European Banking Authority (EBA), European Securities Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA). A Lead Overseer is assigned to each critical ICT third-party service provider by the ESA that manages the largest portion of total assets held by financial entities relying on that provider. As explained in Article 33 of the Digital Operational Resilience Act (2024) the Lead Overseer will be charged with supervising ICT third-party service providers regarding oversight and will serve as the main point of contact. These ICT third-party service providers will typically be large companies like Amazon or Microsoft that offer essential infrastructure or services widely used across the financial sector, as pointed out by Pattison (2024). The Lead Overseer will review to determine whether the critical ICT third-party provider (CTPP) has effective rules and processes in place to manage ICT risks that could impact financial institutions. While the focus is mainly on services supporting critical functions, other services may also be reviewed if necessary. The evaluation will look at several key areas: the security, reliability, scalability, and quality of ICT services, including data protection, physical security of data centers and related infrastructure, risk management, business continuity, and recovery planning. It will also address governance structures and accountability for ICT risk, how cyber incidents are detected, reported, and resolved, as well as support for porting of data and applications to ensure seamless transitions Pattison (2024). Additionally, the review will look at system and control testing, ICT audits, and the use of relevant standards and best practices. Based on the findings, the Lead Overseer will prepare an annual oversight plan explaining desired outcomes and actions for each CTPP. The third-party provider in question was deemed a critical ICT third-party provider.
TIBER-EU (Threat Intelligence-Based Ethical Red Teaming) is an initiative created to enhance cybersecurity within the financial sector. It's been active since 2018, and it offers financial institutions a customized, intelligence-driven, controlled Red Team exercise, commonly known as ethical hacking, as explained by the

[7] Capital Requirements Directive
[8] Markets in Financial Instruments Directive
[9] Revised Payment Services Directive
[10] European Banking Authority

Central Bank of Ireland (2019). While the TIBER-EU framework is carried out at a national level, participation is voluntary. The test simulates real-life cyberattacks on the infrastructure of an organization, identifying both strengths and vulnerabilities, thereby enabling the institution to address these findings and strengthen its overall resilience. Buttigieg and Zimmermann (2024) note that the DORA regulation will require financial entities that meet specific criteria to undergo compulsory advanced testing in the form of Threat-Led Penetration Testing (TLPT). Challenges arise due to the distinctions between DORA's Threat-Led Penetration Testing (TLPT) and the European Central Bank's TIBER-EU framework. Key differences include the mandatory nature and legal applicability of TLPT under DORA, in contrast to TIBER-EU, which is a voluntary framework. While TLPT is binding for certain financial entities as part of their regulatory compliance, TIBER-EU is a non-binding, supervisory tool aimed at enhancing cyber resilience. DORA TLPT builds on existing advanced testing frameworks. It also ensures mutual recognition of test completion across Member States through attestations issued by authorities.
TIBER-EU is a voluntary, non-binding framework focused on improving cyber-resilience through tailored red-team testing at a national level in contrast to TLPT, which is a compulsory testing framework introduced to strengthen the cybersecurity within the financial sector. While both aim to strengthen operational resilience and cybersecurity, DORA TLPT is a mandatory and legally enforceable testing requirement for qualifying financial entities, building upon the principles of TIBER-EU but enhancing its regulatory scope and ensuring cross-border recognition within the EU. The next section covers the relevant selection of Regulatory Technical Requirements looked at in this research.

2.4 Regulatory Technical Standards that relevant to the third-party provider

Prior to the introduction of DORA, its regulatory obligations for financial institutions and their third-party ICT service providers the EBA[11] issued detailed guidelines and implementation rules on outsourcing arrangements, specifically EBA/GL/2019/02. These guidelines, effective since 2019, provided a framework across the EU for assessing and managing outsourcing risks, particularly in relation to critical or important functions. They emphasized the need for robust governance, risk assessment, due diligence, contractual protections, and monitoring, laying essential groundwork for the stricter, legally binding provisions introduced by the DORA legislation. As pointed out by Matheson (2024), under DORA, financial institutions must oversee ICT third-party risk as part of their overall ICT risk framework, and they remain responsible for compliance, even when outsourcing. For critical functions, institutions must enforce a formal strategy, maintain a record of contracts, and report key relevant information to regulators. Before entering into a contract, financial entities must assess risks, conduct due diligence, and ensure providers meet high security standards. Contracts must include audit rights and allow for termination under defined risk conditions. Resilient exit strategies must be in place for critical service providers to make sure that business continuity and regulatory compliance are retained.
The relevant Regulatory Technical Standards identified for this analysis include: Commission Delegated Regulation (EU) 2024/1773 and Commission Delegated Regulation (EU) 2024/1774. 2024/1773 specifically focuses on third-party providers (TPPs) and outlines requirements for them under the Digital Operational Resilience Act (DORA). The second RTS 2024/1774 is primarily directed at financial organizations and provides more detailed specifications about software compliance and technical implementation. The reason why 2024/1774 was selected is because of the interconnected nature of the regulatory framework - DORA is in place to ensure that harmonious cooperation exists between financial institutions and their providers to ensure continuous, uninterrupted services. European Commission (2024) Section 1 Article 28 of DORA mandates that financial entities remain responsible for compliance with regulatory obligations even when outsourcing to TPPs; therefore, an indirect obligation exists for TPPs to help their clients meet these standards. TPPs that want to offer competitive services to financial companies would need to ensure that their solutions meet the requirements outlined in 2024/1774. Lastly, it was selected because of its relevance to the research topic. The research focuses on looking at how Software X can achieve compliance with DORA, and so the most relevant RTSs were selected. At its core, the Digital Operational Resilience Act (DORA) and its associated Regulatory Technical Standards (RTSs) are concerned with the identification, assessment, and mitigation of third-party

[11] European Banking Authority

risks and their potential repercussions on the operational resilience of financial entities. It is therefore reasonable to conclude that the 2024/1774 RTS holds importance to third-party service providers. As outlined by Brauchle, Göbel, Seiler, and von Busekist (2020), the concept of the "cyber network" encompasses the foundational elements of information and communication technology (ICT) - including software, hardware, and communication infrastructures - that underpin the operational processes of financial institutions. Within this network, certain "nodes" represent points at which financial institutions interface directly with the third-party solution providers, such as external software vendors or IT service firms. These shared technological points are critical, as they represent potential entry points through which cyber threats may be introduced into the financial system. A significant cyber incident affecting an essential third-party provider - especially one serving a broad base of financial institutions or one of systematic importance - can propagate across the network and lead to widespread operational breakdown.
The Regulatory Technical Standards 2024/1773 and 2024/1774 complement each other by setting requirements for third-party providers and financial entities, respectively, creating a shared responsibility for compliance. Brauchle, Göbel, Seiler, and von Busekist (2020) highlight the technological interconnectedness between financial institutions and their third-party providers, where unmanaged risks at critical "nodes" can cause widespread breakdowns. Together, these frameworks emphasize the importance of robust oversight to manage both contractual and systemic ICT risks in the financial sector.

2.5 Gap analysis

A gap analysis, according to Miller (2025), is a structured and methodical approach used to identify differences between current operational practices and a defined optimal or desired state. To ensure impartial judgment and reliability, these analyses are often conducted by independent external entities. The process typically starts with outlining specific aims or performance standards, which serve as benchmarks against which existing practices are evaluated. This view is supported by Rees (2025) and Woolard (2024). As noted by Einstein (2024), performance gaps arise when an organization operates below its strategic objectives, measurable outcomes, or stakeholder expectations, such as those related to revenue, profitability, or market positioning. Despite its complexities, a gap analysis planning process strikes a balance between routine operational tasks and strategic objectives, particularly when referring to information security. For the aim of answering this research question, a performance gap analysis was undertaken. This method involved identifying differences between the organization's existing capabilities or operational practices and the standards outlined in the Digital Operational Resilience Act (DORA) legislation. The analysis evaluated the extent to which Software X aligns with this selection of regulatory requirements; any areas of non-compliance were noted and added to a compliance checklist deliverable. The articles addressed in this gap analysis include: Article 6: Due Diligence from Commission Delegated Regulation (EU) 2024/1773 and Articles 1 (Overall risk profile and complexity), 36 (ICT Security Testing), 10 (Vulnerability and Patch Management), 11 (Data and System Security), 12 (Logging), 16 (ICT Systems Acquisition, Development, and Maintenance), 17 (ICT Change Management), 19 (Human Resources Policy), 28 (Governance and Organization), 34 (ICT Operations Security), and 8 (Policies and Procedures for ICT Operations) from Commission Delegated Regulation (EU) 2024/1774.
Miller (2025) and Rees (2025) specify gap analysis as a method to identify discrepancies between current practices and desired standards, focusing on compliance and improvement. Miller (2025) and Woolard (2024) see gap analysis as an essential tool for closing performance gaps, but Woolard emphasizes ongoing planning and resource management. Applied to Software X and DORA, this analysis reveals existing compliance gaps and helps align operations with strategic goals, supporting Einstein's (2024) view on addressing performance shortfalls. In the next section, gaps in the literature will be looked at.

2.6 The gaps in the Literature

Gusiv (2023) conducted a DORA compliance gap analysis through a literature review and a regulatory interpretation, which offered a primarily theoretical view of how financial institutions might approach the regulation. The current project introduces a practical case study based on a real-world, anonymized software solution - Software X. While both studies utilize constructive research and similar analysis methods, this project

places greater emphasis on technical implementation and uses a case study method to reflect an operational environment. A key difference lies in the intended audience: Gusiv's research is targeted towards financial institutions directly; however, this project is designed to provide actionable insights for third-party providers supporting those institutions. Shetty (2023) presents a valuable framework for achieving compliance with ISO 27001:2022, but does not address the specific regulatory specifications of the Digital Operational Resilience Act (DORA), particularly as they pertain to third-party software providers in the financial sector. The research disregards how DORA shapes software design and vendor contractual obligations. Furthermore, it does not attempt to link ISO/IEC 27001:2022 controls to DORA's Regulatory Technical Standards (RTS), nor does it explore how financial institutions or their suppliers are adapting software systems to meet these mandatory requirements.

Buttigieg and Zimmermann (2024) argue that although DORA introduces a harmonised framework for digital operational resilience across the EU, supervision remains fragmented, with differences in national interpretations and, in some cases, insufficient enforcement. Ennis (2024) adds that, based on engagement with firms and working group discussions, certain aspects of DORA are currently being implemented on a best-efforts basis. This is mostly due to the need for firms to self-interpret the RTSs and apply the principle of proportionality. As a result, there is growing demand for further guidance - specifically in defining what qualifies as "critical and important functions".

Gusiv (2023) offers a theoretical analysis of DORA compliance primarily aimed at financial institutions, focusing on regulatory interpretation without practical application. In contrast, this study analyses a real-world case with Software X, targeting a third-party provider and exploring technical implementation. Similarly, Shetty (2023) focuses on a framework for ISO/IEC 27001:2022 compliance but does not address DORA-specific obligations or their impact on software design, leaving a gap that this research looks to fill. While Buttigieg and Zimmermann (2024) highlight the fragmented enforcement of DORA across territories, Ennis (2024) notes the ongoing, often inconsistent, application of its standards by firms, underscoring the need for clearer guidance - an area this study also addresses through its practical analysis. The next section concludes on the areas looked at in this literature review.

2.7 Conclusion

The literature reveals that even though DORA places regulatory responsibility on financial institutions, third-party providers - especially those who are deemed critical - must display their compliance with its requirements through contractual and operational measures. By analysing established models such as ISMS and NIST CSF 2.0, and looking at the core components of DORA - including the designation of critical third-party providers, the role of the Lead Overseer, and TLPT - the review serves as a foundation for the case study. The review of relevant Regulatory Technical Standards offers a glimpse into the technical expectations under DORA. Finally, the discussion on gap analysis reveals what is necessary in practical terms. The research looked at in this review tends to emphasize financial institutions, leaving a gap in practical guidance for third-party providers such as the provider of Software X. This study aims to address that gap by applying a constructive research approach to evaluate compliance readiness from the provider's perspective.

3 Related Work

Riaz and Younas (2024) look at the challenges that the third-party providers to Swedish financial institutions face when attempting to comply with DORA and provide some practical recommendations to improve compliance. Ter Haar (2022) gathered primary data to analyse the perceptions of DORA within financial organizations in the Netherlands. The feedback reported mostly positive perceptions of DORA, with most importance placed on ICT incident reporting and third-party risk management. Gusiv (2023) provides a strong foundation for grasping DORA compliance through a structured gap analysis based on a literature review as well as through regulatory interpretation. The work is noteworthy for its concise explanation of DORA's principles and its methodical recognition of potential areas of non-compliance. However, the work is theoretical in nature, missing real-world application or implementation testing. It does not analyse the impact of DORA on vendor responsibilities, software architecture, or the operational realities of third-party ICT providers. Also, the absence of practical direction and technical conformity with the Regulatory Technical Standards (RTS) limits its

usability for third-party practitioners. This emphasizes the need for more applied research that builds on Gusiv's work while including operational insights, technical tools, and a focus on third-party providers' software systems. Research by Bonifazi (2025) also looks at DORA and, more specifically, how project management methodologies assist in supporting compliance in financial institutions. In contrast, Shetty (2023) describes a clear roadmap for ISO/IEC 27001:2022 compliance but does not consider the regulatory challenges posed by DORA, especially for software vendors in the financial sector. While there are some similarities between ISO standards and DORA's Regulatory Technical Standards (RTS), notable gaps exist - particularly in addressing how sector-specific regulations influence technical changes. Therefore, this research does not fully bridge those gaps in understanding or integration. Karakasilioti (2024) looks at DORA's legal and historical context and lists key components such as ICT risk frameworks and compliance procedures. A case study of 'Bank X' illustrates the practical use of a DORA Assessment Tool, highlighting the importance of preparation, collaboration, and structured evaluations to identify gaps and improve compliance. Ennis (2024) speaks about interpretive challenges companies face in applying DORA - especially around defining 'critical functions' and applying proportionality. This view is also held by research conducted by Tošić (2025), where anticipated DORA implementation difficulties are analysed. This supports the need for clear, operationally grounded techniques that can translate DORA's legal requirements into more practical practices for third-party software providers. Boddy (2024) utilizes primary data to analyse the challenges faced by financial organisations in incident reporting in regard to their existing decision-support frameworks. The thesis focuses on alignment with the DORA regulation in terms of incident notification practices. Sachdeva (2023) contributes a practical framework for evaluating institutional DORA readiness through gap analysis and maturity scoring, supported by tools like OneTrust and Power BI. However, the focus remains on organizational controls, with little attention to how DORA reshapes technical operations or software development among third-party providers. Stanik (2025) argues that the lack of research on how DORA standards are applied within GIS (Geographic Information Systems) is producing difficulties in reaching compliance. The absence of analysis on software adaptation underlines the necessity for research that bridges this gap, which is the exact aim of this study. Both Sachdeva (2023) and Gusiv (2023) share methodological similarities with this research through the use of a constructive research design. Phadnis (2021), while proposing useful insights on audit preparedness and compliance stance, does not address DORA, lacks technical specificity, and excludes supplier perspectives. Even though it is valuable for contextual understanding, the study remains secondary to the software-focused query central to this research.

Yaxiaer (2024) looks at data security practices among SMEs in China's e-commerce sector and reveals broader challenges in translating regulatory needs into technical implementation. Although the study is based on China's Personal Information Protection Law (PIPL), many of the difficulties it uncovers - such as constrained resources, disjointed security practices, and a mismatch between operational goals and regulatory expectations resonate with the struggles faced by third-party ICT providers in the EU financial sector under DORA. These similarities point to a universal need for clear guidance, adaptable solutions, and cooperative approaches to regulatory compliance at the software level. An equivalent precedent can be found in the rollout of the General Data Protection Regulation (GDPR). Reeves (2020), in a study where GDPR was implemented across Irish organizations, found significant inconsistencies in compliance readiness, even though general awareness of the regulation existed. Gaps in training, expertise, and structural preparedness - particularly around documentation - limited the effectiveness of the implementation. Similar patterns are arising from DORA, which enforces equally complex technical requirements on financial institutions and their ICT partners. Just as GDPR started substantial operational reforms, DORA now demands architectural and procedural changes to enforce digital resilience. This investigation continues that line of inquiry, as explained by Reeves (2020), by examining how DORA's Regulatory Technical Standards (RTS) influence software development and operations among third-party suppliers. Through the use of a gap analysis of Software X against DORA's RTS, the research moves beyond policy-level examination and focuses on the preparedness of software systems and vendors to meet evolving compliance expectations. The next section will focus on the research methodology utilized.

4 Research Methodology

4.1 Use of AI Statement

AI tools were employed in a limited, assistive capacity to sketch an initial mind map, suggest synonyms where needed, expand vocabulary, and, in some cases, clarify legislation or reword text for readability. After that, all outputs were critically reviewed, refined, and rewritten to ensure the work reflects the author's own words. Where external references were suggested, independent research was conducted to verify their credibility before usage. The researcher retains full responsibility for the analysis and conclusions.

4.2 Describe the steps you followed in your research

The research focused on eight structured steps to understand how DORA impacts software changes in third-party suppliers to financial institutions. It began by establishing a research problem and refining sub-questions based on initial findings. A literature review of ISMS, DORA, TLPT, and key relevant RTSs (EU 2024/1774 & 2024/1773) revealed some specific areas to focus on. Software X is used by a critical third-party provider and so was selected as a case study. Data collection included analysis of relevant documentation, vulnerability scanning, code reviews, and log analysis. A gap analysis discovered compliance deficiencies against RTS requirements. Based on this, a compliance checklist was developed using constructive research. The findings were validated through expert review, offering key insights and practical implications.

4.3 Describe the materials and equipment used in the research

To ensure the effectiveness of the research, a variety of materials and tools were used. These implementations were used for data collection, analysing the resilience of the software, and assessing compliance with DORA and its associated Regulatory Technical Standards. A summary of the tools is provided in the table below:

Category	***Specific Tools***	***Description of use***
Software Tools:	Vulnerability Scanner	The Qualys cloud-based cybersecurity and compliance platform allows organizations to detect security vulnerabilities across their infrastructure. A VMDR (Vulnerability Management, Detection, and Response) scan was conducted on the server hosting Software X, while a Web Application Scanning (WAS) was performed on Software X to identify vulnerabilities within the application itself. Detailed reports were generated from both scans; these were used to understand the resilience of the system.
	Visual Studio, Visual Studio Code	Development environment
Documentation:	Penetration Testing Report	A penetration testing report was reviewed, providing insights into the weaknesses and gaps in the defences of Software X.
	Release Notes	Software X release notes were examined to understand updates that were made, to review patches and features implemented.
	Regulatory Texts	DORA legislation was looked at, and Regulation EU 2024/1774 and Regulation EU 2024/1773 were selected for analysis to identify relevant compliance requirements.
	Internal Compliance Documentation	The internal compliance documentation from the case study was reviewed to understand how the policies within the company align with the legal requirements and resilience standards.
Meeting and Collaboration Tools:	Document Collaboration Tools	An online document editing platform was used, namely Microsoft Word, to share drafts of the work with the supervisor and the internal members within the company to keep them in the loop of the ongoing research.
	Virtual Collaboration Space	The Teams virtual collaboration platform was used to conduct supervisor meetings and meetings with internal person within the company to discuss the research.
Analytical Frameworks:	Gap Analysis Framework	A gap analysis framework was used to assess the differences between the existing software features and security measures in relation to the relevant RTS.
Data Collection and Reporting Tools:	Document Management System	SharePoint was used to access relevant internal company documentation for revision.
	Code repositories	Utilized subversion, Git, Jira, Visual Studio, Visual Studio Code
	Generative AI tool	sketched out a mind map, identified relevant sources based on its suggestions, and then conducted independent research to verify their credibility before referencing. Used it as a tool for finding synonyms and expanding vocabulary, and in some

		instances, explaining legislation. In some cases, it was also used for rewording some text for clarity, but updated after that to ensure that the text reads in the author's own words. Throughout the process, all suggestions were critically evaluated to ensure reliability and relevance.
	Financial Supplier Qualification System	FSQS or the Financial Supplier Qualification System, was reviewed to understand the compliance and risk management practices of a third-party supplier in relation to DORA
Data Visualization tools	Excel	Pivot tables drawn using MS Excel
	PowerBI	Power BI was used to sketch out some graphs to help display the data

Table 1: summary of materials and equipment used

4.4 Explain how the samples were gathered, any randomization techniques, and how the samples were prepared

The theoretical framework for this study draws on Regulatory Compliance Theory, which, according to Fiene (2023), provides a structured lens for grasping the base principles that underpin effective compliance. This theory focuses on the importance of several core parts: understanding and staying up to date with legal and regulatory obligations, pre-emptively identifying and mitigating compliance risks, setting clear, accessible policies and procedures, and applying robust internal controls to promote accountability. It also emphasizes the need for ongoing employee training, regular monitoring and auditing, comprehensive documentation and reporting, a strong company culture of compliance, clearly defined accountability procedures, and a commitment to continuous improvement. In regard to this research, the theory is applied to understand the pressures placed on third-party software suppliers to align with the Regulatory Technical Standards (RTS) under the Digital Operational Resilience Act (DORA), framing the processes and organisational responses needed for achieving regulatory alignment.

The Information Security Risk Management (ISRM) Framework, part of the broader ISMS, focuses on identifying, assessing, and mitigating information security risks. As noted by SentinelOne (2024), it relies on clear policies risk assessments to ensure that the threats are prioritized, as well as strong management support to ensure implementation. In this study, ISRM provides a foundation for evaluating how Software X and comparable tools address DORA's security requirements, such as vulnerability scanning, incident response, and configuration hardening.

Socio-Technical Systems Theory, as explained by Leeds University Business School (2025), emphasises that organisational systems function through the interaction of social and technical components. Changes in one area, such as the introduction of new regulations, inevitably affect the social component as well. This theory supports the study by explaining how regulatory pressure from DORA influences decisions in software design, development, and integration within the supplier ecosystems. For this research, purposeful nonprobability sampling was used, focusing on a critical third-party software provider to financial institutions affected by DORA. This approach, as noted by Merriam and Tisdell (2015), aims to gain deep insight rather than quantify patterns. Data collection utilized secondary sources, primarily DORA legislation, RTSs, and relevant organisational documentation and procedures. The scope regarding the documentation and/or procedures of the organization that were utilized for conducting this research included:

In Scope:	*Out Of Scope:*
Due diligence documentation	Client onboarding protocols
Some procedures were reviewed from the Customer Support team	Sales and business development operations
Some procedures were reviewed from the Product Implementations team	Marketing and Communications operations
Software mapping charts reviewed	Finance and Billing operations
Staff Training procedures reviewed	Recruitment and HR operations
Data Handling Policies	Contract Management operations
Organizational Structure and Permissions	Contract SLAs (Service Level Agreements)
Audit Trails and Documentation	
Core Development Team Procedures	
Quality assurance team procedures	
Code Repositories and commit history	
Logging practices	
Infrastructure diagrams	

Release notes
Software X code base
Internal Wikis and SharePoint docs
Reports from vulnerability scans
A penetration testing report
Standard Operating Procedures (SOPs)
Risk Management Framework

Table 2: Scope

Randomization techniques were not applied due to the focused nature of the study, which looked at a single software supplier affected by DORA. Data was prepared by excluding any unrelated or outdated information. The data was also categorized to make it more usable. The categories include: software features of Software X and resilience measures (ex-ante and ex-post). The collected data was examined to uncover compliance limitations and to highlight areas for improvement in software design and development practices.

4.5 Explain how the measurements were made and what calculations were performed upon the raw data

To begin, the two key relevant Regulatory Technical Standards (RTS) - namely, Commission Delegated Regulation (EU) 2024/1773 and Commission Delegated Regulation (EU) 2024/1774 - were looked at in detail. Each article and sub-articles from both regulations were transcribed into a separate document to ensure clear visibility of every individual requirement. This process not only helped uncover the structure of the legislation but also assisted in developing a deeper understanding of its content. Following this, the articles and subsections most relevant to Software X were identified using nonprobability sampling. That selection was made using Judgmental or Purposive Sampling, where judgment and experience were utilized to select the most relevant samples. For each relevant subsection, a structured interpretation approach was applied in a separate, dedicated document. This involved several stages: first, the original legislative text ('source content') was extracted; next, key concepts were extrapolated to capture the essence of the clause. Then, a 'natural and ordinary meaning' was written out in plain language to clarify the legal intent. After this, a compliance control theme was selected - this helped group the requirements into a broader, actionable category. Finally, the subsection was reformulated into a gap analysis question, suitable for use in a compliance assessment. An example of this can be seen in table below:

Legislation:	**Article:**	**Source content**	**Key concepts that were derived from the text**	**Natural and Ordinary Meaning**	**Compliance Control Theme**	**Reformulated to be usable in a gap analysis**
For Regulatory Technical Standard: COMMISSION DELEGATED REGULATION (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council	Article 6: Due Diligence 1(b)	'*has the ability to monitor relevant technological developments and identify ICT security leading practices and implement them where appropriate to have an effective and sound digital operational resilience framework,*'	to monitor developments, to identify and implement ICT security best practices, as well as to build a resilient security framework	An organization must be capable of keeping up with new and relevant technologies, recognizing top security standards or methods, and applying them where it makes sense, to maintain a strong and reliable digital resilience system.	Identified for this included ensuring security maturity on an ongoing basis, use of recognized frameworks, and up-to-date security posture.	Have you implemented ICT security measures aligned with industry best practices (e.g., ISO/IEC 27001, NIST, ENISA guidance)?

Table 3: Interpretation example

This process was applied to a total of forty-eight items, which were then gathered in a gap analysis Excel spreadsheet. This document formed the foundation for the following case study. The next phase included a revision of all relevant documentation, conducting code reviews, and performing vulnerability testing on Software X. These activities provided the necessary information to fill in the gap analysis.

A	B	C	D	E	F	G	H	I	J
Legislation:	**Article No:**	**Subsection:**	**Requirement interpretation for TPP:**	**Grouping Gaps into the outcome areas:**		**Actions to Address the Gap:**		**Compliance:**	**Governance Inventory:**
				Outcome	*Is there a gap?*	Process	Status	Rationale to support compliance	Which standard/framework/methodology/policy or procedure is this linked to?
COMMISSION DELEGATED REGULATION (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers	Article 6: Due Diligence	1(b)	How you implemented ICT security measures aligned with industry best practices (e.g. ISO/IEC 27001, NIST, ENISA guidance)	ICT systems are secured according to industry standards, meeting resilience and regulatory compliance	No	N/A	N/A	The organization has been audited by an external company to ascertain compliance with ISO/IEC 27001	ISO/IEC 27001, DORA
COMMISSION DELEGATED REGULATION (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework	Article 1: Overall risk profile and complexity	1	Do you conduct regular vulnerability assessments and penetration testing?	Demonstrated resilience through proactive identification and mitigation of security weaknesses	Yes	will carry out vulnerability checks and external penetration testing frequently. Any issues found will be shared within 10 working days and fixed based on agreed timelines	In Progress (tracked by internal manager)	Vulnerability assessments are being conducted on demand more on this below. Penetration testing is performed regularly	ISO/IEC 27001, DORA

Figure 1: Gap analysis document example

4.6 Describe the statistical techniques used on the data

Starbuck (2023) notes that Descriptive Statistics are basic analytical methods used to summarize and present data in a clear and meaningful way. While they don't enable us to make inferences beyond the data at hand, they are valuable in understanding and interpreting the information available. Descriptive Statistics were used to summarize the data for this research. To begin, below is a mind map of all the articles outlined from the two Regulatory Technical Standards used in this research.

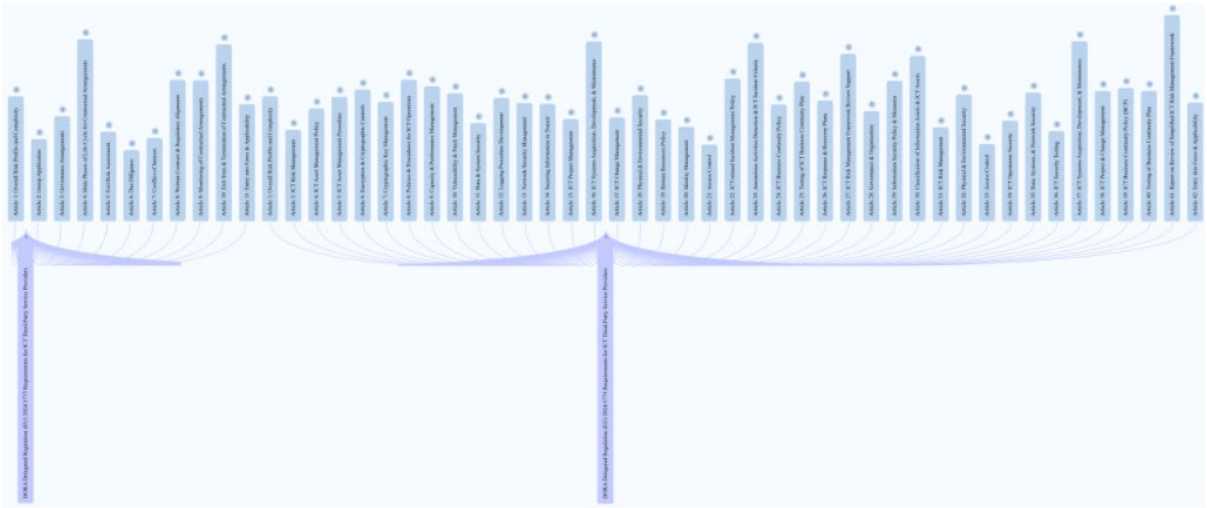

Figure 2: Mind Map

After reviewing the articles and the sub-articles, the most relevant ones were identified and documented in a separate Word file. Each sub-article was then analyzed as outlined in the previous section, with gap analysis questions consequently added to an Excel spreadsheet for data organization. The next step was conducting the research into Software X to be able to fill in the gap analysis and answer the questions posed there. For this, a review was conducted of in-scope documentation, configuration, code, and report files as outlined in Table 2. Once the gap analysis document was filled in, visualization tools were employed to help display relevant information in a meaningful way. After the data had been organized, data analysis was carried out. Some descriptive statistics were created using Excel on data drawn from the gap analysis:

Requirement	Total items addressed	Compliant	Gaps	Percentage of requirements met
Due Diligence	1	1	0	100
Overall risk profile and complexity	1	0	1	0
ICT Security Testing	7	6	1	85.71
Vulnerability and Patch Management	11	7	4	63.64
Data and System Security	2	1	1	50
Logging	2	2	0	100
ICT Systems Acquisition, Development, and Maintenance	3	0	3	0
ICT Change Management	4	4	0	100
Human Resources Policy	1	1	0	100
Governance and Organisation	1	0	1	0
ICT Operations Security	14	11	3	78.57
Policies and Procedures for ICT Operations	1	1	0	100

Sum of Total Requirements	Sum of Compliant	Sum of Gaps
48	34	14

SUM:	
Total Requirements:	48
Compliant:	34
Gaps:	14
Percentage of requirements met:	70.8333333

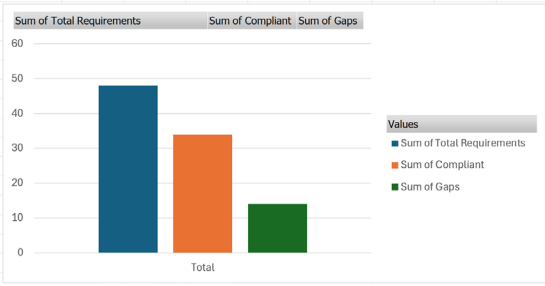

Figure 3: Descriptive Statistics

The pivot table shows the data from the gap analysis organized into a tabular format. A count was then performed on the total requirements, total gaps, and the number of compliant items. Finally, a percentage was calculated to illustrate the total percentage of requirements met. From this, a Pie chart was created as can be seen below:

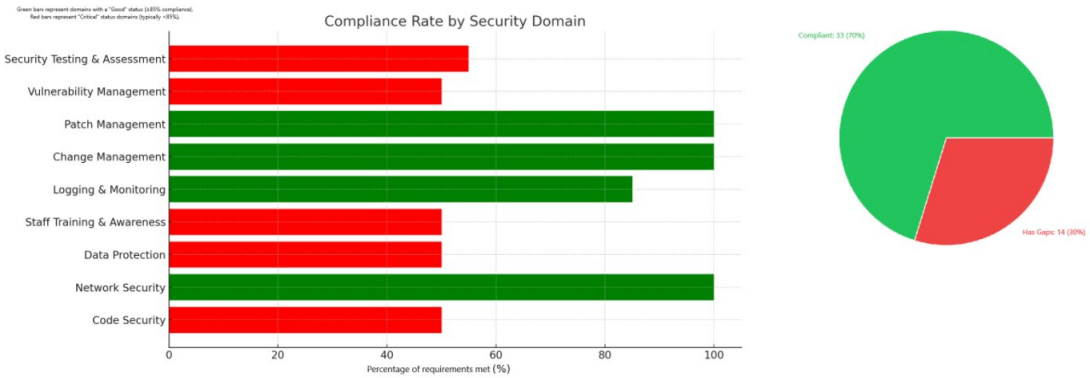

Figure 4: Pie Chart

An additional data table was developed using PowerBI BI tools and can be seen below. This represents a dashboard-like representation which displays information such as the total count of items where gaps exist, displays which articles were used in the gap analysis, etc. The next section will discuss design specifications.

Figure 5: PowerBI table data

5 Design Specification

5.1 The techniques and/or architecture/framework that underlie the implementation and the associated requirements are identified and presented

This research utilized the principles of a mapping matrix as well as a gap analysis to generate a gap analysis document. This was done to evaluate the extent to which Software X aligns with DORA. The techniques and architecture used are outlined below.

- ***Regulatory Mapping Technique***: A custom mapping methodology was developed to be able to interpret the specific relevant Regulatory Technical Standards (RTS), namely COMMISSION DELEGATED REGULATION (EU) 2024/1773 and COMMISSION DELEGATED REGULATION (EU) 2024/1774, which were broken down into assessable software-related controls. This included security testing, vulnerability, change and patch management, logging and monitoring, staff training and awareness, data protection, network security, and code security.
- ***A Matrix-based Architecture***: A table was created in Excel. Please refer to Figure 3. In it, the information was divided into security domain, which indicated the area from which the requirements were taken, then total requirements, or the number of requirements that Software X was compliant against, and status.
- ***Component Level Analysis***: Analysis was performed at the level of individual software modules, each evaluated against relevant articles and sub-articles of DORA RTS.
- ***Supporting Tools and Frameworks***: An Angular CLI web page was created to display a gap analysis dashboard for visualizing compliance status. Please refer to the configuration manual for more details.

6 Implementation

This section presents the deliverables created to assess Software X's alignment with the Digital Operational Resilience Act (DORA), including applicable RTS. The assessment approach was designed to evaluate Software X comprehensively while preserving system confidentiality and data integrity throughout the process. The project began with a structured scoping exercise to set the boundaries and select relevant policies, procedures, and systems (see Table 2). The outputs for the project include:

- ***Compliance Gap Matrix*** - A compliance gap matrix was developed in Excel by mapping RTS obligations to available controls and documentation. To support this, a legislation interpretation framework (Table 3) translated the legal text into clearer evaluation criteria. The case study of Software X involved targeted analysis of internal policies and technical safeguards, identifying areas impacted by DORA as outlined in the scope (Table 2). Please refer to Appendix 1. Supporting Documentation.

- ***Legislation Mapping Framework*** - a comprehensive legislation mapping framework was constructed (Table 3) to translate regulatory requirements into actionable gap analysis criteria, enabling systematic assessment of compliance against DORA obligations.

- ***Case Study: Software X*** - the case study phase included gathering and analysis of Software X's internal procedural and technical documentation, along with some procedures and controls at the business level which were deemed in scope (Table 2). The case study offered a real-world basis for conducting an evaluation of how such providers are impacted by DORA.

- ***Compliance Checklist*** - A compliance checklist was generated that highlighted key gaps, notes, status, and persons in charge of changes. This was designed and gathered in an Excel document. Please refer to Appendix 1. Supporting Documentation.

- ***Compliance Dashboard*** - A compliance dashboard application called GapAnalysisMatrix was created. This was created using Angular CLI. More on this, please see the configuration manual.

- ***Visuals*** - Excel formulas were used to create some Descriptive Statistics to display the results from the gap analysis. As well as that, PowerBI was used to display a compliance dashboard. Additionally, some diagrams were generated using Excel.

7 Evaluation

This section presents the key findings from the compliance gap analysis between Software X and the requirements specified in the Digital Operational Resilience Act (DORA). The analysis addressed the central research question: How is DORA influencing changes at the software level within third-party suppliers to financial institutions? Findings are structured around three pillars: internal risk governance, external regulatory obligations, and software-level readiness.

A compliance gap analysis matrix was developed, which mapped the key conditions of the Regulatory Technical Standards (RTSs) under DORA against the current controls and competencies in Software X. The assessment was divided into the most relevant key articles identified and sub-articles under those. These include:

Regulation:	***Article:***	***Number of items addressed under the Article:***	***No of gaps:***
COMMISSION DELEGATED REGULATION (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers.	Article 6: Due Diligence	1	0
COMMISSION DELEGATED REGULATION (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework .	Article 1: Overall risk profile and complexity	1	1
	Article 36: ICT Security Testing	7	1
	Article 10: Vulnerability and Patch Management	11	4
	Article 11: Data and System Security	2	1
	Article 12: Logging	2	0
	Article 16: ICT Systems Acquisition, Development, and Maintenance	3	3
	Article 17: ICT Change Management	4	0
	Article 19: Human Resources Policy	1	0
	Article 28: Governance and Organisation	1	1
	Article 34: ICT Operations Security	14	3
	Article 8: Policies and Procedures for ICT Operations	1	0

Table 4: Key article categories and findings

Table 4 summarizes the number of sub-requirements addressed per article and the corresponding number of identified gaps. For example, Article 10 on Vulnerability and Patch Management had eleven applicable criteria, of which four were not fully met. Articles such as 16 (ICT Systems Acquisition) and 34 (ICT Operations Security) also revealed several gaps. Additionally, a comparative reference was made to ISO/IEC 27001:2022 controls. This was done to determine where alignment exists and where DORA imposes more strict and specific requirements. Figures 3 - 6 display visuals generated to organize and display the results from the research. Additionally, a bar chart was created to visualize how compliant identified articles are:

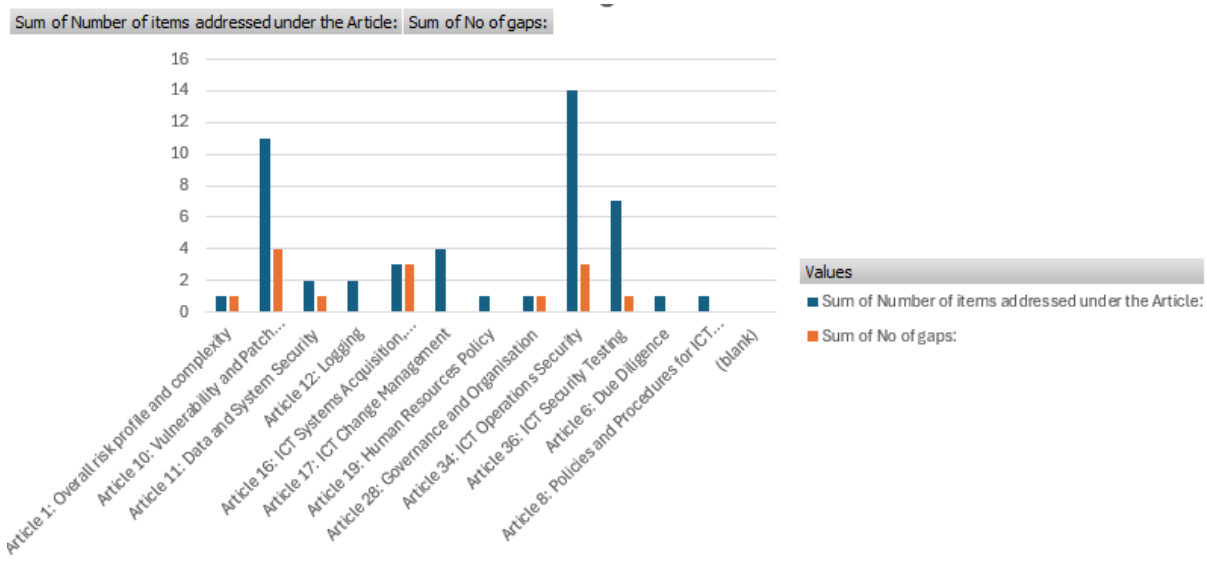

Figure 7: bar chart

The research results indicate that third-party providers, especially the smaller vendors, face significant obstacles in their efforts to align with DORA's expectations. Key implications include:

- Need for Formal Risk Ownership: Lack of accountability mechanisms hinders proactive mitigation.
- Regulatory Complexity: Without dedicated compliance personnel, smaller vendors may misinterpret RTSs.
- Tooling Deficiencies: Inadequate logging, monitoring, and automation limit resilience testing capacity.

7.1 Discussion

The research found that Software X aligns with several requirements of DORA, though not in full, this is largely due to its foundational compliance with ISO/IEC 27001:2022. However, gaps were identified - particularly in Article 10 (Vulnerability and Patch Management) and Article 16 (ICT Systems Acquisition, Development, and Maintenance). These deficiencies originated from informal or undocumented practices, limited tracking of vulnerability remediation, and a lack of structured security-by-design integration in the software development lifecycle.

While ISO/IEC 27001:2022 provided a valuable starting point, its flexible, principles-based approach does not fully align with DORA's more prescriptive and accountability-focused obligations. In particular, DORA demands continuous oversight, traceable risk decisions, and standardized third-party management, which were only partially shown in Software X's current control set.

Although the study successfully identified key compliance gaps, it was limited by its focus on a single piece of software under Software X, a single supplier, and the constraints of confidentiality. Restricted access to certain technical artefacts may have led to cautious interpretations of compliance levels. Future research would benefit from a broader and more diverse sample of third-party providers, expanded software scope, and the inclusion of primary data gathered from regulated financial institutions. Additionally, a detailed control-mapping framework between ISO/IEC 27001:2022 and DORA RTSs could support more precise alignment.

Overall, the findings align with current literature, indicating that smaller third-party software providers often face significant challenges in meeting DORA's heightened operational resilience standards, despite having foundational security practices in place.

8 Conclusion and Future Work

The primary research question guiding this study was*: How is DORA influencing changes at the software level within third-party suppliers for financial institutions*? To answer this, the research established and pursued three key objectives: (1) to develop a compliance gap analysis between the software solution (Software X) and the relevant Regulatory Technical Standards (RTSs) under DORA, (2) to construct a practical compliance checklist for action planning, (3) to evaluate both internal and external risk management practices, including risk

classification, mitigation, and third-party oversight. These objectives were successfully met through the use of literature review, analysis of the legislation, and the software itself. A detailed compliance gap analysis was created, enabling a clear comparison between the selected DORA RTSs and the existing controls and policies implemented in Software X. This analysis revealed several key areas with gaps in compliance, highlighting both the strengths of ISO/IEC 27001:2022 as a foundational security standard and its limitations in satisfying DORA's more prescriptive and operationally demanding requirements. Notably, gaps were observed in areas such as Overall risk profile and complexity, ICT Security Testing, Vulnerability and Patch Management, Data and System Security, ICT Systems Acquisition, Development, and Maintenance, Governance and Organization, and ICT Operations Security - elements that are critical to operational resilience under DORA.

Additionally, the study's use of tools such as a compliance checklist, a legislation mapping framework, and a dashboard gap matrix, along with other visualization tools, helped translate abstract regulatory regulations into actionable evaluation criteria. These tools greatly assisted in the clarity of the findings.

While the study offers some good insights, it is not without limitations. The evaluation was confined to a single software provider, to only one piece of software, and was limited by confidentiality constraints, which may have restricted access to the full list of controls and procedures in place. As such, the findings may not be fully transferable to other third-party vendors or sectors.

Future research could address these limitations by expanding the sample to include a number of third-party software providers across different financial domains. Moreover, future studies could benefit from triangulating data sources - such as gaining perspectives from client financial institutions and/or regulators themselves. Another recommendation could be the development of a detailed mapping framework between ISO/IEC 27001 controls and DORA RTS requirements to streamline dual compliance efforts and avoid duplication.

In conclusion, the findings of this research shine a light on growing regulatory pressure on third-party software providers to go beyond baseline security standards and to adopt a more structured, transparent, and proactive approach to operational resilience. The introduction of DORA marks a change towards more granular and enforceable compliance obligations, and this study provides both a research basis and practical recommendations for organizations seeking to navigate this regulatory evolution.

References

Gusiv, P., 2023. *Development of a compliance gap analysis method for the Digital Operational Resilience Act (DORA).* Unpublished master's thesis. Lapland, Finland: Lapland University of Applied Sciences

Edgar, T.W. and Manz, D.O., 2017. *Research methods for cyber security*. Cambridge, MA: Elsevier

Edwards, J. and Weaver, G., 2024. *The cybersecurity guide to governance, risk, and compliance.* Hoboken, NJ: Wiley

Hanington, B. and Martin, B., 2012. *Universal methods of design*. Beverly, MA: Rockport Publishers

Pattison, A., 2024. *DORA – a guide to the EU Digital Operational Resilience Act*. Ely, UK: IT Governance Publishing

IT Governance Publishing, 2023. *ISO 27001:2022 ISMS lead implementer training course*. [online] Available at: https://learning.oreilly.com/course/iso-270012022-isms/9781787785069/ [Accessed 9 April 2025]

O'Neill, S., 2024. *DORA compliance: Four tips for enhancing third-party management*. 23 September. [online] Available at: https://www.grantthornton.ie/insights/factsheets/dora-compliance-four-tips-for-enhancing-third-party-management/ [Accessed 9 April 2025]

CM Alliance, 2024. *EU DORA requirements for ICT service providers: all you need to know*. 12 September. Available at: https://www.cm-alliance.com/cybersecurity-blog/eu-dora-requirements-for-ict-service-providers-all-you-need-to-know [Accessed 9 April 2025].

Grant Thornton, 2023. *Digital Operational Resilience Act (DORA): Security testing requirements*. 5 April. Available at: https://www.grantthornton.ie/insights/factsheets/impact-of-dora-security-testing-requirements/ (Accessed: 9 April 2025)

Ansari, J., 2023. *Information and cyber security GRC: compliance assessment and reporting*. [Online course] Available at: https://app.pluralsight.com/ilx/video-courses/387ebbbe-ef73-49ba-b306-b5d311748d5e [Accessed 9 April 2025]

Deloitte, 2023. *ISO 27001:2022 and ISMS Compliance*. Available at: https://www.deloitte.com/ie/en/services/risk-advisory/perspectives/ISO-27001-2022-and-ISMS-Compliance.html (Accessed: 9 April 2025)

Pattison, A., 2025. *NIST CSF 2.0 – Your essential introduction to managing cybersecurity risks*. [Cambridgeshire]: [IT Governance Publishing Ltd]

Edwards, J. (2024) *A comprehensive guide to the NIST Cybersecurity Framework 2.0*. [Hoboken]: [John Wiley & Sons Ltd]

European Union, 2024. *Digital Operational Resilience Act, Article 31 – Designation of critical ICT third-party service providers*. Available at: https://www.digital-operational-resilience-act.com/Article_31.html [Accessed 14 April 2025]

Digital Operational Resilience Act, 2024. *Article 33 – Tasks of the Lead Overseer.* Available at: https://www.digital-operational-resilience-act.com/Article_33.html [Accessed 14 Apr. 2025].].

European Commission, 2024. Commission Delegated Regulation (EU) 2024/1773 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of the policy regarding contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. *Official Journal of the European Union*, L series. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1773 [Accessed 14 April 2025]

Krüger, P.S. & Brauchle, J.-P., 2021. *The European Union, cybersecurity, and the financial sector: A primer*. Carnegie Endowment for International Peace. Available at: https://www.jstor.org/stable/resrep30026.1 [Accessed 26 February 2025]

Maurer, T. & Nelson, A., 2020. *International strategy to better protect the financial system against cyber threats*. Washington, DC: Carnegie Endowment for International Peace. Available at: https://www.jstor.org/stable/resrep26915.1 [Accessed 26 Feb 2025]

Klumpes, P.J.M., Chanon, R.D., Habahbeh, L. and Mann, S., 2024. *Operational resilience in the UK financial sector: Practical guidance*. Unpublished working paper, Aalborg University. Available at: [https://vbn.aau.dk/ws/portalfiles/portal/736570091/RM_Operational_Resilience_in_the_UK_Financial_Sector_TFG_Paper_12082024.pdf]

Fiene, R. (2024) *Theory of Regulatory Compliance, Regulatory Compliance Scale, and Differential Monitoring*. Penn State Edna Bennett Pierce Prevention Research Center. Available at: https://download.ssrn.com/2024/6/23/4874059.pdf (Accessed: 29 April 2025)

Fiene, R., 2023. *Importance of the theory of regulatory compliance*. Prevention Research Center, Penn State University. Available at: https://medium.com/@rickfiene/importance-of-the-theory-of-regulatory-compliance-8335b3a5fbc (Accessed: 29 April 2025)

SentinelOne, 2024. *Information security risk management*. Available at: https://www.sentinelone.com/cybersecurity-101/cybersecurity/information-security-risk-management/ (Accessed: 29 April 2025)

Leeds University Business School, 2025. *Socio-technical systems theory*. [online] Available at: https://business.leeds.ac.uk/research-stc/doc/socio-technical-systems-theory [Accessed 29 April 2025]

Merriam, S.B. and Tisdell, E.J., 2015. Qualitative Research: A Guide to Design and Implementation. 4th ed. San Francisco: Jossey-Bass.

European Parliament and Council, 2022. *Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. *Official Journal of the European Union*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554 [Accessed 29 April 2025]

European Commission (2024) *Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 … simplified ICT risk management framework*, Official Journal of the European Union, OJL 123/45. Available at: eur-lex.europa.eu (Accessed: 29 April 2025)

European Banking Authority (EBA), 2024. ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification. *Press release*, 17 January. Available at: https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party (Accessed: 29 April 2025)

Buttigieg, C.P. and Zimmermann, B.B., 2024. 'The Digital Operational Resilience Act: Challenges and some reflections on the adequacy of Europe's architecture for financial supervision', *ERA Forum*, 25, pp. 11–28. Available at: https://doi.org/10.1007/s12027-024-00793-w (Accessed: 26 February 2025)

Central Bank of Ireland, 2019. *TIBER-IE Framework: Threat Intelligence-Based Ethical Red-Teaming – Ireland National Guide*. Dublin: Central Bank of Ireland. Available at: https://www.centralbank.ie/docs/default-source/financial-system/tiber-ie/tiber-ie-national-guide-december-2019.pdf?sfvrsn=dcb0801d_14 [Accessed 26 February 2025]

Matheson (2024) *DORA Toolkit: Harmonizing ICT Risk Management for Financial Entities Across the EU*.

Ennis, B., 2024. 'Preparing for DORA: A guide for intermediaries', *Irish Broker: The Official Journal of Brokers Ireland*, vol. 41, no. 12, pp. 35

Saveleva Dovgal, L., Su, F. & Saalman, L., 2024. *Enhancing Cyber Risk Reduction and the Role of the European Union*. *SIPRI Research Policy Paper* (online). Available at: https://www.jstor.org/stable/resrep65348 [Accessed 2 May 2025]

Miller, K., 2025. *Managing IT: Metrics and Measurements*. Pluralsight. Available at: https://app.pluralsight.com/library/courses/managing-it-metrics-measurements/table-of-contents [Accessed 13 May 2025]

Brauchle, J.-P., Göbel, M., Seiler, J. and von Busekist, C., 2020. *Cyber mapping the financial system*. Washington, DC: Carnegie Endowment for International Peace. Available at: https://www.jstor.org/stable/resrep24291.1 [Accessed 28 May 2025]

Rees, C., 2025. *Information security management: compliance audits* [online video course]. Pluralsight. Available at: https://app.pluralsight.com/ilx/video-courses/clips/59e82621-d749-40a3-84c8-0d1ac5492f24 [Accessed 28 May 2025]

Woolard, M., 2024. *Security framework: NIST CSF* [online video course]. Pluralsight. Available at: https://app.pluralsight.com/ilx/video-courses/clips/f538d841-64e9-4da8-8e1a-629ce2ff5384 [Accessed 29 May 2025]

Mineraud, J., Mazhelis, O., Su, X. and Tarkoma, S., 2016. *A gap analysis of Internet-of-Things platforms*. Computer Communications, 89–90, pp.5–16. Available at: https://doi.org/10.1016/j.comcom.2016.03.006 [Accessed 4 Jun. 2025].

National Institute of Standards and Technology (NIST), 2004. *Card technology developments and gap analysis: Interagency report 7056*. Gaithersburg, MD: NIST. Available at: https://csrc.nist.gov/publications/nistir/nistir-7056.pdf [Accessed 4 June 2025]

Cavoukian, A., Fritsch, L. and Pulls, T., 2018. *Guidance and gaps analysis for European standardization: Privacy standards in the information security context*. Tilburg University. Available at: https://repository.tilburguniversity.edu/server/api/core/bitstreams/86fc532e-6e2e-4750-a5c1-bdecf99a6906/content (Accessed: 9 June 2025)

Shetty, A.D., 2023. *Enhancing information security management system using ISO controls-based framework*. MSc Industry Internship Report, MSc in Cyber Security, School of Computing, National College of Ireland. Available at: https://norma.ncirl.ie/7300/1/abhishekdineshshetty.pdf (Accessed: 9 June 2025)

Einstein, B., 2024. *How gap analysis can drive strategic change in your organization*. 10 December. Available at: https://online.hbs.edu/blog/post/gap-analysis (Accessed: 9 June 2025)

Sachdeva, R., 2023. *Developing a Pre-Readiness Compliance Assessment Framework for Financial Institutions under the EU's Digital Operational Resilience Act (DORA)*. Unpublished Master's project, National College of Ireland. Available at: https://norma.ncirl.ie/7299/1/rishabhsachdeva.pdf (Accessed: 10 June 2025)

Phadnis, N., 2021. *An evidence gathering framework for auditing policy compliance*. Master's thesis, National College of Ireland. Available at: https://norma.ncirl.ie/6040/1/nachiketphadnis.pdf [Accessed 8 Aug. 2025]

Yaxiaer, M. (2024) *The challenge of balancing data-driven security with small and medium-sized enterprise (SME) commerce in China's ecommerce sector*. Master's thesis, National College of Ireland. Available at: https://norma.ncirl.ie/7807/1/muhetaeryaxiaer.pdf (Accessed: 9 August 2025).

Google (n.d.) *NotebookLM* [AI note-taking tool]. Available at: https://notebooklm.google/ (Accessed: 9 August 2025).

Reeves, G. (2020) *A study to identify if there is a clear understanding and awareness of required records management policies and procedures in Irish Organisations, specifically, in relation to compliance with the General Data Protection Regulations (GDPR) which came into force on 28th May 2018*. Master's thesis, Dublin, National College of Ireland. Available at: https://norma.ncirl.ie/4682/1/garyreeves.pdf (Accessed: 9 August 2025).

Starbuck, C. (2023) *The fundamentals of people analytics with applications in R*. Cham: Springer

Chartered Institute of Internal Auditors (2015) *Governance of risk: three lines of defence* [online]. Available at: https://governance.ie/uploads/files/Internal%20Control/Governance%20of%20risk-%20Three%20lines%20of%20defence.pdf (Accessed: 17 June 2025)

Stanik, J. (2025) 'Application of DORA standards in operational risk management in GIS systems', *GIS Odyssey Journal*, 5(1), pp. 203–211. doi:10.57599/gisoj.2025.5.1.203

Karakasilioti, G.M.P. (2024) *Supporting the digital operational resilience of the financial sector: the EU's DORA Digital Operational Resilience Act*. MSc dissertation, University of Piraeus, Department of Digital Systems. Available at: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/16273/DORA%20-%20MTE2109%20Karakasilioti.pdf?sequence=1 (Accessed: 23 July 2025)

Bonifazi, F. (2025) *Project management for the compliance with DORA regulation*. Master's thesis, Politecnico di Torino. Available at: https://webthesis.biblio.polito.it/35655/ (Accessed: 24 July 2025)

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*. Master's thesis, Delft University of Technology. Available at: https://repository.tudelft.nl/file/File_92da7a01-9c45-4f49-917d-642ae45bea93?preview=1 (Accessed: 24 July 2025)

Boddy, S. (2024) *Case study: the decision-support framework and NIS2, CER, and DORA incident reporting obligations*. Jyväskylä University, Faculty of Information Technology. Available at: https://jyx.jyu.fi/jyx/Record/jyx_123456789_95795 (Accessed: 9 August 2025).

Riaz, B. and Younas, Z. (2024) *Investigating the impact of DORA regulations on third party risk management in the Swedish financial sector*. Stockholm University. Available at: https://www.diva-portal.org/smash/get/diva2:1955684/FULLTEXT01.pdf (Accessed: 24 July 2025)

Tošić, I. (2025) 'Insurance companies business in a digital environment – what does DORA bring?' *Tokovi osiguranja* [online]. Available at: https://tokoviosiguranja.edu.rs/wp-content/uploads/2025/03/poslovanja-u-digitalnom-svetu-en.pdf (Accessed: 24 July 2025)

A&L Goodbody LLP (2014) *DORA: key observations regarding the designation of international ICT third-party service providers as critical*. Dublin: A&L Goodbody LLP

Šípková, E. (2021) 'Ireland's Health Service Executive ransomware attack', *International Cyber Law: Interactive Toolkit*, CCDCOE. Available at: https://cyberlaw.ccdcoe.org/wiki/Ireland%E2%80%99s_Health_Service_Executive_ransomware_attack_%282021%29 (Accessed: 31 July 2025)

European Banking Authority (EBA) (2019) *EBA revised guidelines on outsourcing arrangements* [pdf]. Available at: https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf (Accessed: 31 July 2025)

European Insurance and Occupational Pensions Authority (EIOPA) (2025) *Digital Operational Resilience Act (DORA)*. Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en (Accessed: 8 August 2025)

Leuprecht, C. (2019) 'Mitigating cyber risk across the financial sector'. In: Centre for International Governance Innovation, *Governing cyberspace during a crisis in trust: An essay series on the economic potential — and vulnerability — of transformative technologies and cyber security*. Waterloo, ON: Centre for International Governance Innovation. Available at: https://www.jstor.org/stable/resrep26129.15 (Accessed: 8 August 2025).

9 Appendix 1: Supporting Documentation

DORA RTS Legislation Interpretation Document - https://docs.google.com/document/d/1QjlJqFtTjnwUf5W7V_DxYuPG0VBlF6W0/edit?usp=drive_link&ouid=108680219455689495636&rtpof=true&sd=true

Gap Analysis Document - https://docs.google.com/spreadsheets/d/1woX7OznDDFKCQ3FocPH3DMae7FS9UfGt/edit?usp=drive_link&ouid=108680219455689495636&rtpof=true&sd=true

Compliance Checklist - https://docs.google.com/spreadsheets/d/10Hl5pTI1No8xDghgD9k35GPKnT7Laaw1/edit?usp=drive_link&ouid=108680219455689495636&rtpof=true&sd=true

Compliance Dashboard application GitHub repository can be found here - https://github.com/rutaram604/ComplianceDashboard