LAPIN AMK
Lapland University of Applied Sciences

DEVELOPMENT OF A COMPLIANCE GAP ANALYSIS METHOD FOR THE DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

Pavel Gusiv

Master's thesis

Knowledge Management Expertise
Master of Business Administration

2023

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tiedolla johtamisen asiantuntija
Tradenomi YAMK

Tekijä	Pavel Gusiv	**Vuosi**	2023
Ohjaaja	Milla Immonen		
Toimeksiantaja	Deloitte Oy		
Työn nimi	Digital Operational Resilience Act (DORA) -säädöksen noudattamista koskevan gap-analyysimenetelmän kehittäminen		
Sivumäärä	60		

Opinnäytetyön aiheena on Digital Operational Resilience Act (DORA) -säädöstä koskevan gap-analyysimenetelmän kehittäminen. Tutkimuksen päätavoitteena oli kehittää systemaattinen ja tehokas menetelmä, jonka avulla säädöksen piiriin kuuluvat organisaatiot pystyisivät tunnistamaan ja käsittelemään DORA:n asettamien vaatimusten noudattamisen puutteita.

Tutkimuksessa hyödynnettiin kirjallisuuskatsauksen ja sääntelyanalyysin yhdistelmää. Näiden menetelmien avulla pyrittiin löytämään syvällinen ymmärrys DORA-säädöksestä ja sen vaatimuksista. Lisäksi tarkasteltiin DORA-säädökseen liittyviä käsitteitä, kuten vaatimustenmukaisuusanalyysiä ja digitaalisen toiminnan kestävyyttä. Säädösten noudattamista yleisesti myös käsiteltiin osana tutkimusta. Tutkimuksen validointivaiheeseen on sisällytetty palaute asiantuntijoilta, joilla on vuosien kokemus finanssialalta, sisäisistä tarkastuksista ja vaatimustenmukaisuustarkastuksista.

Gap-analyysimenetelmä kehitettiin ensisijaisesti toimeksiantajan tarpeisiin. Menetelmä mahdollistaa asiakasorganisaatioiden DORA-säädösten noudattamisen arvioinnin sekä mahdollisten puutteiden tunnistamisen ja kehittämismahdollisuuksien esiin nostamisen. Menetelmä on suunniteltu hyödynnettäväksi asiakasorganisaatioissa ennen kuin heidän on osoitettava säädöksen noudattaminen viranomaisille.

Opinnäytetyön lopputuloksena kehitettiin uudenlainen DORA-määräysten mukainen gap-analyysimenetelmä. Menetelmän pätevyys ja luotettavuus on osoitettu alan asiantuntijoiden palautteeseen pohjautuen. Tutkimuksen loppuun on koottu jatkokehittämismahdollisuuksia, joissa on otettu huomioon menetelmän peruskäsitteet ja vaatimukset. Kehitetty menetelmä tarjoaa merkittävää käytännön arvoa organisaatioille, joilla on pyrkimyksenä saavuttaa DORA-vaatimustenmukaisuus, ja näin se myös parantaa rahoitusalan digitaalisen toiminnan häiriönsietokykyä kokonaisuudessaan.

Avainsanat DORA, Digital Operational Resilience Act, vaatimustenmukaisuus, regulaatio, rahoitusala, kyberturvallisuus, riskienhallinta, tiedolla johtaminen

LAPIN AMK
Lapland University of Applied Sciences

Abstract of thesis

Knowledge Management Expertise
Master of Business Administration

Author	Pavel Gusiv	**Year**	2023
Supervisor	Milla Immonen		
Commissioned by	Deloitte Oy		
Title	Development of a compliance gap analysis method for the Digital Operational Resilience Act (DORA)		
Number of pages	60		

This thesis focuses on the development of a compliance gap analysis method for the Digital Operational Resilience Act (DORA) regulation. The primary objective of the research was to develop a systematic and efficient method, which would enable organizations within the scope of the act to identify and address compliance gaps in adherence to the requirements set by DORA.

The study employs a combination of a literature review and regulatory analysis to develop an in-depth understanding of the DORA regulation and its requirements, as well as related concepts such as compliance gap analysis, digital operational resilience, and regulatory compliance. The validation phase of the study integrates feedback from professionals with expertise in the financial sector, internal audits, and compliance audits.

The gap analysis method was primarily developed to help the thesis commissioner to evaluate client organizations' adherence to DORA regulations, identify potential gaps, and uncover improvement opportunities before the commissioners' clients are required to demonstrate regulatory compliance to the authorities.

The final result of this thesis was the creation of a novel compliance gap analysis method tailored to DORA regulations. The method's validity and reliability have been demonstrated through feedback from expert professionals. The research concludes with suggestions for additional development opportunities while preserving the method's fundamental concepts and requirements. The developed method has the potential to provide significant practical value to organisations pursuing DORA compliance and therefore contributes to the improved digital operational resilience in the financial industry.

Keywords: DORA, Digital Operational Resilience Act, compliance gap analysis, regulatory compliance, financial sector, cybersecurity, risk management, knowledge management

TABLE OF CONTENTS

1 INTRODUCTION

This thesis' introduction chapter begins with an overview of the study's background information and objectives. Afterwards, the thesis's commissioner is introduced. The selected research methodology is subsequently explored, accompanied by an analysis of the development process for the method to be developed. The chapter concludes by discussing the process of validating the thesis and analysing the ethical implications of the research.

1.1 Thesis background

In September 2020, the European Parliament proposed a new regulatory framework for digital risk management in response to the growing risk of cyberthreats and the need to secure the business continuity of key infrastructure. The proposed regulation would apply to EU-based financial institutions and a selected group of their ICT service providers, to standardize provisions regarding digital operational resilience across the EU financial sector.

The Digital Operational Resilience Act, also known as DORA regulation, intends to improve general information technology risk management and the financial industry's digital operational resilience through unified regulation. The majority of organizations functioning in the financial sector will be subject to the new regulation, yet the most significant for Finland are financial institutions such as banks, insurance companies, and pension institutions. (The Digital Operational Resilience Act 2022/2554)

To ensure the continuity of digital activities, the regulatory framework will require that all organisations within its scope demonstrate their ability to endure, manage, and recover from various forms of interruptions and risks connected to information technology. Compliance with the regulations relating to entities in the financial sector and their ICT-service providers will be supervised by the relevant European Supervisory Authorities (ESA), such as the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA). (The Digital Operational Resilience Act 2022/2554)

The Digital Operational Resilience Act is set to go into force on January 16, 2025, (EIOPA), meaning that as of that date, organisations subject to DORA must fully comply with it. Thereby, these organisations will most likely require services such as compliance analyses and gap assessments to identify potential compliance gaps, as well as possibly further advisory services to address them.

The research topic is relevant to risk management in the financial industry as the regulation will apply to nearly all EU-based entities that provide financial services. The largest organisations operating in the field of risk management have already identified the economic potential given by the regulation and are anticipated to provide comparable gap analysis services, which this study's method is meant to address. Subsequently, it is reasonable to assume that the established method could assist the thesis commissioner to achieve a financial benefit by allowing them to offer DORA gap analysis services to clients.

1.2 Objective of the thesis

The objective of this thesis is to develop a gap analysis method that will enable the thesis commissioner to conduct DORA gap analysis projects, which will evaluate a client organization's compliance with DORA and identify any detected gaps. With this information, client organisations will be able to discover potential improvement areas before being audited by authorities for compliance. The method for gap analysis will include three documents: gap analysis methodology, gap analysis template, and reporting template.

To achieve this objective, a thorough examination of the theoretical foundations in various relevant fields are conducted, synthesizing the knowledge gained from these areas to develop a comprehensive understanding of regulations, compliance, risk management, and cybersecurity. Building on this comprehensive understanding, as well as the author's professional experience and the thesis commissioner's internal methodologies, a gap analysis method specifically designed to meet the requirements of the DORA regulation is created. The process is expected to result in the creation of three documents that serve as the foundation for the gap analysis method: the gap analysis methodology, the gap analysis template, and the reporting template. These documents are designed to provide

an effective framework for organizations aiming to assess their compliance with DORA regulations.

The gap analysis methodology document would act as a manual for the project team and provide an overview of the project's objectives, key activities, and required resources at each phase. It defines the steps and objectives of the compliance gap analysis project over three phases. These phases focus on gaining an understanding of the target organization's existing state, evaluating compliance against DORA requirements, identifying and documenting compliance gaps, and delivering a final report.

The gap analysis template is a checklist-formatted Excel file used to hold all the information gathered during the DORA gap analysis project. There are three types of Excel sheets in the template: a general sheet, a definitions sheet, and several requirement sheets. This document is meant to aid the project team in assessing regulatory compliance by listing all relevant requirements, definitions, and supporting documents.

The reporting template utilizes Power BI software to visually present relevant project key points and provide a full overview of the current status of the gap analysis project. Its objective is to assist the project team in identifying the project's overall status, missing material, and significant gaps, and to simplify reporting to the client. The reporting template utilizes information from the gap analysis template, allowing the project status to be examined in real-time.

1.3 Thesis commissioner

This thesis is commissioned by the Risk Advisory unit of Deloitte Oy, the Finnish member of the "Deloitte" brand. Deloitte is one of the major professional services businesses in the world, providing audit, consultancy, financial advising, risk advisory, tax, and legal services, among others. Member firms of Deloitte, which was founded in 1845, operate in more than 150 countries. The organisation has a reputation for supplying its clients with high-quality services, and its competence in the financial and business sectors is well acknowledged. (Deloitte 2022a)

Deloitte's diverse client base includes Fortune 500 companies, government agencies, and non-profit organisations. The company is dedicated to ethical and responsible business practices and strongly focuses on diversity, equity, and inclusion. Deloitte has a long history of corporate social responsibility and is dedicated to positively affecting the communities in which it operates. (Deloitte 2022b)

Risk Advisory is a business unit of Deloitte whose purpose is to assist client organisations in identifying, assessing, and managing risks that may have an impact on their business. The business unit offers a variety of risk management services, including risk assessment, governance, risk strategy, analytics, and implementation. The team of professionals at Deloitte Risk Advisory are skilled in identifying and assessing diverse risks, including financial, operational, strategic, and regulatory risks. The team interacts with clients to design risk management solutions that are specifically tailored to their needs. (Deloitte 2022c)

1.4 Research method

This thesis utilizes constructive research as its research methodology. During the research planning phase, a comprehensive examination of appropriate research methods was undertaken in a separate research preparation document. The constructive research approach was chosen mainly due to its focus on developing and establishing new constructions rather than researching, documenting, or explaining existing conditions or phenomena.

The objective of this thesis was to develop a comprehensive work method that can be applied in DORA gap analysis projects, which aligns with the objectives of constructive research methodology. This innovative construction provides real-world value and could be applied in the future client projects of the thesis commissioner.

Typically, the constructive research methodology combines theoretical and practical work and often includes prototyping, testing, and refining ideas or concepts. It is defined as an iterative process in which researchers construct and test prototypes, collect input, and then use that feedback to refine and improve their concepts. (Virtanen 2006, 46)

According to Kari Luukka's (Luukka 2014) article "Konstruktiivinen tutkimusote," the process of constructive research may be broken down into six consecutive stages:

(i) Identifying a practically important issue with the ability to make a theoretical contribution.

(ii) Establishing a research partnership with the organization of interest.

(iii) Practically and conceptually gaining an in-depth understanding of the research issue.

(iv) Innovating the solution model and creating a construction that answers the issue and makes a contribution to theory.

(v) Developing and testing the solution's functionality.

(vi) Considering the scope and applicability of the solution.

These phases serve as the basis for the research and innovation activities outlined in the next chapters.

Additionally, it has been observed that constructive research has been utilized in similar research studies, such as in Tuisku Sarrala's "Uncovering Privacy Threats with Soft Systems Methodology" (Sarrala 2021, 8-11) and Krista Kustula's "Sisäisen valvonan ja riskienhallinnan kehittäminen Siikajoen kunnassa," (Kustula 2013, 7-9). Both studies demonstrate the effectiveness and relevance of constructive research methodology in the development of reporting guidelines and models for risk management. These examples support the use of constructive research methodology in the current research project.

1.5 Development process

The process began with a comprehensive review of the Digital Operational Resilience Act's legal document. The requirements of the regulation were identified and documented in an Excel document formatted as a checklist. The requirements were documented in their original order, according to the numbering of individual topics and articles used as an index number for each requirement listed

in the document. This was intended to simplify referencing to specific requirements in the future. The same Excel document would also be used as an analysis template to track compliance to each requirement during the gap analysis process; therefore, fulfilment indicators were added next to each requirement in order for the analysis progress to be conveniently monitored during the project.

Research on comparable work methods was also conducted. Given the likelihood that Deloitte would be the main user of this work method, the primary source of methodology references was the firm's technical library and already-developed methods of a similar sort. In addition, previous research studies that have addressed related topics, such as GDPR compliance, were studied. Based on these materials, a framework for the DORA gap analysis method was constructed.

Only those requirements that support the method's objectives, i.e., those that focus on financial sector entities, were incorporated into the method's body. For instance, criteria aimed towards European Authorities were excluded. The objective was to create a straightforward method that could be employed to assess a commissioner's client's current state in a reasonable timeframe.

The final products of the thesis were validated by a selected group of Deloitte's senior risk management professionals with prior knowledge in the regulation and gap analysis fields. In addition to the author, these professionals would likely be the primary users of the gap analysis method. The purpose of the validations was to verify both the method's validity and reliability.

The proposed improvements and adjustments were thoroughly reviewed, and most of them were implemented after assessing the validation feedback and suggestions based on relevance, consistency, and feasibility. The final thesis results, following the validation procedures, were presented to the thesis commissioner.

1.6 Validation of the results and ethical concerns

The gap assessment method could not be evaluated on a real client project due to the time-consuming nature of obtaining approval from multiple leadership team members and the requirement to make modifications to client contracts. Furthermore, identified findings would be considered sensitive data and could not be

disclosed to the public, making the validation phase of this study confidential and therefore not contributing to the progression of the thesis.

Evaluating the applicability of the method does not necessarily require analysing it using client data. Instead, it was decided to evaluate the effectiveness of the approach by conducting validation and feedback procedures with the assistance of a group of senior specialists from Deloitte Risk Advisory who have experience with similar topics. These individuals possess years of expertise in comparable projects and have utilized similar approaches throughout their careers, making their conclusions reliable enough to infer the overall functionality and effectiveness of the method.

The primary ethical concern of this thesis was the preservation of the anonymity of the validation process participants. In accordance with the article, Research ethical guidelines and anonymity (Walford 2005, 83-93), the anonymity of the individual must not be disclosed in the final report or any possible direct quotes. This is due to the ethical practices designed to preserve the privacy of human subjects throughout data collection, processing, and reporting. Before beginning the validation process, the specialists were informed of its objective and how their replies will be handled. Each respondent was informed in writing how the information gathered during the validation would be processed, where it would be stored and that it would be used only for the purpose of this thesis. Upon the completion of the thesis, the original validation data will be discarded. Participation in the validation process was entirely voluntary.

In order to protect the privacy of validators, this thesis does not reveal any identifying information about the validators, such as their names, genders, ages, and job titles. The work experience of the validators is referenced in a manner that cannot be tied to an individual. This improves the reliability and integrity of the validations, also allowing for less restricted feedback.

The utilization of Deloitte's internal methodology materials was the secondary ethical concern of the thesis. Because the documents include highly confidential business information, they are solely meant for internal use by Deloitte's specialists. The content of the documents cannot be discussed in this thesis, and refer-

ences to techniques should not reveal any information contained in the documents. Thus, methodologies will be examined and studied without any of these details being documented in this thesis. Only information that is not classified in nature, such as document names and high-level purposes, will be disclosed. In addition, documents considering Deloitte’s internal methodology will be stored and inspected exclusively on Deloitte's device and will not be exported from it.

This thesis adheres to the Research Ethics Advisory Board of Finland's ethical guidelines (Tutkimuseettinen neuvottelukunta 2023). Only methods of data acquisition, research, and evaluation that adhere to the standards of scientific research have been employed. References to the publication have been appropriately cited, thereby giving the accomplishments of other researchers their due value and significance.

2 THEORETICAL BACKGROUND

The theoretical background chapter of this thesis discusses a variety of directly relevant subjects. To establish the context, the DORA regulation and regulations at the general level are discussed first. Next, fundamental principles like compliance, cybersecurity, risk management, and internal audit are introduced. To comprehend the objective and contents of this thesis, the reader must have at least a basic understanding of the topics described in the subsequent chapters, as they are directly connected to the gap analysis and DORA regulation.

2.1 Regulations and compliance

For the purpose of ensuring that businesses conduct their operations in a fair and ethical manner, governments and other regulatory organizations create rules and guidelines that are referred to as regulations. The purpose of these regulations is to safeguard the interests of customers, employees, and the environment, as well as to ensure that commercial enterprises behave ethically and do not engage in activities that are fraudulent or harmful. (Shleifer 2005, 439-449)

Compliance is the process of adhering to these regulations and making sure that businesses are following the rules and principles that have been established. In other words, companies that are following these rules and principles can be described as compliant. This also involves the implementation of policies, procedures, and practices that assist businesses in identifying and managing risks, as well as ensuring that they are functioning in accordance with the regulations that are applicable to their sector of the economy. (Shleifer 2005, 439-449)

In the current highly globalized business environment, compliance with a complicated web of laws and regulations has evolved into an important component of the day-to-day operations of any organization. Compliance with the set regulations is necessary for companies, as failure to do so poses significant dangers to both their legal standing and their reputation, both of which have the potential to be expensive and damaging to the organization. As a result of the growth of high-profile cases of corporate misconduct over the past few years, such as Enron and Lehman Brothers, there has been an increasing emphasis placed on ensuring

that businesses are in compliance with applicable regulations. (Yale University 2019)

There are many kinds of compliance risks that confront businesses currently, such as those related to legal and regulatory compliance, financial compliance, data privacy, and cybersecurity compliance. Non-compliance with the laws and regulations that regulate business practices creates risks associated with failing to comply with legal and regulatory requirements. Failure to comply with financial regulations, such as those relating to anti-money laundering (AML) and know-your-customer (KYC), creates the potential for financial compliance threats to occur. On other hand, failure to comply with the laws and regulations that control the protection of personal data and cybersecurity can expose an organization to risks regarding data privacy and compliance with cybersecurity standards (Skibicka 2021)

The most recent changes in legislation and regulations have had a substantial effect on the daily operations of businesses. For instance, in 2018, the European Union passed new legislation known as the General Data Protection Regulation (GDPR), which was designed to strengthen existing data protection laws. The General Data Protection Regulation (GDPR) has established a new standard for data privacy regulations around the world, and in order for businesses to avoid being fined, they must adhere to its requirements. (GDPR.eu 2022)

The administration of complex compliance issues may make it difficult to recognize and manage risks related to compliance. Effective compliance management requires a proactive and risk-based approach. Compliance specialists are often tasked with detecting compliance issues and assessing their potential impact on the organisation. In addition, they are accountable for the design and implementation of compliance programs that are tailored to the organization's particular requirements. (Red Hat 2023)

In conclusion, it cannot be overstated how important it is to comply with all applicable rules and regulations in the modern, globalized corporate world. Organizations are liable for gaining an understanding of the many types of compliance risks they face and being informed of the most recent modifications to laws and

regulations. A proactive and risk-based strategy is required for successful compliance management, which in order is required to guarantee effective identification and management of compliance risks. Ultimately, organisations must have a thorough compliance program in order to conduct their activities responsibly and ethically, protect the interests of stakeholders, and avoid costly legal and reputational risks.

2.2 Digital Operational Resilience Act

The European Union (EU) are enhancing the information technology security of financial enterprises such as banks, insurance companies, and investment businesses in response to the ever-increasing risks posed by cyber-attacks. The Digital Operational Resilience Act (DORA) was pre-approved by the European Parliament on the 10th of November 2022 and final adoption was achieved on the 28th day of the same month. DORA would ensure that the financial sector in Europe can remain robust in the face of a significant operational interruption. Companies and organisations that operate in the financial sector, as well as critical third parties that provide ICT-related services to them, such as cloud platforms or data analytics services, are required to comply with DORA's standardized security requirements for their networks and information systems, which are designed to protect against cyberattacks. DORA establishes a legal framework on digital operational resilience under which all companies in scope are required to ensure that they can withstand, respond to, and recover from all sorts of interruptions and threats connected to ICT. All member states of the EU have the same set of regulations to follow. The core aim is to prevent and mitigate cyber threats. (Council of the EU 2022)

In the year 2020 European commission presented the DORA plan to the public. It was a component of a more comprehensive digital finance package, the purpose of which was to devise a strategy that encourages the advancement of technology while also ensuring the stability of the financial industry and consumers' safety. At the same time, the package assures that new technology and products are subject to financial regulation and operational risk management arrangements for enterprises operating in the EU. Furthermore, by guaranteeing that the

present legal framework is accessible for the use of new digital financial instruments, this package fills a gap in existing EU legislation. As a result, the package's ultimate purpose is to encourage innovation and the adoption of new financial technologies while still ensuring a sufficient degree of safety for consumers and investors. (Council of the EU 2022)

The development of ICT technologies opens up doors of opportunities but also ushers in new dangers. During times of increased pressure, it is necessary to take certain risks, but these must be managed carefully. Because of this, decision-makers and supervisors have emphasized the threats posed by ICT operations. Risks posed by these technologies have been cited as a threat to the resiliency, operation, and stability of the EU's financial system. ICT risks were only dealt with indirectly as part of a specific sub-area that included activities aimed at addressing operational risks and critical ICT deviations in general. (European Commission 2020)

As a result, it was critical to develop a comprehensive framework for the digital resilience of the EU's financial institutions. The addition of this framework increases the common rule book's digital risk management component. It can be used to strengthen and improve financial institutions' implementation of ICT risk management, introduce thorough testing of ICT systems, increase supervisors' knowledge of cyber risks and ICT deviations faced by financial institutions, and grant financial supervisors the authority to monitor third-party risks. Additional possible applications include: The plan sets a standard reporting procedure for deviations, which helps to decrease the administrative cost put on financial institutions and promotes the efficiency with which monitoring is carried out. (European Commission 2020)

Late in 2022, European Union negotiators approved the final Digital Operational Resilience Act (DORA) package, mandating that European Supervisory Authorities (ESAs) refine the definitions of required Regulatory Technological Standards (RTSs) and requirements by early 2025. During this transition period, organizations must align their governance and practices with DORA's resilience pillars and develop a road map for their digital resilience plan, including key deliverables. One way to accomplish this is by conducting an initial gap assessment, which

begins with a profile analysis of the organization, helping to establish the current level of maturity with existing rules and standards. (Goethals & Bosch 2022)

Once the DORA is in the effect, ESAs would require organisations to provide the essential reports designated by DORA upon request, which they will use to analyse for any gaps. Organizations should focus on improving their digital resilience strategy and preparing for yearly assessments, testing, and reporting. Furthermore, obligatory penetration testing will be mandated by the end of 2025, as illustrated in Figure 1. (Goethals & Bosch 2022)

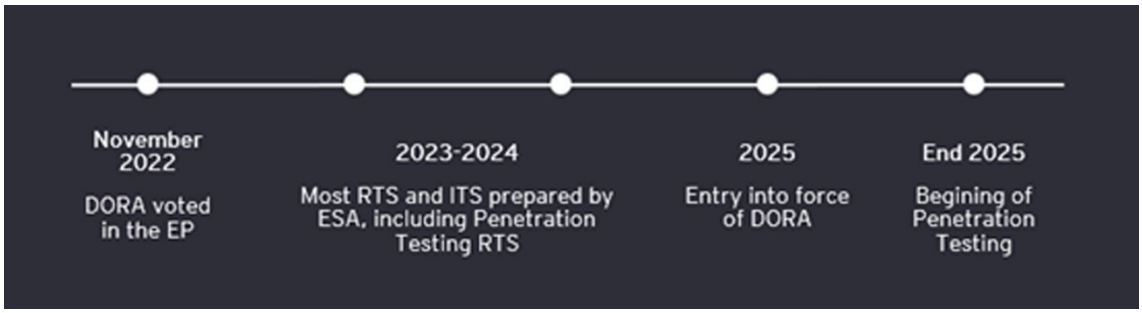

Figure 1. The DORA implementation timeline (Goethals & Bosch 2022)

2.3 Compliance gap analysis & auditing

The compliance function is the system or process designed to reasonably ensure that an organisation complies with all applicable laws, regulations, and rules of behaviour. The compliance function often entails identifying compliance responsibilities, risk assessment, guidance, monitoring, and reporting on the firm's compliance with securities laws and codes of conduct, as well as aiding in avoiding violations within the firm. (Gadziala 2005)

Gap analyses are a process used by organisations to discover the gaps between their present state and their desired future state, as well as the activities required to bridge this gap. Compliance gap analysis is a subcategory of gap analysis that evaluates the difference between an organization's present practices and regulatory or industry requirements. Compliance is the conformance of an organization's systems and procedures to relevant laws, rules, and standards. Noncompliance with these standards can result in legal and financial penalties, reputational harm, and data breaches. The compliance gap analysis tries to identify non-compliant areas that need to be addressed, as well as best practices and

opportunities for improvement in the organization's systems and processes. (Keen 2021)

The process of compliance gap analysis typically involves reviewing the organisations' current systems, processes, and policies and comparing them to relevant regulatory or industry standards. This review may include assessments of the organisations' ICT infrastructure, security measures, data management practices, and compliance with laws and regulations such as the GDPR and HIPAA. Data collection methods for compliance gap analysis may include interviews with key stakeholders, a review of documentation, and on-site observations. It is important to use various data sources to ensure a comprehensive understanding of the organisations' practices. Gap analyses are a way for companies to ensure that they satisfy the legal and regulatory requirements placed on them, as well as to identify areas in which their compliance programs may use some improvement. However, these procedures may also be resource-intensive and time-consuming. (Asaitec 2016)

The findings of a compliance gap analysis may be utilized to develop a strategy for addressing any identified non-compliant areas and achieving compliance. This strategy should contain precise activities, timeframes, and resources required to maintain compliance. To perform a successful gap analysis, clear and quantifiable goals and objectives must be established, stakeholders must be included, and quantitative and qualitative data must be gathered and analysed. The strategy established as a consequence of the gap analysis should be evaluated and monitored on a regular basis to ensure that the organisation stays in compliance with regulatory requirements and industry standards. (Asaitec 2016)

A compliance audit, on the other hand, is an independent and objective assessment of an organization's policies, processes, and activities to determine conformity with relevant laws, regulations, and standards. It is a comprehensive and thorough review of a company's compliance program and associated procedures to identify potential breaches of compliance standards and areas for improvement. Compliance audits can be performed internally by an organization's personnel or externally by a third party such as a consulting firm or an independent auditor. Both approaches have advantages and downsides. Compliance audits

undertaken externally by employees who are not affiliated with the firm being audited and do not have financial or other stakes in the audit's conclusion are more likely to be objective than internal compliance audits. (Marker 2018)

Compliance audits determine the validity of an organization's laws, rules, standards, policies, and processes. These audits are done similarly to gap analyses, employing interviews, document reviews, process observation, and control testing. The audit findings are documented in a report that includes supporting documentation and summarizes the findings, conclusions, and recommendations for improvement. Organizations can perform compliance audits utilizing a variety of frameworks and standards, such as the COSO Internal Control-Integrated Framework and the ISO 37301:2021 standard on compliance management systems. These frameworks outline the requirements for establishing, implementing, maintaining, and improving a compliance management system as well as the concepts and suggestions for developing and accessing internal control systems. (Marker 2018)

Some organizations may choose to submit to a voluntary compliance audit to demonstrate their commitment to compliance and build stakeholder trust. In such cases, firms may choose to perform audits in accordance with a recognised standard or framework, or they may employ an independent auditor to ensure the audit's credibility and independence. Organizations in the business of providing healthcare services inside of the United States of America, for example, are subject to the US Health Insurance Portability and Liability Act's rules and regulations because they handle patients' sensitive health information. Firms that handle payment cards, on the other hand, are subject to the information security regulations and standards set by the industry in which they operate. It is the obligation of organizations to demonstrate compliance, which can be done, for example, via external audit reports and certifications. (Kelley 2018)

When it comes to performing compliance audits, organisations may face a number of challenges, including the need to access and analyse huge volumes of data, the difficulty of identifying and evaluating compliance risks, and the demand to coordinate and communicate with several stakeholders. To be successful in overcoming these difficulties, organizations may need to invest in specialized

tools and resources, as well as create strong internal systems and procedures for managing compliance. (Hatherell 2020)

2.4 Cybersecurity

Cybersecurity refers to the process of defending computer networks, systems, and devices from intrusions and other forms of digital attack. It involves implementing measures to prevent unauthorized access to sensitive data, as well as establishing policies and procedures to ensure that employees follow best practices for maintaining the security of an organisation’s systems and networks. (National Institute of Standards and Technology 2014)

In modern days, cybersecurity measures are counted as standard operating procedures. We are all affected as customers, business owners, and employees. Virtually every business and individual use digital products and services daily. Cyber security is managed by identifying threats, comprehending their impact on one's operations, appropriately preparing for threats, and planning and rehearsing actions in case one of the threats materializes. (Salomaa 2023)

The nature of cyber threats is that they are always changing, which is one of the most significant problems for cybersecurity. Hackers and other malicious actors continuously develop new methods and tactics to exploit computer systems and network infrastructure vulnerabilities. Consequently, organisations and individuals need to take measures to protect themselves from cyber threats in an alert and proactive manner. Malware, ransomware, phishing, and denial of service attacks are just a few of the various types of cyber-attacks that can take place. These attacks could be carried out for various reasons, including the pursuit of personal vengeance, political or ideological objectives, or financial gain. (ENISA 2022)

Cyberattacks can have major repercussions, including financial losses, damage to reputation, and the loss of sensitive or confidential information. This highlights the importance of practising good cybersecurity practices. To effectively manage the risks associated with cybersecurity, enterprises need to adopt a comprehensive and integrated approach. This approach should incorporate technical safeguards, secure management practices, and a culture of security. (NIST 2014)

Effective cybersecurity is dependent on a number of critical criteria, including the following (ENISA 2022):

- Network security is the protection of the integrity and confidentiality of data exchanged through a network. This can be achieved in a variety of methods, including the use of intrusion detection systems.

- Endpoint security involves the safeguarding of endpoint devices, such as computers, laptops, and mobile phones, against cyberattacks using security methods such as antivirus software, firewalls, and other protections.

- Application security is the process of ensuring that software applications are secure and free of weaknesses that might be exploited by cybercriminals.

- A key aspect of identity and access management is controlling who has access to sensitive information and systems and ensuring that only authorized users may access these resources.

- Disaster recovery and business continuity relate to having a strategy to recover from a cyberattack or other disaster and ensuring that the organisation can continue to function properly in the case of an occurrence.

Implementing a combination of technical safeguards and strong management practices is an effective strategy for mitigating the risks that are associated with cybersecurity. Encryption, firewalls, and intrusion detection systems are all technical safeguards that should be established to protect against the threat of cyberattacks. The production of secure passwords, the utilization of two-factor authentication, and the establishment of rules and procedures are some of the management strategies that may be utilized to ensure that employees adhere to the most effective procedures for cybersecurity. (National Institute of Standards and Technology 2014)

Cyber threats must be integrated into the organisations’ daily risk management. Dealing with them separately or merely labelling them as 'IT risks' makes identifying their effects harder. Cybersecurity measures have to support and empower businesses by addressing the risks associated with digital technology. They

must, however, neither obstruct nor slow down important business-promoting actions nor should they incur unreasonable costs. (Traficom 2020)

In addition, organisations may choose to adopt industry standards and frameworks as a way to direct their activities towards cybersecurity. The ISO 27001:2022 standard on information security management is a well-known example of a standard for information security management. This standard outlines the requirements for establishing, implementing, maintaining, and continually improving an information security management system (StandardFusion 2022). The National Institute of Standards and Technology Cybersecurity Framework is another extensively utilized framework. It offers a collection of rules and best practices for managing and securing critical infrastructure. (NIST 2023)

Individual actions and behaviours, in addition to technical safeguards and administrative best practices, are vital to the effectiveness of cybersecurity operations. Employees of an organisation, as well as any other persons who utilize the business's systems and networks, play an important part in the process of maintaining the safety of these resources. Companies must establish a cybersecurity culture inside their organisations, as well as educate and train their workers on the most efficient ways of data protection and cybersecurity. Companies must also invest in the appropriate technology and infrastructure. (Choejey 2018, 61-62 & 138-141)

Because cybersecurity is an issue that is both complex and multi-faceted, a coordinated and integrated approach is essential to manage the risks that are connected with it effectively. This requires not just the installation of technological safeguards but also strong leadership, sound administration, and a culture of security consciousness permeating the business. (Choejey 2018, 158-165)

2.5 Risk Management

Risk management is a process that assists organizations in identifying, evaluating, and mitigating threats to their capital and profitability, such as financial uncertainties, legal responsibilities, strategic management failures, accidents, or natural catastrophes. This method helps organizations make strategic decisions, allocate resources, and improve operations (ISO 31000 2018).

The four-step risk management method, which comprises risk identification, risk assessment, risk control, and risk review, is a popular risk management model. Organizations identify and document the risks relevant to their operations during the risk identification phase to comprehend the full spectrum of dangers they face to focus their efforts. Organizations use risk assessment to estimate the likelihood and impact of identified risks in order to understand the potential consequences and prioritize their actions. Organizations produce and implement risk mitigation or elimination strategies for identified risks, selecting the best risk treatment methods such as avoidance, reduction, sharing, and acceptance. Lastly, during the risk review phase, organizations monitor and analyse the success of their risk management operations, recognizing any changes to the risk profile and adjusting their risk management approach appropriately. Continuous risk assessment requires the participation of all relevant stakeholders, including management, personnel, and external parties (ISO 31000 2018).

The importance of risk management grows as the requirement to establish varied security components increases. This is the outcome of the digitalization of operations, the emergence of new technology opportunities, and the rapid development of novel forms of risks and dangers. Without functional risk management, the company is unable to detect threats to its goals or important risk factors linked with daily operations and so is unable to control them. (Suomidigi 2020)

According to the International Organization for Standardization (ISO), ICT risk management entails recognizing, assessing, and prioritizing risks to ICT assets and applying controls to minimize or eliminate these risks (ISO/IEC 27001 2022).

Over the past years, many high-profile cybersecurity incidents have brought attention to the significance of ICT risk management. For instance, according to the IBM Security report released in 2022, the average cost of a data breach was calculated to be 4.35 million dollars (IBM Security 2022). And according to the research firm Cybersecurity Ventures projection, cybercrime will cost the world up to 10.5 trillion dollars annually by 2025. (Morgan 2020).

To manage ICT risk, organisations must first identify possible risks to their information and communication technology systems. This involves undertaking a risk assessment to detect risks such as hacking, malware, or natural catastrophes

that might destroy ICT assets. Once discovered, these risks must be assessed and prioritized in order to identify the best course of action. According to the NIST guide on conducting Risk Assessments, mitigating, or eliminating risks through controls such as security software or disaster recovery systems may be essential, although accepting low-risk hazards may also be an option (NIST 2012).

The CIS (Center for Internet Security) suggests implementing controls to mitigate or eliminate the risk, such as implementing firewalls or backup systems or accepting the risk if it is deemed to have a low likelihood or impact. A good ICT risk management strategy should also involve ongoing monitoring and review to guarantee that the controls are doing their job. This allows for the identification and mitigation of any new or developing risks. This may involve applying security best practices, such as frequently updating the software and conducting regular cybersecurity training for employees. (SANS 2021)

2.6 Internal audit

Internal audit function should be included in an organization's governance and risk management framework, as it provides independent assurance that the organization's operations align with its goals and objectives. As a result, internal auditing is a necessary component of such a structure. The Institute of Internal Auditors (IIA) describes an internal audit as: "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It assists an organisation in achieving its goals by applying a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance systems." (The Institute of Internal Auditors 2023a)

Internal audit is a strong support function for the board of directors and the executive leadership team. Its mission is to enhance organizational development and goal achievement through objective evaluation, verification, and consulting operations. Internal auditing focuses on the internal control of a company's operations, risk management and administration activities. Internal audit, in its most funda-

mental form, identifies risks that prevent the organisation from achieving its objectives, ensures that management is aware of these risks, and suggests ways to mitigate their consequences. (The Institute of Internal Auditors 2023b)

Internal audit has traditionally been considered as looking for prior errors and deviations that do not contribute to the future development of an organization's operations. Such limits are foreign to a modern internal audit, which focuses on predicting and proactively detecting problems. More and more businesses are considering strategies to strengthen their internal audit function in order to better meet the ever-increasing audit demands. Similarly, organisations that do not yet have active internal audit efforts express similar worries. Organizations seek solutions to allow internal audits to provide value by supporting risk-oriented business growth and performing their fundamental purpose. Technology and analytics, for example, can be employed in inspection planning. The data may be utilized to gather support for determining inspection priorities, following which the actual inspection work can be dispersed to the most appropriate locations. (Deloitte 2022d)

Internal audits may be used to examine an organization's overall compliance and security concerns, as well as to establish if the firm is adhering to its internal rules and external standards. Management teams can suggest areas for improvement based on internal audit findings. Internal auditing can also examine the company's goals in terms of return and strategic risks. (Deloitte 2022d)

One of the most important aspects of an internal audit is the creation of an audit plan, which describes the actions that will be conducted as part of the internal audit for a specific time period. The audit strategy should be based on a risk assessment of the organisation. This involves identifying and analysing the most significant risks the organisation is exposed to and determining the appropriate level of assurance required to handle those risks. Activities related to internal auditing may include but are not limited to assessing financial statements and systems of internal control; examining the efficiency and effectiveness of corporate operations; evaluating the effectiveness of risk management procedures; and so on. The internal audit may also offer advisory services to assist the company in improving its procedures and infrastructure. Internal audit's independence

and objectivity are essential to its effectiveness, and internal auditors should be free from any conflicts of interest that could impair their objectivity in any way. Instead of reporting directly to management, internal auditors should do so either to the board of directors or to a committee of the board. This will ensure the auditors' independence. (Wright 2009, 8-17 & 31-47)

3 COMPILING THE METHOD

This chapter focuses on the practical components of the research, representing the core of the study. Initially, the methodology and analysis of the DORA regulation and its requirements are undertaken. Subsequently, the compilation and development of the method's component documents are explored. The chapter concludes with a description of the validation procedures implemented for the assembled documents.

3.1 Applied methodology

The gap analysis method is based on the approach of Deloitte's other compliance-related methods. Theoretically, reviewing companies' compliance is not a difficult task, since there are only two outcomes. Despite that, it is essential that the method's core principles are similar to those of Deloitte's other existing methods. This is important because these methods have already been proven effective in earlier engagements, and Deloitte's specialists are likely to be familiar with their concepts, allowing for a swift adoption of this novel method to be developed.

Three Deloitte methodologies serve as the primary foundation for this method:

(i) Compliance Program Assessment Methodology

(ii) FSI Assessment Method Methodology

(iii) Regulation W Methodology

Because each of the referenced methods includes at least two documents, the first detailing the general approach and actions to be applied and the second being the actual working paper, it is also regarded as reasonable to include comparable documents in this method. Additionally, to assist the gap analysis process, a reporting template is designed and developed.

To make it easier for Deloitte's specialists to adapt, the methodology paper is following the same structure as the referenced methods, and an analysis template is employing a framework typical in Deloitte's IT audit engagements. The

method is divided into four phases: plan, understand, evaluate, and report, with the following key objectives in mind:

(i) Evaluating the compliance design of the entity's current state and capabilities.

(ii) Identifying gaps between the current state and the state required by DORA regulation.

(iii) Reporting the identified gaps to the entity’s stakeholders.

3.2 Analysis of the DORA regulation

DORA is a comprehensive piece of legislation aiming to secure businesses' digital operational resilience across the financial industry. According to Deloitte’s article (Deloitte 2022e), DORA is a "game-changer" that will require financial sector organizations to understand how their ICT, operational resilience, cyber, and Third-Party Risk Management (TPRM) practices impact the resilience of their most critical functions.

Deloitte's analysis of the final agreement reveals a number of significant implications for financial institutions. First, the DORA's ICT risk management requirements have a broader scope than what many companies are adapted to, focusing on critical business functions in addition to technology failure and cyber incidents. This will require companies to increase their operational resilience capabilities and acquire a deeper understanding of the connections among their ICT assets, processes, and systems (Deloitte 2022e)

The DORA's incident reporting framework consolidates multiple existing EU incident reporting obligations into a more comprehensive framework. This will require that companies enhance their capacity to collect, analyse, escalate, and disseminate information about ICT incidents and threats. To comply with the new business impact analysis requirement, companies will need to develop more sophisticated scenario testing methods and incorporate redundancy and modifiability into their systems to support their critical functions.

The DORA also mandates digital operational resilience testing for all in-scope companies, including an annual security and resilience test of their critical ICT systems and applications and a more advanced Threat-Led Penetration Testing (TLPT) every three years for enterprises exceeding a certain threshold of system importance and maturity. This will require companies to create broader and more precise testing and scenario analysis capabilities, as well as to map their third-party providers to their key functions.

Another important function imposed by the regulation is the requirement for critical ICT service providers of in-scope entities to meet certain requirements. These requirements relate to penetration testing, vulnerability scans, source code reviews, and other practices that would require additional audit or certification procedures of third-party service providers. As a result, it is reasonable to expect that many contract negotiation processes will be initiated by those entities in scope.

Overall, the DORA represents a significant step forward in improving the digital operational resilience of financial institutions in the EU. However, it also poses several challenges for firms, including the need to broaden their operational resilience capabilities, improve their incident reporting capabilities, and develop more sophisticated testing and scenario analysis methods. Firms that are able to meet these challenges will be well-positioned to thrive in the increasingly digital financial landscape.

3.3 Analysis of the regulation document and its requirements

In November 2022, the EU's negotiators reached a consensus on the DORA and the final regulation entered into force in January 2023. The actual regulation document is dated November 17, 2022 and contains 257 pages. Below is a brief explanation of the main parts of the regulation, which is presented in two sections for the convenience of explanation.

The first section of the DORA regulation consists of 106 distinct paragraphs and establishes guidelines for ensuring the digital operational resilience of financial institutions. It emphasizes various themes, such as the need to maintain up-to-

date ICT systems, the requirements for a risk management framework, and the creation of business continuity and recovery plans.

The first section also addresses the issue of digitalization in finance and the need for financial sector resilience in the face of cyber and ICT risks. It considers previous related regulations, the need for unified regulation across member states, and the harmonization of digital operational resilience requirements for all financial entities. It is noted that, to date, only ICT risk provisions have been partially addressed, with gaps and overlaps in important areas such as ICT-related incident reporting and digital operational resilience testing. Therefore, the exchange of information and intelligence regarding cyber threats between financial institutions is encouraged.

Other aspects include the requirement for financial institutions to manage ICT third-party risk and the limitation and outsourcing of certain entities. It also includes provisions for penetration testing and the need for financial entities to have contractual agreements supporting critical ICT functions, including the geographical locations of critical ICT service providers. The first section of the regulation contains no individual requirements against which a gap analysis may be undertaken. Therefore, it is less relevant to this gap analysis method than the second section, which contains such requirements.

The second section of the regulation is divided into nine chapters, each focusing on a different aspect of the regulation. Articles serve to subdivide each chapter, and the regulation as a whole contains a total of 64 articles. The chapters are summarized in more detail below.

The first chapter of the regulation provides an overview of its subject matter and personal scope. This chapter contains articles on the main provisions of the regulation, such as the definition of terminology and the scope of the regulation's applicability.

The focus of Chapter II of the regulation is on ICT risk management. This chapter is divided into two sections and discusses various themes related to the governance and structure of ICT risk management, as well as the protection and prevention of digital incidents. It also addresses the response to and recovery from

digital incidents, as well as the identification, evaluation, and management of risks.

Chapter III of the regulation covers the management and reporting of incidents using information and communication technologies. This chapter contains provisions on the classification and reporting of the most significant incidents, as well as the methods and procedures for responding to and managing incidents. Additionally, this chapter includes regulations on the management and administration of incidents.

The requirements for testers and the execution of digital operational resilience testing are outlined in Chapter IV of the regulation. This chapter contains provisions regarding the qualifications and experience required of testers, as well as the general requirements for the performance of digital operational resilience testing. The management of ICT third-party risk is the subject of Chapter V of the regulation. This chapter is divided into two sections covering the core concepts for successfully managing ICT third-party risk and the framework for key ICT third-party service providers. It contains provisions about the identification and evaluation of risks and the management and mitigation of such.

The regulation's consideration of information-sharing agreements between regulated parties can be found in Chapter VI. This chapter contains provisions regarding the various sorts of information that may be exchanged and the protocols that may be followed to seek information and provide it.

In Chapter VII of the regulation, the competent authorities charged with enforcing the regulation are described. This chapter outlines the powers and responsibilities of the relevant authorities and the reporting and investigation procedures for regulation violations.

The delegated acts are detailed in Chapter VIII of the regulation and their adoption and publication procedures.

Chapter IX includes provisions for the regulation's entry into force and the repeal of previous legislation. The chapter consists of two sections, the first of which is entitled "Review clause of the regulation" and the second "Applied Amendments."

In conclusion, the second section of the DORA regulation provides specific standards for the areas covered in the first section. It addresses a wide range of digital operational resilience-related themes, such as ICT risk management, the handling and reporting of ICT-related incidents, digital operational resilience testing, and the management of ICT third-party risk.

3.4 Compiling the methodology document

The compliance gap methodology document for the Digital Operational Resilience Act is intended to outline the phases and objectives of the compliance gap analysis project. This document is the primary reference for the project team, providing essential information on the DORA regulation, project objectives, and actionable steps for each phase. It is also intended to include contact information for certain Deloitte practitioners familiar with this methodology, in case the project team require assistance with the interpretation of the methodology or has other questions of a general nature. The methodology document is divided into three phases aimed at understanding the client's present state, identifying, and evaluating compliance gaps, and reporting those gaps. Ultimately, this methodology document serves as a guide for the efficient execution of the compliance gap analysis project.

The methodology document is structured similarly to the three Deloitte methodologies described in Chapter 3.1. The structure is also generally following project management guidelines set by the Department for Business Innovation & Skills. (BIS 2010).

The following sequential steps of the analysis are outlined:

(i) Preparation for the engagement kick-off: The project team prepares for the engagement kick-off by leveraging past knowledge and experience with a client, initiating project management protocols, hosting a preparation call with a client representative, scheduling interviews with key stakeholders, and requesting necessary documentation.

(ii) Understanding the client's current state: The project team reviews the client's existing documentation, interviews key stakeholders, and tests

IT systems and infrastructure to understand their current IT security policies, procedures, and practices.

(iii) Evaluation of the client's status against DORA requirements: The project team compares the client's current IT security policies, procedures, and practices to the requirements set by DORA. This comparison is essential for identifying and evaluating compliance gaps, as it allows the project team to determine where the client's current state falls short of DORA requirements.

(iv) Identification and documentation of compliance gaps: The project team identifies and documents any gaps or discrepancies between the client's current state and DORA requirements. This documentation is essential for developing a report considering the identified gaps.

(v) Documentation of the initial findings: The results of the gap analysis conducted by the project team are documented in the initial report.

(vi) Revision of the initial report: A review of the findings listed in the initial report is performed with the client’s key stakeholders. This procedure is intended to confirm our understanding of identified findings with client representatives and, if necessary, to acquire a deeper understanding of them. This phase is intended to ensure the accuracy and completeness of the final report.

(vii) Follow-up procedures: Based on the initial stakeholder review, follow-up procedures such as additional interviews and document examinations may be conducted to validate issues and modification requests raised during the initial review.

(viii) Finalization of the report: As a consequence of the follow-up procedures, a final report is prepared based on the data collected. In the final phase of reporting, all agreed-upon modifications and clarifications are made to the report, and it is prepared for presentation to the client's management team.

(ix) Preparation of the reporting template: At this phase, the template can be modified and made ready to support the reporting in the subsequent phase. Visualizations of the template should be reviewed to ensure that the displayed data is accurate.

(x) Delivery of final report: The final report is delivered to the management team of the client. It includes a Power BI visualization, a detailed description of the findings, and optionally (depending on the agreements), brief recommendations to resolve the identified DORA compliance gaps. This last step of the project must provide a detailed description of the findings to the client, so the client is aware of which items must be addressed to achieve DORA compliance.

The above steps are essential for a comprehensive and systematic approach to identifying and evaluating compliance gaps for the DORA regulation. They ensure that the client's current state is evaluated against DORA requirements, compliance gaps are identified and documented, and an initial report is developed to highlight the identified gaps. In addition, the follow-up procedures with key stakeholders, validation of identified findings, and adjustments based on feedback received contribute to the report's accuracy and completeness. The final step involves delivering and presenting the final report, along with visualizations, to the client's management team. This ensures that the client is provided with the necessary information regarding the identified gaps between their current state and the state required by DORA regulations.

3.5 Compiling the analysis template

When the methods indicated in Chapter 2.7 of this thesis were examined, it was noted that the work document templates used for documenting gap assessments in those methods are Excel files formatted in the manner of checklists. Individual requirements are displayed in separate cells inside the requirement sections, which are grouped into multiple sheets. The author's professional expertise in IT audit engagements has revealed that comparable architectures are commonly

used. Considering the structure's proven effectiveness in various audit and assessment projects, it was regarded as an appropriate choice for use in the gap analysis approach to be created.

To successfully assess compliance with the regulation, it is important to consider that not all the requirements listed in the regulation apply directly to the financial entities in scope. Several sections of the regulation target European financial supervisory agencies, Lead Overseer, and other regulatory entities. Additionally, some requirements are presented in a more general, descriptive manner to provide context for other, more specific requirements. As a result, it is unnecessary to include each requirement in the work program file, as they may not be directly related to the gap analysis work. However, certain "descriptive requirements" must be included in the work file to facilitate the identification of references to other requirements.

Considering the above, a consistent approach was adopted to compile the work document template, which included three distinct sheet types: a general sheet, a definitions sheet, and multiple requirement sheets. This approach aimed to facilitate the review of compliance with the regulation by ensuring that only relevant requirements were considered and that the template was structured in a manner suitable to the gap analysis work.

The general sheet provides an overview of the document, including descriptions and instructions for use, as well as two tables. The first table (left side of Figure 2) contains a list of all supporting documents for the gap analysis project. Each document is labelled with the Article to which it is linked. The second table (right side of Figure 2) includes descriptions of various potential conclusions for the requirements listed on the requirements sheets. The purpose of this sheet is to provide general guidance to the project team conducting the work, list all supporting documents, and present various possible requirement conclusions for reference.

Description
This document is designed to assist in assessing an entity's compliance with DORA regulations. Regulation areas and requirements which does not directly apply to financial entities are removed from the document entirely. The requirements are accessible through the Article tabs. The questions are categorized under different articles and numbered to correspond to the checklist requirements. The fulfilment of some specific requirements can likely be deduced from specific materials. These materials are indicated under the "supporting material" header below. Each material is followed by an article and a requirement that the material most likely corresponds.

Instructions
1. Request supporting materials from the entity and mark "Yes" in the "Received" column once received. If not provided, mark "No". 2. Evaluate compliance based on provided material, person inquiry, or other means. Choose an appropriate result from the **Conclusion options table** on the right. If drawing a conclusion based on other means or in a case that requirements is not satisfied, provide a further justification in the "Comment" column.

Article	Supporting material	Received
5 & 6	Internal governance and control framework	
5, 6, 8, 11 ,13 & 24	ICT strategy Roadmap / Annual plan	
5	Internal ICT risk related training materials	
5	ICT third party risk strategy documentation	
6	ICT risk management framework internal audit report or equivalent	
6	ICT multi-vendor strategy documentation or equivalent	
7	ICT audit report or equivalent	
8 & 9	ICT risk management framework	
8	Risk exposure analysis	
8	Change management process documentation	
8	ICT assets map or equivalent	
8	Documentation of services provided by thirs-party service providers	

Conclusion options	
A	Fulfilled based on person inquiry
B	Fulfilled based on material inspection
AB	Fulfilled based on both
C	Fulfilled by other means (attach comment)
D	Not fulfilled (attach comment)
N/A	Not applicable

Figure 2. General sheet of gap analysis template

The definitions sheet (Figure 3) includes a table that enumerates all the regulations' terminology and definitions as they appear in the regulation. The goal of this sheet is to assist the project team in identifying new and unfamiliar terms associated with the regulation, thus aiding in their understanding of the requirements.

#	Term	Definition	Additional reference
1	Digital Operational Resilience	The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions	
2	Network And Information System	Network and information system as defined in Article 6, point 1, of Directive (EU) .../...+	
3	Legacy ICT System	An ICT system that has reached the end of its lifecycle (end-of[1]life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity	
4	Security Of Network And Information Systems	Security of network and information systems as defined in Article 6, point 2, of Directive (EU) .../...+ (5)	
5	ICT Risk	Any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment	
6	Information Asset	A collection of information, either tangible or intangible, that is worth protecting	
7	ICT Asset	A software or hardware asset in the network and information systems used by the financial entity	
8	ICT-Related Incident	A single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity	
9	Operational Or Security Payment-Related	A single event or a series of linked events unplanned by the financial entities referred to in Article 2(1), points (a) to (d), whether ICT-related or not, that has an adverse impact on the availability, authenticity, integrity or confidentiality of payment-related data, or on the payment-related services provided by the financial entity	

Figure 3. Definition sheet of gap analysis template

Each requirement sheet is organized into three columns: regulatory requirement, conclusion, comment, and supporting material, with each sheet titled according to its corresponding article number. The supporting material and regulatory criteria requirements are listed in the first column. Requirements are following the numbering and wording of the original regulation document for easier traceability. The second column is dedicated to recording conclusions regarding the compliance of each requirement, and the third column is provided for the inclusion of any relevant comments per requirement. To enhance the clarity of the analysis process, different colours are used to indicate the relationship between requirements and the supporting documents that pertain to them.

Governance and organisation (5)		
Supporting material		
1 Internal governance and control framework		
2 ICT strategy Roadmap / Annual plan		
3 Internal ICT risk related training materials		
4 ICT third party risk strategy documentation		
Regulation requirement	**Conclusion**	**Comment**
1 Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.		
2 The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1). For the purposes of the first subparagraph, the management body shall:		
a bear the ultimate responsibility for managing the financial entity's ICT risk;		
b put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;		
c set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely		
d bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8), including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8), point (b);		
e bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8), including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8), point (b);		
f approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them;		

Figure 4. Requirement sheet for gap analysis template, considering Article 5

3.6 Compiling the reporting template

The Power BI reporting template for the DORA gap analysis method is a visual representation of the project's status. The primary purpose of the reporting template is to provide the DORA gap analysis project team with a graphical representation of the project's progression, allowing them to monitor the overall project status, status of material requests and significant areas of noncompliance. This information provides the project team with an efficient method for presenting and analysing data, allowing them to identify issues in the project, make informed decisions, and appropriately prioritize their work based on the inspected data. In addition, the reporting template can be used at the end of the project to present the final results and findings to the project's stakeholders.

A further advantage of the reporting template is its capacity to improve communication and collaboration between team members and stakeholders during the various stages of the gap analysis project. The dashboard's visual nature allows for a clear and concise presentation of data, which facilitates effective collaboration and the sharing of insights. This can lead to more effective decision-making

overall and higher-quality project outcomes. The reporting template may be reused for multiple clients so long as the structure of the analysis template document remains unchanged, thereby saving time and resources when working on multiple projects.

All of the requirements have been included in the reporting template, except for those outlined in Articles 4 and 16. The requirements of Article 4 cannot be evaluated objectively because they are described on a very general level. Article 16 addresses the Simplified ICT Risk Management Framework, which is only relevant for minor entities where Articles 5 through 15 do not apply. Given that comprehensive gap analysis projects are not expected to be required by minor entities, there is no need to consider Article 16 in the reporting template.

The reporting template contains a dashboard (Figure 5) with five distinct visualizations that provide an overview of the project's status. The data for the visualization interface originates from an Excel file containing an analysis template that is continuously updated throughout the duration of the gap analysis project. Consistent with the organization's branding, the dashboard's visuals employ a colour scheme of green, blue, and grey. To improve clarity and overall aesthetics, each visualization is contained within a distinct, green-coloured box. Additionally, each visualization is annotated, and a descriptive note is provided for one most complex visualization.

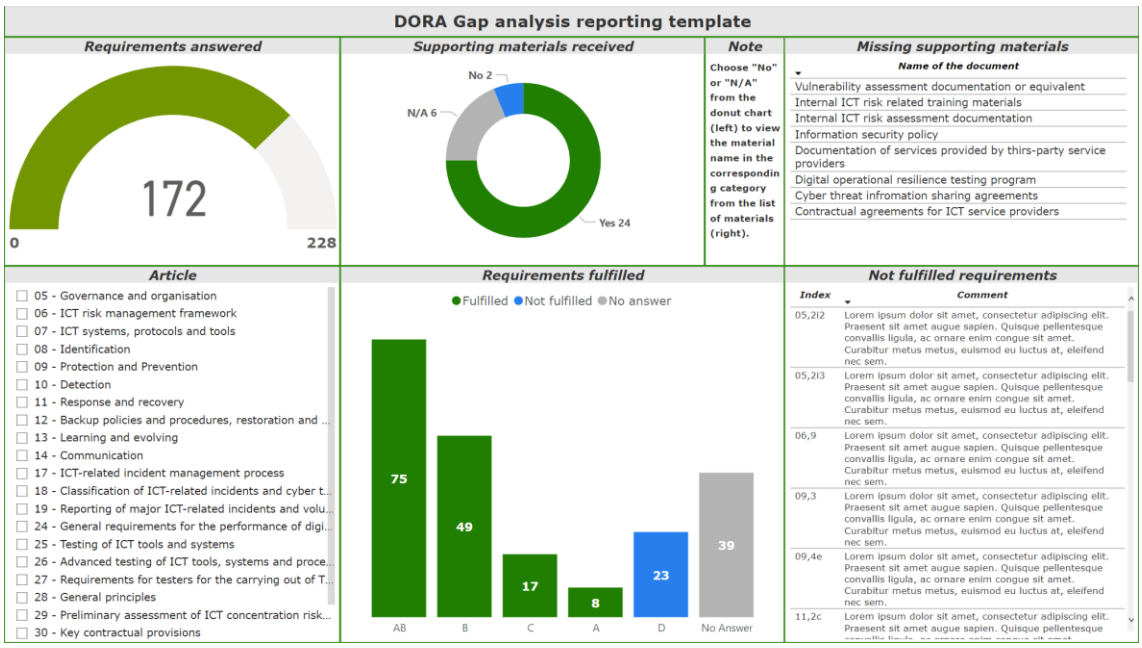

Figure 5. Dashboard of the reporting template

The dashboard's first visualization is a gauge chart that displays the number of regulatory requirements that have been addressed. On the working paper, there are 228 distinct fields containing regulatory requirements; each of these fields must be marked as filled, not filled, or not applicable. In Figure 5, for instance, 172 of these 228 elements are marked as complete. Visualization is helpful for monitoring progress on a broad scale and ensuring that all regulatory requirements are addressed, as this is essential for the successful completion of the project. The gauge chart utilizes a conditional colour scheme, with red indicating zero addressed fields, yellow 100 addressed fields, and green 228 addressed fields. In Figure 5, the measuring bar contains a colour combination of green and yellow when approximately 75% of the requirements have been addressed.

The second visualization is a doughnut chart that summarizes the status of received supporting materials. The graph demonstrates the number of assessment-related materials or documents that have been received, not received or are unrelated to this gap analysis project. The visualization is colour-coded to match the dashboard's theme and is directly linked to the succeeding material list.

The third visualization in Figure 5 is a material list connected to the previous doughnut chart. It includes a separate Note box, which can be seen in the upper centre of Figure 5. The Note box instructs the user to select "No" or "N/A" from

the doughnut chart, thereby filtering the material list to match the selected criteria. This enables the project team to determine which supporting materials are still missing.

A filter list (slicer) is located between the third and fourth visualizations. The slicer contains each article in the regulation separately, allowing the user to select the article they wish to examine in the two final succeeding visualizations.

The fourth visualization is a bar chart that summarizes the conclusions of all the requirements in the analysis template. The chart uses a colour scheme to indicate whether a requirement has been fulfilled (green), not fulfilled (blue), or no response to the requirement has been received (grey). Through the slicer, the chart can be filtered to show data related to only a specific article. By default, the chart displays the status of the entire group of articles.

The final visualization displays a list of indexes of unfulfilled requirements along with their corresponding comments. Each requirement on the analysis template is attached to its own index, which corresponds to the document's original numbering. Additionally, in accordance with the analysis template's instructions, if a regulatory requirement has not been met, an explanation must be provided in the comment field. By selecting an article from the filter list, only the indexes and comments of unfulfilled requirements for the selected article will be displayed. The list displays comments and indexes for all unfulfilled requirements by default.

3.7 Validation initiation

The validation procedure for the DORA gap analysis method began with the selection of six Deloitte Finland professionals with extensive experience in the financial sector, internal audits, and/or compliance audits. One professional in the group already had direct experience with the DORA gap analysis project, and the remaining professionals were selected based on their subject matter expertise and the anticipation that they would apply the final version of the gap analysis method to be developed in their client projects.

In order to reduce the amount of time required to comprehend the method during the validation process, each validator, with the exception of the individual with

direct experience, received a briefing on the method, its documents, and its core concept several weeks prior to the beginning of the process. This ensured that all participants had an understanding of the method and its related components, allowing for an efficient validation process.

The group of validators was requested to provide answers to eleven questions regarding the three documents associated with the method: the gap analysis methodology, the analysis template, and the reporting template. They had 16 days to respond to the questions via email. Validators were informed that their input might be included in the thesis report to demonstrate the method's validity and reliability and that the validated documents could be modified based on their feedback. Validators were also informed that their responses would be utilized solely for the purposes of the thesis, stored in their original form only on Deloitte's laptop and deleted upon completion of the thesis.

The 11 questions included in the email were as follows:

(i) How clear are the DORA gap analysis documents, and are there any improvements that can be made for better visual presentation or clarity?

(ii) How easy is it to follow the methodology document's steps for conducting the analysis?

(iii) Are there any areas in the methodology document that need improvement or expansion to make the process more effective or clear?

(iv) Does the analysis template cover everything needed for the gap analysis projects assessment phase?

(v) Are there any areas in the analysis template that need to be adjusted or added to make it more comprehensive or effective?

(vi) How clear and accessible are the visualizations presented in the reporting template, and do they effectively represent the key data from the analysis?

(vii) Are there any additional data points or visualizations that would be helpful to include in the reporting template?

(viii) Are there any modifications that you would suggest to make the method more adaptable to different client contexts or sectors?

(ix) Considering your present knowledge about the DORA regulation, on a scale of 1 to 10, how confident are you in the method's ability to effectively help the organization and its clients assess gaps between DORA regulations and the client's current state? If you are not confident, please provide improvement points or ideas that could help enhance the method's effectiveness in this regard.

(x) Are there any additional resources, tools or documents that would be helpful to include in the method to enhance its effectiveness?

(xi) If you have any additional feedback or ideas for development, please feel free to share them as your response to this question.

Four of the six validators had responded to the validation request by the time the validation request deadline had passed. Even though communication was established with the fifth and sixth validators, their professional obligations prevented them from providing timely responses. Considering that the majority of requested responses were received, it was determined that proceeding with the validation analysis was appropriate, as the received responses were considered sufficient for meeting the objectives of this thesis. The extensive feedback provided by the individual with direct experience with the DORA gap analysis project further supported this conclusion. The following sub-chapter provides an examination of the feedback received.

3.8 Validation results

This sub-chapter examines the ideas and suggestions collected during the validation process in order to establish the thesis's validity and reliability, as well as improve the method's functionality and overall usability. This sub-chapter pre-

sents the feedback from four validators identified as A, B, C, and D. Some feedback has been slightly rephrased for clarity, but careful consideration has been taken to preserve the feedback's underlying meaning.

It is important to note that not all validator responses are discussed in this chapter, as certain questions were left unanswered by some validators and certain responses were more general in nature or lacked specific suggestions for improvement or modification. In addition, some review comments were provided on the documents shared with the validators, which are also included in this chapter. One validator provided their feedback in Finnish, which was translated in order to be included in the validation process.

Validator A provided the following suggestions:

For the methodology document:

- To better serve different purposes, the text should explore the types of engagements where the method and its assets can be used and clarify how clients can use the findings and final report.
- It would be helpful to explicitly state the factors to consider and evaluate when reviewing client-provided documents (e.g., maturity, up-to-date status, length, document existence, compliance), depending on whether the work is an audit or remediation advisory.
- If documents are reviewed beforehand, it may be beneficial to use this information to prefill the gap analysis and prepare for interviews.

For the analysis template:

- Assessing the importance of the audit trail “where the information is from” regarding the information source.
- Evaluating the size of the GAP instead of focusing on how the material is collected.
- Considering the benefits of having each article in their respective tabs vs. having the articles in one (this question applies to the reporting template as well).

Lastly, Validator A suggested including a template for reporting both initial and final findings to enhance the method's effectiveness.

Validator B provided the following suggestions:

For the methodology document:

- Including a concise example of how the process has already been implemented in a real client project.

For the analysis template:

- Adding a high-level progress summary sheet for more effective tracking of progress.
- Including recommendations on how to address unmet requirements.

For the reporting template:

- Highlighting articles with the lowest answer rate using different colours to emphasize areas needing improvement.
- Further explaining the context of the A, B, AB, and C columns.

Additionally, Validator B recommended incorporating a version tracking sheet to manage updates to the methodology document and analysis template, considering that regulations may evolve over time.

Validator C provided the following suggestions:

For the methodology document:

- Explain how Deloitte can support clients after conducting gap analysis work, such as developing processes or assisting with specific operations.
- Reassess project team composition, exploring the use of cross-functional teams and differentiating necessary competencies for managers versus junior employees.
- Improve document logic and readability through various re-wording and grammatical corrections (marked on the document).

For the analysis template:

- Visualizing DORA sub-areas to provide a high-level overview, incorporating this information into both the framework document and Excel file, with clear markings indicating which tab covers the requirements related to each area.
- Reviewing the supporting material list for more detailed descriptions of the materials and combining materials on the same topic into one.
- Refining the definition sheet by including only key terms, removing references to other regulations, and explaining terms as they are defined in the referred regulation.
- Enhancing gap analysis usability by grouping related requirements together, such as bundling requirements from multiple sheets and providing clearer, more straightforward summaries of regulatory requirements, including a separate field identifying the regulatory issues addressed by each requirement.
- Addressing the difficulty in comprehending certain sections of the regulation text by simplifying the language, making it more understandable and accessible for future project team members without in-depth expertise in the regulation area.

For the reporting template, Validator C suggested:

- Clarifying the meaning of acronyms, A, AB, B, and C, ensuring they are easily understood in the context of the reporting template.
- Introducing additional pie charts for management reporting purposes, for example, to identify areas with the most deficiencies.

Validator D provided the following suggestions:

For the methodology document:

- Creating a diagram or visual representation illustrating various phases, key tasks, and objectives for each phase to better visualize the process.
- Instead of merely listing direct requirements from DORA regulation, describe the tangible impact and changes these regulations have on

financial institutions, responsible parties or organizations, and the most significant differences compared to the current legislative environment.

- Clarifying the desired outcome or future target state of the organization once DORA is fully enforced, to help identify what the organization aims to achieve from the DORA exercise. To consider two possible mindsets for the gap analysis: a pure "compliance mindset" and using DORA as a vehicle to increase cyber/digital resilience maturity. A "compliance mindset" focuses on meeting DORA regulations and adhering to authority demands while maintaining current cyber/digital resilience processes with necessary DORA additions. Alternatively, using DORA to enhance the organization's cyber/digital resilience maturity involves incorporating DORA requirements into processes, activities, and roles, and assessing findings against desired maturity levels.

For the analysis template:

- Recording an assessment regarding the "size" of the gap for each requirement as small, medium, or large, would help prioritize and evaluate required actions.
- Identifying the individuals or groups within the organization who own or are responsible for each specific DORA requirement, gaining insights from respective individuals instead of relying solely on document-based gap analysis.
- Defining the organization's target state for each gap to support the findings and solidify recommendations, determining how to solve a gap and what needs to be updated or amended to address the gap effectively, thereby helping to better understand the recommended actions and their expected outcomes.

Lastly, Validator D recommended focusing on delivering outcomes that outline the subsequent actions and steps for progress. According to their feedback, it might be beneficial to expand the gap analysis by incorporating the organization's target state for DORA requirements and cyber/digital resilience maturity level. By including these elements, organizations can gain a better understanding of the necessary steps to achieve their desired level of compliance and resilience.

Despite not receiving all six expected responses, the validation process has provided valuable insights and suggestions for improving the methodology document, analysis template, and reporting template. The diverse perspectives and high-quality recommendations from Validators have led to a comprehensive set of suggestions that address various aspects of the thesis, such as clarity, usability, and effectiveness. Furthermore, provided feedback also serves to demonstrate the thesis's validity and reliability.

4 POST-VALIDATION CHANGES & CONCLUSION

In the concluding chapter of the thesis, modifications to the method resulting from the validation procedure are described. Afterwards, additional improvement opportunities and the method's validity and reliability are assessed. The chapter concludes with a summary of the thesis development process.

4.1 Modifications implemented to the method

The suggestions presented by validators in Chapter 3.8 were assessed based on the following three factors:

(i) Relevance: To determine if the proposed changes align with the thesis objectives and if they address the specific needs and concerns of the method's target user group.

(ii) Consistency: To ensure that the suggested change maintains a consistent style of the thesis.

(iii) Feasibility: To evaluate whether it is realistic to incorporate the changes within the given timeframe and available resources.

After assessment of the suggestions, they were grouped based on their similarities to create a list of concrete improvement points. Some suggestions were determined to be impractical to implement or beyond the scope of this thesis and its limitations, and therefore were not implemented. The suggestions deemed impractical for implementation are discussed in the next chapter of this thesis as potential future improvement opportunities.

The following changes were made to the methodology document:

- Benefits to client organizations from the findings and final report were clarified. The desired outcomes for client organizations were further elaborated upon from both the "compliance mindset" and "vehicle to enhance cyber/digital resilience process" perspectives.
- A description of the factors to be evaluated when reviewing client-provided materials were included.

- The importance of initially reviewing requested materials to pre-fill the gap analysis template and prepare for interviews was emphasized.
- The project team composition was refined by considering the potential use of cross-functional teams.
- The changes and impacts of DORA regulations on financial services organizations were described and the key differences compared to the existing legislative environment were highlighted.
- In the “Understand & Evaluate” section, clarification was added that the ownership of the requirements should be traceable to individual person(s) or groups within the client organization.
- The "Report" section was expanded to "Report & Next Steps" and now includes a description of how Deloitte can support client organizations after completing the gap analysis.
- The document's logic and readability were improved through various re-wording and grammatical corrections.
- Minor visual changes were made to improve the comprehensibility and overall presentation of the methodology document, including a visualization to show the components of DORA.

The following changes were made to the analysis template:

- Articles were grouped by corresponding regulation chapters and supporting material lists were consolidated from per article to per chapter.
- The supporting material table on the general sheet was revised with more detailed descriptions, unnecessary materials were removed, and chapter-specific lists were updated accordingly.
- Instructions for defining and evaluating gaps and their sizes were added to the general sheet, along with Gap Descriptions and Gap Size boxes for each requirement in chapter sheets.

- A new table was added to the general sheet for monitoring document versions.
- The definitions sheet was simplified to include only essential terms, with explanations provided for some terms instead of referencing other regulations.
- A graphical representation of DORA chapters was incorporated within the analysis template.
- The analysis template's usability and comprehensiveness were enhanced by expanding the description and instruction sections.

The following changes were made to the reporting template:

- The dataset underlying the visualization was updated to align with modifications made to the analysis template.
- A pie chart was added to display the distribution of gaps based on their sizes.
- Columns A, AB, B, and C in the requirements stacked chart visualization were combined and renamed for better clarity.
- The Article filter was replaced with a Chapter filter, and the “Identified gaps” table was updated accordingly.
- The supporting materials guidance visualization was removed, and the remaining visualizations were rearranged to improve the report's usability.

4.2 Further improvement opportunities

Several suggestions were identified as relevant and consistent with the method, but they were not implemented due to the limited time available. Implementing these suggestions would require substantial effort and could potentially necessitate a partial reconsideration of the method, making it impractical at this stage of the thesis. Additionally, given the novelty of the DORA regulation, it is uncertain whether these changes would be cost-effective in terms of time without first testing the method in an actual client project. Consequently, considering the time

constraints and the novelty of the topic, it was decided not to implement these suggestions. Instead, they have been documented in this thesis as potential future improvement points that may be implemented into the method at later stages if deemed necessary.

- Creating a template to report initial and final findings.
- Offering more detailed guidance on factors to consider when reviewing supporting materials.
- Organizing the requirements into logical units for evaluation as a single entity, resulting in clearer and more understandable groups of the regulation's requirements, as opposed to multiple separate requirements.
- Enhancing the gap analysis to include an organization's target state perspective on DORA requirements and cyber/digital resilience maturity level.
- Providing high-level guidance on compiling recommendations to address the identified gaps.

4.3 Validity and reliability of the method

Despite the fact that the validity and reliability of the gap analysis method could not be confirmed through an actual client project due to the limitations outlined in Chapter 1.6, it could still be considered valid and reliable based on the validation process conducted. Four Deloitte Finland professionals with extensive experience in the financial sector, internal audits, and/or compliance audits participated in this process. One of these professionals had direct experience with DORA gap analysis projects, while the others were selected on the basis of their subject matter expertise. These validators provided feedback on the gap analysis methodology, analysis template, and reporting template by responding to eleven questions via email.

The validation process feedback was thoroughly analysed, and modifications were made to the methodology and templates based on their relevance, consistency, and feasibility. The recommendations of the validators led to improvements in the method's clarity, usability, and efficiency, which also contributed to

the validity and reliability of the thesis. Some suggestions were deemed impracticable to implement or outside the scope of the thesis and were noted as potential areas for future method enhancement.

When considering further improvement opportunities, it is important to ensure that the underlying concept and regulatory requirements listed in the method are not significantly altered, as this could potentially compromise the method's reliability. Special consideration should be given to the required fields, as some of the feedback suggested modifying and combining them to improve the efficacy of the method. While this strategy may improve usability, there is a risk that the concepts underlying certain requirements may change because of the modifications. In such a case, the method would fail to achieve its objective, as the requirements listed in the compliance gap analysis may differ from the actual requirements set by DORA. Therefore, a balance between enhancing usability and preserving the method's fundamental concepts and requirements must be established.

4.4 Conclusion

The main objective of this thesis was to develop an effective gap analysis method that would enable Deloitte to conduct DORA gap analysis projects, assessing client organisations' compliance with DORA regulations and identifying detected gaps. Specifically, the method was designed to assist Deloitte in identifying potential gaps and improvement opportunities in client organisations before they need to demonstrate compliance to the authorities.

A detailed examination of the topic's theoretical foundations has been done, covering a wide range of relevant subjects. These include an examination of general concepts of regulations and compliance, as well as an examination of the requirements and implications of the Digital Operational Resilience Act. Furthermore, the principles of compliance gap analysis and compliance auditing have been studied in order to understand the best practices and methodology used in these domains. Cybersecurity and risk management have also been studied, acknowledging their importance in ensuring the successful implementation and maintenance of digital operational resilience. The study concludes with an examination

of internal audit's function in regulatory compliance, highlighting its contribution to the ongoing improvement of an organization's processes and systems.

The method's development process included utilizing expertise gained from several IT audit-related projects and adopting Deloitte's methodology, in addition to building on the thorough study of topics that form the theoretical background of this thesis. This approach resulted in the development of three key documents that comprise the method as a whole: the gap analysis methodology, the gap analysis template, and the reporting template.

The gap analysis methodology document serves as a guide for project teams, detailing each phase's objectives and key activities. The methodology consists of five phases: plan, understand, evaluate, report, and next steps. Its purpose is to guide project teams in assessing client organisations' compliance design, identifying gaps between the current state and regulatory requirements, providing a report on the identified gaps, and determining the next steps the project team can take to assist clients after the gap analysis is complete.

The gap analysis template is an Excel file designed as a checklist and used to gather all requirement-related data from the client. It includes relevant requirements, definitions, and supporting documents, and serves as a main working paper for the project team when assessing regulatory compliance. The purpose of the analysis template is to streamline the process of assessing client organizations’ DORA compliance during the gap analysis project.

The reporting template, which utilises Power BI software to display key project aspects, provides a comprehensive view of the gap analysis project's progression. This approach simplifies client reporting and assists in determining the overall status of the project, in addition to highlighting missing supporting materials and discovered gaps. The reporting template draws data from the gap analysis template, allowing the project team to investigate the project's status at any time, thereby improving project management and reporting capabilities.

Understanding the importance of validating the developed method, the author initiated a validation process aimed at evaluating the method's validity and relia-

bility, while simultaneously identifying areas for improvement to enhance its usability. As a result of this process, the author implemented several improvements to the methodology, analysis template, and reporting template, based on the feedback received from the validators. The outcomes of the validation process indicated that the developed method was generally considered successful in achieving its primary objective: identifying potential DORA-related gaps in client organizations.

From a personal development standpoint, while working on this thesis, the author greatly improved their skills in analysis, problem-solving, and research by studying regulatory information and creating a compliance gap analysis method for a novel regulation. The research process has given the author a broad understanding of DORA legislation and overall knowledge of EU-level regulations, which is considered useful given their background in IT risk management. By achieving their objectives and expanding their expertise in regulatory matters, the author has effectively combined personal development with professional growth in the field of IT risk management.

REFERENCES

Asaitec. 2016. Methodology for Gap Analysis and Compliance Management. Referred 15.1.2023 https://resources.gapanalysislab.com/wp-content/uploads/2016/12/GA-process-methodology-281116.pdf

BIS Department for Business Innovation & Skills. 2010. Guidelines for managing projects. Referred 27.2.2022 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/31979/10-1257-guidelines-for-managing-projects.pdf

Choejey, P. 2018. Cybersecurity Challenges and Practices: A Case Study of Bhutan. Doctoral Thesis. Murdock University, Perth, Western Australia. Referred 23.2.2023 https://researchrepository.murdoch.edu.au/id/eprint/42353/1/Choejey2018.pdf

Council of the EU 2022. Digital finance: Council adopts Digital Operational Resilience Act. Press Release. Referred 10.12.2022 https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/

Deloitte. 2022a. About Deloitte. Referred 10.12.2022 https://www2.deloitte.com/global/en/pages/about-deloitte/articles/about.html

Deloitte. 2022b. Our Purpose & Culture. Referred 10.12.2022 https://www2.deloitte.com/global/en/pages/about-deloitte/articles/our-purpose-and-culture.html

Deloitte. 2022c. Risk Advisory. Referred 10.12.2022 https://www2.deloitte.com/global/en/pages/risk/topics/risk-advisory.html

Deloitte. 2022d. Internal Audit 3.0. Referred 20.12.2022 https://www2.deloitte.com/cy/en/pages/audit/articles/internal-audit-3-0.html

Deloitte. 2022e. The EU's Digital Operational Resilience Act (DORA) has been agreed: implications for the financial services sector. Referred 2.3.2023 https://www2.deloitte.com/fi/fi/pages/risk/articles/eu-dora-implications-for-financial-services-sector.html

ENISA. 2022. Threat Landscape 2022 report. Referred 12.12.2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

European Commission 2020. Proposal for a regulation of the European Parliament on digital operational resilience for the financial sector and amending Regulations. Referred 10.12.2022 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

Gadziala, M. 2005. Integrating Audit and Compliance Disciplines within the Risk Management Framework. Speech by SEC Staff. Referred 30.12.2022 https://www.sec.gov/news/speech/spch113005mag.htm

GDPR.eu 2022. What is GDPR, the EU's new Data Protection Law. Referred 12.1.2023 https://gdpr.eu/what-is-gdpr/

Goethals S. & Bosch B. 2022. How to prepare for the Digital Operational Resilience Act. EY. Referred 22.2.2023 https://www.ey.com/en_be/financial-services/how-to-prepare-for-the-digital-operational-resilience-act

Hatherell, T. 2020. Internal audit Trends and challenges. Deloitte Referred 29.12.2022 https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/internal-audit-trends-challenges_BHI.pdf

IBM Security. 2022. Cost of a Data Breach Report 2022. Referred 13.1.2023 https://www.ibm.com/downloads/cas/3R8N1DZJ

ISO 31000. 2018. Risk management — Guidelines. Referred 31.12.2022 https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

ISO/IEC 27001. 2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Referred 31.12.2022 https://www.iso.org/standard/82875.html

Keen, R. 2021. How to Do a Gap Analysis ~ The Definitive Guide. ISO 9001 Checklist. Referred 15.1.2023 https://www.iso-9001-checklist.co.uk/how-to-do-a-gap-analysis-for-ISO-9001-(in-6-steps).htm

Kelley, K. 2018. Compliance audit definition. TechTarget. Referred 12.12.2022 https://www.techtarget.com/searchcio/definition/compliance-audit

Kustula, K. 2013. Sisäisen valvonnan ja riskienhallinnan kehittäminen Siikajoen kunnassa. Master's thesis. Oulun Seudun Ammattikorkeakoulu. Referred 14.12.2022 https://www.theseus.fi/bitstream/handle/10024/65120/Kustula_Krista.pdf?sequence=1&isAllowed=y

Luukka, K. 2014. Konstruktiivinen tutkimusote. Metodix. Referred 12.12.2022 https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Marker, A. 2018. Compliance Auditing 101: Types, Regulations and Processes. Smartsheet. Referred 17.1.2023 https://www.smartsheet.com/compliance-auditing

Morgan, S. 2020. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine. Referred 13.1.2023 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

National Institute of Standards and Technology. 2014. Cybersecurity Framework. Referred 20.12.2022 https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10

NIST 2023. About NIST. Referred 25.2.2023 https://www.nist.gov/about-nist

NIST. 2012. Guide for Conducting Risk Assessments. Referred 17.1.2023 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Red Hat 2023. What is compliance management? Referred 2.3.2023 https://www.redhat.com/en/topics/management/what-is-compliance-management

The Digital Operational Resilience Act 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations. Referred 2.1.2023 https://data.consilium.europa.eu/doc/document/PE-41-2022-INIT/en/pdf

Salomaa, M. Kyberturvallisuus. VTT. Referred 3.3.2023. https://www.vttresearch.com/fi/palvelut/kyberturvallisuus

SANS. 2021. CIS Controls V8. Referred 14.1.2023 https://www.sans.org/blog/cis-controls-v8/

Sarrala, T. 2021. “Uncovering privacy threats with Soft Systems Methodology”. Master’s thesis. JAMK. Referred 14.12.2022 https://www.theseus.fi/bitstream/handle/10024/495124/Thesis_Sarrala_Tuisku.pdf?sequence=2&isAllowed=y

Shleifer, A. 2005. Understanding Regulation. Harvard university. Referred 11.1.2023 https://scholar.harvard.edu/files/shleifer/files/02_eufm00121.pdf

Skibicka, N. 2021. Examples of the biggest KYC & AML compliance failure cases. Fully Verified. Referred 12.1.2023 https://fully-verified.com/kyc-aml-compliance-failures/

StandardFusion 2022. Everything You Need To Know About The ISO 27001:2022 Update. Referred 15.3.2023 https://www.standardfusion.com/blog/iso-27001-changes-2022/

Suomidigi. 2020. VAHTI 22/2017 Ohje riskienhallintaan. Referred 14.1.2023 https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-222017-ohje-riskienhallintaan

The Institute of Internal Auditors. 2023a. Sisäinen tarkastus. Referred 17.12.2023 https://theiia.fi/sisainen-tarkastus/

The Institute of Internal Auditors. 2023b. Sisäinen valvonta, riskienhallinta ja organisaatiokulttuuri. Referred 17.2.2023 https://theiia.fi/sisainen-tarkastus/sisainen-valvonta-ja-riskien-hallinta-2/

Traficom. 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Traficomin julkaisuja 2/2020. Referred 12.1.2023 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Tutkimuseettinen neuvottelukunta 2023. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa 2023. Tutkimuseettisen neuvottelukunnan julkaisuja 2/2023. Referred 25.2.2023 https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf

Virtanen, A. 2006. Konstruktiivinen tutkimusote. Miten koulutus ja elinkeinoelämän odotukset kohtaavat ammattikorkeakoulun opinnäytetöissä. Ammattikasvatuksen aikakauskirja. Jyväskylä: Jyväskylän ammattikorkeakoulu. Referred 12.12.2022 https://journal.fi/akakk/article/view/114874/67807

Walford, G 2005. Research ethical guidelines and anonymity. International Journal of Research & Method in Education. Referred 25.1.2023 https://www.tandfonline.com/doi/abs/10.1080/01406720500036786

Wright, R. 2009. Internal Audit, Internal Control and Organizational Culture. Doctoral Thesis. Victoria University. Referred 20.12.2022 https://vuir.vu.edu.au/1989/1/R-M-Wright-Thesis-2009.pdf

Yale University. 2019. The Lehman Brothers bankruptcy: Overview. Journal of Financial Crises, Volume 1 Issue 1. Referred 23.3.2023 https://elischolar.library.yale.edu/cgi/viewcontent.cgi?article=1000&context=journal-of-financial-crises