

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Marja-Liisa Soone

232591IVCM

Assessing Post-Quantum Cryptography Readiness in the Banking Sector

Master's Thesis

Supervisor: Jelizaveta Vakarjuk, MSc

Co-Supervisor: Nikita Snetkov, MSc

Tallinn 2026

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Marja-Liisa Soone

232591IVCM

Postkvantkrüptograafia valmisoleku hindamine pangandussektoris

Magistritöö

Juhendaja: Jelizaveta Vakarjuk, MSc

Kaasjuhendaja: Nikita Snetkov, MSc

Tallinn 2026

Author's declaration of originality

I hereby certify that I am the sole author of this thesis and that this thesis has not been presented for examination or submitted for defense anywhere else. All used materials, references to the literature, and work of others have been cited.

Author: Marja-Liisa Soone

19.05.2026

Abstract

Quantum computing threatens public-key cryptography on which banking infrastructure currently relies. Algorithms such as RSA and elliptic-curve cryptographic algorithms support online banking, digital identities, and interbank communication, and a sufficiently powerful quantum computer would render them insecure. The harvest-now-decrypt-later threat means that encrypted data intercepted today can be stored and decrypted once such a machine becomes available, which makes the long data retention horizons of banking a present-day risk. Despite growing regulatory and industry attention, there is limited empirical evidence on how banks are responding.

This thesis assesses the post-quantum cryptography readiness of banks in Estonia and Sweden and develops a sector-specific migration framework. The thesis addresses five research questions covering awareness of quantum threats, integration of quantum risk into enterprise risk management, the current stage of migration efforts, factors that facilitate or hinder preparedness, and migration steps, organisational preconditions, and common pitfalls specific to the banking sector. The research combines a review of EU regulation, including DORA and RTS 2024/1774, the European Commission Recommendation 2024/1101, the NIS Cooperation Group implementation roadmap, and the European Payments Council cryptographic guidelines, with primary data collected through an anonymous online questionnaire and semi-structured validation interviews. PQC readiness is assessed in five dimensions: awareness and risk perception, governance and risk management integration, cryptographic dependencies and migration planning, crypto-agility, and external drivers and barriers.

The central finding is an awareness-action gap. Respondents recognise the urgency of the threat, yet none has formally integrated quantum risk into their enterprise risk management framework, none has started a formal migration project, and no institution has a detailed migration plan with inventories, milestones, budgets, and governance fully specified. The gap is consistent across both countries despite their different banking ecosystems.

Three factors sustain it: PQC migration is treated as a technical IT matter rather than a governance challenge, banks are constrained by vendor dependencies they cannot resolve unilaterally, and the regulatory signal lacks PQC-specific deadlines, which banks treat as permission to defer. Building on these findings, the thesis proposes a sector-specific migration framework comprising seven migration steps and a checklist of 45 items, addressing systemic interdependence, regulatory ambiguity, and vendor concentration as three considerations that general frameworks overlook. The thesis recommends that banks begin cryptographic inventory, risk classification, and definition of a target cryptographic architecture without waiting for further regulatory specification, and that regulators translate existing obligations into supervisory guidance with specific PQC migration milestones.

The thesis is in English and contains 91 pages of text, 8 chapters, 5 figures, 2 tables.

Annotatsioon

Postkvantkrüptograafia valmisoleku hindamine pangandussektoris

Kvantarvutus ohustab avaliku võtmega krüptograafiat, millel pangandussektori infrastruktuur praegu põhineb. Sellised algoritmid nagu RSA ja elliptikõveratel põhinevad krüptograafilised algoritmid toetavad internetipangandust, digitaalset identiteeti ja pankadevahelist sidet ning piisavalt võimekas kvantarvuti muudaks need ebaturvaliseks. Salvestanud-dekrüpteeri-hiljem oht tähendab, et täna pealtkuulatud krüpteeritud andmeid on võimalik säilitada ja dekrüpteerida hetkel, mil selline arvuti muutub kättesaadavaks, mistõttu pangandussektori pikad andmete säilitamise tähtajad kujutavad endast tänast riski. Hoolimata üha kasvavast regulatiivsest ja tööstuse tähelepanust on empiiriliste tõendite hulk pankade reageerimise kohta piiratud.

Magistritöö hindab pankade postkvantkrüptograafia valmisolekut Eestis ja Rootsis ning töötab välja sektoripõhise migratsiooniraamistiku. Töö käsitleb viit uurimisküsimust, mis hõlmavad teadlikkust kvantohtudest, kvantriski integreerimist ettevõtte riskijuhtimisse, migratsioonialaste jõupingutuste hetkeseisu, valmisolekut soodustavaid ja takistavaid tegureid ning pangandussektorile omaseid migratsioonisamme, organisatsioonilisi eeldusi ja levinud vigu. Uurimismeetod ühendab Euroopa Liidu õigusliku raamistiku analüüsi, sealhulgas DORA ja RTS 2024/1774, Euroopa Komisjoni soovitus 2024/1101, NIS koostöörühma rakenduskava ning Euroopa Maksenõukogu krüptograafilised juhised, esmaste andmetega, mis koguti anonüümse veebiküsimustiku ja poolstruktureeritud valideerimisintervjuude kaudu. PQC valmisolekut hinnatakse viies mõõtnes: teadlikkus ja riskitaju, juhtimine ja riskijuhtimise integratsioon, krüptograafilised sõltuvused ja migratsiooniplaneerimine, krüpto-paindlikkus ning välised soodustavad ja takistavad tegurid.

Peamine järeldus on lõhe teadlikkuse ja tegevuse vahel. Vastajad tunnistavad ohu pakilisust, kuid ükski neist ei ole kvantriski formaalselt integreerinud oma ettevõtte riskijuhtimise raamistikku, ükski ei ole alustanud formaalset migratsiooniprojekti ning üheski asutuses ei

ole üksikasjalikku migratsiooniplaani, milles oleksid täielikult määratletud krüptograafiline inventuur, vahe-eesmärgid, eelarve ja juhtimiskorraldus. Lõhe on mõlemas riigis ühtlane, hoolimata nende erinevatest pangandusökosüsteemidest. Seda hoiavad alal kolm tegurit: PQC migratsiooni käsitletakse pigem tehnilise IT-küsimusena kui juhtimisalase ülesandena, pangad on piiratud tarnijatest tulenevate sõltuvustega, mida nad ei saa ühepoolset lahendada, ning regulatiivne signaal ei sisalda PQC-spetsiifilisi tähtaegu, mida pangad tõlgendavad loana tegutsemise edasilükkamiseks. Tähelepanekutele tuginedes pakub töö välja sektoripõhise migratsiooniraamistiku, mis koosneb seitsmest migratsioonisammust ja 45 punktist koosnevast kontroll-loendist ning käsitleb süsteemset vastastikust sõltuvust, regulatiivset mitmetähenduslikkust ja tarnijate kontsentratsiooni kui kolme tegurit, mida üldised raamistikud ei arvesta. Töö soovitab pankadel alustada krüptograafilise inventuuri koostamisega, riskide klassifitseerimisega ja sihtkrüptoarhitektuuri määratlemisega, ootamata täiendavat regulatiivset täpsustust, ning regulaatoritel teisendada olemasolevad kohustused järelevalvejuhisteks koos konkreetsete PQC migratsiooni vahe-eesmärkidega.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 91 leheküljel, 8 peatükki, 5 joonist, 2 tabelit.

List of abbreviations and terms

AES	Advanced Encryption Standard
AI	Artificial Intelligence
BIS	Bank for International Settlements
BSI	German Federal Office for Information Security
CBOM	Cryptography Bill of Materials
CDR	Commission Delegated Regulation
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECC	Elliptic Curve Cryptography
ECCG	European Cybersecurity Certification Group
ECDH	Elliptic Curve Diffie–Hellman
ELCA	Enterprise-Level Crypto-Agility
ENISA	European Union Agency for Cybersecurity
EPC	European Payments Council
EU	European Union
FCA	Financial Conduct Authority
FIPS	Federal Information Processing Standards
FS-ISAC	Financial Services Information Sharing and Analysis Center
GRI	Global Risk Institute
HSM	Hardware Security Module
ICT	Information and Communication Technology
IPsec	Internet Protocol Security
LMS	Leighton–Micali Signature Scheme
MACsec	Media Access Control Security
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
RSA	Rivest–Shamir–Adleman
RTS	Regulatory Technical Standards
SEPA	Single Euro Payments Area

SHA	Secure Hash Algorithm
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SREP	Supervisory Review and Evaluation Process
SSH	Secure Shell
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
Target2	Trans-European Automated Real-time Gross Settlement Express Transfer System
TLS	Transport Layer Security
VPN	Virtual Private Network
WEF	World Economic Forum
XMSS	eXtended Merkle Signature Scheme
X-Road	Estonia's distributed data exchange infrastructure connecting public and private sector information systems

Table of contents

1	Introduction.....	13
1.1	Background	13
1.2	Research Problem	16
1.3	Research Questions	17
1.4	Research objectives.....	17
1.5	Contribution	18
1.6	Structure of the Thesis	19
2	Background and Conceptual Foundations	21
2.1	Key Concepts	21
2.2	Quantum Threats to Cryptography	23
2.3	Cryptography in Banking Systems	27
3	Regulatory and Policy Landscape for PQC in the EU.....	30
3.1	EU Policy Guidance and Timelines.....	30
3.2	Financial-Sector Regulation and Supervisory Expectations	31
3.3	National Strategies and Initiatives	35
4	Research Methodology	41
4.1	Research Objective and Scope	41
4.2	Research Design, Target Group and Data Collection	41
4.3	PQC Readiness Assessment Framework	44
4.4	Limitations	45
5	Findings on PQC Readiness in the Banking Sector	48
5.1	Awareness and Risk Perception	49
5.2	Governance and Risk Management Integration.....	51
5.3	Cryptographic Dependencies	52
5.4	Migration Planning and Crypto-Agility	53
5.5	External Drivers and Barriers.....	55
6	Interpreting Readiness and Gaps	58
6.1	Is the Banking Sector Prepared?	58
6.2	Central Challenges.....	62
6.3	Cross-Country Comparison	69
7	Practical PQC Migration Framework for Banks.....	74
7.1	Banking Needs a Sector-Specific Migration Framework	74
7.2	Recommended Migration Steps	77

7.3	Migration Checklist	84
7.4	Common Pitfalls and Risks	90
7.5	Contribution to Banking-Specific PQC Migration.....	91
7.6	Timeline Consideration	96
7.7	Framework Validation	97
8	Conclusion	99
8.1	Key Findings.....	99
8.2	Recommendations	100
8.3	Future Research.....	102
	References	104
	Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis.....	112
	Appendix 2 – Online Questionnaire	113
	Appendix 3 – Aggregated Questionnaire Results	118

List of figures

Figure 1. Mosca’s inequality applied to the banking sector. 15

Figure 2. PQC transition timeline..... 16

Figure 3. Relevant DORA and RTS 2024/1774 provisions 34

Figure 4. Migration steps undertaken by the four responding banks..... 54

Figure 5. Barriers limiting progress..... 57

1 Introduction

1.1 Background

Quantum computing is advancing in ways that threaten the security of public-key cryptography widely used today. Algorithms such as Rivest-Shamir-Adleman (RSA) encryption and digital signatures, and Elliptic Curve Diffie–Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA) and other elliptic-curve cryptographic algorithms, support online banking, digital identities, and interbank communication. A sufficiently powerful quantum computer running Shor’s algorithm could break these schemes, rendering the cryptographic foundations of current financial infrastructure obsolete [1].

Within the coming decade, cryptographically relevant quantum computers (CRQC) are expected to render these algorithms insecure [2]. Although the exact timeline remains uncertain, recent resource estimates show a continued decline in the hardware requirements for executing Shor’s algorithm at cryptographically relevant scales. Early estimates placed the cost of factoring RSA-2048 at roughly twenty million physical qubits [3]; subsequent work reduced this to under one million qubits within one week [4]; and a March 2026 result demonstrates that as few as 10,000 reconfigurable neutral-atom qubits may suffice, albeit with longer runtimes [5]. Elliptic-curve cryptographic algorithms are a quantum-easier target than RSA at equivalent classical security levels. Google Quantum AI estimates that breaking 256-bit elliptic curve cryptography would require fewer than 500,000 superconducting physical qubits with a wall-clock time under 25 minutes [6]. The German Federal Office for Information Security concludes that a CRQC can reasonably be expected by the year 2040 [7]. In response, major technology providers including Google and Cloudflare have set 2029 as their target for completing post-quantum cryptography migration [8] [9].

For the banking sector, this challenge is particularly acute because the threat is not only technical but systemic. Banks hold financial and customer data that must remain confidential for decades, operate on infrastructure with long replacement cycles, rely on shared financial

networks such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) and Trans-European Automated Real-time Gross Settlement Express Transfer System (TARGET2), and must comply with strict operational resilience obligations under regulatory frameworks such as the Digital Operational Resilience Act (DORA) [10]. The harvest-now-decrypt-later threat means that encrypted data intercepted today can be stored and decrypted once a sufficiently powerful quantum computer becomes available [11] [12]. This makes the risk immediate, even though practical quantum attacks may still be years away.

The timing dimension of this risk can be expressed through the Mosca's inequality: if the number of years that data must remain secure plus the number of years needed to migrate systems exceeds the number of years before quantum computers can break current encryption, then migration is already overdue [2]. For banking, where data retention and confidentiality periods can be ten or even more years, depending on the regulation, jurisdiction and internally set retention timelines, and where large-scale technology migrations often take years to complete, this inequality is close to being violated or may already be.

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to resist both classical and quantum attacks while running on existing hardware. In 2024, the National Institute of Standards and Technology (NIST) finalised its first three PQC standards [13], and the European Commission issued Recommendation (EU) 2024/1101 calling on Member States to begin transitioning critical systems to quantum-resistant cryptography, with a target of completing migration for high-risk systems by 2030 [14]. In the following year, the NIS Cooperation Group has published a coordinated implementation roadmap setting milestones for 2026, 2030, and 2035 [15]. By 2026, organisations are expected to complete cryptographic inventories and develop migration strategies; by 2030, large-scale migration to post-quantum cryptography should be underway, particularly for high-risk systems; and by 2035, the transition is expected to be largely completed, with quantum-vulnerable cryptography phased out.

In the financial sector, DORA imposes obligations on information and communication technology (ICT) risk management that extend to cryptographic controls, though it does not prescribe the use of specific cryptographic algorithms or standards[10]. The Bank

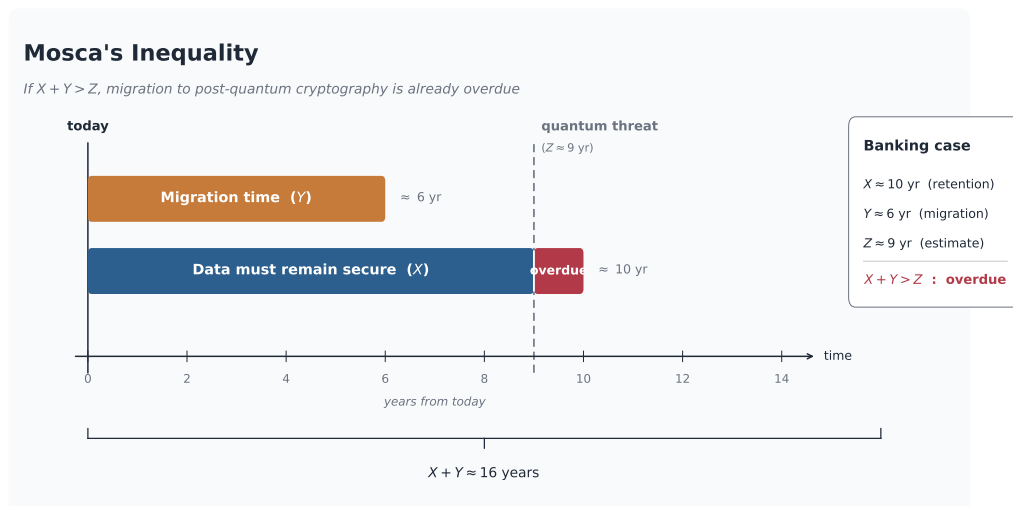


Figure 1. Mosca's inequality applied to the banking sector. If the data confidentiality horizon (X) plus the migration time (Y) exceeds the time to a cryptographically relevant quantum computer (Z), migration is already overdue. Banking retention requirements of ten or more years combined with multi-year migration timelines place the sector close to, or beyond, this threshold. Illustrative values are shown for the banking sector: $X \approx 10$ years (typical retention horizon), $Y \approx 6$ years (multi-year migration), and $Z \approx 9$ years (mid-range estimate of time to a cryptographically relevant quantum computer); specific values vary by institution and source. Adapted from [2].

for International Settlements (BIS) has published a roadmap urging the financial industry to start preparing now [11]. The European Payments Council (EPC), as the governance body for Single Euro Payments Area (SEPA) payment schemes, has since 2026 included a dedicated chapter on PQC in its cryptographic guidelines, recommending that payment service providers establish comprehensive cryptographic inventories, adopt crypto-agility, and plan migrations to hybrid schemes combining classical and post-quantum algorithms [16].

Despite growing regulatory and industry attention, there is limited empirical evidence on how banks are actually responding. Academic research on PQC has concentrated on algorithmic performance, hardware requirements, and cryptanalytic strength, while existing standards and guidance documents provide abstract recommendations without operational depth or empirical validation [17]. A growing body of policy and industry reports addresses the transition at a general level, but few studies examine whether banks have translated awareness into concrete governance action [18] [19]. There is particularly limited insight into how PQC readiness differs between countries operating under the same

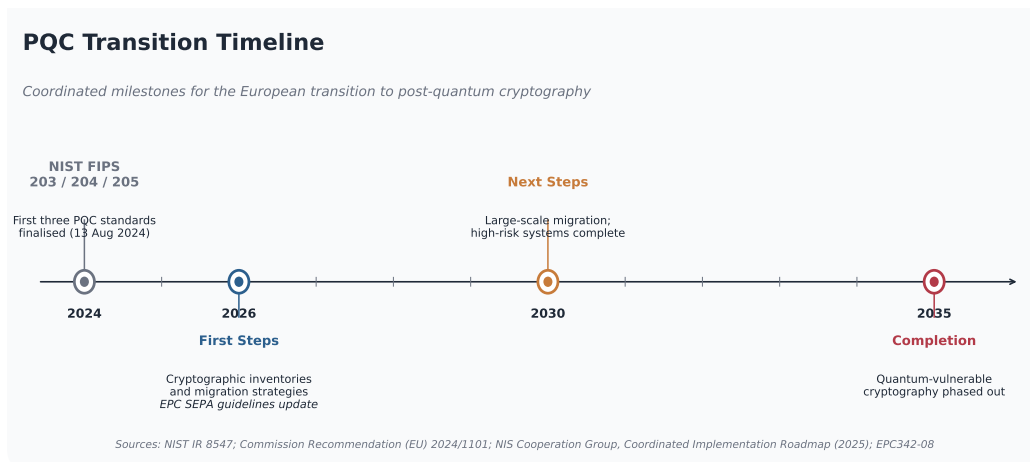


Figure 2. PQC transition timeline. Coordinated milestones from the European Commission’s Recommendation [14], the NIS Cooperation Group’s implementation roadmap [15], and the European Payments Council’s payment-sector cryptographic guidelines [16], anchored on the NIST FIPS standards finalised in 2024 [13].

regulatory framework.

Estonia and Sweden provide a useful basis for comparison. Both are EU Member States with advanced digital economies and well-developed banking sectors, yet they differ in market structure, regulatory culture, and scale [20]. At the time of writing, neither country has issued a dedicated national PQC transition roadmap, leaving banks without a country-level coordinating framework for their migration planning.

1.2 Research Problem

The central problem is a mismatch between the pace of the quantum threat and the pace of institutional preparation. Quantum computing is advancing, regulatory bodies are signaling clear expectations for migration to begin, and the harvest-now-decrypt-later threat creates actual risk. Yet industry sources suggests that awareness of quantum risks does not translate into timely organisational action [19, 21]. Financial institutions report limited strategic planning, governance integration, or migration readiness, even if they acknowledge the seriousness of the threat [21].

For banks, these characteristics combine in ways that generic PQC migration guidance does not address. Banks are systemically interconnected through shared financial networks where migration requires coordinated action across all participants. They operate under sector-

specific regulatory obligations that are directionally clear but operationally leave several unanswered questions. They face concentration risk in vendor ecosystems, particularly in hardware security modules (HSMs), where a small number of providers constrain institutional migration timelines [22]. The existing literature does not adequately explain how banks interpret regulatory signals, whether awareness of quantum threats is translating into concrete governance action, or how readiness differs across countries operating under the same EU regulatory framework.

1.3 Research Questions

The thesis addresses the following research questions (RQs):

1. **RQ1:** How aware are banking professionals of quantum computing threats and post-quantum cryptography?
2. **RQ2:** How are banks integrating quantum-related risks into their enterprise risk management and governance structures?
3. **RQ3:** What is the current stage of banks' PQC migration efforts (e.g., cryptographic inventory, project planning, pilot implementations)?
4. **RQ4:** What factors (e.g., regulation, vendor support, budget, expertise) facilitate or hinder banks' preparedness for PQC?
5. **RQ5:** What migration steps, organisational preconditions, and common pitfalls are specific to the banking sector?

These questions are answered against the cryptographic obligations that already apply to financial institutions under existing regulations. The relevant provisions are introduced and analysed in Chapter 3 and summarised in Table 3. The thesis therefore considers not only what banks are doing in preparation for PQC, but also the extent to which current practice fulfils existing obligations, with particular attention to the maintenance of cryptographic inventories and the state of cryptographic agility.

1.4 Research objectives

The main objective is to assess the post-quantum cryptography readiness of banks in Estonia and Sweden and to develop a practical, sector-specific migration framework. Specific

objectives include:

1. Measure awareness and understanding of quantum computing threats and PQC among banking professionals.
2. Examine governance and risk management practices related to quantum risks, including whether PQC is integrated into enterprise risk management frameworks.
3. Analyse the state of migration planning, such as cryptographic inventories, roadmaps, standards adoption, and stakeholder involvement.
4. Identify obstacles and incentives influencing banks' readiness, such as regulatory pressure, vendor dependence, or resource constraints.
5. Synthesise the findings into a practical migration framework to guide banks in transitioning to post-quantum cryptography.

1.5 Contribution

This thesis makes three contributions. First, it provides empirical evidence on the PQC readiness of banks in two EU Member States. While policy and industry reports increasingly call for migration to begin, there is limited research documenting how banks are actually responding. The questionnaire findings reveal the gap between awareness and action, whereby the banking professionals acknowledge the seriousness of quantum threats, yet governance integration, cryptographic inventory, and migration planning remain at early stages. The comparative dimension, contrasting Estonia's centralised, small-market banking environment with Sweden's larger, more diversified financial system, adds insight into how national context shapes institutional behaviour.

Second, the thesis synthesises the fragmented regulatory, industry, and academic landscape into a common analysis of what PQC migration means for banking specifically. DORA, the European Commission Recommendation, the NIS Cooperation Group roadmap, the BIS quantum-readiness roadmap, the Financial Services Information Sharing and Analysis Center (FS-ISAC) crypto-agility framework, the EPC cryptographic guidelines, and the European Union Agency for Cybersecurity (ENISA) integration study each address different aspects of the problem. This thesis maps them against each other and against the empirical findings to identify where regulatory expectations, industry guidance, and institutional reality converge and diverge.

Third, the thesis proposes a practical PQC migration framework for the banking sector. Existing migration guidance does not address the structural characteristics that distinguish banking from other sectors. The proposed framework incorporates six migration steps, preconditions, and common pitfalls. The proposed framework also addresses systemic interdependence, regulatory ambiguity, and vendor concentration, which are three considerations that general frameworks overlook.

1.6 Structure of the Thesis

The thesis is organised as follows:

1. **Chapter 2: Background and Conceptual Foundations.** Reviews the background and conceptual foundations, covering quantum computing threats to public-key cryptography, the development and standardisation of PQC algorithms, and the concept of cryptographic agility in the banking context.
2. **Chapter 3: Regulatory and Policy Landscape for PQC in the EU.** Examines the regulatory and policy landscape at the EU and national levels, including DORA, the European Commission PQC Recommendation, the NIS Cooperation Group roadmap, and the national strategies of Estonia and Sweden.
3. **Chapter 4: Research Methodology.** Describes the research methodology, including research design, country selection, target group and recruitment, data collection, and the PQC readiness assessment framework.
4. **Chapter 5: Findings on PQC Readiness in the Banking Sector.** Presents findings across five thematic dimensions: awareness and risk perception, governance and risk management integration, cryptographic dependencies, migration planning and crypto-agility, and external drivers and barriers.
5. **Chapter 6: Interpreting Readiness and Gaps.** Interprets these findings in relation to the research questions, discussing overall sectoral readiness, central challenges including governance, crypto-agility, external dependencies, and competing priorities, and a comparative analysis of Estonia and Sweden.
6. **Chapter 7: Practical PQC Migration Framework for Banks.** Proposes a practical PQC migration framework tailored to the banking sector, including preconditions, six recommended migration steps, common pitfalls, three banking-

specific considerations, and timeline considerations.

7. **Chapter 8: Conclusion** Concludes with a summary of findings, recommendations for banks and policymakers, and directions for future research.

2 Background and Conceptual Foundations

2.1 Key Concepts

The following key concepts support the understanding of this thesis.

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to remain secure against attacks from both classical and quantum computers [23]. PQC algorithms rely on mathematical problems that are believed to be resistant to quantum attacks. Families of PQC algorithms include lattice-based, hash-based, code-based, and multivariate polynomial based and other [24]. Some of these algorithms are intended to replace the current public-key cryptographic systems that are vulnerable to attacks using quantum algorithms [13]. The goal of PQC is to provide quantum-resistant cryptographic mechanisms that can be implemented on classical computing infrastructure [25] [26].

Quantum cryptography is based on the principles of quantum physics and uses the unique properties of quantum mechanics to enable secure communication methods, most notable example is quantum key distribution [27]. Unlike post-quantum cryptography, which relies on computational hardness assumptions, quantum cryptography derives its security from the physical properties of quantum systems [28] [26].

Quantum key distribution (QKD) is a quantum cryptographic protocol, first proposed by Bennett and Brassard in 1984 [29], that uses quantum states, typically photons, to establish a shared encryption key between two trusted parties. Unlike PQC, QKD requires dedicated hardware such as quantum transmitters, receivers and specialised fibre-optic or satellite links. Any attempt to intercept the quantum transmission introduces detectable disturbances, allowing the communicating parties to detect eavesdropping attempts [28]. However, QKD has two practical limitations that affect its deployment in network settings. First, it requires an authenticated classical channel to prevent man-in-the-middle attacks [27]. Second, point-to-point QKD links are range-limited, and extending QKD across longer distances requires intermediate trusted nodes that relay keys using classical encryption and decryption.

Because global keys are accessible in plaintext at each relay node along the distribution path, these nodes represent security-critical points that must be physically protected and organisationally trusted [30]. Compromising a single trusted node can expose all keys relayed through it, and providing quantum security over long distances with untrusted relays remains an open research problem [31].

Mosca's theorem provides a compact risk analysis framework that helps organisations determine how urgently they need to migrate to post-quantum cryptography. The theorem is commonly expressed as the inequality $X + Y > Z$, where X represents how long data must remain secure, Y represents the time required to migrate cryptographic systems, and Z represents the time until quantum computers can break current cryptographic algorithms [2]. If $X + Y > Z$, the organisation is already behind in its migration efforts because adversaries can harvest encrypted data now and decrypt it later once cryptographically relevant quantum computers become available [32]. This framework is widely used in quantum risk assessments and migration planning [33] [34] [16].

Hybrid cryptography, in the context of PQC or quantum-safe cryptography, refers to the combined use of classical cryptographic algorithms and post-quantum cryptographic algorithms within the same protocol or system, with the purpose of ensuring security even if one of the algorithms is later found to be vulnerable. Hybrid schemes are recommended as a transition strategy because they allow organisations to introduce post-quantum cryptography gradually [13] [14]. However, hybrid approaches do not guarantee interoperability with legacy systems by default. While it is possible to design hybrid implementations that maintain backward compatibility, such designs may be susceptible to downgrade attacks, where an adversary forces the connection to fall back to the weaker classical algorithm alone. For sectors such as banking, where interoperability and system stability are critical, this trade-off between backward compatibility and security must be carefully evaluated when selecting a hybrid migration path [35]. Hybrid approaches are recommended in practical migration strategies and integration frameworks [36], and are particularly relevant for sectors such as banking, where interoperability and system stability are critical [37].

Cryptographic agility (crypto-agility) is the capability of a system or application to transition securely and efficiently from one cryptographic algorithm or implementation to another without major architectural changes or service disruption [38]. Cryptographic

agility is considered a key requirement for post-quantum migration because organisations may need to update cryptographic algorithms multiple times as standards evolve [22]. Achieving cryptographic agility requires inventorying cryptographic assets, managing dependencies, and designing systems that allow algorithm replacement without redesigning entire infrastructures [18].

2.2 Quantum Threats to Cryptography

This section examines which cryptographic algorithms are threatened by quantum computing, the nature of those threats, and the timeline on which they are expected to materialise.

Cybersecurity focuses on protecting and restoring systems, networks, and data from attacks, unauthorised access, or damage, while ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation [39]. Cryptography is a core component of cybersecurity. It provides the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification [39].

Quantum computing and quantum technologies are evolving rapidly. IBM has published a roadmap to deliver a fault-tolerant quantum computer by 2029, with the proposed Quantum Starling system designed to run quantum circuits with 100 million gates on 200 logical qubits [40].

Beyond cryptanalysis, quantum algorithms have demonstrated theoretical speedups for problems in physics simulation, number theory, and topology [24]. Research interest has extended to many areas. For the purposes of this thesis, the most relevant implication of large-scale quantum computing remains its effect on cryptographic security. The same computational capabilities that enable these advances also pose a direct threat to current cryptographic algorithms. A sufficiently powerful quantum computer could break public key encryption, compromise digital signatures, undermine authentication mechanisms, and render current key exchange protocols insecure [24]. In response, two distinct approaches have emerged. Post-quantum cryptography (PQC) aims to replace vulnerable algorithms with ones that resist quantum attacks while running on existing classical hardware [41]. Quantum key distribution (QKD), by contrast, uses the physical properties of quantum states

to establish shared keys, but requires dedicated quantum communication infrastructure [29]. This thesis focuses on PQC as the approach most immediately relevant to the banking sector.

Current public-key cryptography relies on the computational difficulty of mathematical problems such as integer factorisation and discrete logarithms [42] [1]. Composite-modulus, factoring-related public-key schemes such as RSA and finite-field Diffie–Hellman, the best known classical algorithms run in sub-exponential time. For schemes built on the group of points on an elliptic curve, such as ECDH and ECDSA, no sub-exponential classical attack is known and the best algorithms remain fully exponential, which is why elliptic curve keys can be substantially shorter than RSA keys at equivalent classical security [43]. Both classes are infeasible to break classically at the key sizes used in practice [13], but Shor’s algorithm enables a quantum computer to solve all of them in polynomial time, making today’s widely used public-key cryptography vulnerable to a sufficiently capable quantum computer [1], [44].

Advances in quantum computing have accelerated in recent years, with demonstrations of quantum computational advantage on narrow, purpose-constructed tasks [45]. While these results remain contested and do not directly translate to cryptographic workloads [32], they indicate continued progress toward large-scale, fault-tolerant quantum computers. Such machines would threaten current public-key cryptography: Shor’s algorithm [1] can factor large integers and compute discrete logarithms in polynomial time, breaking schemes such as RSA [42] and elliptic-curve cryptographic algorithms.

The timeline remains uncertain, but the risk is not distant. Recent expert surveys estimate a 19–34% probability that RSA-2048 could be broken by a quantum computer within the next decade [32]. The BSI concludes that it is now reasonable to expect a cryptographically relevant quantum computer by 2040 [7]. However, the threat does not begin when a quantum computer arrives. The European Payments Council (EPC) distinguishes between two threat vectors. One being harvest-now-decrypt-later, which drives urgency for data confidentiality, and harvest-now-forge-later, which is less urgent for typical short-lived signature verification but critical for digital assets and central bank digital currencies where private keys control long-term ownership [16].

The timeline for a cryptographically relevant quantum computer remains uncertain, but resource estimates have decreased steadily. Gidney et al estimated that factoring a 2048-bit RSA integer would require approximately 20 million noisy physical qubits and 8 hours of computation, assuming a gate error rate of 10^{-3} and surface code error correction [46]. By 2025, improved algorithms reduced this estimate to under one million physical qubits, though at the cost of several days of continuous operation [4]. Gheorghiu and Mosca provide a broader resource estimation framework covering both public-key and symmetric cryptographic targets under varying quantum error rates [44]. While such hardware does not yet exist, the downward trend in resource requirements underscores the urgency of migration planning. RSA underpins much of today’s financial infrastructure, securing TLS connections for online banking, interbank messaging systems, digital certificates, and authentication protocols across payment networks [13].

Elliptic-curve cryptographic algorithms, such as elliptic-curve Diffie–Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA), which are widely used for secure authentication, key exchange, and other cryptographic functions in mobile banking and payment applications, are in fact more quantum-vulnerable than RSA at equivalent classical security levels.

Roetteler et al. estimate that computing a 256-bit elliptic curve discrete logarithm would require approximately 2,330 logical qubits [43]. Even after accounting for the physical-qubit overhead introduced by error correction, this remains a smaller resource requirement than the approximately 20 million physical qubits estimated for factoring a 2048-bit RSA key [3]. Elliptic curve cryptographic algorithms therefore require fewer quantum resources to break than RSA, which is why they are expected to be among the first asymmetric schemes to become vulnerable as quantum computing scales. NIST has recommended that elliptic-curve cryptographic algorithms, along with other classical public key algorithms, be deprecated by 2030 and disallowed by 2035 [13].

Symmetric cryptographic algorithms face a different category of quantum threat. Grover’s algorithm [47] enables quadratic speedup in brute-force key search, reducing the effective security of an n -bit key to approximately $n/2$ bits. For AES-128, this implies a reduction to approximately 64 bits of quantum security. Whether this constitutes a practical threat remains debated, as the algorithm requires sequential oracle queries that are difficult to

parallelise and demands a fault-tolerant quantum computer operating without interruption for the duration of the search [4]. Resource estimation frameworks project that, under realistic quantum error rates, AES-256 retains over 160 bits of effective security, whereas AES-128 may degrade to approximately 80 bits as quantum circuit optimisations continue [44].

NIST IR 8547 classifies AES-128 as meeting the requirements of Security Category 1 in the post-quantum standardisation framework and states that existing symmetric cryptography standards are “significantly less vulnerable to known quantum attacks” than public-key standards, concluding that NIST “does not expect to need to transition away from these standards as part of the PQC migration” [13]. Accordingly, the prevailing guidance recommends AES-256 as a conservative measure for long-term protection, while AES-128 is not considered an immediate migration priority.

Hash functions are similarly affected by quantum algorithms, though the threat model differs from that of symmetric encryption. Brassard, Hoyer, and Tapp demonstrated that a quantum computer can find collisions in a hash function with fewer evaluations than the classical birthday attack, reducing the collision resistance of an n -bit hash function from approximately $n/2$ bits to $n/3$ bits [48]. In practice, this means SHA-256 retains roughly 85 bits of quantum collision resistance rather than the classical 128 bits. NIST IR 8547 assigns SHA-256 a collision security category of 2 and a preimage security category of 5, and does not mandate migration away from current hash function standards [13]. The collision-finding algorithm also requires a large amount of quantum memory, which presents a substantial implementation barrier beyond the computational cost alone. These factors suggest that SHA-256 and SHA-3 remain adequate for most applications, though systems with long-term integrity requirements may consider SHA-384 or SHA-512 for additional margin.

In summary, developments in quantum computing and quantum technologies directly affect the timeline at which today’s cryptography may become vulnerable and hence the urgency with which organisations must pursue PQC migration [32].

2.3 Cryptography in Banking Systems

Banks are central pillars of trust and stability in modern society. They handle large volumes of sensitive financial data, facilitate secure transactions, and support critical infrastructure. For this reason, the security of banking operations is intrinsically dependent on robust cryptography. Consequently, any technological development that threatens cryptographic systems directly threatens the security and stability of the banking sector [11].

The banking sector is exposed to the risks posed by quantum computing. Cryptography is deeply embedded in banking systems and supports a wide range of functions across both hardware and software layers. Cryptographic algorithms encrypt customer data at rest and protect backups and archival records, secure online banking sessions and web services while information is in transit (e.g., via TLS/SSL), and support authentication and digital signatures. They also ensure confidentiality for internal systems and interbank communication channels (such as SWIFT and TARGET2), and are embedded in endpoint devices like ATMs, payment terminals (e.g., EMV standards), and point-of-sale (POS) systems to maintain data integrity and authenticity across the network [16].

In practice, these functions rely on a small set of primitives. Confidentiality of data in transit is provided by TLS, which remains the backbone protocol for secure web communication and is typically negotiated using RSA or elliptic-curve key establishment together with ECDSA-based server authentication [49]. Symmetric encryption is provided by AES, while integrity and digital signatures rely on the SHA-2 family of hash functions; legacy primitives such as single DES, two-key Triple-DES, MD5 and SHA-1 are either broken or scheduled for retirement under current payment-industry guidance [16]. In card payments, EMV chip authentication and PIN processing combine symmetric algorithms, which remain resistant to quantum attacks, with RSA-based asymmetric mechanisms used to protect the risk-management data exchanged between card and terminal [49].

Because the public-key algorithms used in banking, principally RSA and elliptic-curve cryptographic algorithms, are vulnerable to quantum attacks [43] and regulatory requirements mandate data retention for extended periods, banks are exposed to store now, decrypt later attacks and, as custodians of digital assets, to the derivation of private keys by a quantum computer [33].

Due to their role as trust providers and operators of systemic infrastructure, banks are expected to lead the transition to PQC [15] [11]. However, cryptography is deeply embedded across banking systems creating complex dependencies between protocols, libraries, digital certificates, key management systems, and external vendors [18]. Many of these components rely on monolithic architectures that were structurally not designed for crypto-agility [22], [38]. These deep-rooted dependencies significantly complicate the migration to post-quantum cryptography.

Replacing cryptographic algorithms is not a simple substitution task. It requires the exhaustive identification of all cryptographic use cases, the rigorous assessment of IT and data dependencies, coordination with external vendors, and the modification of underlying protocols and interfaces [18]. In many cases, individual systems cannot be updated independently due to strict backward compatibility and interoperability requirements.

Legacy systems present an additional challenge. They may rely on hardcoded cryptographic implementations, lack comprehensive documentation, or be tightly coupled with core business processes. Updating such systems is inherently costly, time-consuming, and operationally risky. As a result, migration must often be phased, guided by formal dependency mapping, and carefully prioritized based on asset criticality [36].

Furthermore, cryptographic changes propagate across the entire system architecture. Updating a single component, such as a key exchange mechanism, may necessitate corresponding changes in digital certificates, authentication processes, and communication protocols. This ripple effect reinforces the critical need for comprehensive strategic planning and robust governance frameworks.

Overall, the complexity of cryptographic deployment in banking systems transforms PQC migration from a mere algorithmic upgrade into a large-scale organizational and technical transition. The fundamental challenge lies not only in adopting new mathematical standards but in mapping and managing complex interdependencies, ensuring the continuity of critical financial operations, and maintaining strict regulatory compliance throughout a multi-year transition period [18], [11].

A response to this complexity is emerging in convergent guidance from the European Payments Council, the Global Financial Markets Association, and the UK National Cyber

Security Centre, which all frame the migration as a three-step process. The first step is a comprehensive cryptographic inventory that identifies where, how, and by which algorithms cryptography is used across the institution. The second is the establishment of crypto-agility, so that algorithms and key sizes can be replaced without re-engineering the surrounding systems. The third is a risk-based replacement of vulnerable primitives, prioritised by asset criticality and exposure to store now, decrypt later attacks [16].

3 Regulatory and Policy Landscape for PQC in the EU

3.1 EU Policy Guidance and Timelines

The European Commission Recommendation (EU) 2024/1101, published on 11 April 2024, sets a strategic direction for the transition to post quantum cryptography (PQC) across the EU [14]. It calls on Member States and relevant stakeholders to initiate migration planning and to develop a coordinated implementation roadmap, including inventories of cryptographic assets, risk assessments, and the design of architectures that allow cryptographic algorithms to be replaced without disrupting operations. Although the Recommendation is not legally binding, it sends a clear signal of regulatory intent and establishes a reference timeline that is likely to shape supervisory expectations and industry practices.

Complementing this, the NIS Cooperation Group has issued a coordinated implementation roadmap for PQC migration, which provides more operational guidance on how organisations should approach the transition. The roadmap highlights key preparatory steps, including the identification of cryptographic assets, prioritisation based on data sensitivity and system criticality, and the adoption of hybrid cryptographic approaches during the transition period [15]. ENISA further supports this policy framework through its Post-Quantum Cryptography Integration Study, which offers technical and organisational guidance on PQC integration [36]. The study emphasises that migration is not limited to algorithm replacement but requires system-wide changes, including updates to protocols, infrastructure, key management, and governance processes. It also highlights dependencies across software libraries, hardware modules, and public key infrastructures, reinforcing both the complexity and the long time horizon of migration.

Collectively, these EU-level documents create a layered policy environment. While they do not impose direct legal obligations, they establish a policy and supervisory expectation that organisations, including banks, must begin structured preparation for PQC migration. In practice, these documents function as anticipatory governance tools that influence

supervisory dialogue, risk assessments, and strategic planning within the financial sector. Although these instruments are cross-sectoral in scope and not targeted at specific sectors, they are particularly important for critical and highly regulated industries such as the financial sector, where supervisory scrutiny and operational resilience frameworks are already well developed.

3.2 Financial-Sector Regulation and Supervisory Expectations

Within the financial sector specifically, Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) provides the primary legally binding framework relevant to cryptographic resilience. While DORA does not explicitly reference PQC, it establishes requirements that are directly applicable to the management of cryptographic risks [10].

DORA places explicit personal responsibility on the management body. Under Article 5(2), the management body must bear the ultimate responsibility for managing the financial entity's ICT risk and must put in place policies ensuring the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data [10]. This is not a delegable operational task: the management body is required to define, approve, oversee, and be responsible for the implementation of all arrangements related to the ICT risk management framework. In the context of PQC migration, this means that board-level awareness of quantum-related cryptographic risk is not merely desirable but a regulatory expectation under DORA.

DORA also establishes specific obligations for ICT asset identification and cryptographic controls. Article 8(4) requires financial entities to identify all information assets and ICT assets, map those considered critical, and document the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets [10]. Article 8(6) further mandates maintaining relevant inventories and updating them periodically. These requirements directly underpin what the PQC migration literature refers to as a cryptographic inventory, the identification and mapping of all cryptographic dependencies across an organisation's systems and services. Article 9(4)(d) requires financial entities to implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection

measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes [10]. This provision establishes a risk-based approach to encryption, which means that as quantum computing changes the risk profile of existing cryptographic algorithms, the risk assessment process must account for that change.

Additionally, Article 13(7) requires financial entities, other than microenterprises, to monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience [10]. Quantum computing is one such technological development, and the obligation to monitor its impact on ICT security requirements creates a basis for supervisory authorities to expect that financial entities have assessed the implications of quantum computing for their cryptographic systems.

DORA delegates the further specification of these requirements to Regulatory Technical Standards (RTS). Article 15(a) mandates, in consultation with ENISA, the development of the RTS specifying further elements for ICT security policies, procedures, protocols and tools, including cryptographic techniques [10]. The resulting Commission Delegated Regulation (EU) 2024/1774 explicitly operationalises this mandate. Its Recital 9 directly references the need for financial entities to be prepared for threats from quantum advancements making it the first binding EU financial-sector regulation to name quantum threats [50]. Article 6(4) of the RTS 2024/1774 requires financial entities to have documented policies and procedures for cryptographic key management that would allow them to adopt the leading practices and standards relating to cryptography and for each specific category of use which establishes a concrete crypto-agility obligation [50]. Article 7 complements this by requiring financial entities to maintain a register of certificates, creating a further layer of cryptographic visibility [50].

DORA is further supported by supervisory guidelines issued by the European Banking Authority (EBA) [51]. These secondary instruments and supporting guidelines define supervisory expectations for ICT governance, risk assessment, control design, incident classification and reporting, resilience testing, and ICT third-party risk management. While neither DORA nor its secondary legislation explicitly requires PQC adoption, their combined emphasis on forward-looking ICT risk management, lifecycle governance of

ICT assets, cryptographic controls, and resilience against emerging technological threats makes them directly relevant to PQC migration planning even in the absence of an explicit legal mandate.

The EPC distinguishes two threat vectors: harvest now, decrypt later, which drives urgency for data confidentiality, and harvest now, forge later, which is relevant where private keys control long term ownership such as digital assets and central bank digital currencies [16]. The second vector extends the quantum threat from a data confidentiality problem to an asset custody problem.

Beyond legislation and guiding documents, supervisory authorities such as the European Central Bank and national competent authorities can incorporate quantum-related cryptographic risks into supervisory review processes, including the Supervisory Review and Evaluation Process (SREP), thematic reviews on ICT risk and cyber resilience, and supervisory assessments under DORA. In those contexts, supervisory authorities may assess cryptographic asset inventories, long-term data confidentiality risks, third-party cryptographic dependencies, and the development of crypto-agility or PQC migration strategies not only based on what DORA and secondary legislation stipulates, but based on supervisory expectations informed by non-binding guidance, including the European Commission Recommendation on PQC, ENISA guidance, and frameworks from international bodies.

Beyond the binding obligations summarised in Table 3, non-binding instruments such as the European Commission Recommendation on PQC, ENISA guidance, and international frameworks (for example, the World Economic Forum’s report on quantum security for the financial sector and the Global Risk Institute’s Quantum Threat Timeline) contribute to the evolving interpretation of ICT and cyber-risk management and consequently create an environment where early preparation for PQC migration is regarded as part of sound governance and operational resilience [12] [32].

Instrument	Article	Requirement
DORA	Art. 5(2)	Management body bears ultimate responsibility for ICT risk management.
DORA	Art. 9(1)	Financial entities shall maintain ICT systems that ensure availability, authenticity, integrity and confidentiality of data.
DORA	Art. 9(3)(d)	Protection against data management risks including encryption of data at rest and in transit.
DORA	Art. 9(4)(d)	Protection measures for cryptographic keys including lifecycle management.
RTS 2024/1774	Art. 6	Financial entities shall develop and document an encryption policy based on data classification and ICT risk assessment.
RTS 2024/1774	Art. 7	Controls to protect cryptographic keys through their lifecycle including replacement in case of compromise.

Figure 3. DORA and RTS 2024/1774 provisions relevant to cryptographic risk management.

The regulatory architecture therefore operates on two levels. Legal requirements under DORA, particularly Articles 5(2), 8, 9(4)(d), and 13(7), define binding obligations on governance, asset identification, cryptographic controls, and technology monitoring. The RTS 2024/1774, by explicitly naming quantum threats and mandating crypto-agility, translates these obligations into concrete supervisory expectations. Together, they create a framework in which banks are expected to begin preparing for PQC migration as part of ICT risk management, operational resilience, and regulatory compliance, rather than treating it as a purely technical upgrade.

3.3 National Strategies and Initiatives

While EU-level regulation sets the overall direction for PQC migration, national strategies and initiatives shape how these objectives translate into practical preparedness at the country level. Beyond DORA, the main EU-level cybersecurity framework relevant to cryptographic practices is the NIS2 Directive [52], which requires Member States to transpose its provisions into national law. Both Estonia and Sweden have done so. Estonia through amendments to the Küberturvalisuse seadus [53] and Sweden through the Cybersecurity Act SFS 2025:1506 [54]. Both legislations include cryptographic practices among minimum security requirements.

For the banking sector, however, DORA operates as *lex specialis* to NIS2. It is directly applicable to financial entities across all Member States and addresses cryptographic resilience more specifically through its regulatory technical standards [10].

National NIS2 transpositions therefore provide a general cybersecurity baseline but do not add PQC-specific obligations for banks beyond what DORA already requires. What the national strategies and initiatives examined below add is the forward-looking dimension, i.e. how each country is positioning itself for quantum-era cryptographic challenges beyond current regulatory obligations.

Estonia

Estonia's Cybersecurity Strategy 2024–2030 explicitly identifies quantum computing as a long-term risk to current cryptographic algorithms and digital infrastructure [55]. The strategy recognises that the arrival of quantum computers poses a potential threat to current cryptographic algorithms, as these computers can solve complex computations much faster than conventional computers, and identifies the development of quantum-resistant cryptographic solutions as a strategic objective. Among its goals for the strategy period, the document lists the maintenance of national information with approved and certified quantum-resistant communications security (including cryptographic) solutions, the establishment of scientific centres of competence for the implementation of cloud technologies and cryptographic solutions to ensure the quantum-resistance of data, and the increase of national knowledge in cryptography. The strategy also notes that Estonia currently lacks independent capability in cryptographic assessment and relies on other

countries' evaluations, which consumes time and entails financial costs.

The most detailed assessment of Estonia's PQC migration challenges comes from Vakarjuk, Snetkov, and Laud [56], who map the cryptographic dependencies of Estonia's e-government ecosystem at CyCon 2024. The study identifies that core national systems such as X-Road, i.e. Estonia's distributed data exchange infrastructure connecting public and private sector information systems, the national ID card, Smart-ID, i.e. a mobile authentication and digital signing solution, Mobile-ID, i.e. a SIM-based mobile authentication and digital signing service, and i-voting all rely on quantum-vulnerable public-key primitives: RSA for encryption and signatures in Smart-ID, the ID card, and X-Road; ECDSA for signatures on the ID card and Mobile-ID; and ElGamal for vote encryption in the i-voting system [56]. This is directly relevant to banks because Estonian banking services are deeply integrated with these systems through X-Road and eID-based authentication. Bank-level PQC migration cannot proceed independently of national infrastructure decisions. The study characterises PQC migration as more challenging than previous cryptographic transitions because post-quantum algorithms offer no drop-in replacements for existing schemes [56]. The Cybernetica whitepaper reinforces this, identifying the transition of interoperability platforms and digital identity systems as challenges that go beyond simple software updates [57].

Estonia published its national PQC migration roadmap on 30 April 2026, prepared by Cybernetica and commissioned by the Ministry of Justice and Digital Affairs [58]. The roadmap assigns organisations to four priority categories based on the sensitivity and confidentiality horizon of the data they process, and places banking in the highest priority category. Earlier preparatory work included a quantum risk assessment of a core national database and an update of the national cryptographic algorithms inventory [57]. Domestic cryptographic evaluation capability is also being established: the VÕIME project, funded through 2026, aims to create a national competence centre for auditing and certifying cryptographic security solutions [59]. Cryptographic research capacity exists at the University of Tartu and Tallinn University of Technology, and private sector expertise is concentrated primarily in Cybernetica [56]. At the same time, the small size and centralised nature of the Estonian ecosystem could be an advantage in coordinating migration, as demonstrated during the 2017 ID card crisis when the national certificate infrastructure

was replaced within months [56].

Estonia participates in the European Quantum Communication Infrastructure (EuroQCI) initiative since October 2020 [60] and in the NordicQCI project (2026–2030), which aims to establish cross-border quantum-secured connections between Estonia and Sweden [61]. These initiatives focus on quantum key distribution (QKD) rather than post-quantum cryptography. As Vakarjuk et al.[56] note, QKD and PQC address different problems: QKD requires custom hardware and protects point-to-point communication, while PQC can be deployed on existing infrastructure. The study concludes that experimenting with and deploying PQC is currently more urgent than building QKD networks.

Sweden

As of the writing of this thesis, Sweden does not have an adopted national quantum strategy. In May 2024, the Swedish government commissioned the Swedish Research Council (Vetenskapsrådet) to develop input for a potential strategy for the period 2025–2030, with a deadline of October 2024 [62]. The commission covers research, education, innovation, commercialisation, and research infrastructure, and explicitly references the European Commission’s white paper on digital infrastructure, which notes that the EU needs to “stand ready for developments in post-quantum technologies and already begin developing quantum-safe digital infrastructure” [62]. Among the aspects to be addressed, the commission lists “the security and defence policy significance of quantum technology” and “the need for network resources for research, innovation and testing within quantum communication” [62]. Notably, however, this document is a government commission to produce a strategy proposal, not the strategy itself. As of mid-2025, the strategy proposal has been delivered but not published or adopted, and no binding national PQC migration roadmap has been published [63]. Separate from the broader quantum strategy, the Swedish National Cyber Security Centre (NCSC), published initial recommendations on the transition to quantum-safe cryptography in May 2025, setting an end-of-2035 migration completion target for most cases and an end-of-2030 target for data with confidentiality horizons of ten years or more [64]. Updated and more detailed national recommendations have been announced for publication during 2026 [64].

Sweden’s quantum technology ecosystem is nonetheless substantial in institutional terms.

Sweden coordinates the NordicQCI project through RISE Research Institutes of Sweden, with participation from Ericsson, Stockholm University, KTH Royal Institute of Technology, and Linköping University [61]. The project, funded under the Connecting Europe Facility with approximately 5 million euros in EU contribution, aims to establish cross-border quantum-secured connections between Estonia and Sweden over submarine cable links, and to integrate Nordic quantum networks with the EuroQCI space segment through an Optical Ground Station in Stockholm [61]. As with Estonia's EuroQCI participation, these initiatives focus on quantum key distribution infrastructure rather than post-quantum cryptographic migration.

The contrast with Estonia is instructive but should not be overstated. Both countries' banking sectors are internationally integrated: two of the four largest banks in Estonia are Swedish-owned subsidiaries, and Estonian banks participate in the same international payment networks (SWIFT, SEPA) as Swedish banks. The structural difference lies in the nature of the national digital infrastructure dependencies.

Estonian banking is embedded in a layered digital ecosystem combining state and commercial components: data exchange runs through X-Road, operated by the Information System Authority (RIA), while authentication relies on the national eID system, whose certificates are issued by two qualified trust service providers. SK ID Solutions AS, jointly owned by Telia, SEB, and Swedbank, has historically issued certificates for Estonian eID and continues to support the legacy IDEMIA platform until existing certificates expire in November 2030. Since 17 November 2025, Zetes Estonia OÜ, the Estonian subsidiary of Belgian Zetes SA, issues certificates for the new Thales-manufactured ID-cards under a 10-year contract awarded by the Police and Border Guard Board, and e-services must support both certificate chains in parallel during the transition. PQC migration therefore depends on coordinated action across RIA, a bank-owned certificate authority (SK ID Solutions), and a foreign-owned commercial certificate authority (Zetes Estonia), none of which an individual bank can unilaterally control.

In Sweden, the equivalent authentication infrastructure is BankID, a PKI-based electronic identification system operated by a consortium of Swedish banks through Finansiell ID-Teknik BID AB [65]. BankID uses certificate-based two-factor authentication and is used by over 99% of the adult population for banking, government services, tax filings,

and digital signatures [65]. The mobile payment system Swish, operated by Getswish AB and used by 8.8 million people as of early 2025 [66], relies on BankID for transaction authentication.

The difference between Sweden and Estonia is not bank involvement (bank-owned certificate authorities exist in both) but the absence in Sweden of a state-operated interoperability platform like X-Road. PQC migration of Swedish authentication therefore depends on coordinated action within the BankID consortium, without the additional national infrastructure layer that Estonian banks face.

Swedish banks also rely less on a single national interoperability platform comparable to X-Road and more on cross-border vendor ecosystems and international payment infrastructures such as Target2 and SWIFT.

This structural difference shapes the migration challenge in each country. For Estonian banks, the binding constraint is national infrastructure coordination: even an internally ready bank cannot migrate if X-Road signatures, eID certificates, and Smart-ID keys remain on classical algorithms. For Swedish banks, the binding constraint is vendor and ecosystem coordination across international standards bodies, technology vendors, and cross-border regulatory frameworks, compounded by the organisational complexity of large, multi-jurisdictional banking groups. In the absence of a national PQC migration strategy, Swedish banks are guided primarily by DORA and EU-level frameworks when assessing quantum-related cryptographic risks.

Implications for PQC Migration

Both Estonia and Sweden recognise quantum computing as a future cybersecurity risk and participate in European quantum technology initiatives. However, neither country currently mandates PQC migration through binding national legislation, and neither has published a comprehensive national PQC migration roadmap. Estonia is further advanced in identifying the specific PQC migration challenges for its national digital infrastructure, reflecting both the depth of its e-governance integration and the availability of domestic expertise. Vakarjuk, Snetkov, and Laud have mapped the cryptographic dependencies of Estonian e-government systems and identified key migration obstacles [56]. Cybernetica, commissioned by the Ministry of Justice and Digital Affairs, published the national PQC

transition roadmap in April 2026, covering digital identity, X-Road, and public e-services and assigning banking to the highest priority category [58].

For the banking sector, this means that PQC migration planning is shaped not only by EU regulation and industry frameworks, but also by national digital infrastructure dependencies. In Estonia, the deep integration of banking services with X-Road and the national eID system means that bank-level PQC migration cannot proceed independently of national infrastructure decisions. In Sweden, the greater organisational complexity and international integration of the banking sector means that migration timelines will be influenced by cross-border coordination requirements and vendor ecosystem readiness. The regulatory and policy environment for PQC migration therefore operates as a multi-level framework in which EU policy sets the strategic direction, sectoral regulation establishes operational resilience requirements, and national strategies and infrastructure dependencies shape practical implementation at the bank level.

4 Research Methodology

4.1 Research Objective and Scope

The objective of the thesis is to assess the current level of PQC readiness in the banking sector and to develop practical recommendations for PQC migration. The recommendations are based on the analysis of online questionnaire, semi-structured interviews with security and ICT risk professionals, and regulatory and industry source. The recommendations address governance, cryptographic visibility, technical dependencies, crypto-agility, migration planning, and regulatory alignment. The aim is to provide practical guidance to support banks in improving their readiness for the transition to post-quantum cryptography.

The thesis addresses five research questions. RQ1 examines the awareness of banking professionals regarding quantum computing threats and post-quantum cryptography. RQ2 investigates how banks are integrating quantum-related risks into their enterprise risk management and governance structures. RQ3 assesses the current stage of banks' PQC migration efforts, including cryptographic inventory, project planning, and pilot implementations. RQ4 identifies the factors that facilitate or hinder banks' preparedness for PQC, such as regulation, vendor support, budget, and expertise. RQ5 addresses the migration steps, organisational preconditions, and common pitfalls specific to the banking sector.

The scope of the thesis covers organisational, strategic, and regulatory aspects of PQC readiness. The thesis does not include technical audits of cryptographic implementations, system-level vulnerability assessments, or mathematical evaluation of cryptographic algorithms. The focus is on governance, risk management, migration planning, and organisational preparedness.

4.2 Research Design, Target Group and Data Collection

This thesis uses a qualitative research design to assess post-quantum cryptography readiness in the banking sector. The research focuses on organisational preparedness, governance, risk

management, and migration planning rather than technical cryptographic implementation.

The thesis focuses on licensed banks in Estonia and Sweden. Estonia and Sweden were selected because they operate under the same EU regulatory framework but differ markedly in market size, banking-sector structure, and digital infrastructure maturity. Estonia represents a digitally advanced small EU Member State, where a concentrated banking market and highly centralised e-government infrastructure create relatively short decision chains and enable coordinated cryptographic changes across public services and banks [55]. Sweden, by contrast, has a larger and more diversified banking sector dominated by a few systemically important banks with extensive cross-border activities and complex infrastructures [67].

This contrast is analytically important for PQC readiness, as in a small, highly digitalised market like Estonia, PQC migration may be shaped by central coordination, shared digital identity solutions, and tight integration between government and banks, whereas in a larger and more mature market like Sweden, migration must consider large banks dominating the market, international operations, and many different IT systems [11] [36].

Estonia has eight licensed credit institutions according to the Estonian Financial Inspectorate as of 4 March, 2026, and representatives from these institutions were approached through Information Security Committee within the Estonian Banking Association. Swedish banking system is diverse, comprising commercial banks, savings banks, cooperative banks, credit market companies and branches of international banks according to the Sweden's Central Bank as of 4 March, 2026, the market is dominated by four universal banks that also lead technological advancements. Representatives from major banks were approached Banks Security Committee within Finance Sweden.

The primary data for this thesis was collected using two methods: an anonymous online questionnaire followed by semi-structured interviews.

The questionnaire was distributed through the mailing lists of two industry working groups: the Information Security Committee of the Estonian Banking Association and the Bank Security Committee of Finance Sweden. The questionnaire consisted of 22 questions. The questionnaire collected information on awareness and understanding of quantum-related risks and PQC, current use of cryptography and cryptographic dependencies,

governance and risk management integration, migration planning and crypto-agility measures, organisational and vendor dependencies, and perceived regulatory drivers and barriers affecting post-quantum cryptography migration. The questionnaire was distributed on 3 March 2026 and responses were collected anonymously throughout the whole month. Five responses were received: two from Estonia, two from Sweden, and one indicating multi-country operations. Only responses from Estonia and Sweden were included in the analysis, while the response indicating multi-country operations was excluded. As an equal number of responses was received from both countries, the sample was considered sufficient to allow a cross-country comparison.

In addition to the questionnaire, semi-structured validation interviews were conducted with a separate group of practitioners who did not participate in the questionnaire. The purpose of the interviews was to validate the practical PQC migration framework proposed in Chapter 7 against practitioner judgement and to identify any practical adjustments needed before the framework could be considered usable in a banking context. The interviews followed a semi-structured format with open-ended questions covering each step of the proposed framework. Each interview lasted approximately 30 minutes and was conducted via video call.

Interviews were conducted with security professionals who are members of the Information Security Committee and the Bank Security Committee within the Estonian Banking Association and Finance Sweden, respectively. For both countries, 2 interviews were conducted one with representative from operational information security function in the first line of defense and second interview with ICT risk representative from operational risk functions in the second line of defense, to ensure both first line and second line perspectives.

Interviewees did not provide written consent to be quoted, and for this reason interview material is not used as a source of empirical data in Chapter 5 or Chapter 6. The validation outcome and the practical adjustments incorporated into the final framework are reported in aggregate form in Section 7.7.

The combination of these methods allowed collection of structured comparable data on PQC readiness through the questionnaire and practitioner validation of the proposed migration framework through the interviews. The research design allows comparison between Estonia

and Sweden and supports assessment of differences in PQC readiness between the banks in two countries.

4.3 PQC Readiness Assessment Framework

PQC readiness in the banking sector is assessed in five dimensions: awareness and risk perception (addressing RQ1), governance and risk management integration (RQ2), cryptographic dependencies and migration planning (RQ3), crypto-agility (contributing to RQ3 and RQ5), and external drivers and barriers (RQ4). RQ5 is addressed through synthesis across all dimensions and forms the basis of the practical migration framework presented in Chapter 7. The PQC readiness assessment is not a maturity model nor does it provide the overview of the technical cryptographic implementation but is an analytical structure for analysis on whether and how banks are preparing for the transition to PQC.

These dimensions were derived from a synthesis of available PQC migration guidance, regulatory frameworks, and industry recommendations.

Awareness and risk perception reflects the consistent emphasis across the BIS quantum-readiness roadmap and the WEF/FCA white paper on awareness and understanding as the necessary starting point for any migration effort [11] [68] [12].

Governance and risk management integration draws on DORA and CDR 2024/1774, which require ICT risk management frameworks with clear responsibilities and board-level reporting [10] [69], and on both the BIS roadmap and the FS-ISAC crypto-agility framework, which identify governance structures and executive accountability as core components of quantum readiness [68] [22].

Cryptographic dependencies is grounded in the convergent position across NIST SP 1800-38, FS-ISAC, and BIS Papers No. 158 that cryptographic discovery and inventory is a foundational prerequisite for migration planning, as well as in CDR 2024/1774 Article 6, which requires encryption and cryptographic control policies based on data classification and risk assessment [22] [68] [69].

Migration planning and crypto-agility reflects the phased migration roadmaps proposed by BIS and FS-ISAC, the maturity levels defined by the PKI Consortium PQC Maturity

Model, and the argument advanced by Sikeridis et al. that enterprise-level cryptographic agility requires architectural capabilities beyond simple algorithm substitution [11] [22] [70] [38].

External drivers and barriers captures the regulatory and policy environment analysed in the earlier sections of this thesis, including binding obligations under DORA, non-binding policy expectations from the European Commission PQC Recommendation and the NIS Cooperation Group roadmap, and the WEF/FCA report's identification of regulatory fragmentation and coordination challenges as factors shaping the pace of migration [10] [69] [14] [15] [12].

Readiness within each dimension is characterised qualitatively on the basis of questionnaire responses. As it is not a maturity scoring, the assessment does not assign numerical scores or maturity levels to individual institutions. Instead, it identifies the stage of preparedness observed in each country context and interprets these findings against the expectations established in the regulatory and policy sources discussed in Section 4.1.

This approach is appropriate because PQC migration in the banking sector is at an early stage; and because the research is based on a small number of respondents per country only.

The same five-dimensional structure is used to organise the results analysis chapter.

4.4 Limitations

This thesis has several limitations that should be considered when interpreting the results.

The empirical sample is small. The thesis analyses four usable questionnaire responses and responses from four semi-structured interviews across two countries. The findings are not statistically representative of the Estonian or Swedish banking sectors and cannot support claims about the specific readiness levels in banking sectors in either of the country. However, the research does not aim for statistical generalisation. The purpose is to identify patterns, gaps, and qualitative differences in PQC readiness between two contrasting EU banking markets at an early stage, and to propose practical PQC migration framework for banks.

The research relies on self-reported information from questionnaire responses and interviews.

The responses reflect the knowledge and perspectives of the respondent and may not fully reflect the actual situation in each bank. Respondents may overstate their organisations preparedness, understate uncertainty, or lack visibility into areas outside their immediate function. The deliberate inclusion of both first line of defence and second line of defence perspectives in the interviews partially addresses this risk by capturing complementary viewpoints of different parts of the organisations.

The thesis focuses on organisational, governance, and regulatory aspects of post-quantum cryptography readiness and does not include technical audits or technical assessment of cryptographic implementations or system architectures. As a result, the findings reflect reported preparedness rather than verified technical capability.

The research is cross-sectional and reflects the situation at a specific point in time. Regulatory developments, quantum computing progress, and post-quantum cryptography standards are evolving, and readiness levels will change. Findings that characterise the current state may have limited temporal validity.

Finally, the thesis focuses on Estonia and Sweden, and the findings cannot be directly generalisable to other jurisdictions.

Despite these limitations, the thesis provides insight into PQC readiness and supports the development of practical recommendations for PQC migration in the banking sector and supports the development of a practical PQC migration recommendations.

4.4.1 Ethical considerations

Participation in both the questionnaire and the interviews was voluntary. Questionnaire respondents were informed of the research purpose and the anonymity of their responses before completing the survey. No personally identifiable information was collected through the questionnaire.

Interview participants were recruited directly by the author and were therefore not anonymous. Each participant was informed of the research purpose and interview format before agreeing to participate. To protect confidentiality, interview responses are reported anonymously. No names or organisational affiliations are disclosed in this thesis. All

collected data was stored securely and used exclusively for the purposes of this research.

5 Findings on PQC Readiness in the Banking Sector

This chapter presents the findings from the questionnaire, organised according to the five readiness dimensions established in Section 4.3: awareness and risk perception, governance and risk management integration, cryptographic dependencies, migration planning and crypto-agility, and external drivers and barriers. For each dimension, findings from the Estonian and Swedish respondents are presented and compared. The chapter concludes with a cross-country comparison of the main patterns observed. The principal findings are:

- **Awareness and risk perception.** All respondents consider PQC migration at least moderately urgent, but this awareness has not translated into operational urgency. Threat timeline estimates range from five to fifteen years, and two respondents lack a defined data confidentiality horizon, preventing meaningful assessment of store-now-decrypt-later exposure.
- **Governance and risk management integration.** Quantum risk has been recognised but not formally addressed in any respondent's enterprise risk management framework. PQC remains primarily an IT and security matter; board-level engagement is largely absent.
- **Cryptographic dependencies.** Two distinct findings emerged. First, on *cryptographic inventories*: all four respondents indicated that a cryptographic inventory is either underway or planned, and all reported intending to identify systems with long confidentiality requirements. No respondent reported a completed inventory, and open-ended responses indicate that PQC migration is consistently sequenced behind other cryptography-related projects expected to ease the eventual transition. Practical guidance on performing cryptographic inventories and asset discovery was identified by all respondents as the most useful form of external support. Second, on *vendor dependence*: three of four respondents reported significant or moderate dependence on external software and hardware vendors for cryptographic infrastructure. Hardware security module (HSM) vendors emerged as a particular structural constraint, with respondents observing that PQC support among HSM vendors lags

behind that of software vendors. Banks cannot resolve this dependency unilaterally; broader industry estimates suggest widescale availability of quantum-safe HSMs is not expected before 2035–2040.

- **Migration planning and crypto-agility.** All respondents have draft migration plans but none has started formal implementation. The Estonian respondents have identified specific NIST algorithms (ML-KEM, ML-DSA); the Swedish respondents have not yet selected algorithms. Crypto-agility is not yet embedded as an operational capability: three of four respondents place it at most at the level of "considered but not incorporated into planning or governance", with only one Estonian respondent reporting it as integrated. This indicates that the structural ability to replace algorithms, rather than just keys, has not yet been built into existing encryption policies despite being a requirement under RTS 2024/1774 Article 6(4).
- **External drivers and barriers.** Vendor readiness and competing organisational priorities are the most cited barriers. All respondents identified formal regulatory requirements and production-ready PQC standards as the factors most likely to trigger investment. Banks in both countries are waiting for a combination of regulatory push and vendor readiness before committing to active migration.

5.1 Awareness and Risk Perception

All four respondents consider PQC migration at least moderately urgent. One respondent from Estonia and both respondents from Sweden rated the urgency as moderate, while the second Estonian respondent rated it as slightly urgent. No respondent considered migration either not urgent or extremely urgent. This suggests that both markets have a basic level of awareness, but the sense of urgency is still lower than expected given recent BIS and ENISA policy guidance calling for immediate action.

Perceptions of the quantum threat timeline differ between the two countries. Both Swedish respondents estimate that quantum computers will be able to break commonly used public-key cryptography within five to ten years. The Estonian respondents diverge. One indicated a timeline of ten to fifteen years, while the other reported not being aware of this information. This difference within Estonia is notable, as it suggests uneven awareness even in a small and concentrated banking market.

Closely related to the threat timeline is the question of how long data must remain confidential, as this determines an organisation's exposure to store-now-decrypt-later attacks. If the combined period of data confidentiality and expected migration duration exceeds the estimated time until a cryptographically relevant quantum computer becomes available, the organisation is already within its risk window. On this question, the responses were mixed. One Swedish respondent reported a maximum confidentiality requirement of more than ten years and one Estonian respondent reported five to ten years. The remaining two respondents indicated that their organisation either has no clearly defined maximum confidentiality period or that they were not aware of one. This is a significant gap and without a defined data confidentiality horizon, institutions cannot meaningfully assess whether they are already exposed to harvest-now-decrypt-later risk, which is the primary argument for beginning PQC migration before a quantum computer is operational.

Respondents were also asked to identify the most significant impacts if their organisation's cryptographic mechanisms were compromised or became unreliable. All four respondents selected disruption of interbank communication or payment processing, regulatory non-compliance and supervisory findings, and operational disruption or service unavailability. Three respondents identified loss of confidentiality of customer or transaction data, inability to authenticate users, systems, or transactions, and disruption of online banking or customer-facing services. The Swedish respondents both selected all available impact categories, including financial losses and reputational damage, while the Estonian respondents were more selective. No respondent selected "limited or no immediate impact." The breadth of impacts identified across both countries indicates that respondents understand the pervasive role of cryptography in banking operations and recognise that a cryptographic compromise would not be a narrow technical incident but a systemic disruption affecting operations, compliance, and trust.

Familiarity with key concepts varies across respondents and between countries. Store-now-decrypt-later attacks, was the most consistently recognised concept. All four respondents reported that this concept is at least considered within their organisation, with one Estonian respondent indicating it has been incorporated into planning or governance. However, other concepts showed weaker integration. The distinction between quantum computing and post-quantum cryptography was only "known but not formally considered" or "considered

but not incorporated into planning or governance" across all four respondents, suggesting that while the general quantum risk narrative has reached banking professionals, the specific technical and strategic implications of PQC have not yet been fully internalised.

Crypto-agility showed a noticeable difference between countries. One Estonian respondent reported that crypto-agility had been incorporated into planning or governance, while the other reported it as only "known but not formally considered". Both Swedish respondents placed crypto-agility at the intermediate level of "considered but not incorporated into planning or governance".

Overall, the findings suggest that awareness of the quantum threat exists in both Estonian and Swedish banks, but this awareness has not yet translated into a strong sense of operational urgency. The Estonian respondents showed somewhat wider variation in both threat timeline perception and concept integration, while the Swedish respondents displayed more consistent awareness across all assessed concepts.

5.2 Governance and Risk Management Integration

All four respondents reported that quantum-related cryptographic risk has been "recognised but not yet formally addressed" within their enterprise risk management frameworks. This uniform finding indicates that across both countries and across institutions of different sizes and structures, quantum risk has entered organisational awareness but has not yet been integrated into formal risk registers or subjected to structured risk assessment processes.

The internal groups involved in PQC migration differ between countries. Both Swedish respondents identified IT and security operations alongside risk management as involved functions, with one also including legal and compliance. The Estonian respondents diverged. One reported involvement limited to IT and security operations and risk management, while the other identified a broader set including executive leadership, legal and compliance, and procurement and vendor management. This broader involvement in one Estonian institution may reflect the smaller organisational structures typical of the Estonian banking sector, where cross-functional coordination can occur more readily, or it may indicate a more advanced stage of governance planning in that particular institution.

Neither country showed consistent board-level or executive engagement with PQC as

a strategic issue. While one Estonian respondent included executive leadership among involved groups, the responses overall suggest that PQC remains primarily an IT and information security matter rather than a governance issue elevated to senior management attention. This contrasts with the recommendation in BIS Papers No. 158 to designate a lead executive for quantum readiness and with the FS-ISAC framework, which identifies executive accountability as a core component of any crypto-agility programme.

5.3 Cryptographic Dependencies

Understanding where cryptography is used and what depends on it is a prerequisite for migration planning. The responses reveal both commonalities and differences in how banks approach this issue.

All four respondents reported that their organisation uses cryptography in multiple areas, though the level of specificity in responses varied. Both Swedish respondents noted that cryptography is used in all of the listed areas indicating that cryptography pervades their operations. The Estonian respondents were more selective. One identified authentication and digital signatures as the primary area, while the other identified customer data protection at rest. This selectivity may reflect either narrower cryptographic use or, more likely, a narrower interpretation of the question.

Regarding cryptographic inventory, all four respondents indicated that performing a cryptographic inventory is either underway or planned. With this topic, the open-ended responses add important context. One Estonian respondent explained that PQC migration "is considered within the long-term plan but is postponed in the immediate future due to focus on other cryptography-related projects, which will ease the migration process". The same respondent noted that migration is also delayed by "lack of ready hardware solutions," observing that while some software vendors support PQC algorithms, "this is less of a case with HSM vendors." One Swedish respondent noted that because preparation is still at an early stage, "the information and plans are not widely shared within the organisation," making it difficult to assess all aspects of readiness. These responses suggest that even where banks have begun preliminary planning, PQC migration is not yet an active priority and is sequenced behind other cryptographic initiatives or constrained by vendor readiness.

Vendor dependencies emerged as a prominent theme. Two of the four respondents reported significant dependence on external software vendors for cryptographic infrastructure, one reported moderate dependence, and one responded “do not know”. The HSM vendor constraint identified by the Estonian respondent above is consistent with the broader evidence on hardware vendor readiness. Cryptomathic reports that many HSMs, TLS libraries, and database encryption tools “do not yet support PQC,” and that some solutions marketed as quantum-safe rely on “proprietary schemes that may not align with official standards” [71].

While nearly all HSM vendors now offer PQC algorithm libraries, only one vendor has commercially launched HSMs with a quantum-safe architecture, and widescale support for quantum-safe HSMs is not expected until 2035 to 2040 [72]. The UK National Cyber Security Centre corroborates this timeline, noting that PQC-capable HSMs are expected to become available only in late 2025, with hardware acceleration following in 2026 to 2027 [73]. This creates a dependency that individual banks cannot resolve unilaterally: a bank’s migration timeline is bounded by the pace at which its HSM vendors release certified PQC-capable products.

5.4 Migration Planning and Crypto-Agility

All four respondents reported the same migration stage whereby they have a draft PQC migration project plan but have not yet started a formal migration project. This uniform finding positions all respondents in an early preparatory phase, i.e. past initial awareness but before active implementation.

Despite this shared stage, the planned timelines differ. Two respondents (one from each country) plan to begin migration within the next twelve months, while the other two (also one from each country) plan to begin within two to three years. No respondent indicated a timeline beyond three years, and no respondent reported having no plan. The cross-country pattern here is symmetric rather than divergent, i.e. both Estonia and Sweden contain one institution planning near-term action and one planning on a longer horizon.

Regarding documented migration plans, two respondents (again one from each country) reported having a preliminary plan, while the other two reported planning to develop one.

No respondent has a detailed plan with inventories, milestones, budgets, and governance fully specified. This is consistent with the draft-stage positioning reported above and suggests that migration planning has not yet progressed to the level of specificity that DORA’s requirements for ICT change management and project governance would expect for a major technology transition.

The migration steps taken or planned vary, as summarised in Figure 4.

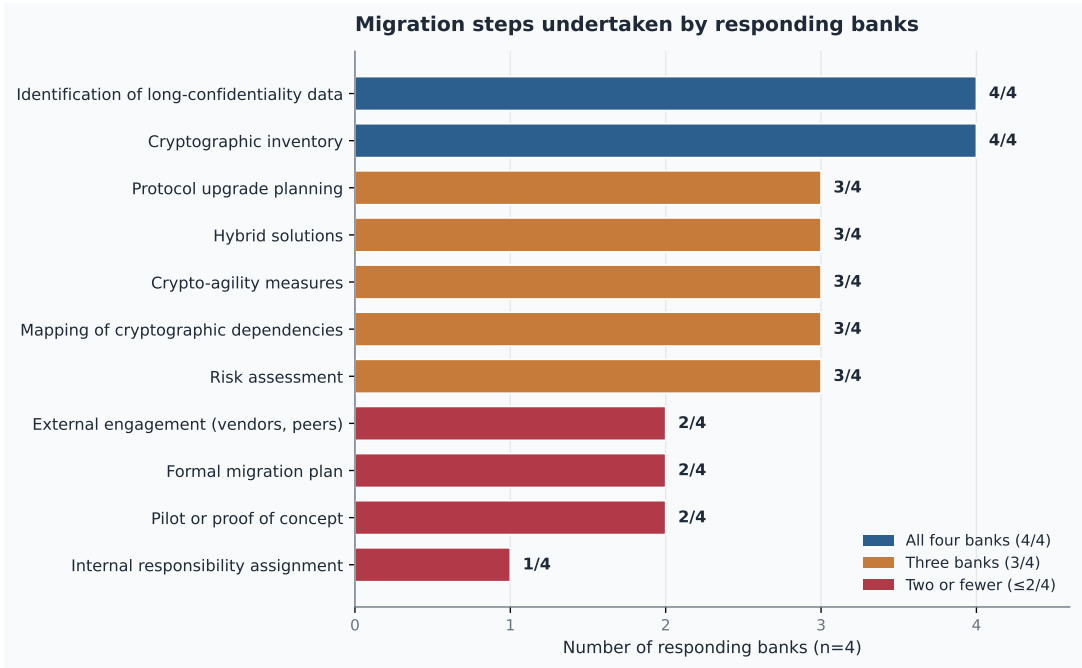


Figure 4. Migration steps undertaken by the four responding banks. Counts are aggregated from the questionnaire and indicate the number of banks that reported having taken each step. Diagnostic actions (cryptographic inventory, identification of long-confidentiality data) are universal, while governance and execution steps (formal migration plan, pilot, internal responsibility assignment) are reported by only half of respondents or fewer.

All respondents reported planning or conducting cryptographic inventories and identifying systems with long confidentiality requirements. Beyond this common baseline, the Estonian respondents showed a wider range of planned activities. One Estonian respondent selected nearly all available migration steps, including assigning internal responsibility, introducing crypto-agility measures, evaluating hybrid solutions, upgrading cryptographic protocols, and starting pilot migration. The other Estonian respondent selected a narrower set focused on inventory, long-confidentiality identification, and dependency assessment. The Swedish respondents fell between these extremes, with both reporting planned crypto-agility measures, hybrid solution evaluation, and enterprise risk assessment, and one also reporting

pilot migration and engagement with external standards bodies.

On PQC algorithm selection, the two Estonian respondents have identified specific NIST standards naming ML-KEM (CRYSTALS-Kyber) and ML-DSA (CRYSTALS-Dilithium) as algorithms they plan to use, although one also noted that "no PQC standards selected yet" alongside these selections, suggesting the choice is preliminary. Neither Swedish respondent has selected specific PQC algorithms. This may reflect a difference in technical specificity of planning between the two markets, or it may reflect the Swedish respondents' observation that PQC planning is still in early stages and not yet widely shared within their organisations.

Prioritisation approaches differ. The Swedish respondents consistently prioritised based on regulatory urgency and classification as critical infrastructure, with one also including data sensitivity. The Estonian respondents' approaches differed. One prioritised based on high-risk and high-value assets, while the other focused on regulatory urgency and technical feasibility. Data sensitivity as a prioritisation criterion, which is directly relevant to store-now-decrypt-later exposure, was explicitly identified by only one Swedish respondent.

5.5 External Drivers and Barriers

The most frequently cited barrier across both countries was dependence on vendors to provide PQC-ready solutions. This response was selected by three of the four respondents. Competing priorities within the organisation was the second most common barrier and was also cited by three respondents. These findings are consistent, meaning that if migration depends on vendor readiness and competes with other organisational priorities, the result is the preparatory-but-waiting posture observed across all respondents.

Unclear or evolving regulatory guidance was cited as a barrier by both the second Estonian and the first Swedish respondent, suggesting that the current absence of explicit PQC requirements creates uncertainty that slows rather than accelerates preparation. Lack of internal expertise or skills was cited by one respondent from each country. One Swedish respondent answered "do not know" to the barriers question, noting that because PQC preparation is still at an early stage, it was difficult to assess which obstacles are most significant.

The open-ended responses provide additional context for barriers. The Estonian respondent who offered the most detailed response explained that PQC migration "is postponed in the immediate future due to focus on other cryptography-related projects, which will ease the migration process". This explicitly identifies competing cryptographic priorities as a deferral mechanism. The same respondent identified HSM vendor unreadiness as a specific technical bottleneck. The Swedish respondent who provided an open-ended response noted the difficulty of assessing readiness when "the information and plans are not widely shared within the organisation," pointing to an internal transparency and communication gap that compounds the early-stage challenge.

The factors that respondents identified as most likely to encourage PQC investment are similar. All four respondents selected formal regulatory requirements or supervisory deadlines and availability of production-ready, widely supported PQC standards and implementations as key drivers. Three respondents also selected pressure from customers or business partners. Two respondents identified demonstrated financial benefits or cost savings.

As Figure 5 illustrates, banks in both countries are waiting for a combination of regulatory push and vendor readiness before committing to active migration. This aligns with the analysis in Section 3. DORA and its delegated acts create forward-looking obligations relevant to cryptographic risk, but the absence of explicit PQC requirements means that the regulatory signal remains indirect for the banks.

When asked what would help accelerate migration, three of the four respondents selected clearer regulatory guidance and compliance timelines. One Estonian respondent selected vendor roadmaps or product availability timelines instead, consistent with that respondent's emphasis on hardware vendor dependencies as the binding constraint.

Regarding knowledge and capability needs to improve preparedness, all four respondents identified guidance on performing cryptographic inventories and asset discovery as beneficial, and three selected case studies or white papers on successful PQC migrations. Participation in industry working groups and external consultancy support were also frequently selected, particularly by the Swedish respondents. This demand for practical guidance and peer learning suggests that while awareness exists, institutions lack the

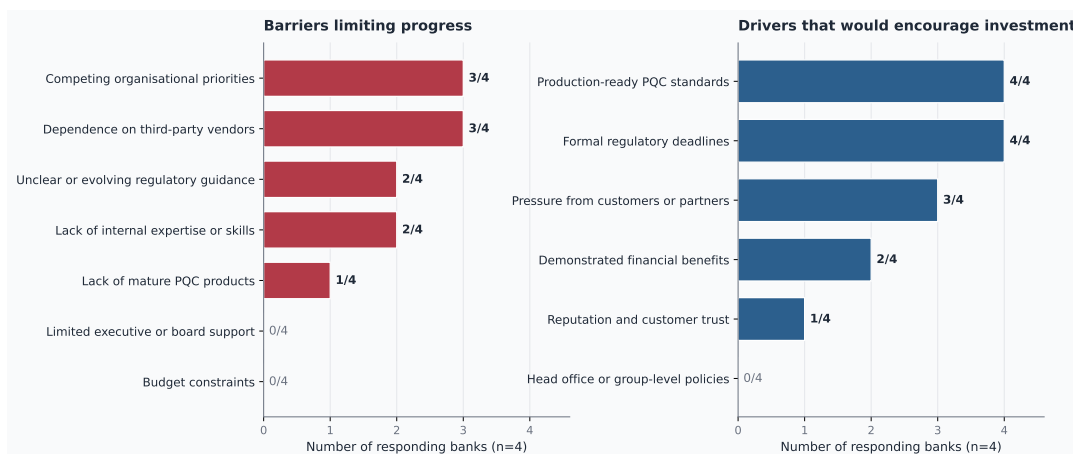


Figure 5. Barriers limiting progress towards PQC migration (left) and drivers that would most encourage investment (right), as reported by the four responding banks. Budget constraints and limited executive support are not identified as barriers by any respondent, whereas formal regulatory deadlines and the availability of production-ready PQC standards are the strongest reported drivers.

operational know-how to translate awareness into action. This could reveal a gap that industry bodies and supervisory authorities could address.

Self-assessed internal knowledge sufficiency varies. One Estonian respondent rated knowledge as "mostly sufficient," one Swedish respondent rated it as "adequate," and the remaining two respondents (one from each country) rated it as "somewhat insufficient." No respondent rated knowledge as fully sufficient or not sufficient at all. The overall picture is one of partial capability, meaning that banks have some internal expertise but do not consider themselves fully prepared to execute PQC migration independently.

6 Interpreting Readiness and Gaps

This section analyses the findings from the questionnaire and interviews by comparing them against prior studies of PQC readiness in the financial sector, including the BSI/KPMG market survey [19], the Dutch banking sector study by Onkenhout [74], and the GRI executive perspectives report [21]. The comparison positions the Estonian and Swedish findings within the broader state of banking sector readiness and identifies the structural challenges that inform the migration framework proposed in Chapter 7.

6.1 Is the Banking Sector Prepared?

The banking sectors shows an adequate level of awareness. All respondents consider PQC migration at least moderately urgent, all recognise that a cryptographic compromise would cause systemic disruption affecting operations, regulatory compliance, and trust, and store-now-decrypt-later attacks are understood as a relevant threat across both countries. The quantum risk narrative has reached banking professionals, and the topic is no longer unfamiliar to information security and risk functions. This finding is consistent with the BSI/KPMG market survey, in which 96 percent of respondents rated the relevance of quantum-safe cryptography as high or very high, and 71 percent agreed that specific cryptographic schemes will be broken once quantum computers reach widespread use [19]. Similarly, in a study of Dutch banking specialists, all eleven participants were fully aware of the quantum threat [74].

Awareness has not yet translated into planning. All four respondents report having a draft PQC migration project plan, and all indicate plans to begin migration within three years. However, these plans remain at a preliminary stage. No respondent has a detailed plan with inventories, milestones, budgets, and governance fully specified. Two respondents are still planning to develop a plan rather than having one in place. This is consistent with the Dutch banking sector study, in which no bank had completed a full organisation-wide PQC migration plan despite strong collaborative structures through the Dutch Banking

Association and De Nederlandsche Bank [74]. The Swiss Bankers Association similarly noted that while NIST published its first three PQC standards in 2024, banks must now begin the process of transitioning to these standards suggesting that even in well-resourced banking markets, active migration has not yet begun[11].

Banks treat PQC migration as a technical IT task rather than a governance and risk management challenge. In practice, this means that cryptographic transition is often left to technical teams, such as security or infrastructure teams, and has not (yet) been elevated to the highest executive levels with executive sponsorship or dedicated project and budget. According to the GRI 2025 report, the financial institution leaders acknowledged that quantum risk is "not in my top five or not even top ten when I present to the board or to the executive leadership" [21]. The BSI/KPMG survey illustrates this gap by presenting that only 25 percent of organisations had included the quantum threat in their risk management frameworks, while 61 percent had not, despite 65 percent rating the risk to their own data as high or very high [19]. Meanwhile, the FS-ISAC working group recommends that institutions address this by establishing a dedicated PQC steering committee with clear governance structures, timelines, and regulatory alignment [22]. This disconnect mirrors the finding in this thesis that quantum risk has been recognised but not yet formally addressed across all four respondents.

No respondent has started a formal migration project. All four are past awareness but not yet implementing, situated in what Baseri et al. call the pre-migration stage, characterised by cryptographic asset discovery, quantum risk assessment, and policy development [33]. Yet the AIVD/CWI/TNO PQC Migration Handbook[75] classifies financial organisations as urgent adopters who should begin migration now, given their handling of personal data and role in critical infrastructure. Against this classification, the banks surveyed in this thesis are aware of the threat but have not yet begun migrating, which represents a notable delay.

Inventories are incomplete, visibility is lacking, and this creates a timeline problem. All respondents report cryptographic inventory work as underway or planned, but in practice this work remains preliminary. Open-ended responses suggest it is embedded within broader cryptographic hygiene initiatives rather than dedicated PQC programmes. One Estonian respondent described PQC migration as "postponed in the immediate future due to

focus on other cryptography-related projects," and one Swedish respondent acknowledged that PQC-related "information and plans are not widely shared within the organisation." A similar pattern was found in the Dutch banking sector, where eight of eleven specialists reported inventories underway but none had achieved a complete, centralised inventory [74]. Without full visibility into where cryptographic algorithms are used, banks cannot effectively prioritise systems for migration. This is a significant constraint given the expected duration of the transition. The PQC Migration Handbook[75] notes that the migration from SHA-1 to SHA-256 took more than five years for most organisations and that PQC migration is likely to be at least as complex. The BSI/KPMG survey found that organisations expected, on average, to complete migration 6.5 years too late relative to when they believed quantum computers would become a threat [19].

Banks have not assessed whether their hardware can support post-quantum algorithms. The questionnaire responses indicate that banks rely on hardware security modules, payment terminals, and network infrastructure with embedded cryptographic implementations, yet none of the respondents reported having assessed the PQC readiness of their hardware estate specifically. This is a significant gap. The Onkenhout study of Dutch banks found that payment cards, point-of-sale terminals, and ATMs pose "logistical and economic problems" for replacement because PQC algorithms require larger keys that may exceed the processing and storage capacity of existing hardware [74]. The FS-ISAC working group similarly noted that hardware is "often not capable of running PQC algorithms," particularly in constrained environments such as IoT devices and payment infrastructure [22]. ENISA's integration study warns that PQC key sizes are ten to one hundred times larger than classical equivalents, creating real performance and bandwidth constraints that affect protocol message sizes and may lead to "fragmentation, additional round-trips, and a more complicated state-machine" at the network level [36]. For banks, where hardware replacement cycles are long and distributed infrastructure is vast, failure to assess hardware readiness early risks discovering that critical components cannot support post-quantum algorithms only at the point of deployment — by which time the replacement lead time may exceed the available migration window.

The treatment of data confidentiality periods remains a concern. Half of the respondents could not identify a defined maximum period for which their data must remain confidential.

This parameter is essential for applying the Mosca inequality, which compares the sum of data shelf life and migration duration against the estimated time until a cryptographically relevant quantum computer becomes available [2]. Without it, institutions cannot determine whether they are already within their risk window and therefore cannot assess whether their current pace of preparation is adequate. The respondents who did provide estimates, more than ten years and five to ten years, reported timelines that, when combined with realistic migration duration estimates, could place their organisations within or close to the risk window under the threat timelines reported by the same respondents. The BSI/KPMG survey reinforces this concern: 79 percent of respondents expected quantum computers to break current cryptography within ten years, yet only 11 percent believed their organisation could become quantum-safe in time [19].

6.1.1 Compliance With Current Cryptographic Obligations

The five readiness dimensions can be read directly against the provisions summarised in Table 3. The questionnaire and interview evidence supports the following assessment for the surveyed banks.

DORA Art. 5(2) – management body responsibility. Not operationalised for quantum-related cryptographic risk. Only one of four respondents reported executive involvement in PQC migration, and no respondent has integrated quantum risk into the risk management framework approved by the management body. The formal accountability required by Art. 5(2) is therefore in place on paper but has not been exercised for this risk category.

DORA Art. 9(2) – availability, authenticity, integrity, and confidentiality of data. Currently met for classical threats, but the forward-looking dimension of Art. 9(2) is not addressed. None of the respondents has assessed whether existing cryptographic protections will continue to satisfy Art. 9(2) once a cryptographically relevant quantum computer becomes available, and two of four could not identify a defined data-confidentiality period.

DORA Art. 9(3)(d) – protection against data management risks including encryption in transit and at rest. Partially met. Banks rely on TLS, HSM-backed key management, and infrastructure-level encryption, but none has completed a cryptographic inventory at the granularity needed to demonstrate which data flows are protected by which algorithms. This is a prerequisite for showing that Art. 9(3)(d) continues to be satisfied as standards

evolve.

DORA Art. 9(4)(d) – protection of cryptographic keys through their lifecycle. Partially met. Key lifecycle management exists for current algorithms, but no respondent has assessed the PQC readiness of HSMs or other key-handling hardware. The extension of Art. 9(4)(d) to post-quantum keys is therefore not yet evidenced.

RTS 2024/1774 Art. 6 – documented encryption policy based on data classification and risk assessment. Partially met. Encryption policies exist, but Art. 6(4) of the RTS 2024/1774 goes further by requiring that those policies include provisions for updating or changing the cryptographic technology on the basis of developments in cryptanalysis – a concrete crypto-agility obligation, reinforced by Recital 9, which references threats from quantum advancements. Three of four respondents reported that cryptographic agility is at most “considered but not incorporated into planning or governance,” indicating that this expectation has not yet been built into existing encryption policies.

RTS 2024/1774 Art. 7 – key lifecycle controls including replacement in case of compromise. Partially met for compromise of classical keys, but the structural ability to replace algorithms (rather than just keys) – crypto-agility – is not yet embedded. No respondent reported a target cryptographic architecture or an abstraction layer that would allow algorithm replacement without application redesign.

Across the six provisions, the surveyed banks meet the static, classical interpretation of each obligation but do not yet meet the forward-looking interpretation that DORA and RTS 2024/1774 together require in light of quantum-related cryptographic risk. This is the compliance gap that the migration framework in Chapter 7 is designed to close.

6.2 Central Challenges

The findings from Chapters 5 and 6 identify six categories of challenges that constrain PQC readiness in banking. This section synthesises each challenge against the regulatory framework and the literature, and concludes each with a specific action point for banks.

6.2.1 Governance and Executive Ownership

The challenges related to governance and executive ownership are:

1. Only one of the four respondents reported executive involvement in PQC migration; none has integrated quantum risk into their risk management framework.
2. The management body accountability required by DORA Article 5(2) has not been operationalised for quantum related cryptographic risk in any of the banks surveyed.
3. Quantum risk does not reach board level agendas. The GRI 2025 executive perspectives report describes the same pattern: one executive acknowledged that quantum risk is “not in my top five or not even top ten when I present to the board or to the executive leadership” [21].

The regulatory expectation is already in place. DORA Article 5(2) assigns the management body ultimate responsibility for ICT risk management and makes them personally liable for non-compliance [10]. The RTS 2024/1774 goes further: Recital 9 references “threats from quantum advancements,” and Article 6(4) requires documented policies for cryptographic key management that enable adoption of leading practices and standards [69]. These provisions create a binding expectation that banks prepare for quantum related cryptographic risks.

The literature treats governance not as an addition but as a prerequisite. The FS-ISAC framework identifies governance as one of nine core elements for crypto agility and recommends a PQC steering committee [22]. The BIS roadmap recommends designating a lead executive for quantum readiness [68]. Kumar defines governance and policy agility as one of seven pillars of enterprise cryptographic agility [76]. Sikeridis et al. argue that enterprise crypto agility requires policy driven governance with administrative control, orchestrated configuration management, and infrastructure monitoring [38].

Conclusion and action point. The gap between regulatory expectation and observed practice is the most immediate risk. Banks should assign a named member of the management body as accountable for PQC migration under DORA Article 5(2), integrate quantum cryptographic risk into the ICT risk management framework, and establish a PQC steering committee with a mandate that covers governance, vendor coordination, and regulatory alignment. This should be completed before the NIS Cooperation Group

milestone of end of 2026.

6.2.2 Cryptographic Visibility

The challenges related to cryptographic visibility are:

1. None of the respondents has achieved a complete overview of their cryptographic footprint, despite all indicating that cryptography is used across most or all areas of their operations.
2. Cryptographic dependencies in third party components and vendor supplied software are not systematically tracked.
3. Connections to shared infrastructure (SWIFT, payment clearing, national digital identity) are not mapped in terms of the cryptographic protocols they use.

Hasan et al. identify eight obstacles to building cryptographic inventories: complexity arising from thousands of applications, heterogeneous environments mixing legacy and modern systems, lack of visibility into distributed assets, cryptographic dependencies that are difficult to trace, the dynamic nature of IT environments, scale, shortage of specialist skills, and cost [18]. Several of these obstacles are visible in the questionnaire responses.

Mastercard introduces the concept of a Cryptographic Bill of Materials (CBOM), a structured catalogue analogous to a software bill of materials, that documents which algorithms, protocols, keys, and certificates are deployed and where [49]. None of the respondents has undertaken this level of systematic cataloguing.

The regulatory basis for this requirement exists. DORA requires financial entities to identify all information assets and ICT assets, map their configurations and interdependencies, and maintain and periodically update these inventories [10]. The inventory gap therefore represents a potential compliance gap under DORA.

Conclusion and action point. Without a cryptographic inventory, banks cannot assess quantum vulnerability, prioritise migration, or coordinate with vendors. Banks should initiate a CBOM covering all production systems, including third party dependencies and shared infrastructure connections. This is the foundation for every subsequent migration step and should be the first operational priority after governance is established.

6.2.3 Crypto Agility

The challenges related to crypto agility are:

1. Crypto agility integration was inconsistent across respondents; no bank reported a systematic capability to replace cryptographic algorithms without disrupting operations.
2. Hardware based cryptographic infrastructure, in particular HSMs, is not designed for algorithm replacement and may require hardware substitution rather than software updates.
3. The threat extends beyond data confidentiality. The EPC distinguishes two vectors: harvest now, decrypt later (affecting data confidentiality) and harvest now, forge later (affecting digital signatures, digital assets, and central bank digital currencies where private keys control long term ownership) [16].

The regulatory obligation for crypto agility is now explicit. RTS 2024/1774 requires financial entities to have documented policies and procedures for cryptographic key management that enable adoption of leading practices and standards, and to maintain a register of certificates [69]. These are binding requirements. The inconsistent crypto agility reported by respondents represents a gap against these obligations.

The literature frames crypto agility as a continuous competency, not a migration capability. Kumar concludes that enterprise cryptographic agility “is not a one-time migration project” but “a continuous capability — a culture of readiness across people, processes, and technology” [76]. The FS-ISAC defines it as a design principle for implementing, updating, replacing, and adapting cryptography with “no significant architectural changes, minimal disruption, and short transition time” [22]. Sikeridis et al. argue that developer and protocol level notions of crypto agility are insufficient for enterprise transitions and that enterprise agility requires decoupling cryptographic services from applications, policy based configuration management, and infrastructure orchestration [38].

The Cryptomathic Tier 1 bank case illustrates a possible solution. The bank faced hundreds of siloed HSMs, fragmented cryptographic operations, and limited ability to adapt to new standards. Centralising cryptographic management through an abstraction layer reduced deployment timelines from months to weeks, eliminated vendor lock-in across multiple

HSM vendors, and freed budget for quantum safe initiatives [77].

Conclusion and action point. Crypto agility is both a DORA compliance requirement and the architectural foundation for PQC migration. Banks should design their target architecture to decouple cryptographic operations from application logic, support multiple vendors through a service abstraction layer, and enable algorithm replacement without service disruption. The harvest now, forge later vector means that this capability is urgent not only for data at rest but also for digital signature and authentication infrastructure.

6.2.4 External Dependencies

The challenges related to external dependencies are:

1. Three of four respondents reported significant or moderate dependence on software vendors for cryptographic implementations.
2. One respondent identified HSM vendors as a bottleneck: “While some of the software vendors are ready to support PQC algorithms, this is less of a case with HSM vendors.”
3. Banks operate as nodes in shared financial networks (SWIFT, Target2, national digital identity) where migration requires coordinated action across all participants, not individual initiative.
4. The vendor ecosystem remains immature. The FS-ISAC warns that “your crypto agility will be determined by your vendors” [22], and the GRI 2025 report documents that financial institutions perceive “a lack of clear strategies and timelines” from cloud providers [21].

Sikeridis et al. describe the coordination problem: enterprise operators find cryptographic change “daunting exactly because it means corralling hundreds of software providers to support the change and with very little control over the process” [38]. The FS-ISAC adds that “cryptography woven into third-party components is not always apparent, leaving customers blind to related vulnerabilities” [22].

The systemic dimension compounds the vendor problem. The BIS Project Leap experiment tested PQC signatures in the Target2 payment system and required coordination between the BIS Innovation Hub, three central banks, two network service providers, and SWIFT

[68]. The BIS roadmap states that actors not adequately protected “could become weak links, impacting the security of the entire financial system” [68]. In Estonia, the banking infrastructure is embedded within the X-Road data exchange layer connecting over 900 institutions through public key cryptography, and the 2017 ROCA incident demonstrated how a vulnerability in one component cascaded across the entire ecosystem [78].

The WEF/FCA white paper identifies the regulatory dimension of this problem: “the lack of regulatory clarity also hinders vendors’ preparedness and reduces investor confidence in the emerging quantum-safe vendor market” [12].

Conclusion and action point. Banks cannot complete PQC migration unilaterally. They should incorporate vendor PQC readiness into third party risk management under DORA Article 28, pursue vendor diversification and abstraction architectures to reduce concentration risk, and engage in sector coordination through national banking associations and central bank working groups to align migration timelines for shared infrastructure. The Dutch model documented by Onkenhout, where banks coordinate through Bankers’ Association’s quantum readiness groups [74], provides a precedent.

6.2.5 Competing Priorities and Timeline Uncertainty

The challenges related to competing priorities and timeline uncertainty are:

1. Three of four respondents cited competing priorities as a barrier to PQC migration.
2. AI governance has “eclipsed discussion of quantum technologies” at the executive level [21], reducing bandwidth for a threat that has not yet materialised.
3. The quantum threat timeline remains probabilistic: the GRI 2024 survey found that more than half of 32 experts estimated a greater than five percent likelihood of a cryptographically relevant quantum computer within ten years, while approximately one third indicated a likelihood of fifty percent or more [32].
4. Executives want to quantify exposure in monetary terms but cannot do so because the threat timeline is uncertain [21]. Without a quantifiable business case, PQC migration struggles to compete for resources.

The BSI/KPMG survey found that the average organisation expects migration completion to lag the threat timeline by 6.5 years [19]. This gap means that deferral itself creates

risk: if migration takes longer than expected and quantum computing arrives sooner than expected, the overlap period leaves banks exposed.

Conclusion and action point. The probabilistic nature of the threat does not justify inaction because the store now, decrypt later vector creates present-day risk regardless of when a quantum computer arrives. Banks should frame PQC migration not as a response to a future event but as a component of ICT lifecycle management and DORA compliance that is required now. The NIS Cooperation Group milestone of end of 2026 for national roadmaps, inventories, and risk analysis provides a deadline that does not depend on when a quantum computer materialises.

6.2.6 Regulatory Signal Gap

The challenges related to the regulatory signal gap are:

1. Two respondents cited unclear or evolving regulatory guidance as a barrier, suggesting that the specificity of the RTS 2024/1774 provisions on quantum threats has not reached bank level compliance awareness.
2. The European Commission PQC Recommendation is not binding, though it includes an escalation mechanism: the Commission will assess whether “additional steps, including proposing binding acts of Union law, are required” [14].
3. All four respondents identified formal regulatory requirements and supervisory deadlines as the primary factor that would drive PQC investment.

The WEF/FCA white paper confirms this across the broader financial sector: “discussions throughout this work programme have highlighted regulations as a catalyst for prioritising and advancing the transition” [12], and 93 percent of regulatory survey respondents agreed that quantum technologies would have implications for their frameworks. The BSI/KPMG survey found that 96 percent of respondents cited regulatory requirements as the primary driver for PQC investment [19]. Regulation is not one driver among many; it is the driver that banks are waiting for.

Yet the regulatory signal is more specific than banks appear to recognise. DORA and the RTS 2024/1774 together create a concrete obligation to prepare for quantum related cryptographic risks. The gap is not in the regulation itself but in the translation of that

regulation into supervisory practice and bank level compliance awareness.

Conclusion and action point. Banks should not wait for PQC to be named in a binding regulation. The existing obligations under DORA Article 5(2), Article 9, and RTS 2024/1774 (Recital 9, Article 6(4)) already require preparation for quantum related cryptographic risks. Banks should interpret these provisions proactively and begin migration planning now. Supervisory authorities should consider incorporating quantum cryptographic risk into SREP reviews and thematic assessments to close the gap between existing regulation and bank level awareness.

6.3 Cross-Country Comparison

Similarities

The most notable finding is that the two countries are similar. Across the core readiness indicators, Estonian and Swedish banks are at the same stage. All four respondents have recognised quantum risk but not formally addressed it. All four have a draft PQC migration plan but have not started a formal migration project. None has formally integrated quantum risk into their enterprise risk management framework. All four identify regulatory requirements as the primary driver that would encourage PQC investment, and three of the four selected clearer regulatory guidance as the most helpful accelerator.

Both countries operate under the same EU regulatory framework. DORA, the European Commission PQC Recommendation, and the NIS Cooperation Group roadmap apply equally to financial entities in Estonia and Sweden. Since Section 6.2 identified regulation as the dominant driver of PQC action, and both countries face the same regulatory signal, a similar readiness level is to be expected.

Differences

Within this shared overall posture, several differences emerge that reflect structural characteristics of the two banking sectors.

The Swedish respondents reported a shorter threat timeline. Both estimated that quantum computers would be able to break commonly used public-key cryptography within five to ten years. One Estonian respondent estimated ten to fifteen years, while the other was

not aware of this information. This difference may reflect the greater exposure of Swedish banks to international threat intelligence and industry dialogue. The BSI/KPMG survey found that larger organisations tended to have greater awareness of the quantum threat timeline [19], which is consistent with this pattern.

Data confidentiality requirements should in principle be similar, as both countries operate under the same EU data protection and banking regulation. However, the responses varied: one Swedish respondent indicated more than ten years, one Estonian respondent reported five to ten years, and the remaining two respondents in each country could not identify a defined maximum period. This inconsistency likely reflects varying levels of awareness of internal data retention obligations rather than genuinely different requirements. Regardless, the Mosca inequality applies equally: respondents who expect the quantum threat within five to ten years and hold data requiring long-term confidentiality may already be within their risk window [2].

The Estonian respondents have progressed further in technical evaluation: both identified ML-KEM and ML-DSA as their planned PQC standards, and one reported planned migration steps across nearly all available categories. Neither Swedish respondent had selected specific PQC standards yet. This difference reflects the stage of evaluation rather than a divergence in approach ML-KEM and ML-DSA are the NIST-standardised algorithms that the ECCG recommends for EU use [79], and Swedish banks are likely to arrive at the same selection. The Swedish respondents instead emphasised regulatory urgency as their dominant prioritisation criterion, suggesting they are waiting for external signals before making technical commitments.

The concept integration patterns differ as well. One Estonian respondent reported the highest level of integration across the board, with PQC, quantum computing threats, store-now-decrypt-later, and crypto-agility all incorporated into planning or governance. The Swedish respondents showed a more uniform pattern at the "considered but not incorporated" level. This suggests that while one Estonian institution has made more progress in governance integration, the Swedish banks maintain a broader but less formalised awareness. Internal knowledge sufficiency was assessed differently. One Estonian respondent rated internal expertise as "mostly sufficient" and one as "somewhat insufficient." Among the Swedish respondents, one rated it as "adequate" and one as "somewhat insufficient." The Swedish

respondents both emphasised participation in industry working groups and external consultancy as priorities, which may reflect the larger organisational complexity of Swedish banks and the greater difficulty of building PQC expertise in-house across multiple business lines and jurisdictions.

Two Different Banking Ecosystems

The structural differences between the Estonian and Swedish banking sectors provide context for interpreting these findings and suggest that the character of the migration challenge differs between the two countries, even if the current readiness level does not.

Estonia's banking sector is small and concentrated, with eight licensed credit institutions and total assets of approximately 31 billion euros. It is deeply embedded in the national digital infrastructure, built from the 1990s under a principle of modular, distributed, and interoperable design [80]. Estonian banks operate within a digital ecosystem built on X-Road, a public-key infrastructure connecting over 900 institutions, and the national eID system used for banking authentication [78]. This creates a distinctive form of systemic dependency: PQC migration for Estonian banks cannot proceed independently of the national digital infrastructure migration. The Cybernetica assessment found that Estonia has no national PQC transition strategy, no domestic cryptographic evaluation capability, and that private-sector cryptographic expertise is concentrated in two companies, Cybernetica and Guardtime [78]. The practical consequence is that Estonian banks, even if individually ready, may be constrained by the pace of national-level coordination. At the same time, the small size and concentration of the Estonian banking sector could be an advantage: fewer institutions to coordinate, shorter decision chains, and a track record of rapid digital adaptation demonstrated during the 2017 eID crisis, when the entire national certificate infrastructure was replaced within months [78]. The Swiss Bankers Association similarly observed that small institutional ecosystems benefit from short pathways for knowledge exchange [11], a structural advantage that Estonia shares.

Sweden's banking sector is larger, more internationally integrated, and structurally more complex. The combined assets of Sweden's four largest banks exceed 1.7 trillion USD [81]. Handelsbanken, Nordea, SEB, and Swedbank operate across the Nordic-Baltic region, with significant operations in Estonia itself. Scale directly increases the number of systems,

protocols, and third-party dependencies that must be migrated, lengthening the migration timeline parameter in the Mosca inequality [2]. The BIS roadmap confirms that PQC migration involves at least nine distinct layers of IT infrastructure, each requiring different approaches [68]. Sweden's payment infrastructure carries acknowledged technical debt: the Riksbank's Payments Report identifies significant challenges in Sweden's bulk payment systems [82], and the transition to the European T2 settlement platform is estimated to take approximately five years [82]. These timelines illustrate that even non-cryptographic infrastructure modernisation in Sweden operates on multi-year timescales, which should inform expectations about the duration of a cryptographic transition. The Dutch banking sector study found that the migration from SHA-1 to SHA-2 took ten years in the Dutch banking environment [74], and Sweden's systemically important banks are comparable in scale and complexity. Swedish banks are also more deeply integrated into international financial market infrastructure, including SWIFT and the Eurosystem's Target2 settlement system, where PQC migration depends on coordinated action across all participants [68].

Interconnectedness Between the Two Markets

A distinctive feature of the Estonian and Swedish banking sectors is their direct inter-connection. Two of the four largest banks operating in Estonia, Swedbank and SEB, are Swedish-owned and operate as subsidiaries of Swedish parent institutions. This means that PQC migration decisions made at the group level in Sweden will directly affect banking operations in Estonia, and conversely, Estonian national infrastructure requirements, including X-Road and eID migration, may create dependencies for Swedish banking groups operating in the country. The Onkenhout study of the Dutch banking sector found that migration planning in subsidiary-parent structures was complicated by the need to align group-level and local regulatory requirements [74]. For the Estonian-Swedish banking relationship, this dynamic is particularly relevant: the same institution may need to satisfy Estonian national infrastructure requirements, Swedish supervisory expectations, and EU-level DORA obligations simultaneously.

Implications

The convergence in overall readiness is the dominant finding. Both Estonian and Swedish banks are at the same pre-migration stage, driven by the same regulatory signals and

constrained by the same vendor dependencies. The structural differences described above may shape the path each country's banks take toward migration, but they have not yet produced meaningfully different levels of readiness. This supports the conclusion that the readiness posture observed in this thesis is shaped primarily by sector-wide and EU-level factors rather than by national context.

Where differences do emerge, they follow the structural characteristics of the two markets. The Estonian respondents showed greater within-country variation, with one institution notably more advanced in planning breadth and algorithm selection. This may reflect the concentrated nature of the Estonian market, where individual institutional differences are more visible. The Swedish respondents displayed more consistent intermediate-level responses, which may reflect the more standardised governance practices of larger, systemically important institutions.

Potential areas for cross-country learning exist. Estonia's experience with centralised digital identity and government-banking coordination may offer models for coordinated cryptographic transitions at the national level. Sweden's standardised governance practices and experience managing complex cross-border environments may offer lessons for structured migration planning at scale. The NIS Cooperation Group roadmap's call for coordinated EU-wide implementation [15], rather than country-by-country approaches, appears well-founded given these findings.

7 Practical PQC Migration Framework for Banks

7.1 Banking Needs a Sector-Specific Migration Framework

Several PQC migration frameworks already exist. NIST provides general migration guidance for public-key infrastructure [13]. The FS-ISAC has published an eight-phase algorithm replacement model for financial institutions [22]. The BIS has proposed a three-phase institutional roadmap covering awareness, planning, and execution [11]. Hasan et al. offer a graph-theoretic security dependency analysis framework for enterprise environments [18]. Onkenhout has developed a three-phase technology roadmap for the Dutch banking sector [74]. Kumar defines seven pillars of enterprise cryptographic agility [76].

These frameworks provide valuable guidance, but they share a common limitation - they treat PQC migration primarily as an organisational or enterprise-level challenge. They assume that an institution can independently inventory its cryptography, select algorithms, pilot solutions, and deploy them. The findings from Chapters 5 and 6 of this thesis show that this assumption does not hold for banking. Three structural characteristics distinguish the banking sector from the general-purpose migration context and require a sector-specific approach.

First, banks are systemically interconnected. They share payment infrastructure (SWIFT, Target2, SEPA), clearing and settlement systems, correspondent banking relationships, and, in Estonia's case, national digital identity infrastructure. The BIS Project Leap experiment demonstrated that even testing post-quantum signatures in the Target2 system required coordination between three central banks, two network service providers, and SWIFT [11]. A bank cannot unilaterally migrate cryptographic protocols that are shared with hundreds of counterparties. To illustrate this – an Estonian bank that wishes to migrate its authentication infrastructure to PQC algorithms could not do so independently. Customer authentication relies on the national eID system (ID card, Smart-ID, Mobile-ID), which is operated by SK ID Solutions and uses RSA and ECDSA. Migrating bank-side authentication to PQC

would require SK ID Solutions to issue PQC-capable certificates, the Information System Authority (RIA) to update X-Road's data exchange signatures, and every other relying institution on X-Road to accept the new cryptographic formats. Similarly, a bank that began signing interbank messages with PQC algorithms would find that counterparties, payment processors, and clearing systems cannot verify those signatures until they too have migrated. The result is a coordination problem where each participant has a rational reason to wait for others to move first, and no single institution can break the cycle unilaterally. Migration of shared infrastructure requires multi-actor consensus on timelines, algorithm selection, and backward compatibility, and the BIS roadmap confirms that cut-off dates for phasing out legacy protocols "need to be approved by all organisations that use those protocols" [68].

Second, banks operate under sector-specific regulatory obligations that generic frameworks do not address. DORA makes management bodies personally liable for ICT risk management, including cryptographic risk [10]. The NIS Cooperation Group roadmap sets milestones that explicitly apply to banking as critical infrastructure [15]. Yet while DORA does not mention post-quantum cryptography by name, its RTS 2024/1774 explicitly references threats from quantum advancements and establishes a binding crypto-agility obligation [69]. The European Commission Recommendation remains non-binding [14]. Banks must therefore plan migration against a regulatory framework that names the threat and mandates preparedness but does not yet specify PQC migration deadlines, a challenge that generic frameworks do not help them navigate.

Third, banks face a specific form of concentration risk in their vendor ecosystems. The FS-ISAC concludes that in many cases "your crypto agility will be determined by your vendors" [22]. Unlike general IT enterprises, banks depend on specialised infrastructure, particularly hardware security modules, where vendor PQC readiness directly constrains institutional migration timelines. One Estonian respondent in this thesis identified HSM vendors specifically as a bottleneck. The Cryptomathic Tier 1 bank case documented how hundreds of siloed HSMs created "limited agility" in adopting new standards [77]. This vendor dependency is not a solvable procurement problem but a structural constraint. A bank's core banking system, its payment processing platform, its HSMs, and its PKI infrastructure are each supplied by different vendors operating on independent development

cycles. Even if one vendor releases a PQC-ready update, the bank cannot deploy it until every other component in the same transaction chain also supports the new algorithms. A payment transaction that traverses a PQC-ready core banking system but passes through a non-PQC payment gateway and terminates at a legacy HSM gains no quantum resistance from the first component's upgrade. The entire chain must be PQC-capable for the migration to be effective, and the weakest vendor in the chain determines the pace. Generic frameworks recommend assessing vendor readiness, but they do not address the structural asymmetry between banking institutions and a small number of critical infrastructure providers whose timelines banks cannot control.

The framework proposed in this chapter builds on the existing migration guidance but adapts it to these banking-specific realities. It draws on the empirical findings from this thesis, the regulatory framework analysed in Chapter 3, and the challenges identified in Chapter 6. The seven migration steps synthesise and consolidate existing guidance from NIST, BIS, FS-ISAC, and other sources into a coherent sequence adapted to the banking context. The contribution of this framework is not in the steps themselves but in the identification of three interacting structural constraints, i.e. systemic interdependence, regulatory ambiguity, and vendor concentration, that together define a migration challenge specific to banking and that existing frameworks do not address as a combined problem. The framework is structured in five parts: preconditions that must be met before migration can begin, seven recommended migration steps, common pitfalls, three structural considerations specific to banking, and timeline considerations.

The element of this framework that most directly reflects the sector-specific character of banking is Step 2. Most existing PQC migration guidance treats cryptographic inventory as an internal exercise, i.e., primarily catalogue the institution's own systems. For a bank, this is insufficient. A bank's cryptography terminates at the boundary of shared market infrastructure such as SWIFT, payment clearing, national digital identity, card networks, HSM vendors, and a vulnerability or transition delay in any of these shared layers propagates back to every connected institution. Step 2 operationalises this by extending the inventory beyond the institution's perimeter to capture cryptographic dependencies in shared market infrastructure. This extension is what distinguishes the framework from generic enterprise PQC migration guidance and is treated explicitly in Section 7.2.

7.2 Recommended Migration Steps

The following seven steps constitute the core of the proposed migration framework. They are presented sequentially but in practice several steps will overlap and iterate. Table 1 provides a summary of each step with its objective, primary activities, and timeline alignment.

Table 1. Summary of recommended migration steps

Step	Objective	Activities	Key Challenge	Timeline
1	Governance and preparation	Assign management body accountability, establish migration team, collect system documentation, define scope and budget	Elevating quantum risk to board level	By end of 2026
2	Cryptographic inventory	Build CBOM covering all systems, third-party dependencies and shared infrastructure connections	Scale and hidden dependencies across legacy systems	By end of 2026
3	Risk classification and prioritisation	Classify assets by NIS three-tier model, assess store-now-decrypt-later and harvest-now-forge-later exposure, map dependency chains	Determining data confidentiality periods for Mosca inequality	By end of 2026
4	Target architecture	Select algorithms per ECCG and NIST, define hybrid strategy, plan AES-256 upgrade, design for crypto-agility	Balancing hybrid backward compatibility against downgrade risk	By end of 2026
5	Pilot projects	Test PQC in protocols (TLS, IPsec, SSH, PKI), measure performance impact, test hybrid feasibility	Protocol constraints in shared infrastructure (e.g. Target2 single-algorithm header)	By end of 2028
6	Production migration	Migrate high-risk systems by 2030, medium-risk by 2035, replace distributed hardware	Vendor and ecosystem coordination across payment networks	By end of 2030 / 2035
7	Crypto-agility and continuous adaptation	Centralise cryptographic operations, implement monitoring, track vendor and standard updates	Sustaining capability beyond initial migration	Ongoing

Step 1: Governance and Preparation

Before migration activities can begin, the institution must establish the governance structure, team, and documentation base required to support the programme. This step addresses the governance gap identified in Section 6.2, where only one of four respondents reported executive involvement in PQC migration and none had integrated quantum risk into their risk management framework.

The management body must assign accountability for PQC migration. DORA Article 5(2) requires the management body to bear ultimate responsibility for ICT risk management, and Article 5(4) requires the allocation of sufficient resources [10]. The BIS roadmap recommends designating a lead executive for quantum readiness [68]. The FS-ISAC recommends establishing a PQC steering committee responsible for overseeing the transition, setting timelines, and ensuring regulatory alignment [22].

The migration team should include representatives from information security, enterprise architecture, IT operations, vendor management, compliance, and risk management. Kumar identifies governance, process management, and education as three of the seven pillars of enterprise crypto agility that require cross-functional coordination [76]. A team charter should specify members, roles, reporting lines, and decision authority.

Before the cryptographic inventory can begin, existing system documentation must be collected and consolidated. This includes architecture diagrams, protocol specifications, certificate maps, HSM inventories, and vendor contract documentation. The Hasan et al. framework identifies the lack of documentation as one of eight obstacles to building cryptographic inventories [18]. Consolidating existing documentation first reduces the scope of discovery work required in Step 2 and prevents the inventory from starting without context.

The scope of migration must be defined, covering internal systems, shared infrastructure connections (SWIFT, payment clearing, national digital identity), and vendor dependencies. The NIS Cooperation Group roadmap requires Member States to identify stakeholders and create supply chain dependency maps by the end of 2026 [15]. In practice, however, the questionnaire results suggest this deadline may be hard to meet, as most responding banks are still in the early stages of the discovery work needed to build such a map. For

banks, this scope definition determines which external actors must be engaged and where the institution's migration depends on decisions it does not control.

Finally, the management body must approve a budget and programme mandate. The GRI 2025 report found that executives cannot quantify quantum risk exposure in monetary terms [21], which makes securing budget difficult. However, the regulatory obligation under DORA does not require a quantified business case for the threat; it requires preparation for identified ICT risks. The budget should cover the inventory and classification phases (Steps 2 and 3) at minimum, with subsequent phases budgeted as the scope becomes clearer.

Step 2: Establish a Comprehensive Cryptographic Inventory

Cryptographic inventory is a standard element of every PQC migration framework. The banking-specific extension proposed here is that the inventory must extend beyond the institution's own systems to encompass the cryptographic protocols used in connections to shared market infrastructure, such as SWIFT, payment clearing systems, national digital identity, card schemes, and the cryptographic dependencies embedded in vendor-supplied hardware such as HSMs and payment terminals. Without this extension, the inventory captures only the part of the bank's cryptography that the bank can independently control, which is not the part most likely to constrain its migration timeline.

The cryptographic inventory is the foundation upon which all subsequent migration decisions rest. Without knowing which algorithms, protocols, keys, and certificates are deployed across the institution's systems, it is impossible to assess quantum vulnerability, prioritise migration, or coordinate with vendors.

The inventory should encompass all cryptographic objects across applications, infrastructure, and networks, covering both data at rest and data in transit [18]. Mastercard recommends building a Cryptographic Bill of Materials (CBOM), a structured catalogue analogous to a software bill of materials, that documents which protocols secure data flows, where public key certificates are located, which processes use which symmetric keys and key pairs, and where the most sensitive data is stored [49]. The FS-ISAC framework adds that the inventory must also identify cryptographic anti-patterns in source code and third-party dependencies where cryptography is embedded in vendor-supplied components [22].

The challenge of building this inventory should not be underestimated. The Hasan et al. framework identifies eight fundamental obstacles, including complexity arising from "thousands of applications and hundreds of thousands of endpoints," heterogeneous environments mixing legacy and modern systems, hidden cryptographic dependencies, and the difficulty of maintaining accuracy in a continuously evolving landscape [18]. The BIS roadmap acknowledges that "manual reviews may still be necessary, particularly for legacy systems or security modules not easily scanned by automated tools" [11]. For the banks surveyed in this thesis, where cryptographic inventories were either incomplete or not yet started, this step represents the most immediate priority. The BIS Project Leap experiment found that even within a single payment system (Target2), multiple stakeholders with distinct configurations required tailored adaptations [11].

For banking specifically, the inventory must extend beyond the institution's own systems to encompass shared infrastructure dependencies. This includes cryptographic protocols used in connections to SWIFT, payment clearing systems, and national digital infrastructure such as Estonia's X-Road. The BIS Project Leap experiment found that even within a single payment system (Target2), multiple stakeholders with distinct configurations required tailored adaptations [11]. A bank's inventory is incomplete if it does not capture where its cryptography intersects with external systems it cannot independently control.

Step 3: Classify Assets by Quantum Risk and Prioritise Migration

Once the cryptographic inventory is established, assets must be classified by their quantum vulnerability and the urgency of migration. The NIS Cooperation Group roadmap adopts a three-tier risk classification system rooted in the Mosca inequality: high-risk use cases where confidentiality compromise after ten or more years would cause significant damage, medium-risk use cases with shorter but still substantial sensitivity periods, and low-risk use cases [15]. The roadmap specifies that for high-risk use cases, "quantum-vulnerable public-key mechanisms shall not be used stand-alone after the end of 2030" [15]. This prioritisation must account for two distinct threat vectors. The store-now-decrypt-later threat affects all data currently protected by quantum-vulnerable public-key encryption if that data retains confidentiality value beyond the arrival of cryptographically relevant quantum computers [32]. The questionnaire responses in Chapter 5 showed that respondents who provided estimates expected their most sensitive data to require confidentiality protection

for at least five to ten years, with one respondent indicating more than ten years, placing these institutions within the high-risk category according to the NIS classification. The second threat vector concerns digital signatures and authentication, where long-lived contracts, certificates, and software authentication mechanisms must be migrated before the systems relying on them can be compromised [11].

The security dependency analysis methodology proposed by Hasan et al. offers a rigorous approach to this classification: a graph-theoretic model that maps dependencies between data assets and cryptosystems, identifies propagation paths where a breach in one cryptosystem could compromise dependent assets, and prioritises migration by vulnerability severity and dependency chains [18]. For banks, where cryptographic dependencies are deeply layered, this dependency-aware prioritisation is essential. Payment systems depend on TLS, which depends on certificates, which depend on key management infrastructure, which depends on HSMs, and a vulnerability at any layer propagates upward.

Step 4: Define the Target Cryptographic Architecture

With the inventory and risk classification in place, the institution must define its target cryptographic state. The European Cybersecurity Certification Group's agreed cryptographic mechanisms document provides the authoritative European reference for algorithm selection [79]. For key encapsulation, ML-KEM (FIPS 203) and FrodoKEM are recommended, with ML-KEM-1024 or ML-KEM-768 as the preferred parameter sizes. For digital signatures, ML-DSA (FIPS 204), SLH-DSA (FIPS 205), XMSS, and LMS are all recommended [79].

A critical architectural decision concerns hybrid deployment. The ECCG draws a sharp distinction: lattice-based PQC algorithms such as ML-KEM and ML-DSA "shouldn't be used in a standalone way" and must be combined with a classical cryptographic mechanism in hybrid mode, whereas hash-based schemes such as XMSS and LMS may be used standalone [79]. The NIS Cooperation Group roadmap similarly recommends hybrid solutions "whenever feasible and suitable" [15], and ENISA's integration study states that hybrid deployment is "recommended even when not required" because the risk of post-quantum proposals being broken remains non-trivial [36]. This extends the quantum threat from a data-confidentiality problem to an asset-custody problem.

For banks beginning their migration, hybrid deployment provides an important safety

margin: if a PQC algorithm is later found to have vulnerabilities, the classical component maintains security until a replacement can be deployed.

The target architecture must also address symmetric cryptography. The ECCG recommends that in quantum-resistant contexts, block ciphers with key sizes smaller than 192 bits should not be used, effectively precluding AES-128 in favour of AES-192 or AES-256 [79]. Mosca explicitly identifies the upgrade from AES-128 to AES-256 as the quantum-safe symmetric transition target [2].

Beyond algorithm selection, the target architecture should incorporate crypto-agility as a design principle. The FS-ISAC defines crypto-agility as the "ability to adapt cryptographic solutions or algorithms quickly and efficiently in response to developments in cryptanalysis, emerging threats, technological advances, and vulnerabilities" with "no significant architectural changes, minimal disruption, and short transition time" [22]. The Swiss Bankers Association emphasises that crypto-agility is essential because "further migrations may be needed soon, for example, to roll out quantum key distribution" [11]. The target architecture should therefore be designed not as a one-time endpoint but as a platform capable of accommodating future cryptographic transitions.

Step 5: Develop and Execute Pilot Projects

Before institution-wide deployment, the selected PQC algorithms and hybrid configurations should be validated through controlled pilot projects. The BIS roadmap recommends that pilot projects "involve systems with varying levels of complexity to provide insight into performance, compatibility, and resource requirements" [11]. ENISA's integration study warns that PQC key sizes, with ML-KEM public keys at 1,184 bytes compared to RSA's 256 bytes, may cause protocol-level problems including "fragmentation, additional round-trips, and a more complicated state-machine" [36]. The pilot phase should address the specific protocol integrations relevant to banking operations. ENISA identifies six critical infrastructure integration scenarios: TLS, IKE/IPsec for VPN, WireGuard, MACsec, SSH, and PKI/certificate infrastructure, each requiring different adaptation strategies [36]. For banks, Mastercard identifies hybrid TLS using ECC combined with ML-KEM as a practical quick win for key management and general communications [49].

The BIS Project Leap experiment provides a direct precedent for banking-sector PQC pilot-

ing. The experiment replaced traditional RSA digital signatures with CRYSTALS-Dilithium in the Eurosystem's Target2 payment system and found that while PQC implementation was technically feasible, verification times increased from 28.1 milliseconds to 209.9 milliseconds, requiring "more computing power and storage" [11]. This performance impact is manageable in controlled testing but must be carefully assessed for high-throughput payment processing environments. The experiment also found that hybrid deployment was not feasible within the current Target2 configuration, which supports only a single algorithm per message header, highlighting that protocol-level constraints in shared banking infrastructure may require system evolution before PQC can be fully integrated [11].

For institutions with complex environments, the ELCA framework proposed by Sikeridis et al. offers a relevant architectural pattern: a proxy-based cryptographic provider that decouples cryptographic services from applications, enabling orchestrated migration of legacy applications "without modifying" the applications themselves [38]. This is particularly pertinent for banks where, as the FS-ISAC notes, "cryptography is deeply embedded in application code" and legacy systems are "particularly difficult to update" [22].

Step 6: Execute Phased Production Migration

Production migration should proceed in phases, beginning with the highest-risk systems identified in Step 2 and progressing through medium- and lower-risk systems according to the institution's risk-calibrated timeline. The NIS Cooperation Group's timeline, with high-risk use cases to be migrated by 2030, means that banks cannot afford to delay migration of their most sensitive systems indefinitely.

Phased migration must account for the coordination challenges inherent in banking infrastructure. The Onkenhout roadmap for Dutch banking emphasises this through its three-phase structure: the first phase focuses on internal preparedness and privacy breach response plans, the second on adopting PQC in online payment networks with mandated vendor PQC requirements, and the third, necessarily the longest, on replacing distributed hardware including payment cards, point-of-sale terminals, and ATMs [74]. This three-phase structure implicitly acknowledges that banking migration cannot proceed as a purely internal exercise: the second phase requires coordinated action with payment

network operators, and the third phase requires coordination with hardware manufacturers and card scheme operators.

Each migration phase should be followed by verification. The FS-ISAC framework includes explicit verification and maintenance phases, encompassing internal and external audit, validation of the new cryptographic configuration, and continuous monitoring to ensure vendor software updates are tracked [22]. The ELCA framework adds that enterprise-level migration requires monitoring and auditing capabilities that provide "cryptographic proofs of configuration state" at the infrastructure level, not merely at the application level [38].

Step 7: Embed Crypto-Agility for Continuous Adaptation

The final step is not an endpoint but a shift to an ongoing operational model. Post-quantum migration is unlikely to be the last major cryptographic transition that banks face. The PQC algorithms standardised today may themselves be superseded, additional post-quantum signature schemes are still under development at NIST, and quantum key distribution may introduce further changes to the cryptographic landscape [49].

Kumar's seven-pillar framework provides the most comprehensive model for this continuous capability, requiring agility across information management, process management, architectural design, infrastructure, operations, governance, and education [76]. The practical benefit of crypto-agility is demonstrated by the Tier 1 bank case: by centralising cryptographic operations and achieving vendor neutrality through a single service gateway, the institution reduced cryptographic change deployment timelines "from months to weeks" and eliminated the vendor lock-in that had previously constrained its ability to adopt new standards [77]. For the banks surveyed in this thesis, where vendor dependencies were universally identified as a key constraint, crypto-agility represents both the solution to the immediate PQC migration challenge and the foundation for long-term cryptographic resilience.

7.3 Migration Checklist

The preceding seven steps describe the logic of migration. To translate them into a trackable programme, Table 3 operationalises the steps into 45 checklist items grouped by 12 sections. Each item specifies prerequisites, a definition of done, an owner, the

applicable regulatory reference, a timeline mapped to NIS Cooperation Group milestones (2026, 2030, 2035), and external dependencies. The checklist extends the seven migration steps with four additional dimensions identified as gaps during the analysis: workforce training and awareness (Section B), data classification as a prerequisite for risk assessment (item D.1), incident response and rollback planning (Section H), and management reporting (items K.3–K.4).

PQC Migration Checklist for Banks

Aligned with NIS Cooperation Group milestones (2026 / 2030 / 2035) and DORA obligations

ID	Checklist Item	Prerequisites	Definition of Done	Owner	Regulatory Reference	Timeline	Dependencies
A. Governance and Preparation							
A.1	Assign management body accountability for PQC migration	None	Board resolution or equivalent document assigns PQC migration responsibility to a named member of the management body.	Management body	DORA Art. 5(2): management body bears ultimate responsibility for ICT risk management	By end of 2026	None
A.2	Establish a PQC migration team with defined roles	A.1 completed	Team charter document specifies members, roles, reporting lines and decision authority.	CISO	DORA Art. 5(4): management body shall allocate sufficient resources	By end of 2026	None
A.3	Collect and consolidate existing system and cryptographic documentation	A.2 completed	Central repository contains architecture diagrams, protocol specifications, certificate maps and HSM inventories for all production systems.	CIO	DORA RTS 2024/1774 Art. 6: encryption policy based on data classification and ICT risk assessment	By end of 2026	None
A.4	Define migration scope covering internal systems, shared infrastructure and vendor dependencies	A.3 completed	Scope document lists all systems, shared infrastructure connections (SWIFT, payment clearing, national eID) and vendor relationships in scope for migration.	CISO	DORA Art. 9(1); NIS roadmap: identify stakeholders and supply chain dependencies	By end of 2026	Payment infrastructure operators and national digital identity providers disclose their migration plans
A.5	Secure budget and management mandate for the migration programme	A.1 and A.4 completed	Approved budget allocation and programme mandate documented and communicated.	Management body	DORA Art. 5(4): adequate resources for ICT security	By end of 2026	None
B. Training and Awareness							
B.1	Deliver PQC awareness programme for the management body and senior management	A.1 completed	Management body members have received a briefing covering: quantum threat timeline, store-now-decrypt-later and harvest-now-forge-later threat vectors, regulatory expectations (NIS roadmap milestones, DORA obligations) and estimated migration scope. Attendance documented.	CISO	DORA Art. 5(2)(b): management body shall follow specific ICT risk management training	By end of 2026	None
B.2	Provide technical PQC training for development, infrastructure and security teams	A.2 completed	Staff involved in migration have completed training on: PQC algorithm properties (key sizes, performance characteristics), hybrid deployment, crypto-agility design patterns and PQC library usage. Training completion tracked.	CISO	DORA Art. 13(6): ICT security awareness and digital operational resilience training	By end of 2026	Availability of PQC training materials or external courses
B.3	Include PQC readiness criteria in procurement and vendor evaluation	A.4 completed	Procurement templates and vendor evaluation scorecards include PQC readiness as a documented criterion: algorithm support, crypto-agility capability and PQC migration roadmap.	Vendor management	DORA Art. 28: ICT third-party risk management	By end of 2026	None
C. Cryptographic Inventory							
C.1	Inventory all cryptographic algorithms, protocols, keys and certificates across applications, infrastructure and networks	A.3 and A.4 completed	Cryptographic Bill of Materials (CBOM) covers 100% of production systems, documenting algorithm type, key length, protocol, location and owning application for each entry.	CISO	NIS roadmap 2026: cryptographic asset inventories; DORA Art. 8(4); RTS 2024/1774 Art. 6	By end of 2026	None
C.2	Identify cryptographic dependencies in third-party components and assess vendor PQC readiness	C.1 in progress	CBOM includes all third-party cryptographic dependencies tagged with vendor, version and algorithm. Each vendor has a recorded PQC migration status. Vendors lacking PQC plans flagged in third-party risk reporting.	Vendor management	DORA Art. 28: ICT third-party risk management	By end of 2026	Vendor cooperation in disclosing cryptographic implementations and roadmaps
C.3	Map cryptographic connections to shared and external infrastructure	C.1 in progress	CBOM documents cryptographic protocols used in connections to SWIFT, payment clearing systems, correspondent banks and national digital infrastructure (e.g. X-Road, eID). Each connection specifies algorithm, certificate chain and controlling party.	CTO	NIS roadmap 2026: supply chain dependency maps	By end of 2026	Payment infrastructure operators and national authorities provide technical specifications

Table 2. PQC migration checklist for banks

Table 2. PQC migration checklist for banks

C.4	Identify legacy systems with hardcoded cryptographic implementations	C.1 in progress	All legacy systems identified; each tagged as updatable, requiring manual intervention or requiring replacement. Systems lacking documentation flagged.	CIO	ENISA: migration requires system-wide changes including updates to protocols and infrastructure	By end of 2026	None
D. Risk Classification and Prioritisation							
D.1	Classify data assets by confidentiality requirements and retention periods	C.1 in progress	Each data category (customer financial records, transaction logs, contracts, credentials, internal communications) has a documented confidentiality requirement and regulatory or business retention period.	Head of IT Risk	RTS 2024/1774 Art. 6: encryption policy based on data classification; GDPR Art. 5(1)(e)	By end of 2026	None
D.2	Classify cryptographic assets using the NIS three-tier risk model (high, medium, low)	C.1 and D.1 completed	Every CBOM entry has a risk classification (high, medium or low) based on the Mosca inequality and data confidentiality period.	Head of IT Risk	NIS roadmap: three-tier risk classification; high-risk use cases must not use quantum-vulnerable algorithms standalone after end of 2030	By end of 2026	None
D.3	Assess store-now-decrypt-later exposure	D.1 and D.2 in progress	Each data category has a documented retention period and a determination of whether it falls within the store-now-decrypt-later threat window.	Head of IT Risk	GRI Quantum Threat Timeline; NIST IR 8547: deprecation of classical public-key algorithms by 2030	By end of 2026	None
D.4	Assess harvest-now-forge-later exposure for digital signatures, certificates and digital asset custody	D.2 in progress	All signature and certificate use cases assessed; long-lived contracts, certificates with validity beyond 2030 and digital asset custody keys flagged as high priority.	Head of IT Risk	EPC: harvest-now-forge-later is critical for digital assets and CBDCs	By end of 2026	None
D.5	Map dependency chains and propagation paths	C.1 and D.2 completed	Dependency graph shows how a vulnerability in one cryptosystem propagates to dependent assets (application to TLS to certificates to key management to HSM). Migration sequence derived from this graph.	CTO	Hasan et al.: graph-theoretic security dependency analysis; DORA: ICT risk management framework	By end of 2026	None
E. Target Cryptographic Architecture							
E.1	Select target algorithms per ECCG and NIST recommendations	D.2 completed	Documented algorithm selection specifying ML-KEM parameters for key encapsulation, ML-DSA or SLH-DSA for signatures and AES-256 for symmetric encryption. Selection rationale references ECCG agreed mechanisms and NIST FIPS 203/204/205.	CISO	ECCG Agreed Cryptographic Mechanisms v2.0; NIST FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA)	By end of 2026	None
E.2	Define hybrid deployment strategy	E.1 completed	Policy document specifies that lattice-based algorithms (ML-KEM, ML-DSA) are deployed in hybrid mode with a classical algorithm; hash-based algorithms (SLH-DSA) may be standalone. Backward compatibility and downgrade attack risks assessed.	CISO	ECCG: lattice-based PQC must be combined with classical algorithm; NIS roadmap: hybrid solutions recommended whenever feasible	By end of 2026	Shared infrastructure (payment systems, eID) confirms hybrid protocol support
E.3	Plan symmetric key upgrade (AES-128 to AES-256)	C.1 completed	All AES-128 use cases identified from CBOM and migration plan to AES-256 (or AES-192 minimum) documented.	CTO	ECCG: block ciphers with key sizes below 192 bits must not be used in quantum-resistant contexts	By end of 2030	Vendor support for AES-256 in all deployed products
E.4	Design architecture for crypto-agility	E.1 completed	Architecture supports algorithm replacement without disrupting operations. Cryptographic services are abstracted from applications. No algorithm is hardcoded in application logic.	CTO	RTS 2024/1774: crypto-agility obligation; FS-ISAC crypto-agility framework	By end of 2030	Vendor support for abstracted cryptographic service layers
F. Pilot Projects and Validation							
F.1	Define pilot scope covering systems of varying complexity	E.1 and E.2 completed	Pilot plan identifies at least one low-complexity system (e.g. internal TLS) and one high-complexity system (e.g. payment interface) for PQC testing.	CISO	BIS: pilot projects should involve systems with varying levels of complexity; NIS roadmap 2026: launch pilots for high-risk use cases	By end of 2026	Vendor availability of PQC-capable software and firmware for selected pilot systems
F.2	Test protocol integrations (TLS, IKE/IPsec, SSH, PKI)	F.1 completed	Each protocol tested with PQC algorithms in a non-production environment. Test results document key exchange success/failure, handshake times, message sizes, error rates and backward compatibility behaviour.	CISO	ENISA: six critical integration scenarios (TLS, IKE/IPsec, WireGuard, MACsec, SSH, PKI)	By end of 2028	Vendor and library support for PQC in each protocol (e.g. OpenSSL, BoringSSL, vendor TLS stacks)
F.3	Measure and document performance impact	F.2 in progress	Performance report quantifies key generation time, signature verification time, handshake latency, throughput impact and storage requirements. Compared against current baseline and BIS Project Leap benchmarks.	CTO	BIS Project Leap: PQC verification time increased from 28.1ms to 209.9ms in Target2	By end of 2028	None

Table 2. PQC migration checklist for banks

F.4	Test hybrid deployment feasibility within existing system constraints	F.2 in progress	Documented assessment of whether current system configurations support hybrid mode. Constraints identified (e.g. single algorithm per message header in Target2). Workarounds or system evolution requirements documented.	CTO	BIS Project Leap: hybrid deployment not feasible within current Target2 configuration	By end of 2028	Shared infrastructure operators confirm hybrid protocol support
F.5	Conduct security validation of PQC implementations	F.2 in progress	Each PQC implementation tested for side-channel resistance, correct parameter usage, key validation and compliance with NIST FIPS requirements. Implementations using third-party libraries verified against known vulnerability disclosures.	CISO	NIST FIPS 203/204/205: implementation requirements; ENISA: implementation correctness is a migration risk	By end of 2028	Availability of PQC security testing tools and expertise
F.6	Conduct interoperability testing with external parties	F.2 completed; J.3 in progress	PQC protocol interoperability verified with at least one correspondent bank, one payment infrastructure operator and one national infrastructure provider. Test results document algorithm negotiation, certificate validation and fallback behaviour.	CISO	BIS Project Leap: interoperability testing across central banks, network providers and SWIFT	By end of 2029	Willingness of counterparties to participate in interoperability testing
F.7	Conduct business process regression testing	F.2 completed	Business processes dependent on migrated cryptographic components tested end-to-end. No functional regressions in transaction processing, authentication, document signing or reporting. Results signed off by business process owners.	CIO	DORA Art. 9(1): ensure resilience of network and information systems	Before each production migration phase	None
G. Production Migration							
G.1	Migrate high-risk systems to PQC	Sections C, D, E completed; F.1-F.7 completed for high-risk systems	All systems classified as high risk in D.2 are running PQC algorithms (hybrid or standalone as per E.2). Quantum-vulnerable public-key algorithms are not used standalone for high-risk use cases.	CTO	NIS roadmap: quantum-vulnerable public-key mechanisms shall not be used standalone for high-risk use cases after end of 2030	By end of 2030	HSM vendors release PQC-capable firmware; payment network operators support PQC; national eID infrastructure supports PQC certificates
G.2	Plan and migrate medium-risk systems	G.1 completed or in progress; pilot results from F available	Migration plan for medium-risk systems approved. Pilots for medium-risk use cases completed. Production migration initiated.	CTO	NIS roadmap: planning and pilots for medium-risk use cases by end of 2030; transition completed by end of 2035	Planning by end of 2030; completion by end of 2035	Same as G.1; backward compatibility with already migrated high-risk systems
G.3	Replace distributed cryptographic hardware (payment terminals, ATMs, HSMs)	E.1 completed; vendor PQC-capable hardware available	All hardware cryptographic devices (HSMs, EMV terminals, ATMs, POS systems) support PQC algorithms. Replacement schedule completed.	CIO	Onkenhout: hardware replacement is the longest phase; DORA Art. 9(4)(d): protection measures for cryptographic keys	By end of 2035	Hardware vendors release PQC-capable devices; card scheme operators (Visa, Mastercard) update EMV standards
G.4	Verify each migration phase through audit and monitoring	G.1 or G.2 phase completed	Internal and external audit of migrated systems completed. Cryptographic configuration validated against target architecture (E.1). Continuous monitoring active for migrated systems.	Internal audit	FS-ISAC: verification and maintenance phases including internal and external audit; DORA: ICT risk management framework	After each migration phase	None
H. Incident Response and Rollback							
H.1	Define rollback procedures for each migration phase	F.1 completed	Each migration phase has a documented rollback plan specifying conditions that trigger rollback, procedure to revert to the previous cryptographic configuration, maximum rollback time and data integrity verification after rollback. Rollback tested in non-production environment.	CISO	DORA Art. 11: ICT response and recovery	Before each production migration phase	None
H.2	Update incident response plans for PQC-specific failure scenarios	A.2 completed; E.2 completed	Incident response playbooks include scenarios for PQC implementation vulnerability disclosure, hybrid mode negotiation failure, PQC certificate validation failure and performance degradation after PQC deployment. Escalation paths and communication templates defined.	CISO	DORA Art. 17: ICT-related incident management process	By end of 2028	None
H.3	Define contingency plan for deployed PQC algorithm compromise	E.1 and E.4 completed	Contingency plan documents procedure to replace a compromised PQC algorithm with an alternative (e.g. SLH-DSA if ML-DSA is compromised), estimated execution time and dependencies on vendor updates. Plan leverages crypto-agility architecture from E.4. SIKE withdrawal in 2022 cited as precedent.	CISO	ECCG: lattice-based algorithms require hybrid deployment as mitigation; FS-ISAC: crypto-agility as risk mitigation	By end of 2028	Crypto-agility architecture (E.4) in place or planned

I. Crypto-Agility and Continuous Adaptation							
I.1	Centralise cryptographic operations through a service abstraction layer	E.4 completed	Cryptographic operations are provided through a centralised service layer that supports multiple HSM vendors and algorithm families. Vendor lock-in eliminated for cryptographic infrastructure.	CTO	RTS 2024/1774: crypto-agility; Cryptomathic Tier 1 case: centralisation reduced change timelines from months to weeks	By end of 2030	Vendor support for standardised cryptographic service interfaces
I.2	Implement monitoring and audit of cryptographic configuration state	I.1 in progress	Automated monitoring detects cryptographic algorithm usage, certificate expiry and non-compliant configurations across all production systems. Alerts generated for any system using deprecated algorithms.	CISO	DORA Art. 9: maintain ICT systems ensuring integrity and confidentiality	By end of 2030	None
I.3	Track regulatory and standards developments on PQC and vendor PQC roadmaps	C.2 completed	Documented process for monitoring updates from European Commission, NIS Cooperation Group, ENISA, NIST, EBA, ECB, ECCG and national competent authorities, together with vendor PQC roadmap changes. Quarterly review with impact assessment and update scheduling.	Compliance	DORA Art. 28: ICT third-party risk management; NIST: additional signature schemes still under standardisation	Ongoing from 2026	Vendor willingness to share PQC roadmaps
J. Ecosystem Coordination							
J.1	Engage national banking association and central bank working groups on PQC coordination	A.1 completed	Bank is an active participant in a national or sectoral PQC coordination group. Alignment on migration timelines and algorithm selection discussed with peers.	CISO	BIS: cut-off dates for phasing out legacy protocols need to be approved by all organisations that use those protocols	By end of 2026	Existence of national coordination forums; central bank willingness to convene
J.2	Assess national digital infrastructure migration status	C.3 completed	Documented assessment of PQC migration status and timelines for national digital identity (eID), data exchange platforms (e.g. X-Road) and qualified electronic signature infrastructure. Gaps between national infrastructure timelines and bank migration needs identified.	CISO	NIS roadmap: Member States to establish national PQC transition roadmaps by end of 2026	By end of 2026	National authorities publish their PQC transition plans
J.3	Coordinate migration timelines with correspondent banks and payment infrastructure operators	J.1 in progress; D.2 completed	Bilateral or multilateral agreements on migration timelines, algorithm selection and backward compatibility periods documented with correspondent banks, SWIFT and payment clearing operators.	CTO	BIS Project Leap: testing PQC in Target2 required coordination between three central banks, two network providers and SWIFT	By end of 2028	Willingness of counterparties and infrastructure operators to engage in migration planning
K. Regulatory Alignment and Reporting							
K.1	Map DORA obligations to PQC migration actions	A.4 completed	Compliance mapping document links each DORA article and RTS 2024/1774 provision relevant to cryptography (Art. 5(2), 9(1), 9(3)(d), 9(4)(d), RTS 2024/1774 Art. 6, 7) to specific migration actions in this checklist.	Compliance	DORA; DORA RTS 2024/1774	By end of 2026	None
K.2	Prepare documentation for supervisory review	D.2 and E.1 completed	Documentation package ready for supervisory review (SREP or thematic review) covering cryptographic asset inventory, risk classification, target architecture, migration timeline, vendor dependency assessment and management body accountability.	Compliance	DORA Art. 5(2); NIS roadmap milestones	By end of 2027	None
K.3	Establish regular migration progress reporting to the management body, including annual programme review	A.2 completed	Quarterly reporting process delivers to the management body: migration progress against milestones, budget status, risk register updates, vendor dependency changes and regulatory developments. Annual review covers budget adequacy, staffing, vendor contract alignment, scope changes and timeline adjustments.	CISO	DORA Art. 5(2): management body bears ultimate responsibility; Art. 5(4): management body shall review ICT risk management framework at least once a year	Quarterly from 2026; annual review from 2027	None
K.4	Define communication plan for customer and counterparty facing changes	G.1 in progress	Communication plan documents which migration phases affect customer-facing services (e.g. certificate changes, authentication updates), notification timelines and support procedures.	CISO	DORA Art. 14: communication policies	Before each customer-facing migration phase	None

Table 2. PQC migration checklist for banks

7.4 Common Pitfalls and Risks

The migration framework outlined above must be executed with awareness of several pitfalls that have been documented across the literature and that the findings of this thesis confirm. The most frequently documented pitfall is treating PQC migration as a simple algorithm replacement rather than a systemic transformation. The BIS roadmap explicitly cautions against this misconception, noting that PQC migration involves changes across at least nine layers of IT infrastructure and that the migration from SHA-1 to SHA-2, which took over a decade even after the algorithm was known to be insecure, demonstrates that cryptographic transitions are fundamentally more complex than they appear [11]. The GRI executive perspectives report found that many organisations were "naively equating the quantum threat to the attacks we see today" and were surprised by "the vastness of their cryptographic infrastructure" [21].

A second pitfall is the assumption that major technology vendors will manage the transition on the institution's behalf. The GRI 2025 report documents this directly: financial institutions assume that cloud providers such as Microsoft, Amazon, Google, and Apple will handle the migration, yet "most felt there was a lack of clear strategies and timelines" from these vendors [21]. The Cryptomathic analysis confirms that the vendor ecosystem remains immature: many HSMs, TLS libraries, and database encryption tools "do not yet support PQC," and some solutions marketed as quantum-safe use "proprietary schemes that may not align with official standards" [71].

A third pitfall is deferring action until regulatory requirements become binding. The BSI/KPMG survey found that 96 percent of respondents cited regulatory requirements as the primary driver for PQC investment [19], and the GRI 2025 report states that financial institutions "expect that until regulators start enforcing steps relating to migration to quantum, it won't be considered in the day-to-day risk management of the organisation" [21]. This wait-and-see posture ignores two critical factors: the store-now-decrypt-later threat creates present-day risk regardless of regulatory timelines [32], and the BSI/KPMG survey found that the average expected migration completion is 6.5 years later than the threat timeline, meaning that waiting for regulatory enforcement may make timely migration impossible [19].

A fourth pitfall is underestimating the protocol-level impact of PQC algorithms. ENISA's integration study documents that PQC key and ciphertext sizes, "even when small in absolute numbers, might in aggregate introduce unexpected problems for specialized use cases," and that "none of the candidates in the NIST competition matches the data flow and versatility of the Diffie-Hellman key exchange," requiring protocol rewrites across TLS, IKE/IPsec, SSH, and other core protocols [36]. The BIS Project Leap experiment confirmed this in practice: the sevenfold increase in signature verification time and the inability to implement hybrid signatures within the current Target2 message format demonstrate that PQC integration in banking infrastructure is not a drop-in replacement [11].

7.5 Contribution to Banking-Specific PQC Migration

The general PQC migration frameworks reviewed in the literature provide valuable guidance but do not fully address three structural characteristics that are specific to the banking sector and that emerged from the analysis in this thesis. These three dimensions represent the contribution of this framework.

7.5.1 The Systemic Interdependence Problem

Banks do not operate as isolated entities. They are nodes in interconnected financial networks, including payment systems, clearing and settlement infrastructures, correspondent banking relationships, and shared market utilities, where the security of any individual institution depends on the cryptographic posture of the network as a whole. The BIS roadmap articulates this directly: "private sector financial institutions, central banks, regulatory organisations, various branches of government and cross-border payment systems are intrinsically integrated and connected," and actors that are "not adequately protected against the quantum threat could become weak links, impacting the security of the entire financial system" [11].

This systemic interdependence means that PQC migration in banking cannot be treated as an institution-by-institution exercise. The WEF/FCA white paper's principle of "avoid fragmentation" is grounded in precisely this concern: "fragmentation creates compliance burdens for global entities operating across multiple jurisdictions and undermines the weakest-link security model of the interconnected financial sector" [12]. The BIS Project

Leap experiment demonstrated this concretely: testing PQC signatures in a single payment system required coordination between the BIS Innovation Hub, three central banks (Bank of Italy, Bank of France, Deutsche Bundesbank), two network service providers (Nexi-Colt and SWIFT), and multiple solution vendors, each with distinct configurations requiring tailored adaptations [11]. If a controlled experiment requires this level of multi-actor coordination, production migration across the full financial infrastructure will require orders of magnitude more.

The framework's most distinctive contribution to banking-specific PQC migration is the extended scope of cryptographic inventory proposed in Step 2. Generic enterprise migration guidance treats inventory as a within-institution catalogue. The framework proposed here treats inventory as an exercise that necessarily crosses institutional boundaries, capturing dependencies on shared market infrastructure and on hardware supplied by a limited number of vendors. This reframing is consistent with the position taken by BIS that banks are nodes in interconnected financial infrastructure [11] and is empirically supported by the BIS Project Leap finding that PQC integration in Target2 was constrained not by the institution's own cryptography but by the single-algorithm header of the shared payment system [11].

The Estonian context illustrates this problem at the national level. Estonian banking infrastructure is embedded within the X-Road data exchange layer connecting over 900 institutions through public-key cryptography, and the national digital identity framework is integral to banking authentication [78]. PQC migration for Estonian banks therefore cannot proceed independently of migration across the broader national digital infrastructure. The 2017 ROCA incident demonstrated how vulnerability in one component of this interconnected system cascades across the entire ecosystem [78]. The Swedish context presents a different form of the same problem: Swedish banks operate across the Nordic-Baltic region, and two of the four largest banks in Estonia are Swedish-owned subsidiaries. PQC migration decisions at the group level in Stockholm directly affect operations in Tallinn, and Estonian national infrastructure requirements create reverse dependencies for the Swedish parent.

The digital signature ecosystem illustrates this interdependence with particular clarity. Estonian qualified electronic signatures, which carry legal equivalence to handwritten

signatures, are built on the eID public-key infrastructure. If the national signature scheme transitions to PQC algorithms, every relying party — banks, government agencies, notaries, courts, and businesses — must be able to verify the new signatures. Conversely, if the national infrastructure has not yet migrated, banks cannot issue or accept PQC-signed documents regardless of their own internal readiness. This creates an asymmetric dependency: banks depend on infrastructure decisions made by national authorities, certificate service providers, and standards bodies over which they have limited influence. The CyCon 2024 study identifies this explicitly, noting that PQC migration for Estonia’s e-governance systems cannot follow the same pattern as previous transitions because there is no drop-in PQC replacement for the existing signature and key exchange primitives [56].

The practical implication is that banks must engage in sector-level coordination, through national banking associations, central bank working groups, and international bodies, to align migration timelines and interoperability requirements. The Dutch model documented by Onkenhout, where banks collaborate through Bankers’ Association’s quantum readiness groups and coordinate with DNB [74], represent emerging patterns for such coordination. However, the BSI/KPMG finding that non-binding guidance is insufficient without regulatory follow-through [19] suggests that voluntary coordination alone may not achieve the systemic alignment required.

7.5.2 The Regulatory Specificity Gap

Banks operate under sector-specific regulatory obligations that general PQC migration frameworks do not address. DORA requires financial entities to implement ICT risk management measures incorporating state-of-the-art cryptography, Article 5(2) creates personal liability for management bodies. As mentioned previously, the RTS 2024/1774, which operationalises DORA’s mandate, goes further than the parent regulation. These provisions create a concrete regulatory basis for supervisory expectations around PQC preparedness, yet the findings from Chapter 5 show that respondents perceive the regulatory signal as unclear, suggesting these specific RTS 2024/1774 provisions have not yet reached bank-level compliance awareness. The NIS Cooperation Group roadmap explicitly notes that DORA and NIS2 require entities’ management bodies can be held liable for failing to comply with these requirements [10] [15].

This regulatory specificity gap operates in both directions. On one side, banks lack clear guidance on what quantum-related compliance looks like under existing frameworks. The WEF/FCA white paper identifies this explicitly: "a tangible action plan to establish global and harmonised regulatory approaches remains elusive," and the "lack of regulatory guidance has led to industry uncertainty about how to prepare and manage quantum cyber risks" [12]. On the other side, regulators themselves acknowledge that they have not yet translated the quantum threat into specific supervisory expectations, with 93 percent of regulatory survey respondents in the WEF study agreeing that quantum technologies will have significant implications for their frameworks but lacking a concrete action plan [12].

The Cryptomathic analysis captures the resulting dynamic: regulators have begun to "require cryptographic inventories and PQC transition plans with fixed target dates," yet the technology supply chain "cannot yet fully support" the transition, creating "a fundamental gap" where "organisations face regulatory pressure to act now even while the ultimate threat remains probabilistic" [71]. For banks, this means that migration planning must simultaneously satisfy existing regulatory expectations under DORA while anticipating evolving requirements that have not yet been finalised.

The practical recommendation is that banks should interpret their DORA obligations proactively: the requirement for state-of-the-art cryptographic risk management can reasonably be read to include assessment and planning for the quantum threat, even before PQC-specific regulatory guidance is issued. Institutions that have already begun migration planning will be better positioned when binding requirements materialise.

7.5.3 The Concentration Risk Dimension

The findings from this thesis and the broader literature reveal a specific form of vendor risk that is insufficiently addressed in general PQC migration frameworks: the concentration of cryptographic dependencies on a small number of vendors whose PQC readiness directly constrains institutional migration timelines.

The FS-ISAC working group concluded that "your crypto agility will be determined by your vendors" and that "cryptography woven into third-party components is not always apparent, leaving customers blind to related vulnerabilities" [22]. Sikeridis et al. found that enterprise operators face a daunting challenge "exactly because it means corralling

hundreds of software providers to support the change and with very little control over the process" [38]. Mastercard warned of "supply chain immaturity," noting that "given the immaturity of the supply chain, there is little further concrete action that can be taken" for some cryptographic components beyond assessment [49].

For banks specifically, the concentration risk manifests in HSM infrastructure. The Cryptomathic Tier 1 bank case documented how managing "hundreds of siloed Hardware Security Modules" from multiple vendors led to "rising infrastructure costs and inefficiencies" and "limited agility" in adopting new standards [77]. HSM vendor lock-in creates fragility because the institution's ability to migrate depends on specific vendors releasing PQC-compatible firmware or hardware, a timeline the bank cannot control [77].

This concentration risk is compounded by the structural asymmetry between banking institutions and their technology providers. The GRI 2025 report documents that financial institutions assume major cloud providers will manage the transition, yet perceive "a lack of clear strategies and timelines" from these providers [21]. The circular dependency identified in Section 6.2.4, where banks wait for vendors, vendors wait for regulators, and regulators wait for industry, is most acute in the HSM and payment infrastructure segment where alternatives are limited.

This circular dependency produces what amounts to a coordination trap specific to banking. Unlike a software company that can unilaterally adopt PQC in its own products, a bank operates within a web of bilateral and multilateral dependencies where its cryptographic choices must be compatible with those of counterparties, infrastructure operators, and vendors simultaneously. The bank cannot migrate ahead of its HSM vendor, cannot migrate ahead of the payment network, cannot migrate ahead of the national eID infrastructure, and cannot migrate ahead of its correspondent banking partners. Each of these actors faces the same constraint in reverse. The practical consequence is that no individual institution, no matter how well-prepared internally, can complete PQC migration without coordinated movement across the ecosystem. This distinguishes banking from sectors where organisations have greater autonomy over their technology stack and can migrate at their own pace.

The practical recommendation is twofold. First, banks should actively diversify their

cryptographic vendor dependencies and pursue vendor-neutral architectural patterns, as exemplified by the Tier 1 bank's centralisation strategy that enabled "multiple HSM vendors" to be supported through a single service layer, "eliminating vendor lock-in and providing flexibility for future-proofing" [77]. Second, banks should incorporate vendor PQC readiness into their third-party risk management processes, treating vendors' cryptographic transition plans as a material component of counterparty risk assessment, consistent with DORA's requirements for ICT third-party risk management.

7.6 Timeline Consideration

The migration framework must be executed within externally imposed timelines that do not allow indefinite preparation. The NIS Cooperation Group roadmap establishes that national PQC transition roadmaps should be in place by the end of 2026, high-risk use case migration should be completed by the end of 2030, and medium-risk use case migration by the end of 2035 [15]. The GRI expert survey data reinforces this urgency: 19 to 34 percent of experts estimate a cryptographically relevant quantum computer within the next decade [32], and the BSI/KPMG survey found that the average organisation expects migration completion to lag the threat timeline by 6.5 years [19].

For banks, the NIST report's observation that "it has taken almost 20 years to deploy our modern public key cryptography infrastructure" [13] provides a sobering benchmark. The Dutch banking experience of a ten-year SHA-1 to SHA-2 migration [74], which involved only a hash algorithm replacement rather than the full-stack protocol rewrites that PQC migration requires, suggests that banking-sector PQC migration will operate on a similar or longer timescale. Sweden's Riksbank estimates approximately five years for the transition to the T2 settlement platform alone [82], and this is a non-cryptographic infrastructure change. The BIS Project Leap experiment found that even a controlled PQC test in one payment system required substantial development effort, tailored adaptations for each participant, and highlighted the need for further testing "with broader participation of all users of the Eurosystem market infrastructure" [11].

The practical conclusion is that Steps 1 through 3 of this framework, the cryptographic inventory, risk classification, and target architecture definition, should be initiated immediately, regardless of remaining uncertainties about regulatory specifics or vendor readiness.

Steps 4 through 6, piloting, production migration, and embedding crypto-agility, should commence as soon as inventory and classification are sufficiently mature. The GRI 2024 report captures the appropriate posture: "a successful transition cannot take the form of reactive and rushed crisis management, but should rather be made an integral part of a proactive technology lifecycle management" [32].

The validation outcome and the practical adjustments incorporated into the final framework are reported in aggregate form in Section 7.7.

7.7 Framework Validation

The migration framework presented in this chapter was reviewed by four practitioners across Estonia and Sweden as described in Section 4.2. The interviewees raised no objections to the seven-step structure, considered the framework usable in a banking context, and noted that the checklist presented in Section 7.3 would be of practical value in an in-house migration programme.

The validation produced the following practical adjustments, which have been incorporated into the version of the framework presented above:

- Performance impact measurement was made an explicit checklist item under pilot projects and validation (Item F.3, “Measure and document performance impact”), so that the operational cost of PQC algorithms is quantified before production migration rather than discovered during it.
- PQC readiness criteria were added to the training and awareness section as a procurement and vendor evaluation requirement (Item B.3, “Include PQC readiness criteria in procurement and vendor evaluation processes”), reflecting the practitioner observation that vendor commitments need to be established at contracting stage rather than negotiated after the fact.
- The “Definition of Done” column of the checklist was expanded across multiple items to specify concrete acceptance criteria, for example documented Cryptographic Bills of Materials, signed-off rollback plans, and quarterly management body reporting, so that each step has an unambiguous completion condition rather than a directional aim.

No step was identified as unrealistic or removable. The validation does not constitute empirical evidence of sector-wide consensus on the framework, but it does indicate that the framework reflects current practitioner thinking in two banking markets.

8 Conclusion

8.1 Key Findings

The central finding is that awareness of the quantum threat exists but has not translated into organisational action. All respondents consider PQC migration at least moderately urgent, recognise that a cryptographic compromise would cause systemic disruption, and understand the store-now-decrypt-later threat. Yet none has formally integrated quantum risk into their enterprise risk management framework, none has started a formal migration project, and no institution has a detailed migration plan with inventories, milestones, budgets, and governance fully specified. The banking sector is aware but not yet acting.

This awareness-action gap is consistent across both countries. Estonian and Swedish banks are at the same readiness stage despite operating in structurally different banking ecosystems — Estonia’s small, concentrated market embedded in national digital infrastructure, and Sweden’s larger, internationally integrated financial system. The shared EU regulatory framework, particularly DORA, the European Commission PQC Recommendation, and the NIS Cooperation Group roadmap, produces a regulatory signal that is more specific than banks appear to recognise. Yet banks in both countries interpret the framework as directionally clear but not yet a mandate to act.

Three factors sustain this gap. First, PQC migration remains positioned as a technical IT matter rather than a governance challenge. Only one respondent reported executive leadership involvement, and none has elevated quantum risk to board-level attention, despite DORA’s requirement for management body oversight of ICT risk. Second, banks are constrained by vendor dependencies they cannot resolve unilaterally. HSM vendors were identified as a specific bottleneck, and three of four respondents cited dependence on vendors as the primary barrier to migration. Third, the regulatory signal, while more specific than banks recognise, lacks PQC-specific deadlines, which banks treat as permission to defer. All respondents identified formal regulatory requirements as the factor most likely to drive PQC investment.

Read against Table 3, the cryptographic technical controls under DORA Art. 9(2), 9(3)(d), 9(4)(d) and RTS 2024/1774 Art. 6, 7 are satisfied for classical threats but not for the forward-looking dimension that RTS 2024/1774 Recital 9 and Art. 6(4) make explicit in referring to “threats from quantum advancements” and to provisions for updating cryptographic technology in response to developments in cryptanalysis. The governance obligation under DORA Art. 5(2) is unmet for this risk category in any of the surveyed banks. The gap is therefore not a matter of new obligations but of operationalising existing ones.

The cross-country comparison revealed that the character of the migration challenge differs even where the readiness level does not. Estonian banks face a systemic dependency on national digital infrastructure — X-Road and the eID system — that ties their migration to broader national coordination. Swedish banks face the challenge of scale: more systems, deeper legacy infrastructure, longer replacement cycles, and cross-border operations that multiply coordination requirements. The direct interconnection between the two markets through Swedish-owned subsidiaries in Estonia means that migration decisions in one country propagate to the other.

Based on these findings, the thesis proposed a sector-specific PQC migration framework that addresses three structural characteristics distinguishing banking from other sectors: systemic interdependence through shared payment infrastructure, a regulatory specificity gap where obligations are directionally clear but operationally unspecified, and concentration risk in vendor ecosystems where a small number of providers constrain institutional migration timelines. The framework comprises six migration steps — from cryptographic inventory through embedding crypto-agility — and identifies common pitfalls including the misconception that PQC migration is a simple algorithm replacement, the assumption that vendors will manage the transition, and the risk of deferring action until regulatory requirements become binding.

8.2 Recommendations

8.2.1 Recommendations for Banks

Banks should begin the first three steps of the proposed migration framework immediately: establishing a comprehensive cryptographic inventory, classifying assets by quantum risk,

and defining a target cryptographic architecture. These steps do not depend on regulatory specifics or vendor readiness and represent the minimum preparation needed to avoid being caught unprepared when binding requirements or a credible quantum threat materialises. The NIS Cooperation Group roadmap expects high-risk use case migration to be completed by 2030, leaving limited time for institutions that have not yet begun.

PQC migration should be elevated from an IT initiative to a governance-level programme with executive sponsorship, dedicated budget, and cross-functional oversight. DORA already requires management bodies to approve and oversee the ICT risk management framework, and Article 5(2) creates personal liability for non-compliance. Interpreting these obligations proactively to include quantum risk assessment positions institutions ahead of the regulatory curve rather than behind it.

Banks should actively manage vendor concentration risk by diversifying cryptographic dependencies, requiring PQC readiness commitments from key vendors, and pursuing vendor-neutral architectural patterns. Crypto-agility should be embedded as a design principle, not as a one-time migration goal, ensuring that the institution can adapt to future cryptographic transitions without repeating the current multi-year preparation cycle.

Given the systemic interdependence of banking infrastructure, individual institutions should engage in sector-level coordination through national banking associations and central bank working groups. The Dutch and Swiss models of collaborative quantum readiness provide relevant precedents for both Estonian and Swedish banks.

8.2.2 Recommendations for Regulators and Supervisors

Regulators should build on the existing regulatory foundation, by translating these provisions into concrete supervisory guidance with specific PQC migration milestones. The findings confirm that banks treat regulation as the primary driver of action, and the current absence of explicit PQC requirements creates uncertainty that slows preparation rather than accelerating it. Incorporating quantum risk into supervisory review processes — for example through the SREP framework — would provide the signal that banks are waiting for.

National PQC transition roadmaps, as called for by the NIS Cooperation Group, should be

developed for both Estonia and Sweden. Neither country had issued such a roadmap at the time of writing. These roadmaps should include sector-specific milestones for banking, given the sector's role as critical infrastructure and the extended migration timelines that shared payment systems require.

Supervisory authorities should also address the vendor concentration risk identified in this thesis by requiring financial entities to assess and report on their vendors' PQC readiness as part of ICT third-party risk management under DORA, and by engaging directly with critical infrastructure providers — particularly HSM vendors and payment network operators — to establish coordinated migration timelines.

8.3 Future Research

This study has several limitations that have been acknowledged in Section 4. The sample of four respondents from two countries provides indicative rather than generalisable findings. The questionnaire captured self-reported assessments of readiness, which may not fully reflect actual institutional capabilities or gaps. Access to detailed internal migration plans, technical architecture documentation, or board-level risk registers was not available, limiting the depth of analysis possible for each institution. The comparative design was constrained by the small number of respondents per country, making it difficult to distinguish institutional variation from country-level patterns with confidence.

Future research should expand the sample to include more institutions and additional countries, particularly those with national PQC roadmaps, to assess whether the presence of a national strategy produces measurably different institutional outcomes. Longitudinal studies tracking the same institutions over time would reveal whether the current preparatory posture evolves into active migration or remains stalled. Research examining the vendor ecosystem — particularly HSM vendors' PQC development timelines and their impact on banking migration — would address a constraint that this thesis identified as critical but could not investigate in depth. Finally, as banks begin pilot projects and early migrations, case studies documenting the practical challenges, costs, and timelines of PQC implementation in banking environments would provide the empirical foundation that the sector currently lacks.

The sector-specific migration framework proposed in this thesis could also be developed further through practitioner workshops and expert validation, refining the migration steps, preconditions, and pitfalls based on broader industry input. Publication of the framework as a standalone guidance document, potentially through banking associations or industry bodies, would extend its practical reach beyond the academic context.

8.3.1 Practical Relevance and Dissemination

This thesis was designed to produce a practically useful document rather than an academic exercise with limited application beyond the university context. The five-dimensional readiness assessment and the sector-specific migration framework were developed in response to a gap identified not only in the literature but in current industry practice: banks recognise the quantum threat but lack sector-specific guidance to translate awareness into action.

The practical relevance of the findings has been confirmed by early engagement with the industry. Both the Estonian Banking Association's Information Security Committee and Finance Sweden's Banks Security Committee, which served as the access channels for data collection, have expressed interest in the results and have invited the author to present the findings to their respective memberships. These presentations provide an opportunity to validate the proposed framework against a broader set of practitioners and to contribute directly to the sector-level coordination that the thesis identifies as a prerequisite for effective PQC migration.

The thesis findings may also inform future regulatory and supervisory initiatives. The NIS Cooperation Group roadmap calls for national PQC transition roadmaps by the end of 2026, and neither Estonia nor Sweden had issued such a roadmap at the time of writing. The cross-country analysis and sector-specific framework presented here could serve as input for these national processes, particularly given the detailed mapping of banking-specific dependencies, regulatory gaps, and vendor constraints.

References

- [1] Peter W. Shor. „Algorithms for Quantum Computation: Discrete Logarithms and Factoring“. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.
- [2] Michele Mosca. „Cybersecurity in an Era with Quantum Computers: Will We Be Ready?“. In: *IEEE Security & Privacy* 16.5 (2018), pp. 38–41. doi: 10.1109/MSP.2018.3761723.
- [3] Craig Gidney and Martin Ekerå. „How to Factor 2048-bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits“. In: *Quantum* 5 (2021), p. 433. doi: 10.22331/q-2021-04-15-433.
- [4] Craig Gidney. *How to Factor 2048-bit RSA Integers with Less Than a Million Noisy Qubits*. arXiv:2505.15917. 2025. doi: 10.48550/arXiv.2505.15917.
- [5] Madelyn Cain et al. *Shor’s Algorithm is Possible with as Few as 10,000 Reconfigurable Atomic Qubits*. 2026. arXiv: 2603.28627 [quant-ph]. URL: <https://arxiv.org/abs/2603.28627>.
- [6] Ryan Babbush et al. *Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations*. Tech. rep. Google Quantum AI, Ethereum Foundation, and Stanford University, Mar. 2026. URL: <https://quantumai.google/static/site-assets/downloads/cryptocurrency-whitepaper.pdf>.
- [7] Frank K. Wilhelm et al. *Status of Quantum Computer Development (Entwicklungsstand Quantencomputer), Version 2.2*. Tech. rep. Bonn: Federal Office for Information Security (BSI), 2025. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_2.html.
- [8] Heather Adkins and Sophie Schmieg. *Quantum Frontiers May Be Closer Than They Appear*. Google Blog, 25 March 2026. Accessed: 2026-04-18. Mar. 2026. URL: <https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/>.
- [9] Bas Westerbaan. *Cloudflare Targets 2029 for Full Post-Quantum Security*. Cloudflare Blog, 7 April 2026. Accessed: 2026-04-18. Apr. 2026. URL: <https://blog.cloudflare.com/post-quantum-roadmap/>.
- [10] European Parliament and Council. *Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA)*. 2022. URL: <https://eur-lex.europa.eu/eli/reg/2022/2554>.
- [11] Bank for International Settlements (BIS). *Quantum-Readiness for the Financial System: A Roadmap*. 2024. URL: <https://www.bis.org/publ/bppdf/bispap158.htm>.

- [12] World Economic Forum and Financial Conduct Authority. *Quantum Security for the Financial Sector: Informing Global Regulatory Approaches*. Tech. rep. Published 17 January 2024 at the World Economic Forum Annual Meeting, Davos-Klosters. World Economic Forum, Jan. 2024. URL: <https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/>.
- [13] Dustin Moody et al. *Transition to Post-Quantum Cryptography Standards*. Tech. rep. NIST IR 8547. National Institute of Standards and Technology, 2024. doi: 10.6028/NIST.IR.8547.ipd.
- [14] European Commission. *Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. 2024. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024H1101>.
- [15] NIS Cooperation Group. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. 2025. URL: <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>.
- [16] European Payments Council. *Guidelines on Cryptographic Algorithms Usage and Key Management – 2026*. Tech. rep. EPC342-08, Version 16.0. Produced by the Payment Security Support Group (PSSG). European Payments Council, 2026. URL: <https://www.epc-cep.eu>.
- [17] Paul Chammas et al. „Towards a Comprehensive Risk Framework for PQC Migration in Legacy Systems“. In: (July 2025). Accessed: 2026-04-18. URL: https://www.qurisk.fr/s/Towards_a_Holistic_Risk_Framework_For_PQC_Migration_in_Legacy_Systems.pdf.
- [18] K. F. Hasan et al. „A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies“. In: (2024). doi: 10.1109/ACCESS.2024.3360412.
- [19] Federal Office for Information Security (BSI) and KPMG. *Market Survey: Cryptography and Quantum Computing – German Market Developments*. 2023. URL: <https://kpmg.com/de/en/home/insights/2023/04/market-survey-cryptography-and-quantum-computing-kpmg-bsi-2023.html>.
- [20] Finance Denmark et al. *Nordic-Baltic Financial Sector EU Policy Recommendations 2024–2029*. Accessed: 2026-04-18. Feb. 2024. URL: <https://finansdanmark.dk/media/crnfs4vj/nordic-baltic-2024-2029.pdf>.
- [21] World Economic Forum. *The Global Risks Report 2025*. Tech. rep. Published 15 January 2025. Based on Global Risks Perception Survey 2024–2025 with over 900 experts. Covers 33 global risks across economic, environmental, geopolitical, societal, and technological categories. World Economic Forum, Jan. 2025. URL: <https://www.weforum.org/publications/global-risks-report-2025/>.
- [22] FS-ISAC. *Building Cryptographic Agility in the Financial Sector*. 2024. URL: <https://www.fsisac.com/pqc-crypto-agility>.

- [23] National Institute of Standards and Technology. *What Is Post-Quantum Cryptography?* 2025. URL: <https://www.nist.gov/cybersecurity/what-post-quantum-cryptography>.
- [24] Lily Chen et al. *Report on Post-Quantum Cryptography (NISTIR 8105)*. Tech. rep. National Institute of Standards and Technology, 2016. DOI: 10.6028/NIST.IR.8105.
- [25] J. S. Arun, R. Harishankar, and W. Rjaibi. *Becoming Quantum Safe: Protect Your Business and Mitigate Risks with Post-Quantum Cryptography and Crypto-Agility*. 2025. DOI: 10.1002/9781394406784.
- [26] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, eds. *Post-Quantum Cryptography*. 1st ed. Mathematics and Statistics. Berlin, Heidelberg: Springer, 2009. ISBN: 978-3-540-88701-0. DOI: 10.1007/978-3-540-88702-7.
- [27] ANSSI et al. *Joint Position Paper on Quantum Key Distribution*. 2024. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html.
- [28] C. Rubio García et al. „Enhanced Network Security Protocols for the Quantum Era: Combining Classical and Post-Quantum Cryptography, and Quantum Key Distribution“. In: (2025). DOI: 10.1109/JSAC.2025.3568011.
- [29] Charles H. Bennett and Gilles Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing“. In: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India: IEEE, 1984, pp. 175–179.
- [30] Nilesh Vyas and Paulo Mendes. *Relaxing Trust Assumptions on Quantum Key Distribution Networks*. 2024. DOI: 10.48550/arXiv.2402.13136. arXiv: 2402.13136 [quant-ph].
- [31] Bruno Huttner et al. „Long-Range QKD Without Trusted Nodes is Not Possible with Current Technology“. In: *npj Quantum Information* 8.108 (2022). DOI: 10.1038/s41534-022-00613-4.
- [32] Global Risk Institute. *Quantum Threat Timeline Report 2024*. 2024. URL: <https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/>.
- [33] Yaser Baseri et al. „Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition“. In: *Computers & Security* 150 (2025), p. 104272. DOI: 10.1016/j.cose.2024.104272.
- [34] Oscar Covers et al. *Prioritising Post-Quantum Cryptography Migration Activities in Financial Services*. Tech. rep. Luxembourg: Europol, 2026. DOI: 10.2813/9782176.
- [35] National Institute of Standards and Technology. *Considerations for Achieving Crypto Agility: Strategies and Practices*. Cybersecurity White Paper (CSWP) 39. NIST, 2025. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf>.
- [36] European Union Agency for Cybersecurity (ENISA). *Post-Quantum Cryptography – Integration Study*. 2024. URL: <https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study>.

- [37] S. Sadeghi et al. „Securing Financial Sector Applications in the Quantum Era: An Evaluation of NIST’s Recommended Algorithms through Use-Case Analysis“. In: (2025). DOI: 10.1016/j.eswa.2025.128243.
- [38] Dimitrios Sikeridis. *ELCA: Introducing Enterprise-Level Cryptographic Agility for a Post-Quantum Era*. Cryptology ePrint Archive, Report 2023/1539. 2023. URL: <https://eprint.iacr.org/2023/1539>.
- [39] National Institute of Standards and Technology. *Cybersecurity (NIST Glossary)*. <https://csrc.nist.gov/glossary/term/cybersecurity>. Accessed: 2026-03-23. 2024.
- [40] IBM. *How IBM Will Build the First Large-Scale Fault-Tolerant Quantum Computer*. 2025. URL: <https://www.ibm.com/quantum/blog/large-scale-ftqc>.
- [41] National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. <https://doi.org/10.6028/NIST.FIPS.203>. Federal Information Processing Standards Publication (FIPS) 203. Aug. 2024. DOI: 10.6028/NIST.FIPS.203.
- [42] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems“. In: *Communications of the ACM* 21.2 (1978), pp. 120–126. DOI: 10.1145/359340.359342.
- [43] Martin Roetteler et al. „Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms“. In: *Advances in Cryptology – ASIACRYPT 2017*. Vol. 10625. Lecture Notes in Computer Science. Springer, 2017, pp. 241–270. DOI: 10.1007/978-3-319-70697-9_9.
- [44] V. Gheorghiu and M. Mosca. „Quantum Resource Estimation for Large-Scale Quantum Algorithms“. In: (2025). DOI: 10.1016/j.future.2024.107480.
- [45] Frank Arute, Kunal Arya, Ryan Babbush, et al. „Quantum Supremacy Using a Programmable Superconducting Processor“. In: *Nature* 574 (2019), pp. 505–510. DOI: 10.1038/s41586-019-1666-5.
- [46] Craig Gidney and Martin Ekerå. „How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits“. In: *Quantum* 5 (2021), p. 433. DOI: 10.22331/q-2021-04-15-433.
- [47] Lov K. Grover. „A Fast Quantum Mechanical Algorithm for Database Search“. In: *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*. ACM, 1996, pp. 212–219. DOI: 10.1145/237814.237866.
- [48] Gilles Brassard, Peter Høyer, and Alain Tapp. „Quantum Cryptanalysis of Hash and Claw-Free Functions“. In: *SIGACT News* 28.2 (1997), pp. 14–19. DOI: 10.1145/261342.261346.
- [49] Mastercard. *Migration to Post-Quantum Cryptography*. 2024. URL: <https://www.mastercard.com/europe/en/news-and-trends/Insights/2025/post-quantum-cryptography-white-paper.html>.
- [50] European Commission. *Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework*. http://data.europa.eu/eli/reg_del/2024/1774/oj. OJ L, 2024/1774, 25 June 2024. In force. 2024.

- [51] European Banking Authority. *Guidelines on ICT and Security Risk Management*. Tech. rep. EBA/GL/2019/04, issued 28 November 2019; amended 14 October 2024 to align with DORA (Regulation (EU) 2022/2554). European Banking Authority, 2019. URL: <https://www.eba.europa.eu/publications-and-media/press-releases/eba-amends-its-guidelines-ict-and-security-risk-management-measures-context-dora-application>.
- [52] European Parliament and Council of the European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union*. Official Journal of the European Union, L 333, pp. 80–152. 2022. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>.
- [53] Riigikogu. *Küberturvalisuse seadus*. Riigi Teataja, RT I, 22.05.2018, 1; as amended RT I, 30.12.2025, 4. Adopted 09.05.2018, NIS2 amendments entered into force 01.01.2026. 2018. URL: <https://www.riigiteataja.ee/akt/130122025015>.
- [54] Sveriges riksdag. *Cybersäkerhetslag (SFS 2025:1506)*. Svensk författningssamling. Issued 2025-12-11, in force 15 January 2026. Transposing Directive (EU) 2022/2555 (NIS2). 2025. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/cybersakerhetslag-20251506_sfs-2025-1506/.
- [55] Ministry of Economic Affairs and Communications of Estonia. *Cybersecurity Strategy 2024–2030: Cyber-Conscious Estonia*. https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf. Accessed 2026. 2024.
- [56] Jelizaveta Vakarjuk, Nikita Snetkov, and Peeter Laud. „Identifying Obstacles of PQC Migration in E-Estonia“. In: *CyCon 2024: Over the Horizon – 16th International Conference on Cyber Conflict*. Ed. by C. Kwan et al. Tallinn: NATO CCDCOE Publications, 2024, pp. 63–81.
- [57] Cybernetica AS. *Quantum Safety with Cybernetica: Whitepaper on Post-Quantum Cryptography*. Whitepaper. 2025.
- [58] Cybernetica AS. *Eesti postkvant-krüptograafia ülemineku riiklik teekaart*. Aruanne. Estonian. Research Report D-16-1248. Version 1.0. Funded by the European Union NextGenerationEU. Project ROAD2PQ. Cybernetica AS, Apr. 30, 2026, p. 112.
- [59] Cybernetica. *VÕIME – Krüptograafiliste turbelahenduste hindamisvõimekuse loomine*. Funded 2024–2026, 133 000 EUR. ETIS project ID: d2dd979a-c7cf-4a1f-a8d3-1d4afd398ad1. 2024. URL: <https://cyber.ee/research/projects/voime/> (visited on 04/17/2026).
- [60] European Commission. *Estonia Latest Country to Sign Up to EuroQCI Initiative*. Shaping Europe’s Digital Future. Oct. 2020. URL: <https://digital-strategy.ec.europa.eu/en/news/estonia-latest-country-sign-euroqci-initiative>.

- [61] RISE Research Institutes of Sweden AB. *Nordic Quantum Communication Infrastructure (NordicQCI)*. EU Funding & Tenders Portal, Connecting Europe Facility. Project ID: 101249648, January 2026 – June 2029, EU contribution: EUR 4,995,554. 2026. URL: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/org-details/911424126/project/101249648/program/43152860/details>.
- [62] Government of Sweden. *Uppdrag att inkomma med underlag för en nationell strategi inom kvantområdet*. Government decision U2024/01451, Utbildningsdepartementet. Commission to Vetenskapsrådet (Swedish Research Council) to develop input for a national quantum strategy 2025–2030, deadline October 2024. May 2024.
- [63] Swedish Government. *National Quantum Strategy for Sweden 2025–2030*. <https://qsip.se/2024/05/28/swedish-government-takes-initiative-for-a-national-quantum-strategy>. Accessed 2026. 2024.
- [64] Nationellt cybersäkerhetscenter (NCSC). *Rekommendationer för övergången till kvantsäker kryptografi*. Swedish. National Cyber Security Centre of Sweden, FRA. May 2025. URL: <https://www.ncsc.se/siteassets/publikationer/rekommendationer-for-overgangen-till-kvantsaker-kryptografi.pdf> (visited on 05/18/2026).
- [65] Finansiell ID-Teknik BID AB. *About BankID*. Accessed: 2026-04-17. 2024. URL: <https://www.bankid.com/en/om-oss>.
- [66] Getswish AB. *Swish 2025: New Services, New Behaviors and How Sweden Pays*. Accessed: 2026-04-17. 2025. URL: <https://www.swish.nu/newsroom/stories/swish-2025-new-services-new-behaviors-and-how-sweden-pays>.
- [67] Government Offices of Sweden. *Sweden in a Digital World: Security Policy and Cybersecurity*. <https://www.government.se/government-policy/sweden-in-a-digital-world/security-policy>. Accessed 2026. 2023.
- [68] BIS Innovation Hub Eurosystem Centre et al. *Project Leap Phase 2: Quantum-Proofing Payment Systems*. Tech. rep. Published 9 December 2025. Tested post-quantum cryptography in an operational payment system, replacing traditional digital signatures with PQC algorithms. Bank for International Settlements, Dec. 2025. URL: <https://www.bis.org/publ/othp107.htm>.
- [69] European Commission. *Commission Delegated Regulation (EU) 2024/1774 supplementing Regulation (EU) 2022/2554 with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies*. Delegated Regulation of 13 March 2024, published in Official Journal L series, 2024/1774. 2024. URL: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj.
- [70] PKI Consortium PQC Working Group. *Post-Quantum Cryptography Maturity Model (PQCMM)*. Draft maturity model, published 27 October 2025. Defines five maturity levels (Initial through Optimized) for PQC adoption. Oct. 2025. URL: <https://pkic.org/2025/10/27/defining-quantum-readiness-introducing-the-post-quantum-cryptography-maturity-model/>.

- [71] Cryptomathic. *PQC Migration Challenges for Financial Institutions*. 2025. URL: <https://www.cryptomathic.com/blog/pqc-migration-challenges-compliance-risks-for-financial-institutions>.
- [72] Michela Menting. *What Does Quantum-Safe Really Mean for HSM Vendors? Vendor Playbook for Internal and External PQC Support*. ABI Research. Nov. 2025. URL: <https://www.abiresearch.com/blog/quantum-security-for-hardware-security-modules-hsms>.
- [73] National Cyber Security Centre. *Timelines for Migration to Post-Quantum Cryptography*. 2025. URL: <https://www.ncsc.gov.uk/guidance/pqc-migration-timelines> (visited on 04/17/2026).
- [74] J. S. Onkenhout. „Secure Payments in the Quantum Era: A Technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector“. Master thesis. Delft University of Technology, 2023.
- [75] AIVD, CWI, and TNO. *The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography*. Tech. rep. Published 3 December 2024. Covers quantum-vulnerability diagnosis, migration planning, execution, and cryptographic agility. Includes PQChoiceAssistant tool. General Intelligence, Security Service (AIVD), Centrum Wiskunde & Informatica (CWI), and TNO, Dec. 2024. URL: <https://english.aivd.nl/latest/news/2024/12/03/aivd-cwi-and-tno-publish-renewed-handbook-for-quantum-safe-cryptography>.
- [76] Gireesh N. Kumar and Santhosh M. Kumar. *Enterprise Cryptographic Agility: Beyond Algorithms and Protocols*. Tech. rep. Whitepaper outlining seven strategic pillars of enterprise cryptographic agility: information, process, architecture, infrastructure, operations, governance, and education. AvinyaSQ Technologies, 2025. URL: <https://avinyasq.com/building-enterprise-cryptographic-agility-the-seven-key-pillars>.
- [77] Cryptomathic. *Tier-1 Global Bank: Crypto-Agility Case Study*. 2025. URL: <https://www.cryptomathic.com/case-studies/tier-1-bank-pqc>.
- [78] Cybernetica AS. *Post-Quantum Cryptography and Estonia’s Digital Identity Infrastructure*. <https://e-estonia.com/cybernetica-post-quantum-cryptography-joins-to-menu>. Accessed 2026. 2022.
- [79] European Cybersecurity Certification Group. *Agreed Cryptographic Mechanisms*. Tech. rep. Version 2.0. European Cybersecurity Certification Group, 2025.
- [80] Rainer Kattel and Ines Mergel. „Estonia’s Digital Transformation: Mission Mystique and the Hiding Hand“. In: *Great Policy Successes*. Ed. by Mallory Compton and Paul ’t Hart. Oxford University Press, 2019. doi: 10.1093/oso/9780198843719.003.0008.
- [81] Sveriges Riksbank. *Payments Report 2024*. Sveriges Riksbank. Mar. 2024. URL: <https://www.riksbank.se/globalassets/media/rapporter/betalningsrapport/2024/engelsk/payments-report-2024.pdf>.

- [82] Sveriges Riksbank. *The Riksbank Wants to Use the European T2 Platform for Payment Settlement*. Press release, 18 June 2024. Transition expected to take approximately five years. June 2024. URL: <https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/press-releases/2024/the-riksbank-wants-to-use-the-european-t2-platform-for-payment-settlement/>.

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis¹

I Marja-Liisa Soone

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis “Assessing Post-Quantum Cryptography Readiness in the Banking Sector”, supervised by Jelizaveta Vakarjuk and Nikita Snetkov
 - 1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
 - 1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright
2. I am aware that the author also retains the rights specified in clause 1 of the nonexclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons’ intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

19.05.2026

¹The non-exclusive licence is not valid during the validity of access restriction indicated in the student’s application for restriction on access to the graduation thesis that has been signed by the school’s dean, except in case of the university’s right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive licence shall not be valid for the period.

Appendix 2 – Online Questionnaire

1. Primary country of operation (select one)

- A. Estonia
- B. Sweden
- C. Other, specify: __

2. How urgent does your organisation consider migration to post-quantum cryptography (PQC)? (select one)

- A. Not urgent at all
- B. Slightly urgent
- C. Moderately urgent
- D. Very urgent
- E. Extremely urgent

3. When do you believe quantum computers will realistically be able to break commonly used public-key cryptography? (select one)

- A. Within the next 5 years
- B. Between 5 and 10 years
- C. Between 10 and 15 years
- D. After 15 years
- E. Do not know

4. Has your organisation assessed quantum-related cryptographic risks within its enterprise risk-management framework? (select one)

- A. Integrated into the risk register and regularly assessed
- B. Identified and being incorporated
- C. Recognised but not yet formally addressed
- D. Not considered
- E. Do not know

5. What is the maximum length of time your organisation must keep data confidential? (select one)

- A. Less than 1 year
- B. 1–5 years
- C. 5–10 years
- D. More than 10 years

6. Which statement best describes your organisation's current stage in migrating to post-quantum cryptography (PQC)? (select one)

- A. We have migrated to PQC algorithms in at least one system.
- B. We have initiated a formal PQC migration project, but no migration yet.
- C. We have a draft PQC migration project plan but have not started the formal PQC migration project yet.
- D. We have discussed PQC but have do not have a draft PQC migration project plan.
- E. We have not considered PQC.
- F. Do not know

Appendix 2 – Online Questionnaire

7. If your organisation has not yet started migration, when do you plan to begin migration process to post-quantum cryptography (PQC)? (select one)

- A. Within the next 12 months
- B. Within the next 2–3 years
- C. After 3 years
- D. No plan yet

8. Which post-quantum cryptographic (PQC) standards does your organisation currently use or plan to use? (multiple choice)

- A. ML-KEM (Crystals-Kyber)
- B. ML-DSA (Crystals-Dilithium)
- C. SLH-DSA (SPHINCS+)
- D. FN-DS (Falcon)
- E. No PQC standards selected yet
- F. Other, describe: _____

9. Do you have a documented post-quantum cryptography (PQC) migration project plan that includes inventories, milestones, budgets and governance? (select one)

- A. Yes, a detailed plan
- B. Yes, a preliminary plan
- C. Not yet, but planning to develop one
- D. No plan

10. Which of the following steps have you taken or plan to take as part of post-quantum cryptography (PQC) migration? (multiple choice)

- A. Assign internal responsibility for PQC or quantum-related cryptographic risk
- B. Perform a cryptographic inventory
- C. Assess quantum-related risks as part of enterprise risk-management framework
- D. Identify systems or data with long confidentiality requirements
- E. Assess dependencies on quantum-vulnerable algorithms
- F. Introduce cryptographic agility measures
- G. Evaluate or test hybrid cryptographic solutions
- H. Upgrade to cryptographic protocols or infrastructure
- I. Start pilot migration of PQC cryptography
- J. Develop a formal PQC migration project plan
- K. Engage with external guidance or standards bodies
- L. Other, describe: _____
- M. No steps taken yet

11. How do you plan to prioritise which systems or processes will migrate first? (multiple choice)

- A. Based on data sensitivity or confidentiality requirements
- B. Based on regulatory urgency or classification as critical infrastructure
- C. Based on vendor support and product availability
- D. Based on technical feasibility or resource constraints
- E. No prioritisation scheme defined
- F. Other, describe: _____

Appendix 2 – Online Questionnaire

12. Which internal groups are involved or will be involved in post-quantum cryptography (PQC) migration? (multiple choice)

- A. Executive leadership
- B. IT and security operations
- C. Risk management
- D. Legal and compliance
- E. Procurement and vendor management
- F. Other, describe: _____

13. How familiar are you with the following concepts? (scales for each: Not familiar, Aware of the concept, Understands the concept at a high level, Understands the concept and its relevance to banking operations, Actively considers or applies the concept in the organisation)

- A. Post-quantum cryptography (PQC)
- B. Difference between Quantum Computing and Post-quantum cryptography (PQC)
- C. Quantum computing threats to cryptography
- D. Store-now-decrypt-later attacks
- E. Cryptoagility (flexible cryptographic design)

14. How sufficient is your organisation's internal knowledge and expertise to initiate post-quantum cryptography (PQC) migration? (select one)

- A. Not sufficient at all
- B. Somewhat insufficient
- C. Adequate
- D. Mostly sufficient
- E. Fully sufficient

15. Which of the following would most improve your organisation's preparedness for post-quantum cryptography (PQC)? (multiple choice)

- A. Formal training or certification on PQC standards
- B. Guidance on performing cryptographic inventories and asset discovery
- C. Case studies or white papers on successful PQC migrations
- D. Participation in industry working groups or forums
- E. External consultancy or technical support
- F. Other, describe: _____
- G. None of the above

16. What are the primary obstacles limiting your organisation's progress towards post-quantum cryptography (PQC) migration? (multiple choice)

- A. Lack of internal expertise or skills
- B. Unclear or evolving regulatory guidance, expectations and timelines
- C. Dependence on third-party vendors to provide PQC-ready solutions
- D. Budget constraints
- E. Competing priorities within the organisation
- F. Lack of mature, widely adopted PQC products or implementations

Appendix 2 – Online Questionnaire

G. Limited executive or board support

H. Other, describe: _____

17. To what extent does your organisation depend on external software vendors for cryptographic infrastructure? (select one)

- A. Significant dependence (vendor decisions will determine timing)
- B. Moderate dependence (some systems are vendor-managed)
- C. Minimal dependence (mostly in-house)
- D. No dependence
- E. Do not know

18. To what extent does your organisation depend on external hardware vendors for cryptographic infrastructure? (select one)

- F. Significant dependence (vendor decisions will determine timing)
- G. Moderate dependence (some systems are vendor-managed)
- H. Minimal dependence (mostly in-house)
- I. No dependence
- J. Do not know

18. What would help your organisation to accelerate post-quantum cryptography (PQC) migration? (multiple choice)

- A. Clearer regulatory guidance and compliance timelines
- B. Industry forums for knowledge sharing and collaboration
- C. Vendor roadmaps or product availability timelines
- D. External consultants for technical or project management support
- E. Staff training and educational resources
- F. Other, describe: _____

19. Which factors would most encourage your organisation to invest in post-quantum cryptography (PQC) migration? (multiple choice)

- A. Formal regulatory requirements or supervisory deadlines
- B. Availability of production-ready and widely supported PQC standards and implementations
- C. Pressure from customers or business partners
- D. Demonstrated financial benefits or cost savings
- E. Reputation, customer trust, and competitive positioning
- F. Head office or group-level policies
- G. Other, please specify: _____

20. Where does your organisation currently use cryptography? (multiple choice)

- A. Customer data protection (data at rest)
- B. Online banking and web services (data in transit)
- C. Authentication and digital signatures
- D. Internal communications and system integration
- E. Interbank or third-party communication
- F. Backup, archival, or long-term data storage
- G. Endpoint devices (e.g. ATMs, payment terminals, POS systems)

Appendix 2 – Online Questionnaire

H. Other, describe: _____

21. If the cryptographic mechanisms used by your organisation were compromised or became unreliable, what would be the most significant impacts on your organisation? (multiple choice)

- A. Loss of confidentiality of customer or transaction data
- B. Inability to authenticate users, systems, or transactions
- C. Disruption of online banking or customer-facing services
- D. Disruption of interbank communication or payment processing
- E. Regulatory non-compliance and supervisory findings
- F. Operational disruption or service unavailability
- G. Reputational damage and loss of customer trust
- H. Financial losses or liability exposure
- I. Limited or no immediate impact
- J. Other, describe: _____
- K. Do not know

22. Do you have any reflections, comments, concerns or insights regarding the readiness for post-quantum cryptography (PQC) migration?

Describe here: _____

