J.S. Onkenhout
4595769

Secure Payments in the Quantum Era

A Technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector

Secure Payments in the Quantum Era

A Technology Roadmap for the Post-Quantum Cryptography Transition
in the Dutch Banking Sector

Master thesis submitted to Delft University of Technology
in partial fulfillment of the requirements for the degree of
MASTER OF SCIENCE
in **Engineering and Policy Analysis**
Faculty of Technology, Policy, and Management
By

J.S. Onkenhout
Student number: 4595769
15 May 2023

Graduation committee

Chair / First Supervisor:	Prof. Dr. ir. N. Bharosa	TU Delft
Second Supervisor:	Dr. Y. Zhauniarovich	TU Delft
Advisor:	L.V.C. Christiansen	TU Delft
External Supervisor:	D.T. Nadort	EY
External Supervisor:	T. Filippo	EY

Preface

Dear reader,

Before you lies the Master Thesis report: “Secure Payments in the Quantum Era: A Technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector”. This research has developed a Technology Roadmap, based on semi-structured interviews conducted with security-, cryptography-, and payment- specialists from Dutch banks, that outlines a transition plan for the Dutch banking sector to shift towards post-quantum cryptography. The Thesis has been written as part of the completion of the Master of Science Engineering & Policy Analysis at the faculty Technology, Policy & Management from the Technical University of Delft. This research has been conducted from November 1st until May 5th.

I would like to express my deepest gratitude to some people that have helped me to get where I am now and have made it possible for me to have finished this thesis. First of all, I would like to thank my First Supervisor and Chair on my Graduation Committee, Nitesh Bharosa. Thank you for your guidance, and for our interesting discussions about the complex world of PQC. I am very grateful that you agreed to supervise me on this specific topic. Where other professors saw merely obstacles, you showed me how to scope this problem and shape it to what is required for a Master Thesis in a positive and friendly way. Secondly, I would like to thank Yury Zhauniarovich for being my Second Supervisor. Although smaller than Nitesh’s role, your deep technical knowledge and sharp feedback provided me with valuable insights that helped me to improve the quality of this thesis. Thirdly, I would like to thank Lærke Christiansen for fulfilling the role of Advisor in a way that surpassed my expectations of the role. You always made time for a quick call if I had questions, you provided me with many useful articles and gave valuable advice on sections such as the thematic analysis.

I also would like to thank the people at the EY’s cyberteam, who have provided me with supervision over the past six months, enabled me to host a live webcast on this topic to their clients, and truly made me feel like a member of the team. To my supervisors from EY, Daniel Nadort and Taco Filippo, I would like say thank you for showing me what the vision of a cybersecurity consultant entails related to this topic, and thank you for helping me shape this thesis to what it is now. Furthermore, I would like to thank Jeroen, Alexander, and Wilan, without whom I would not have been able to finish TB and EPA in the manner in which I now have.

I am forever grateful to my parents, who have been nothing but supportive of all the educational decisions I have made and have always motivated me to strive for the best. Without them, I would never have been able to accomplish what I have thus far. Lastly, I would like to thank all my friends, and especially my girlfriend, Lisanne, for having to listen to all my post-quantum cryptography stories for the past 6 months and for being positive and supportive every step of the way.

Thank you all, and I hope you enjoy reading this report.

J.S Onkenhout
Amsterdam, May 2023

Executive Summary

In 2019 a quantum computer performed a highly complex operation in 4 minutes, which would have taken the most powerful supercomputers of today around 10,000 years. Performing calculations unimaginably faster than is currently possible may bring great opportunities, but may implicate a threat to digital communications. Digital communication is kept secure through cryptography, which uses mathematical problems to protect sensitive information and communication from malicious acts of cybercrime. Cryptography is widely adopted across the cyberspace. The world's fastest classical computers of today are unable to break cryptography's underlying mathematical schemes, ensuring confidentiality and integrity of everyone's data. However, it is predicted that future quantum computers could theoretically break current cryptography in just a few hours. The moment that a powerful enough quantum computer exists (called Y2Q) thus implicates that cryptography systems will become unusable as digital services are no longer secure. This could have catastrophic consequences for society's critical digital infrastructures, such as those provided by Dutch banks. This problem is very relevant for banks, because of the sector's abundance of sensitive data and information streams that rely on cryptography, as well as their critical role in society's functionality (facilitating payments).

Because of the serious disruptions in critical financial infrastructures that the quantum threat could ignite, decision-makers within banks will be needing governing tools to mitigate risks. Adopting new quantum-resistant cryptographic algorithms, known as post-quantum-cryptography (PQC) is absolutely critical in facilitating safety and security from the quantum threat. However, there is currently little or no governance, or guidance, for the management of this transition towards PQC and guidance is urgently needed. The formulation of these guidance-measures is one of the main challenges regarding the transition towards security in the quantum-era. Therefore, this research focusses on ensuring the Dutch banking sector's safety and security of its digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology – from not merely a technological perspective, but with a holistic approach, considering the involved socio-technical challenges. In order to provide guidance to decision-makers from Dutch banks, this thesis aims to answer the following research question:

How can the Dutch banking sector ensure the safety and security of its digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology?

In order to answer the main research question, the Technology Roadmap (TRM) framework will be used. This framework provides the vital link between a first idea phase (i.e., banks' digital infrastructures face a threat from quantum computing technologies) and the concrete implementation phase (i.e., how do we ensure protection from this threat?). The TRM is a diagram which consists of features, services, systems, resources, and drivers in relation with one another, that together facilitate an overview of what is required for the banks to become quantum-safe. Constructing this roadmap required three main methods:

(1) Exploratory research to identify in which parts of the banks' processes and operations the vulnerabilities to the quantum threat are the highest. This included describing key concepts within cryptography, PQC-developments, and banking services, as well as stakeholder- and dependency-mapping of the Dutch banking environment.
(2) Semi-structured interviews with security architects, payment security specialists, and cryptography specialists from Dutch banks. Herein the perceptions of the Dutch banks on the impact, challenges, resources, capabilities, preparedness, and governance were obtained.
(3) TRM development based on thematic analysis of qualitative data derived from semi-structured interviews in which the perceptions were translated into elements fit for the TRM.

Lastly, the TRM was validated and revised by presenting it to experts and asking for critique, which enabled the final TRM to be developed. after which conclusions and recommendations could be drawn up.

The core banking services were analyzed in terms of the role that cryptography plays to ensure the security of these services, which helped to identify in which parts of the banks' processes and operations the vulnerabilities to the quantum threat are the highest. The exploratory analysis identified the critical processes that entail the certain infrastructures that need to transition towards PQC. These being within the online payment process, the physical card transaction process, and the ATM transaction process. Within these processes the main vulnerabilities lie in: data channels through external public networks and service providers relating to payment gateways, payment processors, local store webservers, online merchant webservers, card association networks and Point-of-Sale (PoS)-terminals. Less vulnerable infrastructures, due to their primary use of symmetric cryptography, are: ATM networks, internal storage and communication infrastructures, inter-bank data exchange, and ATM controllers.

Through combining these insights with findings from the thematic analysis of perceptions derived from the semi-structured interviews, the TRM was developed which presented a 3-phase transition plan that aims to ensure the Dutch banking sector safety and security of its digital infrastructures from cryptography-related cyber threats posed by quantum computing technology. Phase 1 of this transition plan entails the development of a response plan for a potential privacy breach and the development of central cryptographic inventory, through management priority, internal alignment, and experimentation with to-be-standardized PQC algorithms. After PQC algorithms have been standardized, Phase 2 involves the adoption of PQC algorithms in online payment networks, requiring banks to draw up a PQC requirement list for vendors and external service providers. With a hardware replacement strategy in place, Phase 3 entails the replacement of all relevant hardware related to payment processes (payment cards, PoS-terminals, and ATM controllers), updating less prioritized software and network infrastructures, and overcoming technical challenges related to PQC algorithms' larger key-sizes. It is important to note that the implementation of PQC is not a one-time event, but rather an ongoing, ever-evolving, and uncertain process. The continuous development of quantum computing technology means that banks must remain vigilant and adaptable to stay ahead of potential threats, and may need to accelerate certain phases within the transition on a relatively short notice. Additionally, the success of this transition relies heavily on organizational awareness, as well as close collaboration between various stakeholders, vendors, service providers, regulators, and other financial service organizations.

Based on this conclusion, this research has made several recommendations to the Dutch banking sector:

Accomplish management priority. Management priority is crucial for allocating resources to execute the first steps that have to be taken to ensure quantum-safety. Therefore, the banking sector should shift the focus of management toward addressing the quantum threat and transitioning towards post-quantum cryptography (PQC) as a top priority, integrating quantum-readiness into the key strategic goals of the bank by means of organizational awareness. Organizational awareness can be created through workshops, seminars, and events that are aimed at educating management on the business implications of the quantum threat, as well as presenting them with solutions on addressing this threat.

Execute initial risk-free actions. Banks can already take certain risk-free actions in preparation for the PQC-transition, which will strengthen the preparedness of the banks. These actions include:

- Developing a privacy breach response plan
- Developing a centralized cryptographic inventory
- Doubling key-lengths for symmetric-key cryptography algorithms
- Developing a hardware replacement strategy

Extend continuous collaborative research to PQC. Dutch banks should proactively utilize their existing collaborative structures with other vendors, service providers, regulators, and other financial service organizations., to share their experiences and jointly develop strategies for addressing the quantum threat. This will benefit the Dutch financial market as a whole, as sharing experiences with executing the risk-free actions or experimenting with PQC-algorithms is highly relevant for creating a comprehensive understanding of the practical implications and technical challenges associated with becoming quantum-safe.

Content

Nomenclature

Abbreviation	Definition
AES	Advanced Encryption Standard
ATM	Automated Teller Machine
BSN	Burger Service Number (Citizen number)
CISO	Chief Information Security Officer
CPU	Central Processing Unit
CVV	Card Verification Value
DES	Data Encryption Standard
DNB	De Nederlandsche Bank
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EMV	Europay, Mastercard, and Visa
EPA	Engineering & Policy Analysis
FSO	Financial Services Organization
IBAN	International Bank Account Number
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
IT	Information Technology
KYC	Know Your Customer
LFT	Large Fault Tolerant
NIST	National Institute of Standards and Technology
NVB	Nederlandse Vereniging van Banken (Dutch Banking Association)
PIN	Personal Identification Number
PKC	Public Key Cryptography
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PoS	Point of Sale
PQC	Post-Quantum Cryptography
QC	Quantum Computing
QKD	Quantum Key Distribution
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SNDL	Store Now, Decrypt Later
SQ	Sub-Question
SSL	Secure Sockets Layer
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TLS	Transport Layer Security
TRM	Technology Roadmap
Y2Q	Year 2000-and- Quantum

List of Figures

List of Tables

1. Introduction

1.1 Background

Interconnectedness through networks and digital infrastructures affect every aspect of human life in today's society. At the very core of this lies cryptography, facilitating that all the information in these digital infrastructures is safe and secure (Pandeya et al., 2021). Cryptography is a set of technologies most commonly used to ensure integrity, confidentiality, and thereby privacy throughout the cyberspace, providing services such as authentication, identity validation, and data encryption (Dubrawsky, 2010). Not only does cryptography protect sensitive information and communication from malicious acts of cybercrime, it is also widely adopted across the cyberspace because it provides its services without the need for physical individuals to be present (Bharosa et al., 2015; Hunt, 2001; Linn, 2000). As most of the critical digital services, including financial services, rely heavily on cryptography, it is of vital importance that its functionality and integrity will not be compromised. However, as one might now anticipate, cryptography is facing a luring threat from a disruptive emerging technology…

Quantum computing often gets classified as a rudimentary and imperfect technology as of today, wherein vast technological evolution is still needed for it to achieve application (Joseph et al., 2022). Without going into detail on the technological foundations behind quantum computing (see Section 2.4), quantum computers can be seen as machines that are able to solve a variety of scientific, or business problems, in an exponentially faster manner than classical (super)computers (IBM, 2021). It may be true that wide-spread applications of quantum computers are currently not yet out there, but Grimes (2020) and IBM (2021) argue that this may be just a few years away. Cryptography will be affected by the emergence of quantum computing, as it is hypothesized that quantum technology will be able to crack the currently used (public- and symmetric-) key cryptosystems on which cryptography relies (Grimes, 2020; Joseph et al., 2022). The world's fastest classical computers of today are unable to break cryptography's underlying mathematical schemes, or more specifically: they would up to 16 billion years (Dasso et al., 2020). Quantum computers however, could theoretically accomplish this in just a few hours (Gidney & Ekerå, 2021). The moment that a powerful enough quantum computer exists, thus implicates that current cryptography systems will become unsafe as digital services are no longer secure (de Wolf, 2017). This is very worrisome because it endangers individuals, organizations, governments, and therefore society as a whole (World Economic Forum, 2021). As the banking industry is one of the most critical sectors on which society relies (Allen & Carletti, 2008), protecting the banks' digital infrastructure from this threat is of the utmost importance.

The moment quantum computing technology breaks current cryptography is by some researchers humorously called Y2Q – referring to the Y2K situation at the turn of the millennium (Grimes, 2020), but this time around society does not know exactly when this will take place. For society to be safe and secure for when this so-called Y2Q occurs, actions must be taken now to transition organizations towards a new form of quantum-resistant-cryptography. Cryptographic algorithms that are quantum-resistant are the first step (World Economic Forum, 2022). There are many

more aspects related to a successful transition towards quantum-resistant-cryptography. Because of the serious disruptions in critical financial infrastructures that the quantum threat could ignite, decision-makers within banks will be needing governing tools to mitigate risks (Csenkey & Bindel, 2022). However, there is currently little or no governance, or guidance, for the management of this transition and guidance for cryptography governance is urgently needed (World Economic Forum, 2021). The formulation of these guidance-measures is one of the main challenges regarding the transition towards quantum-resistant-cryptography (Mosca, 2018; Pandeya et al., 2021).

1.2 Research problem

The threat that quantum computers pose implicates a very large risk to banks, because of the sector's abundance of sensitive data and information streams that rely on cryptography (Rabah, 2005), as well as their critical role in society's functionality (Allen & Carletti, 2008; Bouma et al., 2017). Therefore, it is of the utmost importance that the digital infrastructures, that the banking sector rely on, are safe and secure from the quantum threat to cryptography. The National Institute of Standards and Technology (NIST) is publishing standards for quantum-resistant cryptography algorithms, better known as post-quantum-cryptography (PQC), in the summer of 2023 (NIST, 2022a). Standards for PQC are highly anticipated, because researchers have already found that adopting some form of PQC is absolutely critical in facilitating this safety and security for many types of organizations, such as banks (Joseph et al., 2022), as well as for governments (Kong et al., 2022).

The problem, however, is that transitioning banking's digital infrastructures towards safety and security from the quantum threat to cryptography is very complex (Joseph et al., 2022), and the associated challenges are not merely technological, but actually socio-technical in nature (Kong et al., 2022). This entails challenges as: knowledge gaps, unclear governance, lack of urgency, in-house management support, institutional void, stakeholder collaboration, lack of awareness, and lack of policy guidance (Kong et al., 2022). The identification of these non-technological aspects of this transition call for research to a complete overview on the requirements needed for banks to transition towards safety and security from the quantum threat to cryptography, including guidance in governance (Mosca, 2018; Pandeya et al., 2021). Therefore, this study's research focusses on ensuring the Dutch banking sector's safety and security of its digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology – from not merely a technological perspective, but with a holistic approach, considering the involved socio-technical challenges.

1.3 Scope

As this research has been carried out in collaboration with Ernst & Young Advisory Netherlands LLP (EY), their interest also needed to be considered. The results of this research must have some added value for the clients that the Cybersecurity Consultancy team at EY serves, namely Financial Service Organizations (FSOs). FSOs include banks, asset management firms, insurance organizations and capital markets. Within FSOs, the banking industry is the most influential and critical sector in terms of societal impact (Allen & Carletti, 2008). Moreover, the quantum threat poses a very large risk to banks, because of the sector's abundance of sensitive data and information streams that rely on

cryptography (Rabah, 2005). Secondly, the banking industry encompasses many different processes that rely on digital infrastructures (Galazova & Magomaeva, 2019; Zamaslo et al., 2021), which need to be identified and analyzed in terms of their relationship with the quantum threat to cryptography. If this research would also address insurance organizations, asset management firms and more other FSO-types, the research objectives would not be reached within the required timeframe. Therefore, these other FSO-types are out of scope.

Because of these arguments, this research focusses on the aforementioned quantum threat from a cybersecurity perspective, within the banking sector. For data-availability and research feasibility reasons, the focus is geographically limited to the Netherlands.

1.4 Main research question

This section formulates and clarifies one high-over main research question, that encompasses all elements of the problem (section 1.2) and takes the scope (section 1.3) into account. The question is stated below:

How can the Dutch banking sector ensure the safety and security of its digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology?

In order to answer the main research question, the Technology Roadmap (TRM) framework is used. This framework is the vital link between a first idea phase (i.e., banks' digital infrastructures face a threat from quantum computing technologies) and the concrete implementation phase (i.e., how do we ensure protection from this threat?) (Pandeya et al., 2021). The TRM approach is suitable to introduce a new service to the marketplace, or transition towards new technology, wherein companies within the sector must make a number of complex decisions, in which there is usually uncertainty regarding trends and channeling resources in the new direction (Pandeya et al., 2021).

Thus, this is an approach that can be seen as a planning technique for an innovation in a new direction that involves the most important actors from within and outside the company and is consistent with the company's strategic goals (Garcia & Bray, 1997; Pandeya et al., 2021). Ensuring the safety and security of digital infrastructures from the quantum threat fits with this approach because it entails planning (Joseph et al., 2022), it can be seen as an innovation in a new direction (Grimes, 2020), and the problem involves multiple stakeholders (Kong et al., 2022). Moreover, the TRM approach was used in similar research, wherein researchers investigated *how* companies, or whole sectors, could transition towards a new technology, or mitigate risks from a threat of an emerging technology (Barney et al., 2016; Carvalho et al., 2013; Daim et al., 2018a; Pandeya et al., 2021; Schimpf & Abele, 2019; Schneier, 1999; Willyard & McClees, 1987).

1.5 Approach and Sub-Questions

In this section the sub-questions are identified and formulated, in order to structure answering the main research question, which involves developing a TRM Framework. The development of a TRM Framework will typically result in a visual representation, consisting of multiple layers. This entails relationships between (1) drivers, (2) services, systems, and capabilities that will help the organization achieve its vision or strategy, and (3) resources required to achieve the goals (Pandeya et al., 2021). A visual representation of this is shown in Figure 1, and is based on the works of Kostoff & Schaller (2001), Probert et al. (2005), and Wells et al. (2004).

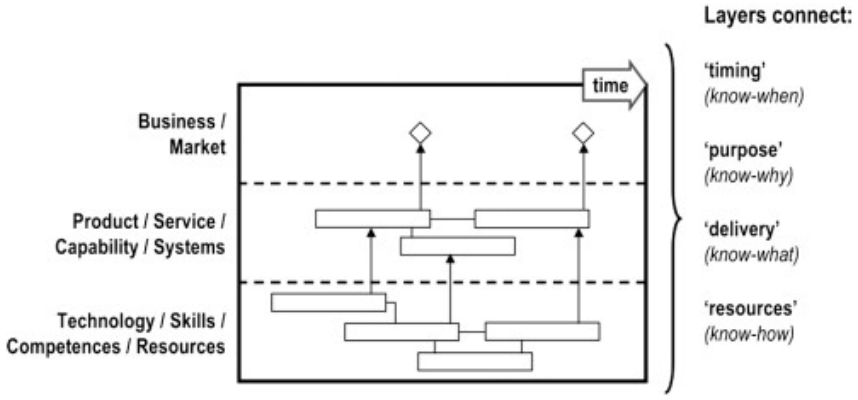


Figure 1: Technology Roadmap by of Kostoff & Schaller (2001), Probert et al. (2005), and Wells et al. (2004)

The subquestions that facilitate answering the main research question are identified in line with the manner in which TRMs should be developed. The process of developing a technology roadmap consists of answering three simple questions, from an organization's perspective (Garcia & Bray, 1997; Pandeya et al., 2021)**:**

1. *Where do we want to go?*
    - This is the long-term vision and strategy element of the organization. Exploring which services and features the organization desires to have in the future, aligning with the organizational ambitions.
        - Is related to *SQ1 and SQ2*
2. *Where are we now?*
    - Herein the current capabilities and preparedness for the innovation of the organization get explored. The results of answering this question provide insights on the required effort to accomplish the goals set in the question 1.
        - Is related to *SQ3 and SQ4*
3. *How do we get there?*
    - This question serves to identify the resources needed and possible guidance and collaborations necessary to enable the organization to reach its the vision and goals outlined in question 1.
        - Is related to *SQ5 and SQ6*

The TRM is developed in the form of a diagram similar to Figure 1, containing the underlined elements as boxes along with process arrows that connect them. These elements are obtained through exploratory analysis, which will be further explained in Chapter 3, as well as through qualitative data gathering, which will be further explained in Chapter 4.

Obtaining these elements relates to answering research-subquestions. Translating the TRM-questions into research-subquestions, involves identifying the critical elements in the TRM-questions (see aforementioned underlined words) and encompassing these into the scope of enabling banks' digital infrastructures to become resistant against the cryptography-related cyber threat posed by quantum computing technology (hereafter referred to as the *quantum threat*).

SQ1: Which digital infrastructures within banking operations and processes are vulnerable to the quantum threat and should transition towards PQC?

In order to determine which services and features banks desire to have in the future related to the protection of its digital infrastructures, these infrastructures first need to be identified. This question aims to accommodate that by means of desk research including multi-stakeholder- and dependency-mapping (Enserink et al., 2010; Luko, 2014).

SQ2: What is the perception of banks towards the expected impact of the quantum threat?

In order to identify broader services and features as discussed in *SQ1*, the banks' perceived impact of the quantum threat must be brought to light. Banks' expert knowledge on their own processes and operations might bring forward certain impacts of the quantum threat that a desk study simply does not identify. This needs to be taken into account when developing a holistic long-term vision and strategy regarding the quantum threat.

SQ3: What is the perception of banks towards their preparedness for the countering the quantum threat?

The preparedness of banks regarding the PQC transition measures the amount of effort required to reach the goals set out by the insights obtained from *SQ1* and *SQ2*. Preparedness is a critical element in addressing the '*where are we now?'* question (Garcia & Bray, 1997).

SQ4: Which capabilities do banks possess that can be utilized for countering the quantum threat?

It is evident that this question is useful to address the '*where are we now?'* TRM- question in the same sense as for *SQ3*.

SQ5: Which resources and governance-measures can provide guidance to banks, regarding countering the quantum threat?

Answering the '*how do we get there?'* question entails two elements. Firstly, for banks to be able to 'get there' (i.e., ensure safety and security from the quantum threat), they would need certain resources. These resources may come in many forms, but can already be split up into operational-type resources and governance type resources (Wells et al., 2004).

SQ6: What is the perception of banks towards the challenges of countering the quantum threat?

Secondly, it can be predicted that certain resistance and problems may arise in the process of '*getting there'.* Identifying which form these challenging encounters might take is vital for successfully mitigating the risks associated with these challenges, using resources identified in *SQ5*. This leads to the insight from answering *SQ6* being the final element needed in the TRM process.

1.6 Societal relevance

From section 1.1 in this research, once could derive the presence of a relevance to society that the quantum threat and PQC transition entails. Cryptography is at risk from the quantum threat, and cryptography facilitates that all the information in digital infrastructures is safe and secure (Pandeya et al., 2021). As digital infrastructures affect all facets of society (Khazieva et al., 2018), and the banking sector make up society's most influential and critical sector (Allen & Carletti, 2008; Bouma et al., 2017), it is clear that research to ensure its safety and security from an emerging threat is of great value to society.

If the PQC-transition has not successfully taken place before the aforementioned Y2Q occurs, an environment will be created wherein malicious cybercriminals (state and non-state) exploit quantum computing's disruptive characteristics to target society's critical infrastructures, which would have devastating impacts on lives of ordinary people in terms of health, safety, and economic well-being (Csenkey & Bindel, 2022). Adding to this is that a form of quantum-related attack may already be practicable today (Section 2.4), implying that organizations are already late with the PQC-transition (Institute for Business Value, 2019; Joseph et al., 2022; Kabanov et al., 2018), which emphasizes the urgency of the problem.

1.7 Relevance for EPA

In the Engineering & Policy Analysis (EPA) MSc program, the central focus is analyzing and solving complex problems that involve multiple actors. Complex problems require solutions that not only solve the technological aspect of it, but also to address the societal and political aspects by the interactions and participation of different parties involved. Within EPA, students should focus on so called 'Grand Challenges'. What are the Grand Challenges for the coming decades? Water, Energy, Food, Health, **Safety and Security issues**, Development, **Cyber Security.**

The research that this proposal describes fits with EPA's requirements because of several reasons, which are summarized in this section below. Each point emphasizes a key-aspect that EPA is involved in:

- PQC and quantum computing involves very **complex novel technology**
- The PQC-transition is a challenge in the world of **digitalization** and the **future of technology**
- Protecting information from the quantum threat involves the **grand challenge in Safety & Security**
- The PQC-transition involves challenges for **Cybersecurity** Infrastructures
- **Societal impact** is most likely very significant
- The PQC-transition challenge is **socio-technical** in nature
- The problem involves **multiple actors** (tech-providers, tech-users, R&D companies, security-providers, malicious hackers, emerging new tech startups, strategic firms, governmental bodies, standardization bodies, research institutes, international community)
- Role and responsibility of **policy and law & regulation** is currently vague and **governance** guidance is urgently requested

1.8 Outline

This report will firstly provide a background discussion on the key concepts in Section 2. Hereafter, in Section 3, an exploratory analysis will be carried out in order to identify banking operations and critical processes, that rely on digital infrastructures - at risk from the quantum threat. Section 4 then elaborates on the methodology used to answer the research questions. The analysis will be carried out in Section 5, presenting findings in the form of a thematic analysis, using qualitative data-gathering. After this, Section 6 discusses the findings and finalizes the Technology Roadmap through expert validation. The main research question will be answered, and recommendations will be given in Section 7. Future research possibilities and limitations of this research are discussed in Section 8. Lastly, Section 9 will briefly reflect on the research's academic contribution and societal relevance.

2. Key concepts

In this chapter an overview of the key concepts associated with the research problem are presented and discussed. Note that this section is not an extensive literature analysis, but serves mainly to provide background information and context, as well as helps to further highlight the core of the problem within this topic.

2.1 Cryptography in Banking

Banks use cryptography in a wide range of services and processes to protect the integrity, and confidentiality of their systems and the sensitive data they handle (Seito, 2017). The specific cryptography methods used by banks may vary, depending on the specific security needs and requirements of their systems and the types of data and information they need to protect (Kar & Dey, 2014). This will be further identified in Section 3. In general, banks use three main cryptography techniques:

1. **Symmetric-key cryptography**
    - Symmetric-key cryptography involves the use of one single shared secret key to both encrypt and decrypt data (Easttom, 2021). This type of cryptography is used by banks in a variety of areas, such as protecting account information, payment applications, and hashing (Al-Shabi, 2019). Using the same key to encrypt and decrypt the data ensures that only authorized individuals can access the data.
    - Grover's (1996) algorithm has shown that symmetric cryptography can theoretically be heavily damaged by quantum computing's properties (Section 2.3).

2. **Asymmetric-key cryptography (public-key cryptography)**
    - Public-key cryptography (asymmetric-key cryptography, or PKC) is the underlying cryptography technique of PKI. It uses a pair of mathematically related keys for encryption and decryption, where one public key is used to encrypt data, and another private key is used to decrypt it (Easttom, 2021). This allows for secure communication without the need to securely share a secret key between the sender and receiver.(Easttom, 2021).
    - Shor's (1994) algorithm has shown that asymmetric cryptography can theoretically be broken by quantum computing's properties (Section 2.3).
3. **Hashing**
    - Hashing is a cryptographic technique that involves the use of a mathematical function to convert an input value into a fixed-size output called a hash value. Hashes are used to verify the integrity of data by comparing the computed hash value of a message with the expected hash value (Easttom, 2021). For hashing, symmetric cryptography is typically used and therefore will not be separately discussed further
    - Grover's (1996) algorithm has shown that symmetric cryptography (and therefore, hashing) can theoretically be heavily damaged by quantum computing's properties (Section 2.3).

The most common cryptographic algorithms that banks use, symmetric, asymmetric, or hash-based, are presented in Table 1. This Table shows the purpose and type of cryptography per algorithm, as well as the impact that large fault-tolerant (LFT) quantum computers may have on these cryptographic algorithms.

Table 1: Cryptographic algorithms and impact from the quantum threat (Rao et al., 2017)

Cryptographic Algorithm	Type	Purpose	Impact from LFT quantum computer
AES (advanced encryption standard)	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3 (secure hash algorithms)	Hash function	Hash functions	Larger output needed
RSA (Rivest-Shamir-Adelman)	Public key / Asymmetric key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key / Asymmetric key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key / Asymmetric key	Signatures, key exchange	No longer secure

Specifically, why some algorithms are no longer secure and why others are more resilient depends on the characteristics of asymmetric/symmetric-key cryptography in combination with the underlying mechanisms of Grover's (1996) and Shor's (1994) algorithms. This will be further discussed in section 2.5. However, what can already be depicted from Table 1 is that the focus lies on Public-key cryptography (asymmetric-key cryptography).

2.2 Quantum computing

It is always amusing to read explanations of how quantum mechanics or quantum computing works. Authors go through great lengths to come up with metaphors and analogies that 'normal' people should be able to relate with, in order to make *all things quantum* more comprehensible. The fact of the matter is that even the most renowned theoretical physicists, who dedicate their life to understanding how quantum mechanics is able to achieve the magic-like properties that it has, themselves don't even fully understand it (Shoup, 2019). Therefore, this section will explain what a quantum computer is and what it can do, but it will not waste words, so to speak, on an attempt at explaining *how* and especially *why* it works.

2.2.1 Defining a quantum computer

Quantum computers can be seen as machines that are able to solve a variety of scientific, or business problems, in an exponentially faster manner than classical (super)computers (IBM, 2021). Classical computers execute operations based on bits, which can either have the state of a 0 (off) or the state of a 1 (on). Quantum computers, however, execute operations based on quantum-bits, or better known, qubits. A qubit can have the state of a 0, or a 1, or both a 0 and a 1 at the same time. The 0 and 1 act as base-states and in between them the qubit has an infinite state (Rawal & Peter, 2022). This is possible due to the 'strange' behavior of sub-atomic particles, on which quantum mechanics is based. The most important features of a qubit that make this possible are:

- **Superposition**: a qubit can be in multiple states at the same time.
- **Entanglement**: a qubit is able to influence the state of another qubit with which is it entangled
- **Non-locality**: a qubit instantaneously knows the state of an entangled qubit, despite their distance.

Lastly, it needs to be noted that the 'strange' behavior of sub-atomic particles is not always very stable. One of the main challenges involves decoherence, which means that qubits lose their state due to external circumstances, or noise (electromagnetic, or acoustic for instance). These noisy qubits result in the necessity for quantum computers to have many more qubits to correct for the error that decoherence inflicts. This issue currently prevents large fault-tolerant quantum computers, that pose a threat to cryptography, from existing (yet) (IBM, 2021).

2.2.2 Current landscape and quantum supremacy

Google's 54-qubit Sycamore Quantum Processor executed a complex calculation in 200 seconds, which would have taken the most powerful supercomputer of today approximately 10,000 years (Arute et al., 2019; Martinis & Boixo, 2019). With this achievement, Google announced 'quantum supremacy', a working machine that is able to solve a problem that is impossible for classical supercomputers. Since then, many organizations and research institutes have made significant progress in quantum computer development, with IBM announcing its 433-qubit 0sprey quantum computer recently, claiming to be the world's most powerful quantum computer.

However, for quantum computers to be able to break current cryptography, or more specifically, break the most-commonly-used underlying encryption scheme RSA-2048, a processing power of around 20 million qubits is required (Gidney & Ekerå, 2021). This might 'feel' like a distant future to some, but expert opinions estimate this will likely become a reality in 5-25 years from now (World Economic Forum, 2021).

2.3 Origin of the quantum threat to cryptography

In this section the origin of the quantum threat to cryptography will be explained. The threat that quantum computing poses to cryptography will be explained by dividing cryptography in the two techniques relevant for this research, namely: (asymmetric) public-key cryptography and symmetric cryptography.

2.3.1 Shor's algorithm and (asymmetric) public-key cryptography

Nearly three decades ago, the mathematician Peter Shor (1994) published a research paper which introduced a quantum algorithm that *"promised an exponential speed-up for factoring integers and finding discrete logarithms over non-quantum algorithms",* as Joseph et al. (2022) describes it. To break down what this means, one needs to consider the following aspects:

- The asymmetric cryptosystems on which PKI relies are underpinned by closely related mathematical problems.
- These mathematical problems are based on the *(1) integer factorization problem* or the *(2) discrete logarithm problem.*
- The security of these cryptosystems relies on the hardness of solving these problems *(1)* or *(2).*

(1) The *integer factorization problem* can be defined as finding the prime factors of a large integer. This is the underpinned mathematical problem used in Rivest–Shamir–Adleman encryption (RSA) (Rivest et al., 1983). In RSA encryption, the public and private key-pair are generated by two large prime-numbers, for example 9.677 and 5.653 – multiplying them gives 54.356.881. One can imagine this does not require much computational power to calculate. However, the factorization problem is the reverse of this scenario: which combination of prime numbers, when multiplied, result in 54.356.881? Answering this question (but then with even larger numbers) is computationally so exhaustive that is unfeasible for classical computers (Mosca, 2018) and serves as the foundation of RSA (Rivest et al., 1983).

(2) The *discrete logarithm problem* can be defined as finding a secret integer that is the result of raising a publicly known integer to a certain power. This is the underpinned mathematical problem used in elliptic curve cryptography (ECC) (Miller, 1986). In ECC encryption, the public and private key-pair are generated by a somewhat more elaborate process than in RSA, but it can be oversimplified by the example of generating two numbers A and B - then the discrete logarithm problem is to find the integer x such that $A^x = B$.

It would take classical silicon-based processing computers such a long time to solve problem *(1)* or *(2)* in the manner in which they are implemented into cryptography schemes, that it is infeasible for hackers to even try (Pandeya et al., 2021). However, Shor (1994) showed with his algorithm, that quantum computers could theoretically solve these fundamental mathematical problems exponentially faster than classical computers, and therefore crack the majority of PKI's cryptosystems (such as RSA and ECC).

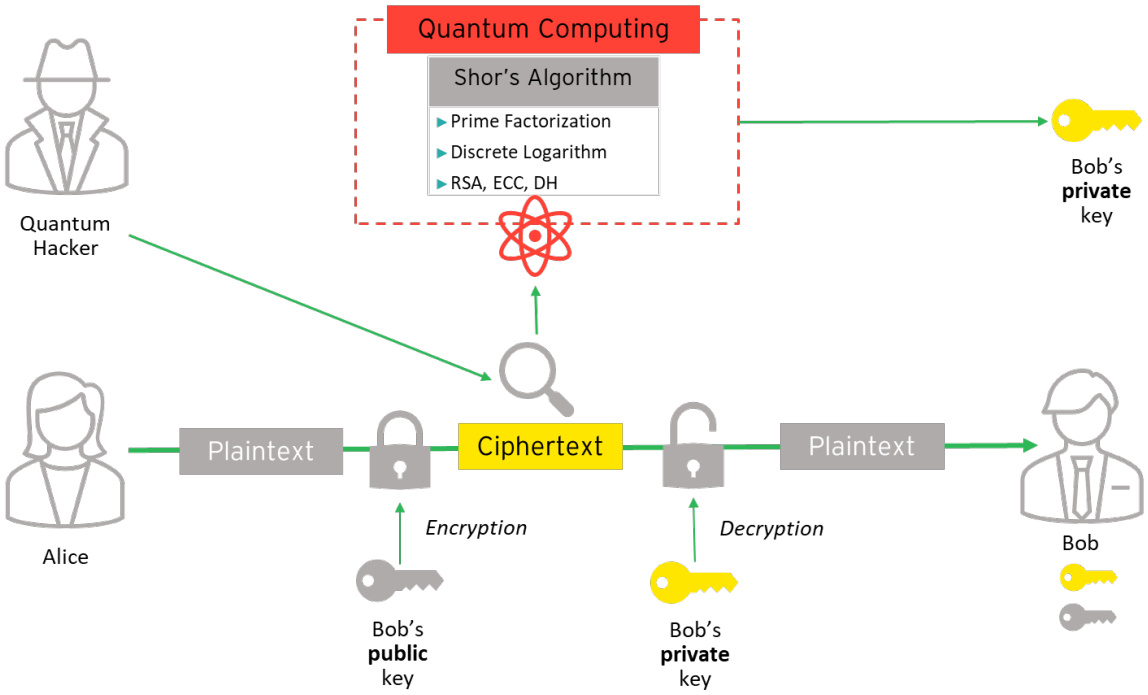


Figure 2: Schematic of quantum threat to public-key cryptography

Figure 2 schematically shows the process of a hacker, using quantum technology, decrypting information in the process of Alice and Bob communicating with public key cryptography. What this figure shows, besides a clear overview of the PKC process, is that the quantum hacker is able to steal the information that Alice and Bob intend to communicate with each other, without the need for interaction between the hacker and the victims. This emphasizes the urgency of this threat because future victims of quantum-hacks might not even be aware that they were hacked.

2.3.1 Grover's algorithm and symmetric-key cryptography

Around the same time as Shor, Grover (1996) showed that with the use of a quantum computer, brute-force attacks on symmetric ciphers can be sped up significantly. Traditionally, brute-force attacks entail checking every possible combination of some code, key, or password, to find the correct one, usually requiring a long time (Knudsen & Robshaw, 2011). To obtain secret keys with brute-force using traditional computers, is infeasible (Pandeya et al., 2021), but Grover's algorithm exploits some characteristics of quantum-computing, such as superposition, so that not all possibilities need to be checked, but just a few. This makes Grover's algorithm a threat to current symmetric cryptography. However, as can be depicted in Table 1, most symmetric cryptographic algorithms currently in use are relatively easy to update to become quantum safe (Rao et al., 2017). Doubling key-lengths will most probably be sufficient to withstand Grover's algorithm (Cramer et al., 2022; Jaques et al., 2020; Mavroeidis et al., 2018; Rao et al., 2017). For AES this is not a problem; for DES, however, this is not possible.

Ever since Shor (1994) and Grover (1996) published their articles, the research field in quantum-resistant algorithms has seen a massive increase, as the scientific community realized that the older encryption systems needed to be replaced one day (Grimes, 2020; Joseph et al., 2022). This has led to the construction of a vast number of different theoretical algorithms that could be resistant to the quantum threat, known as post-quantum-cryptography (PQC) algorithms. However, a threat may already exist today, and sensitive data may already be compromised, which will be explained in the Section 2.4.

2.4 Store Now, Decrypt Later

Discussions about when Y2Q will happen are negligible in terms of the urgency for a quantum-resistant-cryptography transition. Not only do quantum computers pose a threat to sensitive data in the future, but the treat already exists today (Kabanov et al., 2018). Some data need to be protected for longer periods of time and some digital infrastructures and systems must operate for decades (NIST, 2022a). This data remains longer in the field and is regularly moved through public networks, encrypted with a combination of symmetric-key cryptography and PKC. A malicious adversary with sufficient resources could record all encrypted traffic (being worthless today because the encryption cannot be broken), store it somewhere, and simply wait until quantum computers are available to decrypt it. This is known as the "store now, decrypt later" (SNDL) attack model (Kabanov et al., 2018; World Economic Forum, 2021).

The implications that the SNDL-attacks may have on a global scale are commonly discussed in mainstream media and news articles. Scenarios entailing threats to national security and all-out cyber war are mostly brought to light (Forbes Technology Council, 2022; The Frontier Post, 2022; The Hill, 2022), but solutions remain elusive. Moreover, industry is currently not measuring whether this sensitive data might already be harvested for malicious future decryption purposes today (Carlson & Sharkey, 2022).

Sensitive data that organizations consider securely protected right now are thus already lost to prospective future cybercriminals, if harvested now (World Economic Forum, 2021). Researchers confirm that this SNDL-attack is already practicable now and therefore argue that organizations are already late and at an ever-increasing risk (Institute for Business Value, 2019; Joseph et al., 2022; Kabanov et al., 2018). This indeed emphasizes that even though large fault-tolerant (LFT) quantum computers may be years away, it is vital that organizations start transitioning to be resistant to the quantum threat (Institute for Business Value, 2019), and move towards aforementioned post-quantum-cryptography (PQC). This is especially the case for organizations involved in critical services, with long data lifespans, such as banks. Figure 3 shows an overview composed by Joseph et al. (2022) that presents a timeline of this necessary PQC transition. It portrays three timelines: the quantum threat to cryptography (top), the migration process that organizations should consider to keep their data secure (middle), and standardization (bottom) by multinational standards organizations. One can instantly notice that the middle timeline is what needs to be executed, but what these *planning* and *transition* phases actually entail is hugely underexposed.

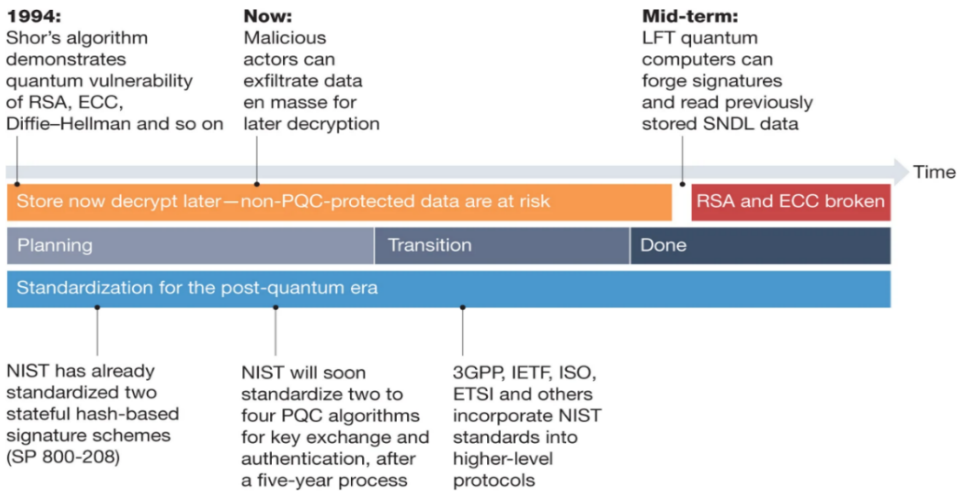


Figure 3: Post-Quantum-Cryptography timelines

2.5 Post-Quantum-Cryptography

Understanding what aspects are needed to facilitate the *planning* and *transition* towards quantum-resistant cryptography, one must explore the development process of the technology behind it, being PQC.

2.5.1 PQC Standardization effort by NIST

In 2016, the National Institute of Standards and Technology (NIST) initiated a series of competitions for cryptographers to compose the most fault-tolerant, effective, and efficient PQC algorithms, fit for standardization (NIST, 2016). Currently this process is in its fourth round, expecting the final candidate algorithms to be completed by the summer of 2023 (NIST, 2022a). Standards for PQC are highly anticipated, also because researchers have already found that adopting some form of PQC is absolutely critical for organizations (Joseph et al., 2022) as well as for governments (Kong et al., 2022).

The researchers who proposed the final algorithm candidates for round 4 of the NIST standardization procedure stated – at a PQC Symposium in the Hague (Cramer et al., 2022) - that there would not be any large changes to the algorithms in the last round (Ducas, 2022; Hülsing, 2022; Prest, 2022). The speakers of the Symposium stated that simply some terminology-amendments and specificity-clarifications will be added, but large changes in terms of performance and security of the algorithms are not expected. This means that organizations should already be able to experiment with these different technologies and that knowledge about the algorithms' functionality and performance is already relevant today. Table 2 and 3 show an overview of some insights into the technical characteristics and performance of the final NIST-standardization PQC candidates, based on the works of Westerbaan (2022) and Bong (2022), as well as a NIST publication (NIST, 2022b) :

Table 2: Final Digital Signature candidates in the NIST Standardization for PQC

Digital Signatures to be Standardized			
	CRYSTALS - Dilithium	**FALCON**	**SPHINCS+**
Strengths	Creates small signatures. Fast operations.	Fast verification. Fast signing.	Small keys. Use of established building blocks possible.
Weaknesses	Large keys which are still too large for some use cases.	Very delicate signing procedure. Floating-point arithmetic required.	Very large signatures. Low operating speed.
Public-Key Sizes (bits)	10,496 - 20,736	7,176 - 14,264	32 - 64.
Private-Key Sizes (bits)	20,224 - 38,912.	7,176 - 14,264	64 - 128
Implementation difficulty	Easy	Difficult	Easy
Additional information from NIST	NIST declares Dilithium as primary algorithm to be implemented for most use cases	NIST recommends FALCON for use cases where Dilithium may be too large	SPHINCS+ will be standardized to not rely solely on lattice-based algorithms

Table 3: Final PKE/Key Encapsulation Methods candidates in the NIST Standardization for PQC (NIST, 2022b)

Public-Key Encryption/Key Encapsulation Methods to be Standardized	
Algorithm	**Comments by NIST**
CRYSTALS – KYBER	NIST anticipates that this algorithm will function optimally in the majority of applications due to its robust security and exceptional performance.
Final round candidates: Not officially being Standardized yet	
BIKE	Based on structured codes and suitable as a general-purpose key encapsulation method
Classic McEliece	Despite being considered secure, NIST does not expect widespread adoption of this algorithm due to its large public key size. NIST may decide to Standardize it after the fourth round.
HQC	Based on structured codes and suitable as a general-purpose key encapsulation method
SIKE	Small key sizes and small ciphertext sizes. Recently cracked by a classical computer (Castryck & Decru, 2022).

Besides the algorithms in Table 2 and 3, symmetric algorithms also need to be addressed. A recent study recommends the use of AES-256 or ChaCha20 with a 256-bit key in all future cases in which symmetric encryption is used (TNO et al., 2023) .

It should be noted that organizations often do not implement the aforementioned algorithms from Tables 2 and 3 themselves, but rather us certain libraries that execute widely adopted cryptographic protocols, such as TLS (TNO et al., 2023). Using these cryptographic libraries entails that different cryptographic options can be selected (for instance, key sizes). However, it is typically not the duty of the organization to develop their own cryptographic algorithms within these libraries (TNO et al., 2023). NIST will be publishing the algorithms from Tables 2 and 3 in the form of such libraries (NIST, 2022b).

2.5.2 The PQC-transition challenge

As previously stated, the moment that quantum computers will be able to break cryptography is still in the future, so one could argue that, with the coming of NIST's standards for PQC within the coming 1-2 years, all problems will simply be resolved by that time. However, current PKI has taken almost two decades to be successfully deployed (NIST, 2022a). In light of this, regardless of whether we can predict the exact moment when quantum computing breaks cryptography, society must begin now to prepare its information security systems to be able to resist the quantum threat (NIST, 2022a). Moreover, the deployment of PQC should not be seen as simply 'another simple cryptography transition', Joseph et al. (2022) argue. In comparison with previous transitions, this migration covers a broader and more complex scope. Therefore, this migration requires more planning, time, and resources than others did in the past (Joseph et al., 2022).

There is a sufficient amount of research available concerning the technological aspects of PQC, where the focus mainly lies on testing and comparing algorithm performance (Das & Sadhu, 2022). However, literature on transitioning PKC systems towards quantum-resistance is limited, and the focus within the transition is perceived as merely technological only (Kong et al., 2022).

The PQC-transition thus entails more than just a technological solution tied to a NIST standardization. The *planning* and *transition* phase in Figure 3 needs to be translated into tangible aspects, that organizations can utilize to start with the transition as soon as possible. Now is the time to take critical steps in order to reduce future shortcomings caused by poorly planned countermeasures (Joseph et al., 2022). Moreover, the identified challenges by Kong et al. (2022) imply that organizations should begin preparing early, as awareness of the PQC-transition process is currently lacking, and organizations therefore feel no urgency for initiating a transition yet.

2.6 IT Governance

Since this research aims to integrate the governance related challenges of transitioning towards quantum-safety, it is necessary to define what governance of IT systems typically involves. Luckily this is a field of research in which many insightful publications can be found, as well as entire literature reviews. Almeida et al. (2013) found that in order to encourage desirable IT behavior, organizations must establish and execute three types of IT Governance strategies. These three strategies are the result of Almeida et al. (2013) their summary of many IT Governance related articles, claiming that even though phrasing is often different, there is a general consensus on these three mechanisms, namely:

1. **Structure Mechanisms**: The most evident IT Governance mechanisms are organizational units and roles within a company, responsible for making IT decisions. These commonly consist of committees, executive teams, and business/IT relationship management.
2. **Processes Mechanisms**: Ensuring that daily behaviors are in alignment with IT policies and provide input into decision-making. Among these are IT investment proposals, exception processes for architecture, Strategic Information System Planning, and chargebacks.
3. **Relational Mechanisms**: Relational mechanisms are crucial for achieving and maintaining business-IT alignment, even with the appropriate structures and processes. The use of mechanisms such as announcements, advocates, channels, and education efforts help to achieve and sustain business-IT alignment.

In order to integrate these governance strategies into this research, the three mechanisms will be considered within the interview. This tests the banking's preparedness for facing the quantum threat and helps to identify which governance-related resources should be considered for the TRM.

2.7 Vulnerabilities in the banking industry

Since this research is focused on the Dutch banking sector, it is necessary to provide a definition of banking. Moreover, the importance of digital facilities and infrastructures within the banking sector must be brought to light, in order to identify banking's risk of the quantum threat. A more detailed overview of banking's critical processes and its dependencies on certain systems and stakeholders will be laid out in Sections 3.1 and 3.2, respectively.

2.7.1 Defining banking

Horace White (1968) defined banking as a '*manufacture of credit and a machine for facilitation exchange'*. This definition still holds up, but needs to be complemented because of the many (technological) developments of the late 20th century and 21st century. Besides globalization, digitalization has had the largest impact on the evolution of the banking industry (Wewege & Thomsett, 2019). Digital banking can be defined as '*delivery of banking products and services to customers through electronic channels, that can be conducted from anywhere*' (Pappu & Saranya, 2019). These channels include Automated Teller Machines (ATMs), telephones, mobile phones, and the internet. Banking has evolved from merely buildings where people deliver their cash to and apply for loans, mortgages, and advice, towards a full-scale digital financial service provider.

2.7.2 Data vulnerabilities

As it is the case with any digital service provider, the customer data, corporate data, core digital services, and other sensitive information are critical for its business operations and need to be securely protected (Nationaal Cyber Security Centrum, 2022). Generally speaking, the quantum threat brings a risk to data and information streams in banks on two-levels: (1) future risk (Y2Q) and (2) current risk (SNDL).

1. **Future risk (Y2Q)**

If banking's data is encrypted with currently used cryptography methods at the time that a LFT quantum computer is available, then the impact will be severe (Csenkey & Bindel, 2022). The information that regularly moves through public networks will be available for anyone to decrypt. Adding to this, information that moves through private networks are at risk as well. Of course, these private networks offer more layers of security compared to public networks, but if a hacker would gain access to the network, for instance by means of a social engineering attack, the encrypted data is at risk. Social engineering attacks are a very common method hackers use to gain to access to private networks and cases are increasing (Krombholz et al., 2015). Therefore, it can be assumed that information streams in public networks, as well as in private networks (lower risk than public) are at risk from the future risk of quantum computing. This results in the following type of banking data being at risk (Berger et al., 2012; Galazova & Magomaeva, 2019; Kar & Dey, 2014; Priya et al., 2019):

- Customer account data (name, address, BSN, account-number/IBAN, balance, transaction history, loans)
- Credit card data (name, card number, expiration date, CVV, balance, transaction history)
- Transaction data (purchase amount, purchase date, merchant name)
- ATM data (withdrawal amount, location)
- Interbank transaction details (transaction amount, transaction date)
- Customer support data (internal documents, logged customer conversations)
- Internal communication and operations data (internal documents related to strategy, marketing, business processes, etc.)
- Internal security and access control data (security protocols, login credentials)
- Employee data (name, address, payroll details)
- Audit, compliance and regulatorily data (financial statements, risk assessments, KYC documentation)

The degree of risk varies among these different types of data. If data is solely stored within banks, then banks can mitigate risks by re-encrypt it using new quantum-safe algorithms, once they become available. However, if data is transmitted through networks regularly or, more importantly, encrypted and stored outside the banks' own infrastructures, these data types may be considered more susceptible to the quantum threat. The above-mentioned data types all move through networks (Berger et al., 2012; Galazova & Magomaeva, 2019; Kar & Dey, 2014; Priya et al., 2019), but exactly how this is encrypted, and in which locations data is stored, will be addressed in Chapter 3.

2. Current risk (SDNL)

The data that regularly moves through public networks is currently easily accessible for anyone to view and store (Carlson & Sharkey, 2022). However, this data is encrypted in some form, making it useless and uninterpretable ciphertext which doesn't qualify as information. As was explained in section 2.4, this stored data can be decrypted later once a LFT quantum computer is available. For this to be impactful, the information must be relevant and impactful for a long period of time (Kabanov et al., 2018). The type of banking data that this applies to are:

- Customer account data (name, address, BSN, account-number/IBAN, balance, transaction history, loans)
- Credit card data (name, card number, expiration date, CVV, balance, transaction history)
- Transaction data (purchase amount, purchase date, merchant name)
- Customer support data (internal documents, logged customer conversations)
- Internal communication and operations data (internal documents related to strategy, marketing, business processes, etc.)

This selection of data types is based on the accessibility to monitor and store the encrypted data, as well as future relevancy/impact. For instance, *ATM data* and *Interbank data* are less vulnerable to SNDL-attacks, because it uses private networks to exchange data (Khalifa & Saadan, 2013) and an attacker would need to first hack into this system to be able to store the encrypted data for potential future decryption. This process would be very complex and would unlikely be carried out if there currently is no guarantee that the data can later be decrypted. The same principle holds for *internal security and access control data,* and *employee data.* One would then expect this principle to apply to *internal communication and operations data* as well, but these data streams are often transmitted through public networks (Rommer et al., 2020). Also, this type of data is regularly uploaded to third-party services, such as cloud providers, which uses (public) internet service providers (ISPs) for exchanging data (Kemmerich et al., 2015).

The remaining listed data types, holds valuable information which remains relevant for years, making them appealing for SNDL-attacks. The first four datatypes in the list are generally quite static over the course of years, as changes in address in the Netherlands occurs once every 15 years on average (CBS, 2019), most citizens rarely change banks (BNR, 2019), and these banking details have a long shelf-life (McGowan, 2022). Should this data fall in the wrong hands, this can result in identity fraud, card fraud, financial fraud, and blackmailing with information on sensitive/compromising transactions (National Fraud & Cyber Crime Reporting Centre, 2021). This obviously would be very harmful for the bank's clients, but since it is the bank's responsibility to keep their clients secure, they would also be accountable (Nederlandse Vereniging van Banken, 2019), resulting in enormous potential losses in settlement payments (Federal Trade Commission, 2019).

The datatype *Internal communication and operations data* can provide the SNDL-hacker insights into a company's operations and potentially take advantage of vulnerabilities, or it could expose classified sensitive information that may lead to a scandal of some sorts (Doward, 2012). Moreover, holding this decrypted sensitive internal information can be used to execute a ransomware attack (Muhammad & Ejiyime, 2017).

3. Exploratory Analysis

3.1 Banking's digital processes

In order to answer SQ1, the core digital services that banks provide need to be identified. In Section 2.7 the vulnerable data types where presented, which will relate to the core services. These services will be analyzed in terms of the role that cryptography plays to ensure the security of these services. This helps to identify in which parts of the banks' processes and operations the vulnerabilities to the quantum threat are the highest. With this knowledge, the first step in constructing a TRM for the PQC transition can be made, resulting in a skeleton framework which is partially filled in and can provide guidance in collecting the data for answering the remaining subquestions.

Banks are typically involved in a wide range of services that rely on digital infrastructures (Rabah, 2005). Reviewing the current literature on digitalization in banking and the role of cryptography in the banking sector results in the identification of core banking services that rely on cryptography, presented in Table 4. The insights from Table 4 are a result of combining academic knowledge on banking services, with research on cryptography in the financial industry, as well as research on cryptography in general.

Table 4: Role of cryptography per banking service

Banking Service	Role of Cryptography	Articles used
ATM transactions	To protect the confidentiality and integrity of cardholder information and transaction data. To verify the integrity of transaction data.	(Berger et al., 2012; Galazova & Magomaeva, 2019; Kar & Dey, 2014; Priya et al., 2019)
Online banking transactions and payments	To protect the confidentiality and integrity of transaction data. To verify the authenticity of the transaction.	(Berger et al., 2012; Kar & Dey, 2014; Zamaslo et al., 2021)
Physical card transactions	To protect the confidentiality and integrity of cardholder information and transaction data. To verify the identity of the parties involved in the transaction.	(Berger et al., 2012; Kar & Dey, 2014; Kerr, 2018; Priya et al., 2019)
Other transactions (loans, mortgages, investment services, corporate payments)	To protect the confidentiality and integrity of transaction data. To verify the authenticity of the transaction.	(Berger et al., 2012; Kar & Dey, 2014; Zamaslo et al., 2021)
Online banking authentication	To securely authenticate users and verify their passwords and credentials	(Berger et al., 2012; Kar & Dey, 2014)
Compliance with Regulation	Used to protect the confidentiality and integrity of communications with regulatorily bodies	(Galazova & Magomaeva, 2019; Rawal & Peter, 2022)

These services, along with the associated cryptographic purposes for providing these services, are taken into further analysis. Bear in mind that these identified critical banking services are relatively high-over representations and may fail to encompass every detailed process. This means that, for instance, the service *Online banking transactions and payments* consists of multiple sub-processes, because payment can take on many forms (e.g., periodical bill pays, wire transfers, e-check deposits, mobile payments etc.). However, it is not feasible, or viable, to decompose the identified services into such detailed sub-services, because they will already be decomposed in terms of their related external facilitators and stakeholders. Furthermore, banks offer perform more tasks that rely on cryptography, such as facilitating internal network security, data storage and transmission, fraud prevention, and secure client messaging, however these are all supportive, or secondary, services (see section 3.3) and are therefore not presented in Table 4.

3.2 Stakeholder analysis

The services described in Table 4 all rely on combinations of symmetric-key cryptography and PKC. In order to determine exactly which digital infrastructures underly these cryptography-related banking services, it is necessary to map out which systems are in place that facilitate them. These systems are a combination of internally and externally provided systems, due to banking's dependency on other stakeholders and digital facilitators (Schmidt et al., 2017). Therefore, it is necessary to map out the relevant stakeholders in terms of the banks' dependencies on them, which will bring these required systems to light. A visual representation of the stakeholder map is portrayed in Figure 4. The chart is constructed along the guidelines of Enserink et al. (2010) for mapping multi-actor systems. However, in this case the actor playing field is not demarcated from the perspective of all actors at the same time (as is usually the case in Enserink et al. (2010) their work), but merely from the banks' perspective. This follows logically from why this map is being constructed in the first place: finding the critical digital infrastructures *within banking operations and processes* that are at risk from the quantum threat.

The actor map uses two different colored arrows that connect the actors to each other via their dependencies. All arrows represent a dependency, but the red-colored arrows highlight the dependencies which are critical for providing the primary processes within the bank. Business processes can be categorized into primary and secondary processes. The primary process involves the operations that serve the clients' needs for the bank's services, and secondary processes support this, but do not directly add value to the clients' needs.

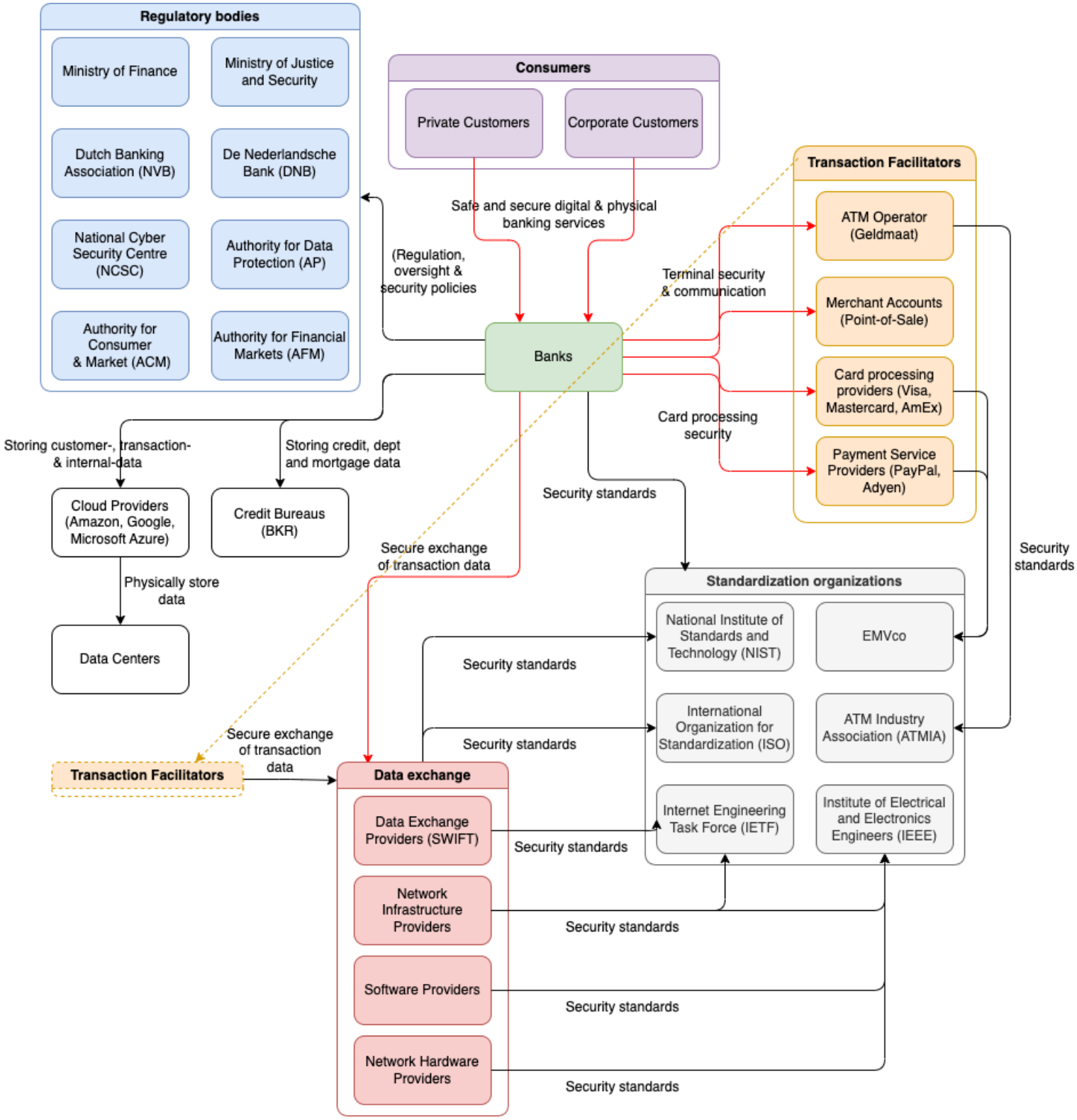


Figure 4: Visual overview of stakeholders and dependencies - from the banks' perspective

The required systems are identified based on the dependency that the banks have with the certain stakeholders that are needed to facilitate the aforementioned services. These stakeholders along with the systems are presented in Table 5.

Table 5: Systems and stakeholders involved per banking service

Banking Service	Related stakeholders	Systems required to provide service
ATM transactions	Card processing providers Card issuer ATM operator Network infrastructure providers Standardization organizations	ATM terminals Network infrastructure (private) Monitoring systems Cryptography systems
Online banking transactions and payments	Payment Service Providers (PayPal, Adyen) Data exchange providers (SWIFT) Merchant accounts Other financial institutions	Payment processing gateway Database systems Card processing networks Network infrastructure Anti-money laundering systems Monitoring systems Cryptography systems
Physical card transactions	Card processing providers (Visa, MasterCard, American Express) Merchant accounts Standardization organizations	Payment processing gateway Point-of-sale (POS) systems Card processing networks Fraud detection systems Anti-money laundering systems Monitoring systems Cryptography systems
Other fund transfer services (Loans, mortgages, investment services, corporate payments)	Other financial institutions Loan servicers Investment service providers Credit bureaus Standardization organizations	Loan origination systems Mortgage servicing systems Investment management systems Payment processing gateway Database systems Network infrastructure Monitoring systems Cryptography systems
Online banking authentication	Identity verification service providers Network infrastructure providers (ISP's, router and hardware vendors) Standardization organizations	Online banking website Mobile application Database systems Network infrastructure Monitoring systems Biometric authentication systems Authentication systems Cryptography systems

Compliance with Regulation	De Nederlandsche Bank (DNB) Authority for the Financial Markets Dutch Data Protection Authority Dutch Banking Association (Nederlandse Vereniging van Banken – NVB) National Cyber Security Centre Authority Consumer & Market	Cryptography systems Network infrastructure Database systems

3.3 Cryptography systems and data flows in primary processes

Based on the identification of the banking services and stakeholders, this research will dive deeper into the mechanisms that underly the primary processes in the banking operations. The primary processes will be investigated in terms of the dataflows and cryptography systems involved.

3.3.1 Primary processes: Payments & Transactions

Executing payments and transactions are the most vital customer desires that banks need to fulfill (Berger et al., 2012). As is the case in most industries, banks depend the most on their customers (Schmidt et al., 2017). All the dependencies in Figure 4 would be irrelevant if the customers were not able to utilize the bank's services. Identified services such as *Compliance with regulation* and supportive services such as internal network security safeguard that the customer can indeed exploit the bank's services, but the customers do not directly interact with these services, or secondary processes. Hypothetically, should these services fall away, then banks would be in trouble, but customers would still be able to use their debit or credit cards to spend their money. Customers would still be able to perform transactions, merchant-accounts would still be able to receive payments in exchange for goods, and ATMs would still be able to give out cash. The secondary processes are of course vital for the bank's organizational health, but their criticality for the customer's needs does not come close to that of the primary processes that underly the payment and transaction architecture.

Customer-centric criticality and disruptive impact are not the only reasons to continue the analysis with only the primary processes. The criticality of the involved data per service is an important consideration as well. Section 2.7 highlights which datatypes are vulnerable to the quantum threat and some of these are indeed related to secondary processes. That is why these will be taken into account while drawing up the answers to the research questions and while presenting the final recommendations, but the focus within the TRM-framework development will be on the primary processes: payments and transactions. Kerr (2018) states that cybersecurity within these processes is one of the most vital aspects in providing services to the customers. The identified services in Table 5 that relate to this are:

1. ATM Transactions
2. Online transactions and payments
3. Physical credit card and debit card transactions

3.3.3 Data flows in Payments & Transactions

This section will provide an overview of the dataflows between systems and entities that are involved in the payment & transaction process (aforementioned services 1,2,3). This will identify the cryptography systems as well and finalizes the search for which digital infrastructures within banking operations and processes are vulnerable to the quantum threat and should transition towards PQC (SQ1). The Figures 5, 6 & 7 portray the processes and dataflows of financial transactions and is based on research articles related to banking, payment architectures, payment gateway systems, electronic funds transfer systems and ATM systems (Kar & Dey, 2014; Kerr, 2018; Khalifa & Saadan, 2013; Pappu & Saranya, 2019; Radonić, 2018; Schmidt et al., 2017; SWIFT, 2023; Wewege & Thomsett, 2019; Zay Oo, 2019).

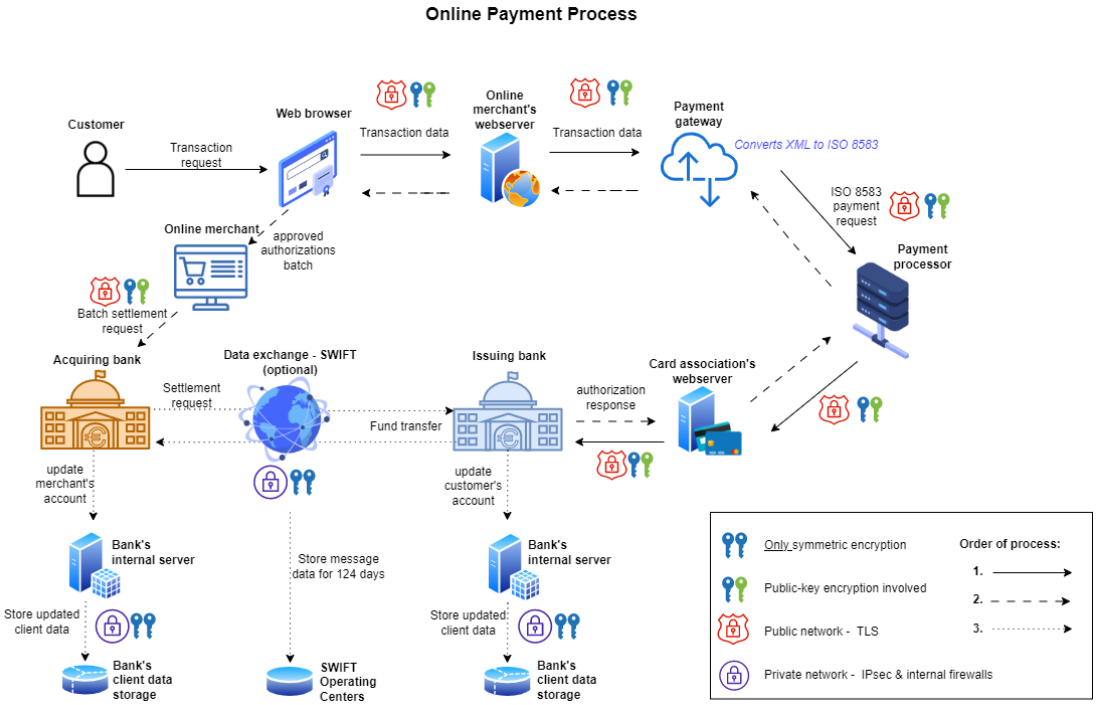


Figure 5: Online transactions and payments process

In Figure 5, in the bottom-right corner, the legend and instructions to read the diagram are laid out (these apply to Figure 6 & 7 as well). What can be observed from Figure 5 is that the online payment process is very dependent on dataflows through external networks and service providers, in which public-key encryption is involved. These dataflows are more vulnerable to the quantum threat than the channels in which only symmetrical encryption is used. In the online payment process the private networks are mostly located within the banks' own internal storage and communication infrastructures (Radonić, 2018). Moreover, inter-bank data exchange (which may involve the SWIFT-network) also relies on private networks in which data is encrypted symmetrically (SWIFT, 2023).

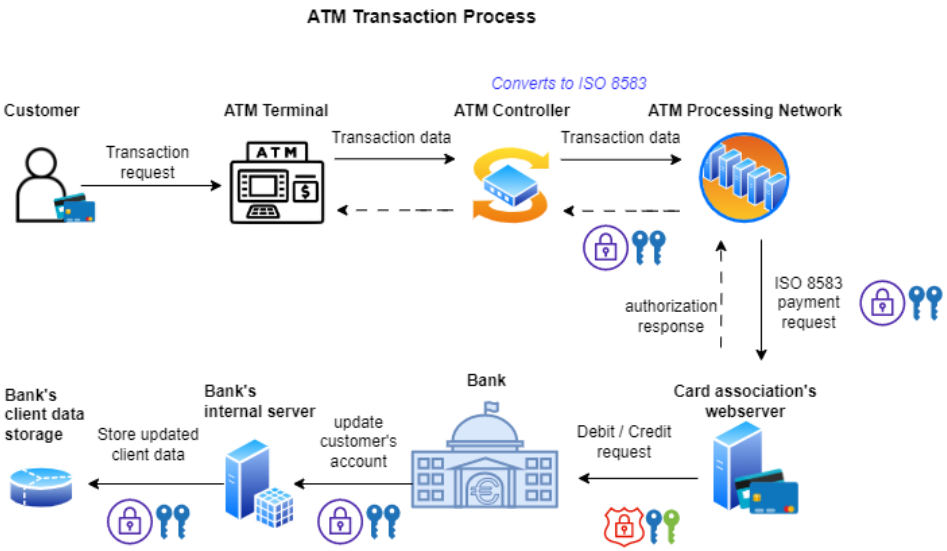


Figure 6: ATM Transactions process

Figure 6 shows the process of customers retrieving cash from physical Automated Teller Machines (ATMs). What can be observed in this process is the presence of private networks, which are less likely to be tapped into by a malicious hacker. Vulnerabilities to the ATM process lie in the physical security of the machines, which primarily relates to the ATM controller (Khalifa & Saadan, 2013) and in the communication channel from the Card Association to the Bank.

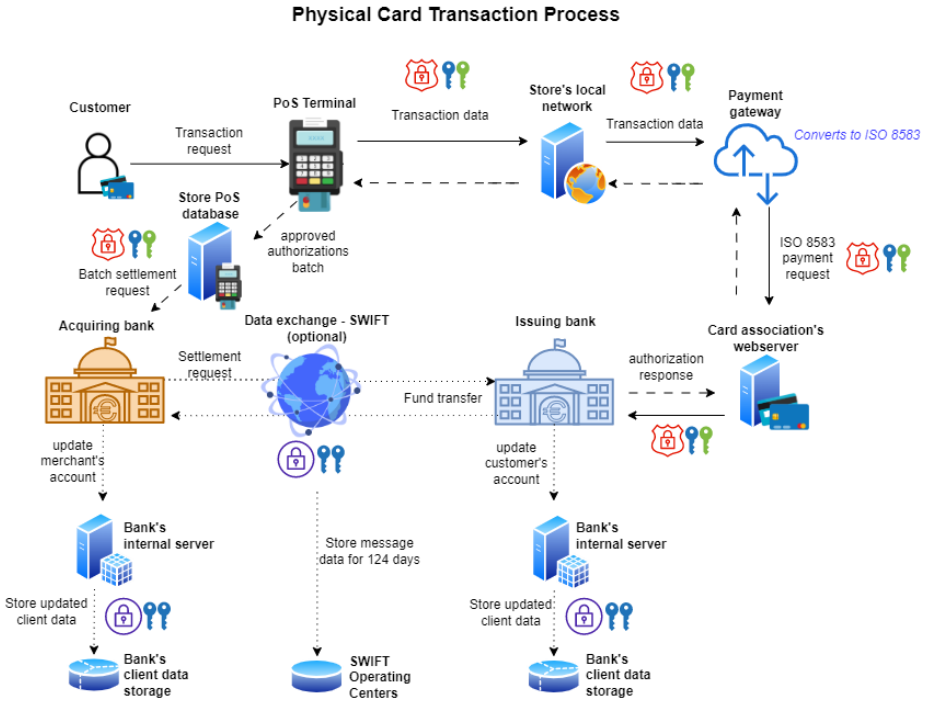


Figure 7: Physical credit card and debit card transaction process

Lastly, Figure 7 shows the process of a customer engaging in a transaction through a Point-of-Sale (PoS) terminal in a physical store. This process shows great similarities with the online payment process because it also heavily relies on dataflows through external networks and service providers where public-key encryption is involved. PoS-terminals, for instance, are not manufactured by banks themselves and their communication with the store's local network is not something that the banks directly influence, in terms of security. This makes these PoS-terminals and the local networks that they are connected to vulnerable for the quantum threat.

3.4 Drivers for the PQC-transition

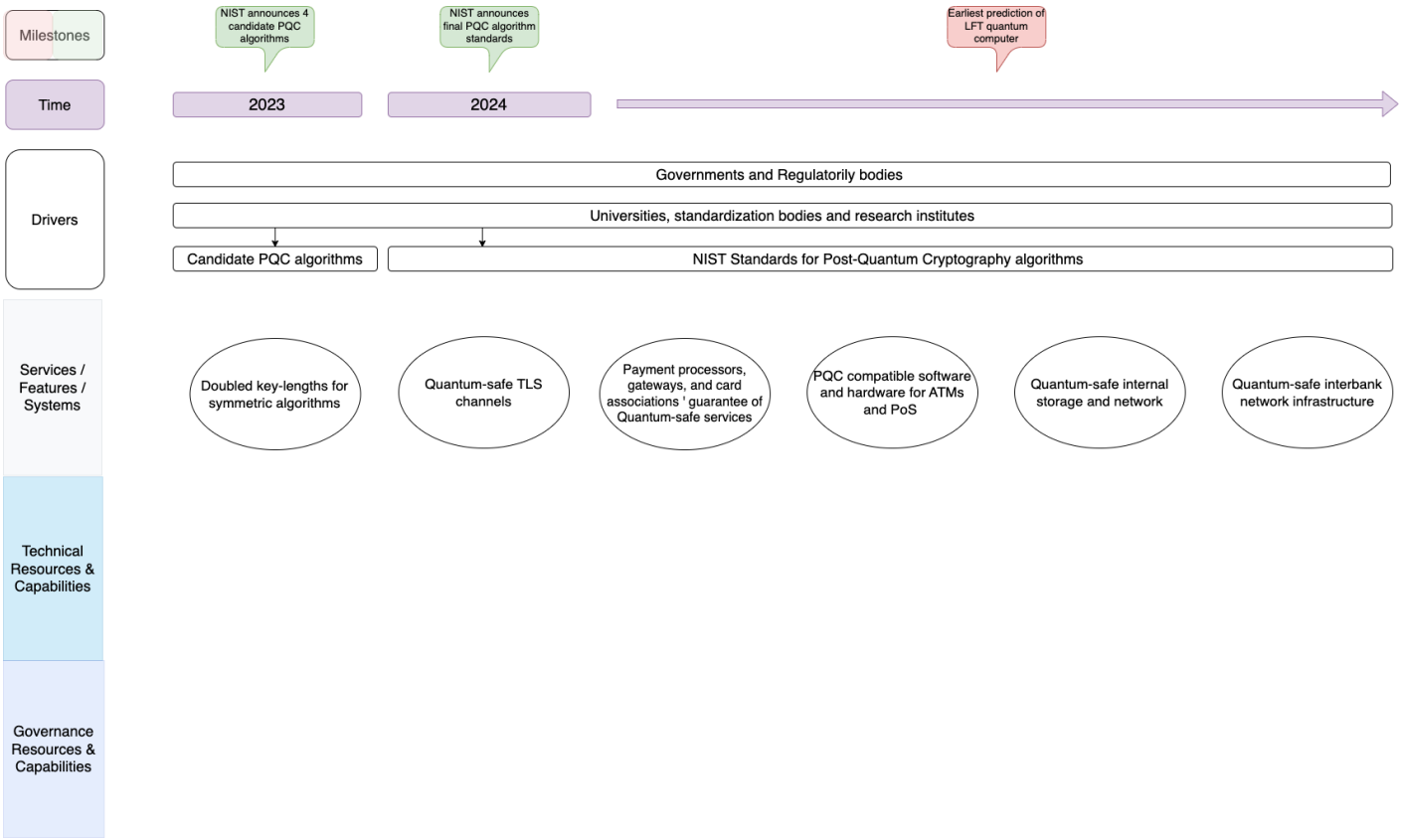
Besides the identification of the critical infrastructures, in order to develop the TRM-framework skeleton, the main market drivers for the PQC-transition need to be identified as well. This usually does not require extensive research and is not embedded into the research questions related to this phase of the TRM development, but it should be taken into account for completeness (Carvalho et al., 2013; Pandeya et al., 2021; Schimpf & Abele, 2019). This research already discusses the main driver for the PQC-transition extensively in Chapters 1 and 2, being the quantum threat to cryptography itself. Furthermore, the remaining drivers are based on the research by (Pandeya et al., 2021) and are summarized below:

1. NIST Standards for Post-Quantum Cryptography algorithms and the candidate algorithms
2. Universities, standardization bodies, and other research institutes: these institutes drive research forwards
3. Governments and Regulatorily bodies: Government organizations have secrets to protect for a longer period

3.5 TRM Framework skeleton

This section aggregates the findings from Chapters 2 & 3 into a first draft of TRM framework, which will also function as information during the interviews.

Figure 8: TRM skeleton



4. Methodology

In this section the methodology for gathering qualitative data is explained. It serves as the set-up for the analysis of the qualitative data and explains how this will be integrated into the TRM framework.

4.1 Qualitative research

Several studies have demonstrated that interviews provide a deeper understanding of the subject matter and a more comprehensive context picture because of their interactive nature (Whiting, 2008). Semi-structured interviews yield qualitative data. A disadvantage of this is that it is difficult to make generalizations with qualitative data, and it takes more time to analyze it. Generalizability is something researchers often desire. However, within this research generalizability does not play a vital role in order to reach the research objectives. This research aims to create a deeper understanding into complex processes, by contributing to improving policies and strategies. For these purposes framework development using qualitative data (obtained from interviews) is very suitable (Collaço et al., 2021).

The insights obtained from the first sub-question (Chapter 3) will provide insights that will be tested and complemented by conducting the interviews with banks. The 5 sub-questions associated with this research-phase have been decomposed into shorter formulations and have been interviewed with Security Architects, who report to the Chief Information & Security Officers (CISOs) from Dutch banks, as well as Payment Security Specialists and Cryptography Architects from Dutch banks. Hereafter, the answers (or qualitative data) will be thematically analyzed to be able to be integrated into the TRM framework. The goal of this qualitative data gathering is to obtain the elements of which the TRM consists in the form of perceptions on impact, strategy, capabilities, preparedness, challenges, resources, and governance, related to the PQC transition within in the participant's organization and the banking sector. This will enable that the TRM is grounded in real-world experiences and perceptions of banking professionals who are actively engaged in field of work related to the PQC transition process.

4.2 Participant recruitment

Defining the scope of this study is essential for a suitable participant recruitment. As this research focusses on the Dutch banking sector, it is obvious that Dutch banks will be the focus. This phase of the research aims to obtain insights into perceived impact, preparedness, capabilities, resources, and challenges related to the PQC-transition. Within banks, this is mainly relevant for: (1) security architects, (2) payment security specialists and (3) cryptography specialists. These organizational roles together aim cover banks' perspective. Namely, (1) relates to overall strategy for designing and implementing security systems and protocols, (2) relates specifically to security design of the identified primary processes (payments and transactions), whereas (3) is involved in designing, analyzing, and implementing cryptographic algorithms and protocols.

Furthermore, the participants should represent banks within the Dutch market, preferably with different organization sizes. Also, the level/ranking of the participants should be high enough that they are involved in some form of (operational or strategical) decision-making. The knowledge of the participants on banking's critical processes that rely on cryptography should be adequate, but they do not necessarily need prior knowledge on quantum-computing, the quantum threat, or PQC, as this will be explained in the pre-interview briefing (e.g., 1st interview question).

4.3 Participant profile

As was explained in the previous sections of this chapter, the participants in this study are involved in three different areas for which the quantum threat to cryptography in banking is relevant. All participants are currently employed by one of four Dutch banks. The participant division per group is presented below:

- **Security Architects** [P1, P2, P3, P4]
  All participants qualified for the participant requirement criteria and the organizations that they represent had employee amounts ranging from 1,500 to 50,000.
- **Payment Security Specialists** [P5, P6, P7]
  All participants qualified for the participant requirement criteria and the organizations that they represent had employee amounts ranging from 1,500 to 50,000.
- **Cryptography Specialists** [P8, P9, P10, P11]
  All participants qualified for the participant requirement criteria and the organizations that they represent had employee amounts ranging from 1,500 to 50,000.

The recommended sample sizes for qualitative research, where semi-structured interviews are used as data acquisition method, varies depending on the project size and scope. Clarke et al. (2015) recommend that for Master's or PhD research a sample size of 6 – 15 is sufficient, thus qualifying the 11 participants as adequate.

4.4 Ethical governance and data management

This research has approved by the Human Research and Ethics Committee of the TU Delft. The interviews were recorded. All interviews were transcribed by means of an external speech recognition tool provided by Microsoft Teams. This tool automatically deletes the recordings once the transcription is complete and complies with the latest security standards and regulations. All participants took part in the interview via Microsoft Teams, as they could not physically be present.

4.5 Study design

The study consists of semi-structured questions which will be accommodated with a 'one-pager' with information which creates the right context for the participants. This overview will consist of Table 1, Figure 2, and a simplified Figure 4 & 5. This will ensure that the answers are specific to the subject and facilitate the participants throughout the interview without the need for the researcher to (re-)explain the concepts. Furthermore, the questions are designed in

such a manner that the banks perceptions can be interpreted from the participant's answers, ensuring that the research-subquestions can be answered. The relation between the interview questions, research subquestions, and the TRM-framework can be depicted in Figure 9.

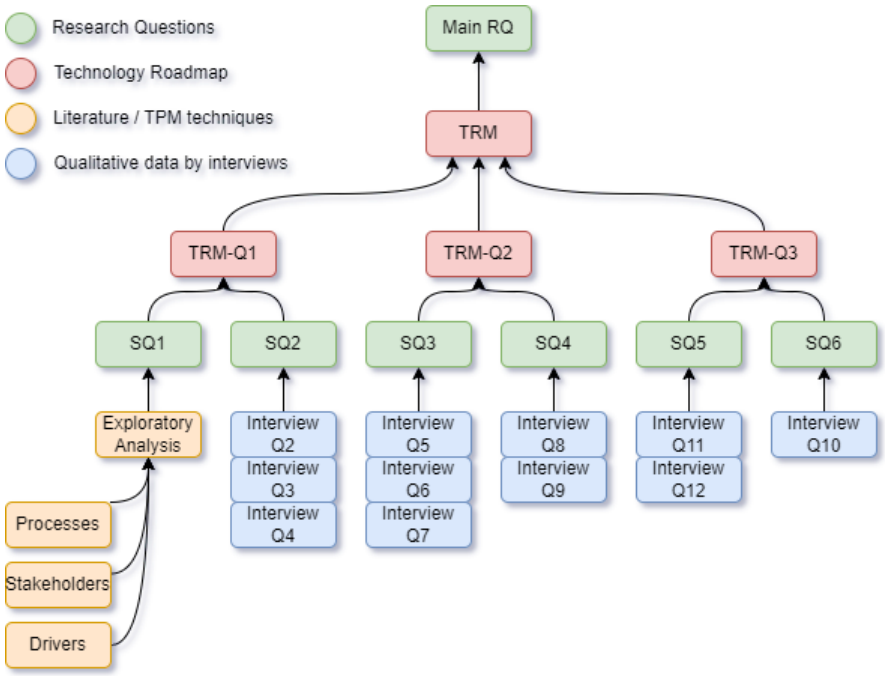


Figure 9: Relation between questions and methods

4.5.1 Semi-structured questions

The questions that will be used in the interviews are guiding in nature. This means that participants are allowed to deviate from the questions in some manner, so that all different possible perceptions and information is explored and extracted. The questions are presented below, in table 6.

Table 6: Interview questions

Context	Interview question
Opening question to determine participant's awareness and to determine researcher's tone	1. *Are you aware of the quantum threat? (If not, explain)*
Confirms or suggests amendments for the findings from SQ1	* Present findings from Chapter 2 & 3 (summarized in a one-pager) and ask for comments, criticism and feedback*.
Impact (SQ2) on the short, medium, and long term are identified and conceptual strategy begins to take form	2. *How would your organization be impacted if the PQC-transition has not been completed before QC breaks current cryptography?*

	3. *How would your organization be impacted if all encrypted transaction data was recorded, stored, and then decrypted ~15 years later?* 4. *What is your organization's long-term strategy on limiting these impacts?*
Preparedness (SQ3) in general is identified in an open-ended manner. The current governance mechanisms are identified as well as the knowledge and teams in place for the technical aspect of the PQC-transition	5. *How prepared do you estimate this organization is to transition towards PQC?* 6. *Does your organization have specific governance guidance in place for the PQC-transition?* 7. *Is your organization currently experimenting with the NIST-standardized PQC-algorithm final candidates?*
Capabilities (SQ4) are identified and prioritized by the participant	8. *Which capabilities do you think your organization currently possesses that can address the quantum threat?* 9. *Which of these capabilities would you say are the most critical in addressing the quantum threat?*
Challenges (SQ6) are identified and one specific challenge, relating do dependency on external actors, is addressed.	10. *What challenges do you think the PQC-transition will bring for your organization?* 11. *How will your organization address the dependencies on external service providers and systems within the payment process, when transitioning towards PQC?*
Resources (SQ5):	12. *What resources and governance tools would your organization require to face those challenges?*

4.6 Data Analysis

After the interviews are conducted and the transcription process has been finalized, the qualitative data can be analyzed. Firstly, a thematic analysis will be carried out in order to identify certain recurring themes, as well as recognize patterns of meaning in the data. The tool that will be used to carry out this analysis is Atlas. The basic process of thematic analysis has been laid out by (Clarke et al., 2015) and entail the following steps:

1. **Familiarization**: having in-depth knowledge with the dataset and making initial analytical notes
2. **Coding**: systematic process of labelling relevant features in the dataset that relate to the research objectives
3. **Searching for themes**: clustering codes together to create a mapping of patterns in the data
4. **Reviewing themes**: checking if candidate themes exhibit a good fit with the coded dataset
5. **Defining and naming themes**: defining and conceptualizing clarifications of every theme
6. **Writing the report**: combining the analytic narrative with compelling data extracts

This process will be carried out for the analysis of the transcripts, wherein codes are grouped by related themes which are then translated into final themes. This identifies the most relevant topics across the multiple interviews.

4.7 Framework development

The actual end-product that this research aims to deliver is a complete TRM framework which banks can utilize for ensuring the safety and security of their digital infrastructures, from the quantum threat. All the insights obtained from the sub-questions contribute to this framework and are all complementary. Processing all insights into one comprehensible framework is structured along the Technology Roadmap framework development guidelines. This is carried out by firstly constructing the TRM-skeleton, based on previous research (Barney et al., 2016; Carvalho et al., 2013; Daim et al., 2018; Pandeya et al., 2021; Schimpf & Abele, 2019; Schneier, 1999) and the insight obtained from the Exploratory Analysis (Section 3.4). Hereafter, during the thematic analysis, the qualitative data is analyzed to be transformed into elements fit for the TRM framework. Lastly, the framework is validated and possibly amended through expert critique.

4.8 Expert validation

As (Garcia & Bray, 1997; Pandeya et al., 2021) state, there are several follow-up activities that should be perused once the TRM has been developed. These include critique & valuation, as well as review & updating. Therefore, the final framework must be validated. This will be carried out by presenting the TRM framework to the interview participants and asking for their criticism, feedback, and necessary amendments. Other research that entails TRM development have used a similar approach, using experts for validation purposes (Daim et al., 2018b; Khanam & Daim, 2017). After this phase has been completed, conclusions can be drawn up, recommendations for banks can be summarized, and the limitation and suggestions for further research can be discussed.

The TRM will be sent to the interview participants, along with the anonymized summaries of their transcripts. This allows them to revoke or amend certain quotes if they wish. The TRM will be presented as a diagram in PNG format. This is accompanied by the 4 questions that act as means for critique & validation:

1. Are there any important technologies, capabilities, or resources missing from the roadmap?
2. Are there any currently presented technologies, features, capabilities, or resources that you would remove from this roadmap?
3. Can the roadmap in its current format be utilized tomorrow by your organization to reach its targets?
4. Do you have suggestion to make the framework more actionable and usable?

These questions are based on recommended elements by Garcia & Bray (1997) that should be covered for the critique & validation stage, namely: missing elements (question 1 & 2), will it enable targets to be met (question 3), and usability (question 4). Question 3 also contains ‘tomorrow’, which urges the respondents to suggest tangible actions that can already be taken now (figuratively tomorrow) that will enable the TRM-goals to be achieved. This may also further identify which elements or actions receive, or should receive, more priority within the framework.

5. Findings & Framework Development

In this section, the results of the conducted interviews will be presented in a structured manner, according to the aforementioned thematic analysis methodology. The presentation of the findings will be structured around the identified themes, which link to the sub-questions. The purpose of this section is to provide answers to the sub-questions and enable the development of the TRM-framework. The themes and patterns extracted from the qualitative data provide an insight into the perceptions of the participants. These participants have been selected according to this research's identified prerequisites that enables them to represent Dutch banks. This enables this research to draw conclusions from the findings. However, this does not mean that the participants speak for their organization, or that they are official external communications representatives. This has to be taken into account when reading the findings. The implications that this has for the generalizability of the results will be further discussed in Section 8.1.

The first interview question determined the participant's awareness regarding the research problem to establish the tone of the interview and thereby the level of depth. All 11 participants have been categorized as being fully aware of the problem. This small result is worth noting, because it enabled the interviews to go into the level of depth that was desired, but this will not be further discussed in the thematic analysis. The themes found through the thematic analysis, along with their descriptions, are presented in Table 7. More details regarding the codes of the themes can be found in Appendix A.

Table 7: Identified themes after analysis

Theme	Description
Perceived impact of the quantum threat and SNDL	Codes related to the expected impact that the Y2Q problem and the SNDL problem have on payment processes and the banking environment
Current strategy for the PQC-transition	Codes related to the organization's current strategy regarding the PQC-transition, organizationally, collaborative, and technically
Current capabilities & preparedness	Codes related to the overall preparedness of the organization for the PQC-transition in terms of the capabilities that the organization possesses
Challenges of the PQC-transition	Codes related to the challenges that the PQC-transition will bring for banks, that need to be overcome
Required features & resources	Codes related to all the future features and resources that the banks will need to overcome the mentioned challenges and successfully execute the PQC-transition
Governance guidance	Codes related to the bank's dependencies on external actors and the current governance guidance in place

5.1 Perceived impact of the quantum threat

The perceived impact of the quantum threat has been measured along two different levels of the threat. Firstly, the threat of quantum computing technology breaking current encryption schemes before the transition to PQC has been completed. Or in short: the 'Y2Q problem'. And secondly, the threat that malicious actors could already be monitoring and storing sensitive information today, and decrypt it in the future when a LFT quantum computer becomes available, known as the SNDL-attack model. Or in short, the 'SNDL problem' (see Section 2.7.2 for further explanation).

5.1.1 Impact SNDL is limited to privacy

What is instantly noticeable when analyzing the data, is that the participants are rather aligned on their perceptions of the impact of the SNDL problem. Nine participants mentioned that the impact of SNDL on their processes and data would probably be quite limited. For example, P11 states: "*I don't think the impact would be that great, (…) for instance, if I want to make a payment now, or transfer funds now, then in 15 years a PIN number on my card is not useable anymore, as a lifetime of a card is typically 5 years.".* This gets confirmed by P3 with his statement: *"5 years would be a big problem, but 15 years? I'm not so sure that that will be a problem.".* Participants P2, P4, P5, P6, P7, P8, and P9 make similar notions, wherein they mention that transaction data is simply not that valuable for hackers in 15+ years, and therefore not worth the effort of stealing it. The worth of hacking into a payment process lies more in the ability to disrupt, which is only relevant if the data is real-time (in transit). P7 illustrates this from the perspective of a hacker: *"If I were in possession of a quantum computer, I wouldn't choose to look into old transactions, I would go for the live data, for the live access, because in the end, I assume, you'd either attack for disruption, or to steal outgoing payments from the bank.".*

However, eight participants do recognize that the impact could be more severe on a customer trust level, relating to privacy. P8 brings this to light by illustrating a scenario where SNDL on transaction data relates to future privacy issues: "*I think store now decrypt later in this context mostly has an impact on privacy (…) So, you could build a database on what people have bought in the past, what kind of person they are. And potentially get insights into their banking account balance*". Participants illustrated more scenarios relating to SNDL's impact on privacy, such the implications of publishing all past transactions from the Dutch Royal Family (P1), as well as P9 finding stored client data very much more interesting than the in-transit transaction data. This links to overall customer trust in banks and the financial sector as a whole. If the privacy of the customer is in danger, then "*this customer does not want to do business with that organization any longer"*, P6 states. Overall, the disruptive abilities and the impact on payment processes of the SNDL problem are perceived as quite limited. The confidentiality of customer data, or privacy, are more heavily impacted and so *"the public's perception would probably require a lot of steering, making sure that banks are still able to operate and that the trust in the banking and financial system will remain."* (P2). What is noticeable is that participants do not mention how long banks are obliged to store certain types of data and what kind of impact that could have on SNDL.

5.1.2 Severity of Y2Q's impact differs per process

In general, there is a consensus on the notion that the impact of the Y2Q problem would be severe. For, eight participants indicated that they would see massive negative consequences if this were to happen. P8 summarizes what all other agreeing participants have said about this in some way or form, namely: "*If you consider breaking asymmetric cryptography then this entire online payment system would not be possible anymore, if we don't transition to other algorithms"* and P4 adds, *"(...) then we have a huge, huge problem."* But as stated, this is generally speaking. Where specifically in the payment processes the impact actually materialized, is another notion.

The most mentioned impact materialized itself in the online payment process. Five participants indicated that within this process the impact of Y2Q is severe. This is the case because online payments rely so much on TLS sessions over the internet. As P3 states it: *"We use TLS everywhere, for all these communications and traffic. In the case that quantum will become available, TLS, by today's standards, will be broken."* Regarding physical transactions, using PoS-terminals, the impact is less mentioned among the participants. P6 and P11 discuss the role of PoS-terminals in the payment communication chain briefly and acknowledge its vulnerable position. P8 adds that the impact would probably be in the fact that these terminals might need to be replaced and that this will be "*(...) a huge thing to replace".* Within the ATM transaction process, the participants do not even mention negative impact, besides hardware replacement issues (which will be addressed in Section 5.3). Two participants do mention specifically that the ATM process is relatively safe, mainly due to the fact that mostly symmetrical cryptography is involved. P8 states: "*With ATM's there is a lot of symmetric cryptography involved on which this doesn't really have an impact. For instance, between the ATM controller and the ATM processing network (...), so I think that for the entire ATM part, the impact will be very limited."*

5.2 Current strategy for the PQC-transition

All eleven respondents indicated that their organizations were already taking some steps to address the quantum threat. While this is a comforting thought, this does not mean that these organizations all have outlined strategies, or organization-wide plans in place to ignite the PQC-transition. Also, because the participants descent from various profile groups (Section 4.2 and 4.3), their approach on strategy differed. For instance, one can easily imagine that a participant involved in technical implementation on a daily basis, would articulate a strategy primarily from an implementation perspective. However, combining and merging all these perspectives enabled the most relevant strategy elements to be identified. These are grouped into three different main strategies. These being: experimenting with NIST algorithms, building a cryptographic inventory, and using sector cooperation as a strategy.

5.2.1 Experimenting with NIST algorithms

Seven participants explicitly mentioned the to-be-standardized PQC algorithms from NIST as being part of their strategy. This varied from actively following what is happening with the NIST-effort, to actively experimenting already with the candidate algorithms. This difference comes to light by comparing two statements. P4 stated: "*We know about*

the few NIST finalists and the right cryptography experts are keeping a close eye on those things". Whereas P2 already lays out a more detailed manner in which the NIST-algorithms are being monitored, by explaining that their team is *"executing test on those (NIST algorithms) to see what the impact would be and where the interactions are. We are evaluating those together with other parties that know where crypto is used".* P3 mentions that they are already testing different algorithms and schemes for various applications, and are mostly using CRYSTALS-Dilithium in their efforts to do so. However, the participants do mention that there is some sense of abstention since there is not finalized standard yet, which will be further discussed in Section 5.3.

5.2.2 Building a cryptographic inventory

Waiting for finalized standards to arrive, without then knowing in which systems you would need to implement which specific scheme or algorithm, is not something the participants find useful. Therefore, eight participants mentioned (in various forms) that the development of a cryptographic inventory is an essential part of their strategy. P10 states this as the focus being "*first on knowledge, cryptographic agility, making sure there's an overview of the cryptographic pain-points, but also all places where crypto is used, a cryptographic inventory"*. What this means operationally is well described by P1, as *"an inventory of in which systems we use which algorithms, so that when that quantum computer is here, you can say: on that system we still use RSA and, there we use ECC, and there we still use triple DES- 112 bits, etc. So, then, you know where to start troubleshooting first".* However, this same participant also indicated that even though the development of the cryptographic inventory has already started, there is still no bank-wide complete overview. This is also recognized by P4: "W*e have taken the small first steps for an inventory of all the different encryption types on the fronts of the different applications, connections, and processes (...), but there's no central inventory"*

5.2.3 Sector cooperation as a strategy

All of the banks included in this research had at least one participant who emphasized the significance of sector cooperation in their strategy. The quantum threat and the PQC-transition are thus not seen as competitive project in which one bank gains an advantage if they address the problem better than the other banks. The participants recognized the importance of transitioning the Dutch financial environment as a whole and mentioned that cooperation is a meaningful aspect all their strategies. This is mainly facilitated by the Dutch Banking Association (Nederlandse Vereniging van Banken, or NVB) as well as the regulatorily body DNB (De Nederlandsche Bank). P1 indicated that their organization collaborates with these parties, as well as with other banks in a *"quantum readiness group"*. P2 talks about similar (or perhaps even the same) groups, mentioning *"standardization committees"* that were founded because *"together with the other banks, we said we need to do something about this".* All parties within these collaborations have knowledge to gain from cooperating, as P4 states it: *"It make sure that we share our knowledge with other banks, but also that we get knowledge from other banks to see, how they are doing this and what they are running into".* This specific cooperation is also a part of the overall collaborative capabilities, which will be further discussed in Section 5.4.2.

5.3 PQC-transition challenges

In Figure 10 the participants' identified challenges regarding the PQC-transition have been presented and ranked based on the number of participants that mentioned them. These challenges are all relevant to consider when developing the TRM-framework, but the frequency of the mentions may indicate which challenges are more pressing than the others. This section could individually discuss all these challenges, but it is more efficient to discuss them in terms of the two types of challenge that these challenges can be grouped by. These being: technical challenges and organizational challenges.

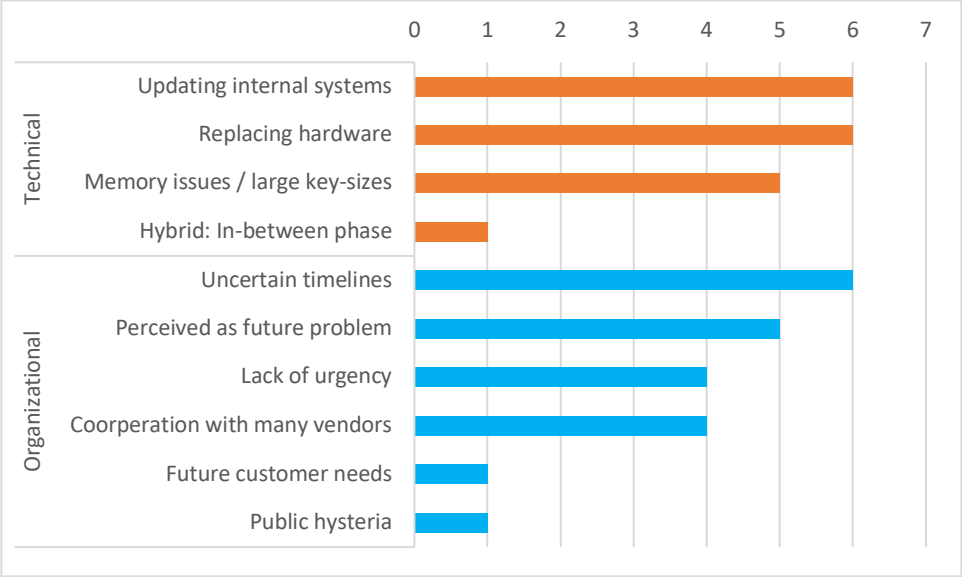


Figure 10: Frequency of challenges, grouped

5.3.1 Technical challenges

The top three technical challenges that are presented in Figure 10 are all in some way or form connected to one another. Updating internal systems is challenging because replacing hardware is challenging. Replacing hardware is challenging due to (among other reasons) memory issues. The issue of updating all these systems lies in the abundance of different connections, applications, software, and hardware. P4 states this as: "*we've got thousands of connections and applications which we built ourselves and also thousands of applications which we buy from others. Upgrading all that stuff is a huge, huge, huge job".* What makes this so challenging is partly due hardware related to ATMs, PoS systems and physical debit/credit cards. The reason that this is challenging twofold. Firstly, these systems are widely distributed across the country and replacing them is economically and logistically difficult. P1 explains this, by also linking the systems to their lifetimes: "*ATMs and PoS systems, those are systems that are sometimes operate for 5 to 10 years. Those also need to be updated if the current hardware is not suitable to run PQC. Then all those systems need to be replaced, but if those are not yet on the list for replacement because they are not yet economically depreciated, then you are going to run into issues".*

P8 shared a similar concern regarding the PoS terminals, by comparing the PQC-transition to the replacement of all terminals for the contactless payment transition. This had apparently also been a *"difficult project that took a while for everyone to adopt"* and P8 expected the PQC-transition to entail similar difficulties.

The second reason for challenges relating to the replacement of hardware, is due to the memory issues and large key sizes that are expected to be associated with the PQC algorithms and schemes. First experiments with the NIST algorithms have shown that there are issues regarding CPU and memory, due to the algorithms' encryption key sizes. "*This may also lead to keys being fragmented in the package handshakes of networks, which leads to trouble in hardware",* P2 states. This has implications for the entire payment system, as P3 mentions: "*As of now, PQC algorithms are slower, and keys are larger. This will bring problems for the current systems capacity".* Specifically banking cards were identified as having difficulties with this problem. P1 mentions: "*The thing that I worry about is also digital signing with PQC-algorithms that just doesn't fit on, say, a bank card or on smart card logon, or that kind of environment anymore",* and P8 notes: "*A major issue is legacy systems that may not be able to handle the new algorithms. For example, some debit cards currently use RSA certificates, (...) if a move to PQC-algorithms is necessary, it may be difficult and costly to replace all the debit cards".* Overall, the technical challenges can be found in the abundance of distributed systems, the logistical and economic problems associated with PoS and ATM terminals, and legacy systems' / bank cards' incompatibility with the new PQC-algorithms.

5.3.2 Organizational challenges

The top three organizational challenges that are presented in Figure 10 are connected to one another in a similar manner in which the technical challenges were connected. Due to the uncertainty of the timelines associated with the quantum threat and the PQC-transition, it is primarily perceived as a future problem. By being perceived as a future problem by different parts of the organization, there is a lack of urgency to address the situation. The uncertainty of the timelines associated with the PQC-transition is being laid out by P7: *"Where is the starting point? Is that 2 years, 10 years, 15 years? To make the change that's likely necessary, one should start early, but it's difficult to be preemptive in such a way that you start early, and you end up exactly where you need to be when the target is not that clear".* Because of this 'moving target', organizations are reluctant to dedicate time and resources to this issue. Even though some divisions in a bank would want to give the PQC-transition more priority, other layers of the organization should also be on board. This is difficult if these layers indeed perceive the issue as that of something far off in the future. P1 recognizes this problem, and stated that his team is *"trying to work on it, but programmers and some layers of management still operate in terms of 'today versus tomorrow' and they see this issue more as a 'day after tomorrow' matter."* Other participants share similar notions and translate this into a matter of priorities, or a lack of urgency. Within banks, priorities dictate resource allocation, as P4 observes: *"We've got a lot of developers, but they also have a lot of things to do, and this is simply not a high priority for everybody. Except for a few security people, nobody cares, because the business is what dictates what features are being built and PQC doesn't add any value for them yet."* Overall, this illustrates a text-book organizational issue, namely short term versus long term thinking.

Lastly, a noticeable number of participants found the cooperation with many vendors challenging. This relates to the technical challenges too, as these vendors are involved in providing software, hardware, and intermediary services for the payment processes. The challenge is twofold. Firstly, it is operationally exhaustive because there are many vendors involved, as P5 states: *"The fact that we have to cooperate so much with other parties (...) and vendors that also use cryptographic keys (...), that makes it more complex".* Secondly, the banks are being held accountable for the services they provide, but they rely on vendors the systems they provide execute their operations according to the required standards. The vendors need to be pushed by the banks to transition towards PQC, P7 and P10 argue. P10 formulates this as: *"I think the dependencies of external products might be the hardest change to make, to push the vendors to change".*

5.4 Current capabilities & preparedness

As the section on strategy pointed out, all eleven respondents indicated that their organizations were already taking some steps to address the quantum threat. The capabilities that enable that have been grouped based on the distinction that the participants made between internal capabilities on the one hand, and collaborative capabilities on the other. Overall preparedness is difficult to measure and also difficult to express, but it shows the amount (and type) of effort required to enable the transition towards PQC.

5.4.1 Internal capabilities

What can be observed when the participants address their organization's internal capabilities, is that their attitude is quite positive towards past experiences and technical knowledge. P8 is confident in his organization's capabilities to successfully transition towards PQC, based on the capabilities they currently possess: *"We have the capabilities to handle it. If it doesn't go as fast as we expect, it would be almost business as usual, like phasing out another algorithm, which we've done before".* This relies on the past experiences the organization has had when transitioning towards new cryptographic algorithms, but what that requires is deep technical knowledge on these topics, within the organization. P3 mentions: "*Knowledge on cryptography is really important. We have people that understand how it works, how it affects everything, and also have broader technical knowledge".* The fact that these people are in place and that the knowledge is thus internally there, has positive implications on the implementation front. With good enough technical knowledge, and time and effort, *"technically, it's not that difficult to replace algorithms"* (P4).

5.4.2 Collaborative capabilities

As it is mentioned in Section 5.2.3, sector cooperation is embedded into the banks' current strategy in addressing the quantum threat. Seven participants explicitly mentioned collaborative capabilities as being very important. These collaborations are related to inter-bank collaborations, as P8 describes: *"There is collaboration between the top banks of the Netherlands on security, where this is also a recurring topic. It's hard to predict if this will be enough or fast enough once we get there. However, a lot is already in place, and we are on top of it, so I think we're in a good position".* The participant notes that even though the topic is getting enough priority, the fact that the collaborative structures are in place is a positive notion. Furthermore, the collaborative initiatives also go beyond bank-to-bank, but

also involve regulators and the sector association, as Section 5.2.3 highlights. Moreover, collaborative structures with service providers are also in place, according to P3. He mentions that his organization has "*collaborations with the service providers and other banks, but these are not yet focused on PQC. But when quantum will become really urgent, then there will be a higher priority to collaborate on this front".* This shows how valuable it is that these collaborative channels already exist today even though the lack of urgency still plays a part. These collaborations can be quickly utilized once this lack of urgency fades out, instead of having to be built up from the ground up. P7 confirms this and add that these structures are not only in place for security related topics, but also for *"other developments in payments in the financial service industry".* Lastly, P1 discusses collaborations with tech companies, such as Microsoft and Google. It is important to be in contact with these types of organizations, because of their involvement in PQC and the development of quantum-related technology. P1 states: "*They are frontrunners and have already begun with running systems on quantum cryptography, so collaborating with them is important".* Overall, collaborative structures are in place within the Dutch banking environment. These involve banks, regulators, service providers, and tech companies, and topics within these structures encompass security in general, developments in the payment sector, and development in quantum-related technology innovations.

5.4.3 Overall preparedness

What is instantly noticeable is that P5, P6, and P7 indicate that they do not perceive their organization to be very prepared for the quantum threat. Since these participants descent from the same profile group, they might all perceive the issue differently than their colleagues from the other (more directly involved in cryptography) profile groups. For, participants from these other profile groups explained their long-term preparedness based on the aforementioned internal and collaborative capabilities, and showed a positive perspective on their preparedness. This difference in perception on preparedness between these profile groups actually says something meaningful about the organization-wide preparedness. Namely, that organizational-wide the banks are relatively unprepared, as there is a structural difference between the perceptions of the different involved groups. Of course, this is mainly due to a lack of internal information-sharing between these groups, as Payment Specialist are relatively unaware of what the other groups are doing in terms of preparing. But this information-asymmetry is a sign of unpreparedness in a wider-sense.

In terms of short-term preparedness, four participants shared that there is a structure in place that could counter the quantum threat on the short term in case of an unexpectedly fast disruption from quantum technology. The long-term preparedness is more relevant for this research, as it is not expected that quantum technology will be able to break current cryptography tomorrow. However, should that hypothetically happen, there is a measure in place which could limit the damages on the short-term. P1 explains: *"We can fall back completely to symmetric encryption on the short term, so if one of the superpowers next year announces that they have a quantum computer that is able to break asymmetric encryption, then in our payment system we can reasonably easily switch".*

5.5 Required features & resources

In Figure 11 the participants' identified features and resources required for the PQC-transition have been presented and ranked based on the number of participants that mentioned them. These requirements are all relevant to consider when developing the TRM-framework, but the frequency of the mentions may indicate which are more pressing than the others. This section could individually discuss all these challenges, but it is more efficient to discuss them in terms of the two types of challenge that these challenges can be grouped by. These being: external requirements and internal requirements.

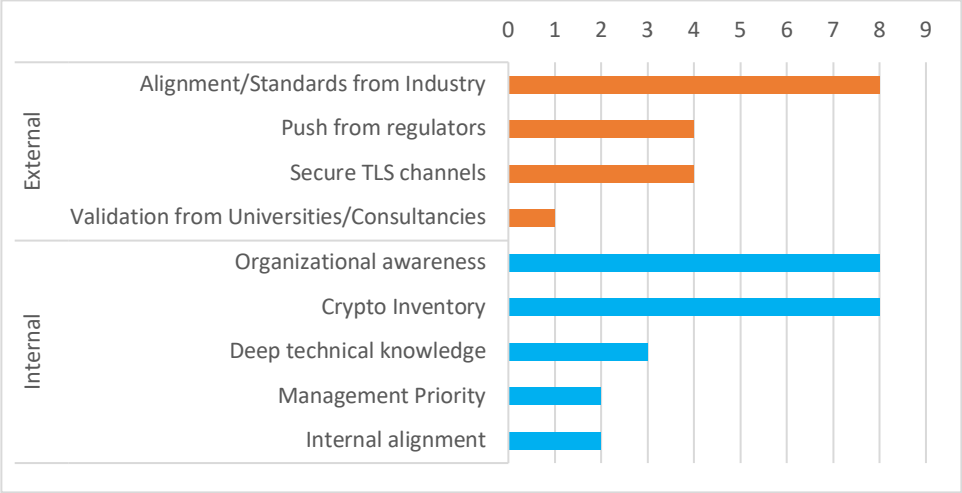


Figure 11: Frequency of required features and resources, grouped

5.5.1 External resources

The required resources are related to the challenges that the participants mentioned. In order to overcome these challenges certain resources are required that don't necessarily fall under the capabilities that the banks currently possess. The problem with external resources is that these are dependent on other actors, and the availability of these resources depend on processes which the banks cannot always directly influence. The resource which illustrates this well is the alignment/standards from industry. Eight participants mentioned that this would be something that they very much need in order to ignite the PQC-transition within their organization. P10 explains this, by highlighting the dependency on external actors: *"We can't do anything without VISA, EMV, SWIFT. With them, we need alignment to solve the major problems"*. Why the banks cannot do anything without these actors is because they set the international payment standards. The EMV (Europay, Mastercard, VISA) standard dictates the technical standard for payment cards, and thereby influences the compatibility of these cards with PoS and ATM terminals. P2 recognizes this as the most pressing issue: *"The EMV standard is basically the biggest problem, and it's the whole problem within the industry. (...) as long as we don't have standardized algorithms, we can't do anything"*. P1 confirms this and argues that this task of standards and alignment lies with the organization responsible for developing the EMV standards, EMVco.

This resource is not simply developed over night, also because the EMV standards will depend on the finalized standards from NIST.

Furthermore, push from regulators is also a resource which the participants would require. P7 states that this is a very high impact resource: *"I think as most things in the banking industry, what is required is, evolving regulations that will push everyone to a high enough standard".* Regulations can be a very powerful resource to align the industry, by setting the required standards. However, push from regulators do not only bring alignment to the industry, but also address the lack of urgency challenge. P4 explains this by arguing from a scenario in which a LFT quantum computer would be close on the horizon: "*If we get the feeling that there would be a quantum computer that would crack all cryptography, and then the government would advise us to start implementing PQC today, then we would start to run. I think when the regulator says we have to do something, then suddenly there's a lot of urgency".* This gets confirmed by P7, as he explained that clear guidance from regulators on the current state and consequences would help organizations to come out of the *"'well let's wait and see' mode"*.

Lastly, a more technical external requirement, that was often mentioned by the participants, was related to secure TLS channels. Looking at the process charts in Figures, 5, 6, and 7, one could notice that TLS secured communication channels are one of the most crucial infrastructures within the payment processes. P8 notices this as well and labeled these TLS protected channels the *"most impacted areas".* The banks are dependent on other organizations to develop these channels and embed them into their infrastructure, as P11 states: *"You are not going to develop that (TLS channels) yourself, so that needs to be implemented by the suppliers of those kind of packages, open SSL for instance".* This is confirmed by P3.

5.5.2 Internal resources

In terms of resources that the banks can directly influence themselves, the ones that were most commonly mentioned can all be linked to aforementioned findings. Organizational awareness relates to the challenges associated with the lack of urgency and future-problem-perception. With more organizational awareness, the bank-wide preparedness can be influenced, as through awareness campaigns more different teams within the organization will become have an interest in integrating PQC related topics into their day-today operations or goals. However, at the moment this is not yet the case, as P11 notices: *"You are dependent on a lot of teams that just don't have anything with crypto. They see it more as a burden than having importance".* P5 makes the comparison with the technical implementation of PQC and highlights that awareness is far more critical: *"Technically it's not that difficult to replace algorithms. I mean it's not easy, but it's doable. However, convincing all these people that it's important and getting budget and people to do this to give the priority, that's the difficult part".*

Lastly, the required internal resource that has also been identified as critical by the participants is a cryptographic inventory. This has already been discussed in the strategy findings, so one could expect that this is already in place. However, note that this is not yet a complete strategy, as these inventories are not yet complete in most cases. P4

explains: "W*e have taken the small first steps for an inventory of all the different encryption types on the fronts of the different applications, connections, and processes (…), but there's no central inventory"*

5.6 Governance guidance

The participants mainly discussed two different governance mechanisms that were currently in place within their organizations. Firstly, external governance from regulatorily bodies and associations were mentioned by seven participants. Secondly, current governance structures in place regarding their cryptography and security standards were discussed by 6 participants. These structures are currently not per se focused on quantum, or the PQC-transition specifically. However, the existence of these structures can be a powerful capability, as was mentioned in Section 5.4.2.

5.6.1 Guidance NVB & DNB

Even though push from regulators is a resource that the banks still require, there are already some structures in place in which regulators communicate the issue towards the banks. Several documents are being published and knowledge sharing sessions are being held to inform the banking sector of all that is associated with the PQC-transition. These structures do not entail binding policies for the banks, but the information they provide are being taken seriously, as P1 notes: "*The Dutch banking association and the DNB have published some recommendations, which we follow".* P8 adds: *"NVB (Dutch Banking Association) has a lot of interest in quantum cryptography and holds sessions on the topic".* However, these sessions and recommendation documents are not yet binding, which therefore may create the lack of urgency. P3 has a positive attitude towards this notion as he thinks that *"as time progresses, it will no longer be just the advice, but there will be regulations for everyone".* How much time has to progress, is not yet clear.

5.6.2 Current cryptography Governance

Six participants explained that the lack of governance on PQC specifically is not that big of an issue. This is due to the current internal structures in place that address security and cryptography in general. Regular changes in infrastructure, incident management, and safety of current algorithms were mentioned. PQC governance can be seen as a part of a broader concept of cryptography governance, as P2 explains: *"Quantum breaking crypto is just one thing. (…) We always need to keep on our toes to prevent breaches in our crypto, so we need to be aware of where our crypto is in our current state".* Cryptography governance is a dynamic process in which policies on cryptography keep algorithms up to date that are considered safe, or as P8 says, those that *"need to be phased out as soon as possible".* Thus, the participants are confident in their current governance structures, even though there often is "*no governance in place specifically for the PQC transition"* (P3).

5.7 Findings overview and input for TRM-Framework

This section provides an overview of the elements that were most relevant within the themes derived from the thematic analysis. Table 8 functions as a summary table of the findings that have been presented in all of Chapter 5. It contains the codes identified by the participants, per theme. This overview thus summarizes which elements need to be embedded into the TRM, along with the findings from the exploratory research (see Section 3.5 for skeleton).

Table 8: Findings overview of most relevant codes per theme, as input for TRM-framework

Impact	Strategy	Challenges		Capabilities		Resources		Governance
		Technical	Organizational	Internal	Collaborative	External	Internal	
Privacy impact SNDL	Experimenting with NIST algorithms	Updating internal systems	Uncertain timelines	Past experiences with transitions	Communications bank-bank	Alignment/ Standards from industry	Organizational awareness	Documents NVB & DNB
Severe impact Y2Q on online payments	Developing a cryptographic inventory	Replacing ATM hardware	Perceived as future problem	Broad technical knowledge on cryptography	Communications service providers	Push from regulators	Central cryptographic inventory	Knowledge-sharing sessions NVB
Severe impact Y2Q on PoS	Sector cooperation	Replacing PoS hardware	Lack of urgency	Broad technical knowledge on payment processes	Communications tech companies	Secure TLS channels	Deep technical knowledge	Current cryptography governance
Limited impact on ATMs	-	Replacing payment cards	Cooperation with many vendors	-	-	Validation from Universities/ Consultancies	Management priority	Involvement with EMV
-	-	Memory issues / large key-sizes	-	-	-	-	Internal alignment	-

What can be noticed when looking at the elements in Table 8, is that there is a difference in word structures / syntax. Some elements are presented as verbs, or actions, and some are presented as nouns, or things. This is logical, as participants would indicate strategy or challenges often as action (i.e., executing a strategy and overcoming a challenge). Capabilities or resources for instance are indicated as 'things' that the organization has or needs to have. Despite this logical explanation, this difference in syntax could be perceived as confusing in the TRM. Therefore, all elements will be embedded into the TRM as nouns.

5.8 First draft for TRM-Framework

5.8.1 Diagram instructions

The elements in the first draft of the TRM (see Figure 12) have been spatially prioritized on the x-axis based on the participants' perceptions on the element's importance, as well as their criticality. Criticality in this sense means that if an element B cannot exist without the existence of another element A, then A has to come before B in time. Also, the elements have been somewhat grouped so that the number of crossing arrows is minimal (for readability purposes). The x-axis of the diagram represents a timeline, but this does not necessarily mean that for instance [*PQC requirement list for vendors and service providers*] has to be completed before [*Hardware replacement strategy*]. Their position is just more convenient to present in such a manner that the diagram is more readable. This interferes somewhat with the criticality aspect that was just mentioned. To address this, the roadmap has been divided into three phases. Within each phase the elements' position may also be based on convenience for readability, but between phases however, the criticality criterium holds up. Meaning that Phase 2 cannot be completed entirely before Phase 1 has taken place.

The y-axis contains the categories of the elements, based on the general format of a TRM-framework, as described by Kostoff & Schaller (2001), Probert et al. (2005), and Wells et al. (2004). However, these authors make no distinction between technical resources/capabilities and governance related resource capabilities. The TRM draft in Figure 12 will make this distinction. This has been done because, firstly, it provides the reader with a clearer overview of the different types of resources, secondly, because the sub-questions of this research make this distinction as well, and lastly, because it increases the readability of the diagram.

Finally, the arrows that connect the elements should be interpreted as input/output arrows. The elements are connected to each other through these arrows, but not all possible connections have been presented in the diagram. Only the most important connections have been presented. What this means is that for instance [*Management priority*] is a requirement for the element [*Hardware replacement strategy*], but these are not shown to be connected to each other. This because the [*Management priority*]'s connections to earlier stage elements are more important and these earlier stage elements will eventually realize that [*Hardware replacement strategy*] is able to exist. This indirect connection is not presented visually in the diagram, but can be logically derived from the context of this research.

The TRM is developed to address the bank as a whole, but would be most relevant for the Chief Information Security Officer (CISO) within a bank. This person is responsible for overseeing the bank's information security program and plays a critical role in ensuring that the digital infrastructure is protected from cyber threats. Therefore, the TRM will be addressed to the CISO's of Dutch banks.

5.8.2 Draft Technology Roadmap

Figure 12 presents the draft of the TRM-framework. Appendix B consists of further explanation on how thematic analysis findings relate to certain TRM elements. The framework in Figure 12 has not been validated yet.

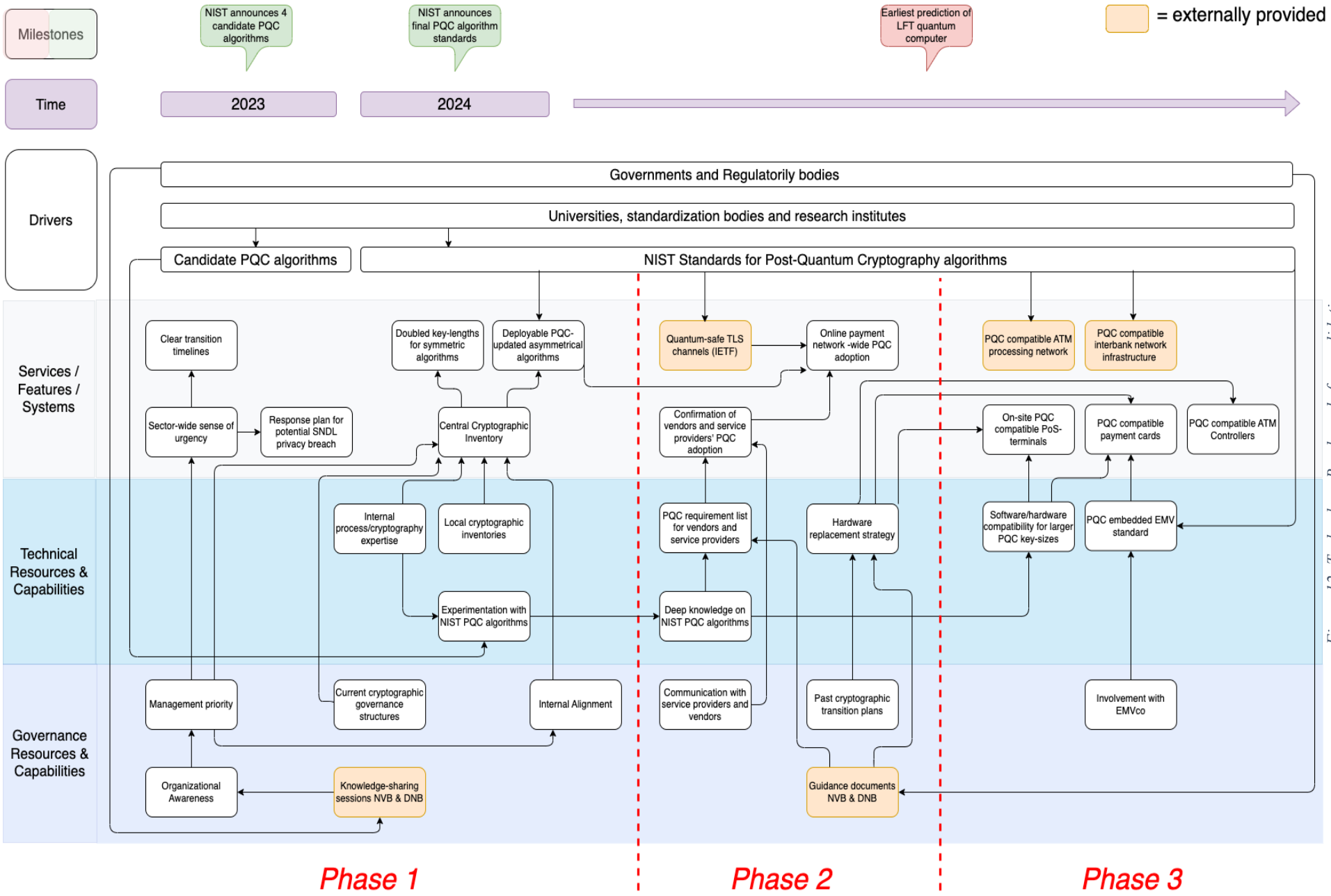


Figure 12: Technology Roadmap before validation

6. Discussion & Validation

The purpose of this research was to develop a TRM-framework for ensuring the Dutch banking sector's safety and security of its critical digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology – from not merely a technological perspective, but with a holistic approach, considering the involved socio-technical challenges. The answers that the participants provided contained the required elements to develop the TRM and to answer the sub-research questions of this research. This section will briefly assess the initial results, after which the expert critique and validation on the TRM will be discussed. Lastly, the final TRM will be drawn up.

6.1 Discussion of results from thematic analysis

The participants have shown their perceptions on impact, strategy, capabilities, preparedness, challenges, resources, and governance, related to the PQC transition within in their organization and the banking sector. Firstly, the results show that the impact of SNDL is overall perceived as quite limited and that the implications mainly relate to customer trust, due to privacy concerns. In contrast, the Y2Q problem is perceived as very severe by most participants, but this severity seems to differ per process. The online payment process is identified as the most vulnerable, mainly due to the many dependencies on other stakeholders and the reliance on TLS. Physical transactions using PoS-terminals were perceived as less vulnerable, although the participants acknowledged that these PoS-terminals needed to be replaced. Furthermore, the ATM process is considered to be relatively safe because of the use of symmetric cryptography. What this result means is that banks can prioritize processes when transitioning towards quantum-safety. The investigated processes were already identified as the primary processes in Chapter 3, which showed that these processes should be the first ones to assess when transitioning towards PQC. Now, the argument could be made that between these three processes there indeed is a ranking of importance. This is can be seen in the TRM in Figure 12, as the processes have different positions in time.

Secondly, the participants perceived their organization's strategy to be mainly related to experimenting with NIST algorithms, building cryptographic inventories, and using sector cooperation as a strategy. Of course, the participants differed in their involvement per strategy, as cryptography specialists focus more on experimenting with NIST algorithms, whereas security architects have a more holistic view and should also consider sector cooperation, for instance. What this result says is that banks have already taken some first measures to address the quantum threat along the three axes that make this problem so complex. Experimenting with NIST algorithms relates to preparing for technical implementation of new PQC algorithms and schemes, building cryptographic inventories relates to knowledge on where cryptography is used, and sector cooperation relates to the complex stakeholder landscape within the banking industry. However, no participants indicated that there already was a central cryptographic inventory in place, which could be caused by the lack of internal alignment within the banks, as the results on required resources suggested.

In terms of preparedness for the PQC-transition, the above would suggest that the banks are actually quite prepared. The organizations seem to have a similar strategy in place and their perceptions on their capabilities were mainly positive. Most participants argued that internal knowledge on cryptography and processes were not an issue, and it was also mentioned that experiences with past cryptographic transitions would be a meaningful capability within the PQC-transition. Furthermore, the participants emphasized their collaborative capabilities as being important. This can also be found back when looking at the required resources results, as the participants do not mention that this is currently lacking. This means that the Dutch banks have a strong position as a sector when it comes to becoming quantum-safe. Although there are still major concerns, such as a lack of urgency, organizational unawareness, and uncertain timelines, the fact that the Dutch banks already have strong collaborative capabilities is a positive notion. However, the results also showed that payment specialist are relatively unaware of what the other groups (security architects and cryptography specialists) are doing in terms of preparing for the PQC-transition. As stated, this information-asymmetry is a sign of unpreparedness in a wider-sense. These types of issues relate to organizational unawareness and can be mitigated by management priority (as can be seen in the TRM in Figure 12).

The participants identified both organizational and technical challenges. Organizationally it can be stated that the identified challenges all relate to the lack of a long-term vision. This shows that it is crucial that communication and collaboration between different layers of the organization is in place. Priority from management is required to address these issues, which can also be seen in the required resources results. Moreover, some participants perceived cooperation with many vendors to be challenging. This somewhat contradicts the results regarding the positive collaborative capabilities. The participants indicated that these collaborative structures are in place, but they still see this as a challenge. What this means is that even though the collaborative capabilities with vendors are in place, the actual confirmation of these vendors' effort to transition towards PQC is critical, which can be seen in the TRM in Figure 12. Furthermore, the technical challenges mainly related to the abundance of distributed systems, the logistical and economic problems associated with PoS and ATM terminals, and legacy systems' / bank cards' incompatibility with the new PQC-algorithms. The identification of these challenges also further identified resources that the participants did not even mention in the resource-section. Namely, a hardware replacement strategy (which is supported by results 'experience with past cryptographic transitions' and 'guidance from NVB & DNB') could help overcome some of these challenges.

The participants made a clear distinction between external and internal resources required to overcome the identified challenges. It can be stated that banks have limited control over all the resources that they require. For instance, alignment/standards from industry are something for which banks are heavily dependent on other organizations, such as EMVco for payment cards, SWIFT for interbank communication, NIST for standardized PQC algorithms, and IETF teams for secure TLS channels. This dependency on external resources reveals the importance of collaboration and coordination within the industry, to ensure that the transition is successful. Furthermore, the lack of sector-wide standardized algorithms disrupts the banks' ability to effectively address PQC-related challenges at this point in time. However, since final standards are expected to be announced by NIST in the summer of 2024, one could argue that proactive steps could already be taken in anticipation of the standards. These steps relate to the internal resources. If

by the time the standards arrive, the organizational unawareness is still prevalent, then the banks will still face though challenges in pursuing a smooth PQC-transition. The same goes for the development of a central cryptographic inventory. If there is not one comprehensive overview of cryptographic algorithms and schemes per service and process present, how can the bank then possibly implement PQC organization-wide, ensuring safety from the quantum threat? While some progress has already been made in this area, as the participants mentioned it to be part of their strategy, these inventories are still mainly incomplete and un-centralized. Overall, the internal required resources are within the banks' own control and are crucial for transition. Therefore, the TRM in Figure 12 shows that these elements set the tone for phase 1 of the PQC-transition.

Lastly, the participants perceived governance guidance to be also divided into external and internal in a certain sense. Internally, the participants emphasized that the current governance structures involving cryptography and security standards, serve as a solid foundation for addressing the PQC-transition challenges. Although these structures may not yet be focused on PQC, or the quantum threat in general, these structures can serve as a valuable asset in guiding the PQC-transition within the organization. This also relates to the 'experience with past cryptographic transitions' element, which actually is an example of one these structures. As for the external guidance, this was mainly perceived as revolving around DNB and the NVB. Even though the guidance documents they provide and the knowledge-sharing sessions they host on quantum-related topics are not binding, they still serve as a crucial source of information on which the banks base their policy. These sources of information can support the banks in providing organizational awareness, but could also help in developing operational/implementation plans such as a hardware replacement strategy, or requirement lists. This can be seen in the TRM in Figure 12, but can also be derived from the results on collaborative capabilities.

6.2 Framework validation

The combined perceptions of the participants, together with the insights from the exploratory research aimed to develop a complete overview on the requirements needed for banks to transition towards safety and security from the quantum threat to cryptography, thus the TRM-framework. The framework has been validated by presenting the TRM to an interview participant from each profile group (cryptography specialist, security architect, payment security specialist) as well as an external expert (PQC-transition researcher) and asking for their criticism, feedback, and necessary amendments. Four validation questions have been asked (see Section 4.8), which related to missing/redundant elements, targets, and usability.

Table 9: Expert identifier per participant

Expert	Interview participant	Profile
E01	P01	Security Architect
E02	P07	Payment Security Specialist
E03	P08	Cryptography Specialist
E04	External	PQC-transition researcher

6.2.1 Missing or redundant elements

In terms of important technologies, capabilities, or resources missing from the TRM, the experts have indicated that an improvement could be made by adding more details regarding systems that need to be updated. E01 mentioned that cryptographic algorithms and libraries are often hard-coded in the source code of software. This is often *"very old mainframe code"* (E01), which makes it difficult to make old software quantum-safe. Therefore, E01 suggests to add in an element that encompasses **reprogrammed internal software.** As this is mainly internal software, it does not directly affect the payment processes. Therefore, this feature will be inserted in phase 3. Secondly, E02 did not mention a specific missing element, but raised some concerns regarding the allocation of budget. He stated: *"If you say that you will now partly focus on this risk and ensure that the payment infrastructure is resilient, it will come at the expense of other things"*. Adding this concern to the TRM is rather difficult because it is more of a concept than a specific resource/capability/technology. However, adding in the resource **risk-based cost analysis** could address this concern, linking to management priority and internal alignment. Thirdly, E03 identified a similar missing element as E01, relating to the updating certain software to become quantum-safe. He stated: *"The TRM seems to primarily focus on payment traffic (both PoS and online-banking), but of course there's more that needs to be considered when transitioning to PQC, e.g., replacement of all TLS certificates, web hosting software, file transfer channels"*. This critique does not take the specific scope of the TRM and this research into account, as the TRM indeed focuses on the payment processes and not takes all other (secondary) processes into the analysis (see Sections 3.2 and 3.3). This critique will be taken into account when presenting the suggestions for further research. Lastly, E04 pointed out that it is unclear from the TRM who it is actually addressed to. As there are many departments within banks and there are many decision-makers, it would be helpful to clarify which person or department the TRM is addressed to, E04

suggests. This suggestion is already considered when describing the TRM development in Section 4.7. The critique is very relevant, but does not explicitly mention a missing technologies, capabilities, or resources that needs to be added in. E04 also noted that there are a lot of service providers that support the banks' services in terms of providing software and hardware. Banks cannot make decisions for these actors and this especially affects phase 2. E04 suggests that this needs to be explained when discussing the roadmap.

In terms of technologies, capabilities, or resources that could be removed from the TRM, or redundant elements, experts E01 and E03 indicated that all elements seem to be relevant and nothing should be removed. Also, E02's attitude was overall positive. He did have one suggestion, which stated that it would be good to prioritize the payment processes over time based on risk. However, this has already been considered while exploring the online payment process, physical transaction process, and ATM process in Chapter 3, as well as when presenting these to the interview participants during the interviews. The prioritization as it currently is, is based on the vulnerability to the quantum threat per process. This can be seen back in the TRM by the chronological position of the elements relating to these processes. Finally, E04 saw great resemblance between the external elements in the chart and the drivers on top of the chart. This expert suggested that the drivers-layer therefore could also be placed at the bottom of the diagram. However, due to the readability of the diagram and the chosen format based on Kostoff & Schaller (2001), Probert et al. (2005), and Wells et al. (2004), this will not be changed.

6.2.3 Feasibility of reaching targets

The TRM should be able to reach the targets effectively in its current format. While E03, stated that the TRM could *"definitely be used to reach PQC readiness"*, E01 stated that there is still an issue with management priority. The validation question 3 also contains 'tomorrow', which urged to suggest tangible actions that can already be taken now (figuratively tomorrow) that will enable the TRM-goals to be achieved. E01 identified that the largest issue in reaching the targets relates to the lack of management priority. Even though this element is present in the TRM itself, there is management priority needed to even start reading the TRM, E01 implies. He states: "*I could map most points (elements) to some initiatives within the bank. But many quantum things have been put on hold because management has other priorities (shorter terms) and quantum is mainly seen as 'far away'."* What this means is that E01 is convinced that his organization is able to reach targets organizationally in theory, but that due to a lack of management priority this will not be executed at the moment. This cannot be translated into a tangible element that can be implemented into the TRM, because it is more a matter of convincing decision-makers to even consider using the TRM in the first place. This is outside of the TRM's scope, but will be considered when drawing up recommendations. E02 shares a similar notion, but pins the 'call to action' more on external sources such as NVB, DNB, and consultants, rather than his organization's own management. In order to consider this, as well as E01's concerns, the *Management Priority* element will be depicted in the TRM as the starting point of the roadmap and will be made to appear more critical. Lastly, E04 mentioned that in terms of risk appetite, banks often do not look further ahead than 3 years. Since the timeline stops being explicit after 2024, this may decrease the urgency for the banks. E04 thus suggested to add in

an estimate of how long it will take to complete the PQC-transition. An analysis on the duration of completing certain steps within the TRM has not been carried out in this research, so an estimate would be based on prior cryptographic transitions in the Dutch banking atmosphere. E04 mentioned the SHA-1 to SHA-2 update taking 10 years, and that was a "*pretty basic update in comparison to what is expected for the PQC-transition, so one could assume that this will take a minimum of 10 years",* E04 notes. Adding this to the timeline in the roadmap would help to show the urgency

6.2.3 Usability

In terms of suggestions to make the TRM more actionable and usable, the experts gave various different inputs. The management priority issue that E01 identified in the previous section also relates to actionability and usability, E01 argues. He suggests that *"the fact that it is mainly a management issue, should be phrased more strongly"*. How this can be implemented into the TRM is to make the management priority resource appear more critical in its lay-out appearance. Secondly, E02 suggested to involve the entire infrastructure and widen the focus to beyond the payment processes. He states: *"You give a very good overview of the topic of quantum computing, focused on payment traffic. The question is what's involved when you zoom out, not only looking at individual banks but at the entire infrastructure".* This is an intelligent question, which will be taken into account when presenting the suggestions for further research. Within this research, however, it is out of scope to look at every aspect of the entire infrastructure underlying the financial market. Therefore, this suggestion will not be implemented into the TRM, but will be taken into account when discussing the overall validity of the TRM. E03 indicated that *"more details make it more actionable, but this would decrease the readability, so the current level of detail is sufficient".* This positive feedback confirms that the current level of detail makes this TRM actionable and usable. More layers of detail help to avoid mis-interpretations and could add more actionability to the TRM. However, as E03 states, this would also negatively affect the readability, and therefore the usability of the framework. What E03 also notes, is that the fact that there is a timeline present at the top of the diagram makes it somewhat confusing that inputs (arrows) go back (in time). This is indeed not desired, but was in some cases necessary for arrows not to cross each other or cross elements. This is a lay-out / readability issue and does not address the content of the TRM. However, this does relate to usability and therefore needs to be addressed. The most practical way to fix this issue is to list all elements with backward-going input arrows, and change the position or size of these elements. This will not be carried out for the drivers (top of the diagram). Lastly, E04 pointed out that the TRM successfully carries out what it is meant to. Suggestions for actionability and usability that could be added into the TRM were not given by E04, but this expert did suggest to clarify further how phase 1 could already be completed by the banks themselves without the need for externally provided deliverables. Furthermore, E04 noted that it would be helpful to know which banking department is responsible for delivering the various mentioned features, resources, or systems. Since this requires an in-depth analysis to the banks' organizational structures and different departments' roles and responsibilities, this will be considered as a suggestion for further research.

6.3 Final TRM-framework

The first draft TRM has been extended by implementing the recommendations from the expert validation & critique. This has been done by implementing the following amendments:

- Add element: Reprogrammed old software (E01)
    - Phase 3 service/feature/system
    - Gets input from Deep knowledge on NIST PQC algorithms
    - Gets input from NIST Standards for PQC algorithms

- Add element: Risk-based cost analysis (E02)
    - Phase 1 Governance resource / capability
    - Gets input from Management priority
    - Outputs Internal alignment

- Add element: timeline duration estimate: >10 years (E04)
- Management Priority appearing more critical and serving as starting point (E01)

- Changing position or size of elements:
    - Knowledge sharing sessions NVB & DNB
    - Central Cryptographic Inventory
    - Communication with service providers and vendors
    - Guidance documents NVB & DNB. (E03)

- Supporting text: Clarify dependency on service providers (E04)

Implementing these amendments result in the final TRM, which can be seen on the next page in Figure 13. For diagram instructions, see Section 5.8.1. The supporting text suggestion will be added into the conclusion (Chapter 7), as this discusses the TRM in relation to the main research question.

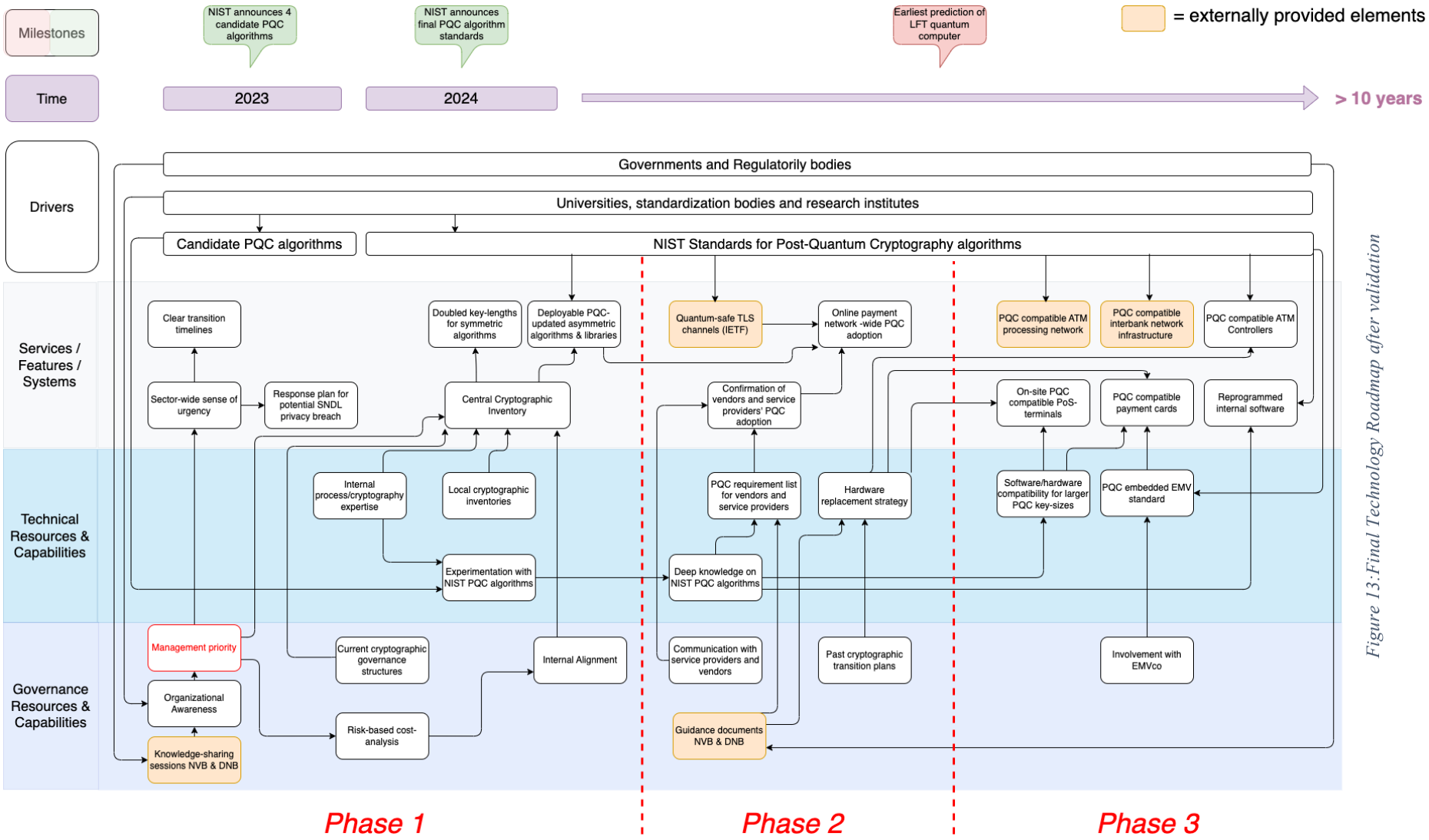


Figure 13: Final Technology Roadmap after validation

7. Conclusion and Recommendations

This section will answer the main research question, based on the sub-questions and the TRM. Hereafter, this section will provide recommendations.

7.1 Conclusion

Using the development of a TRM, by conducting an exploratory analysis and a thematic analysis of semi-structured interviews with high-level security/payment/cryptography specialists from Dutch banks, this research aimed to answer the following research question:

How can the Dutch banking sector ensure the safety and security of its digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology?

This question can be answered by the TRM and the answers to the sub-questions. The sub-questions will be answered, based on insights from the exploratory analysis, as well as the discussion of the results.

SQ1: Which digital infrastructures within banking operations and processes are vulnerable to the quantum threat and should transition towards PQC?

The exploratory analysis identified the critical processes that entail the certain infrastructures that need to transition towards PQC. This research focusses on (1) the online payment process, (2) the physical card transaction process, and (3) the ATM transaction process. The thematic analysis of the semi-structured interviews further identified that this is the order of importance of transitioning these processes, based on the vulnerability of the underlying systems within these processes. These being: data channels through external public networks and service providers relating to payment gateways, payment processors, local store webservers, online merchant webservers, card association networks and PoS-terminals. Less vulnerable infrastructures, due to their primary use of symmetric cryptography, are: ATM networks, internal storage and communication infrastructures, inter-bank data exchange, and ATM controllers. Within these infrastructures/systems there is another level of detail that should be considered when the PQC-transition will be executed, but the high-over prioritization of the aforementioned infrastructures is a sufficient starting point for the Dutch banks to begin their planning and implementation phase of the PQC-transition process.

SQ2: What is the perception of banks towards the expected impact of the quantum threat?

The thematic analysis pointed out that the impact of SNDL is overall perceived as quite limited and the implications mainly relate to customer trust, due to privacy concerns. In contrast, the Y2Q problem is perceived as very severe because of its disruptive effect on the aforementioned digital infrastructures, and thereby on the banks' services. The trust in the financial sector as a whole could be in danger if the threat materializes before the PQC-transition has been completed. However, the severity of these impacts differs per process, resulting in

the ranking of importance between (1) the online payment process, (2) the physical card transaction process, and (3) the ATM transaction process.

SQ3: What is the perception of banks towards their preparedness for the countering the quantum threat?

Dutch banks all seemed to have some form of a strategy in place and the perceptions on their own capabilities to address the quantum threat were mainly positive. Some banks have short-term fallback measures in place, which adds to the overall preparedness. However, due to information-asymmetry between organizational layers and departments, there is a sign of unpreparedness in a wider-sense. Internal alignment through management priority could address this. The lack of management priority at the current time is a worrisome indicator that the banking sector is more unprepared than they perceive.

SQ4: Which capabilities do banks possess that can be utilized for countering the quantum threat?

The capabilities that banks possess are divided into internal capabilities and collaborative capabilities. Deep internal knowledge on cryptography and processes are present within the organization, and experiences with past cryptographic transitions is also perceived as a meaningful capability within the PQC-transition. In terms of collaborative capabilities, Dutch banks have a strong position as a sector when it comes to becoming quantum-safe. Collaborative channels with regulators, other banks, service providers, and tech-companies are in place. While these channels do not serve the purpose of actively addressing the PQC-transition just, the fact that they exist is positive. Within these collaborations there are still major concerns, such as a lack of urgency, organizational unawareness, and uncertain timelines. As can be seen in the TRM, not all the capabilities that support the required features for the PQC-transition are within the banks' own control. These relate to the NVB and the DNB. The collaborative channels that the banks have with these stakeholders do offer opportunities for continuous dialogue and the aim for alignment within the industry, but ultimately the regulatory and standardization resources are outside of the banks' direct control. Therefore, continued collaboration efforts with these external parties will be crucial in ensuring a successful and timely PQC-transition for the Dutch banking sector.

SQ5: Which resources and governance-measures can provide guidance to banks, regarding countering the quantum threat?

The thematic analysis resulted in a relatively long list of resources which banks require in order to successfully transition their organizations towards PQC. These are divided into external and internal resources. Internally, banks would require the development of a central cryptographic inventory, which can only be achieved through internal alignment and deep technical knowledge. The banks are quite positive that the knowledge is already sufficient within their organizations, but internal alignment is something that is currently not present. Through organizational awareness the banks' management may give organization-wide priority to the PQC-transition, which would be necessary to develop this central cryptographic inventory. In terms of governance, the current governance structures involving cryptography and security standards serve as a solid foundation for addressing the PQC-transition challenges. Although these structures may not yet be focused on PQC, these structures can

serve as a valuable asset in guiding the PQC-transition within the organization. Externally, banks require industry-wide standards for PQC algorithms, payment cards, and interbank communications, as well as secure TLS channels. The arrival of these standards is very dependent on other organizations, as the discussion of the results point out. This has further emphasized the importance of collaboration and coordination within the industry. The banks require regulators to push the urge for transitioning towards PQC more, as current governance structures wherein DNB and NVB are involved are not yet fully focused on PQC. Since external governance is mainly perceived as revolving around guidance documents and knowledge sharing sessions from the NVB and DNB, these structures have a critical role to play in igniting the transition towards PQC.

SQ6: What is the perception of banks towards the challenges of countering the quantum threat?

Dutch banks face a worrisome organizational issue, namely: short term versus long term thinking. Due to the uncertainty of the timelines associated with the quantum threat and the PQC-transition, banks primarily perceive it as a future problem, which creates a lack of urgency to address the situation. This slows the transition down drastically and postpones the necessary actions that could (and perhaps should) already be taken to start becoming quantum-safe. These actions relate to (among others) overcoming certain technical challenges related to operationally transitioning the payment infrastructure toward PQC. These challenges can be found in the abundance of distributed systems, the logistical and economic problems associated with PoS- and ATM terminals, and legacy systems' / bank cards' incompatibility with the new PQC-algorithms. Updating or replacing these systems involves cooperation with many vendors and external service providers, which banks perceive as a challenge as well.

Main research question

To conclude and answer the main research question, the Dutch banking sector can ensure the safety and security of its digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology, by executing a three-phase transition plan which aims to implement standardized post-quantum cryptography algorithms into online payment networks, PoS-terminals, payment cards, ATMs, interbank network infrastructure, and the banks' internal software. Phase 1 entails the development of a response plan for a potential SNDL privacy breach, as the impact of SNDL is related to customer trust and a response plan may mitigate the risks of a decrease in customer trust. This phase further aims for the development of a central cryptographic inventory, which can be achieved through management priority and internal alignment organizationally, and through bundling local cryptographic inventories and internal process/cryptography expertise, technically. The central cryptographic inventory enables the banks to determine which symmetrical cryptographic algorithms need to be updated with doubled key-lengths to become quantum-safe, and which asymmetric cryptographic algorithms need to be updated to a new standardized PQC-algorithm. The final standardized PQC algorithms will be available by NIST in mid 2024, which means that up until that moment, all prior steps in phase 1 could already be taken, marking 2024 as the desired end of phase 1. With the final standardized PQC algorithms from NIST made available and the specifications for updating certain algorithms in place, Phase 2 can begin.

The availability of quantum-safe TLS channels will be externally provided to the market as soon as the IETF announces the adoption of PQC algorithms in an updated version of TLS. This, in combination with the banks' specifications for deployable PQC-updated asymmetric algorithms, is required in order to accomplish online-payment-network-wide PQC adoption. Moreover, the online payment network is very dependent on vendors and external service providers, which requires banks to draw up a PQC requirement list for these parties, which they should adhere to. Payment processors, gateways, card associations, SaaS-supporting software, and merchants should embed the banks' required quantum-security standards into their processes. Existing communication channels with these vendors and service providers, experimental knowledge on PQC-algorithms obtained in phase 1, and guidance from NVB and DNB, support this deliverable. Estimating how long this phase will take is difficult, but what is clear is that it should be completed before the first LFT quantum computer, able to break current encryption standards, exists. Because, if not, then Dutch banks will not be able to provide any form of payment services securely which may have catastrophic societal consequences. In Phase 2, the banks should formulate a hardware replacement strategy in preparation for replacing payment-related hardware in the next phase. This can be accomplished with guidance from the NVB and DNB, as well as with the support of past cryptographic transition execution plans.

Phase 3 entails the replacement of all relevant hardware related to the payment processes, by executing the hardware replacement strategy. Moreover, it entails updating all less prioritized software and network infrastructures which rely on symmetric cryptography. Herein on-site PoS-terminals should be replaced with PQC-compatible terminals, ATM controllers should be replaced with PQC-compatible controller devices, and payment cards should be made PQC compatible as well. The compatibility of the payment cards relies on the EMV standard for debit/credit cards, provided by the organization EMVco. Dutch banks have authoritative involvement within this organization and can drive the development of this standard. For this to be achieved, a technical challenge needs to be overcome, which relates to the fact that PQC-algorithms use larger key-sizes than traditional algorithms, which does not currently fit on payment cards and may be incompatible with certain hardware. Deep knowledge on PQC algorithms obtained in phase 2 should resolve this, which emphasizes the need for continuous experimentation and R&D efforts with standardized PQC algorithms. Lastly, interbank data exchange infrastructure should also be updated to support PQC algorithms, which is externally carried out by SWIFT. The same goes for ATM processing networks. Internal storage and communication infrastructures should be updated or replaced as well, which could be dependent on old software which is often hardcoded. This phase involves collaborations with various external vendors, service providers, and other financial service organizations.

It is important to note that the implementation of PQC is not a one-time event, but rather an ongoing, ever-evolving, and uncertain process. The continuous development of quantum computing technology means that banks must remain vigilant and adaptable to stay ahead of potential threats, and may need to accelerate certain phases within the transition on a relatively short notice. Additionally, the success of this transition relies heavily on organizational awareness, as well as close collaboration between various stakeholders, vendors, service providers, and other financial service organizations. By working together and prioritizing this transition adequately, the Dutch banking sector can keep its digital infrastructures secure.

7.2 Recommendations

Based on the conclusion of this research, recommendations can be given to the Dutch banking sector. The recommendations will relate back to the three phases of the TRM as well as the answers to the sub-questions. The recommendations are meant to address banks in the present time. This means that the recommendations are aimed to be actionable and implementable for the short term, and not merely state all the things that banks must do in the coming years.

7.2.1 Accomplish management priority

A reoccurring theme throughout the findings and conclusions of this research has been the need for management priority. This seems to be highly critical in igniting the PQC-transition, as without it, the required services, features, and systems, necessary for Phase 1 of the TRM, cannot be developed. This research evidently found that banks' management currently has other, more short-term focused, priorities and the threat of quantum is mainly seen as a future problem. Therefore, this research recommends that the Dutch banking sector shifts the focus of management toward addressing the quantum threat and transitioning towards PQC as a top priority, integrating quantum-readiness into the key strategic goals of the bank. To accomplish this, this research found that organizational awareness and knowledge-sharing sessions from NVB and DNB may be effective resources. Organizational awareness can be created through workshops, seminars, and events that are aimed at educating management on the business implications of the quantum threat, as well as presenting them with solutions on addressing this threat. For management it is often deemed important that the benefits of projects or transitions outweigh the costs, corrected for risk. Therefore, it is important that the workshops that aim to create awareness, address these specific management-related concerns, so that management can actually prioritize adequately, instead of merely being enriched with knowledge on yet another tech-trend. The knowledge-sharing sessions that DNB and the NVB host should shift to a more actionable tone, in order to accomplish management priority. It is important that management not only becomes aware through their own organizations, but that they notice that the entire financial sector needs to shift towards prioritizing quantum-readiness. These sessions are currently perceived as meaningful because of the insights into trends that they provide, but if these sessions could become more actionable by presenting the steps that banks should already take, then management could possibly feel the urge to further prioritize the transition towards PQC. Overall, without management priority, banks are not able to allocate resources to execute the first steps that have to be taken to ensure quantum-safety, and therefore must be swiftly achieved.

7.2.2 Execute initial risk-free actions

In the uncertain environment that is the financial sector, with the rise of a disruptive technology at an uncertain pace, management may be hesitant to execute certain transition steps that may have a negative pay-off in the (uncertain) future. Indeed, the three phases of the TRM entail elements for which this holds true, for instance, replacing all PoS-terminals too early and then finding out that they are incompatible with the new PQC standardized algorithm is a costly effort. However, there are certain actions that banks can already take that can be seen as risk-free in this regard, and

do not depend on actions from other stakeholders such as NIST. These mainly relate to phase 1 of the transition. These actions are listed below and are briefly discussed:

1. **Developing the SNDL privacy breach response plan**

Developing a response plan for a potential SNDL privacy breach can help mitigate the future risks associated with customer trust and privacy concerns. This plan should entail clear steps and protocols that should be followed in the case of a future SNDL breach. These steps should include communication strategies to inform customers and stakeholders about the breach's impact on their data and privacy, as well as actions that the banks are taking to address the breach. If in the future a malicious hacker publishes that he/she has decrypted old, stored, transaction/client data with a quantum computer, then the bank can immediately respond adequately, instead of having to struggle to come up with a plan in the midst of a crisis. Additionally, such a plan may help the bank to further identify potential vulnerabilities in their current systems.

2. **Developing the centralized cryptographic inventory**

This research pointed out that department-specific cryptographic inventories are often in place or in development within the banks. Bundling these inventories and centralizing them into one comprehensive overview of all cryptographic assets used within the organization will provide a solid foundation for planning and implementing the PQC-transition once the standards from NIST are made available. This process requires strong internal communication and alignment between various departments and teams, which can only be achieved through the previously discussed accomplishment of management priority.

3. **Doubling key-lengths for symmetric cryptography algorithms**

Doubling the key-lengths of symmetric algorithms is a relatively low-risk effort which increases the security-level of existing cryptographic systems. This action does not rely on standardized PQC algorithms from NIST (this is the case for asymmetric algorithms) and adds in an additional layer of security. Of course, this is easier said than done, for there are still many systems that need to be updated, which may be a time-consuming effort. However, this is something that banks could already be doing without the need for the quantum threat to be imminent, as better security is always advantageous on the long term.

4. **Developing a hardware replacement strategy**

The development of a hardware strategy has been found to be a necessity in Phase 2 of the transition. However, it is something that can already be developed internally, without having to actually execute anything yet. This replacement strategy should outline the logistical and budgetary requirements for replacing PoS-terminals, payment cards, and ATM controllers, as well as the coordination plan with stakeholders (e.g., geldmaat for ATMs and Albert Heijn for PoS-terminals). By having this strategy already in place, banks can be ready to act swiftly once the need for hardware updates or replacement becomes urgent, thereby minimizing the potential disruption to their operations.

7.2.3 Extend continuous collaborative research to PQC

Of course, risk-free actions also relate to engaging in industry-wide discussions and initiatives to promote addressing the quantum threat, continuous experimentation with PQC algorithms, and strengthening collaborations with external stakeholders, vendors, and service providers. This research has shown that these efforts are critical in getting the PQC-transition underway. With communicative structures already in place with other banks, service providers, tech-companies, and regulators, it is simply a matter of maximizing these existing connections to facilitate the best possible information exchange. Therefore, this research recommends that Dutch banks take a leading role in the continuous collaborative research to PQC within the financial sector. Instead of waiting for the NVB, DNB, or government to publish binding documents, the banks should proactively utilize their existing collaborative structures to share their experiences, and jointly develop strategies for addressing the quantum threat. This will not only further enrich the banks' own knowledge on the latest development in the field of PQC, but will also enable banks to contribute their own insights and experiences with the entire industry, which will benefit the Dutch financial market as a whole. Banks could share their experiences with executing the aforementioned risk-free actions, or present timelines of the transition to manage expectations from the vendors. Also, it is important that banks share their experiences with experimenting with the finalist PQC-algorithms from NIST. Although these finalists are still in development and have not yet been officially standardized, many technical functionalities have already been made public. Banks do already somewhat experiment with these finalists, mostly on the innovation front. However, this research recommends that the banks start testing the performance of these finalists within certain processes and start actively monitoring the performance metrics and identifying strengths and weaknesses of the algorithms. This knowledge is highly relevant to share within the financial industry, as it helps create a more comprehensive understanding of the practical implications and technical challenges associated with the adoption of PQC algorithms.

8. Limitations and Future work

In this section the limitations of this research will be discussed in Section 8.1, after which several directions for future work will be presented in Section 8.2.

8.1 Limitations

As this research entails many different aspects, the limitations will be structured along two different dimensions, being: the scope of this research in relation to the real world, and the development of the technology roadmap through thematic analysis of semi-structured interviews.

8.1.1 Research scope

Firstly, the purpose of this research was to develop a TRM-framework for ensuring the Dutch banking sector's safety and security of its critical digital infrastructures, from the cryptography-related cyber threats posed by quantum computing technology – from not merely a technological perspective, but with a holistic approach, considering the involved socio-technical challenges. This goal has been achieved, but there are several aspects of the problem that were not considered, although they might be relevant to create a holistic overview. Due to the feasibility of this thesis, many aspects of the quantum threat in the Dutch financial industry needed to be demarcated. This resulted in leaving out the following aspects of the problem:

- Besides nationally, the Dutch banks also operate on an EU- and intercontinental-level. The fact that SWIFT facilitates international interbank exchange is not the only relationship outside of the Netherlands that should be considered. This research does not address the implications of the PQC-transition in the international environment and this is not reflected in the TRM.
- This research only considers implementing standardized PQC algorithms as a technical solution to the quantum threat. Although research points out that adopting PQC is indeed critical step that organizations should take to address the quantum threat, this does not mean that other technologies should be ruled out. Quantum-Key Distribution (QKD), for instance, is a technology that relies on quantum-hardware and quantum-principles to achieve secure encryption key distribution between two parties and could also provide security in the quantum-era. Using quantum technology to your advantage and leveraging it to enhance security was not considered in this research. This research considered the threat of quantum computing and addressed this in the manner in which the market, as well as scientific research, is moving.
- This researched analyzed banking services and identified primary services, to be further analyzed. These related to the payment process along three main services: online transaction, physical PoS transactions, and ATM transactions. However, when transitioning towards PQC, it should be noted that banks offer other kinds of transactional services (e.g., loans, mortgages, investment services, corporate payments, person-to-person payments) that have not been included in the TRM and the recommendations. These services make use of software, hardware, and digital channels which are also affected by the PQC-transition. The three payment

processes that were taken into analysis were identified as most critical in terms of disruptiveness in case they should fall. However, these other services, along with the other identified secondary services in Chapter 3, are all relevant to the PQC-transition and should be considered too if the sector starts transitioning.

- Lastly, future banking services might look different than they currently do. Are there even banks in the future? This research considered banking services as they currently exist, but the rise of digital currency and the changing landscape of the financial industry could play a part in the quantum-era too. Concepts such as biometrical payments and decentralized monetary institutions affect the manner in which the PQC-transition should be shaped and are therefore relevant to consider.

Scoping is an important process in writing a thesis and it enabled this research to be feasible and comprehensible. However, these limitations address the problems with the scope related to the real problem of the quantum threat and highlight the distinction between conclusions based on specific scoped research on the one hand, and the real-world situation on the other.

8.1.2 Technology roadmapping through semi-structured interviews

The data on which the conclusions and the TRM were based, was gathered through semi-structured interviews with specific people from banks. A limitation of this is that the participants may not fully represent the banks on all levels. Although the participant requirements are well substantiated and the three profile groups (cryptography, payments, security) are all very relevant to this problem, there could be more profiles for which the quantum threat and PQC-transition is relevant. Secondly, the interviews themselves have limitations that relate to biases that the participants might have expressed. Response bias relates to participants that may have responded inaccurately to questions relating to their organizations' abilities. Participants might overestimate or underestimate their organization's abilities to address the quantum threat based on their own subjective perception of the organization, the employees, or simply personality. Considering the overall positive perceptions of the banks' preparedness for the quantum threat, there might have been some overestimation of abilities. This could also be explained by the fact that the participants do not want to inflict reputational damage upon the company they work for, by stating that they are unprepared for certain developments in the market. This links to the social desirability bias, which entails providing untruthful answers according to expectations set by the social (or in this case industry) environment. For example, the fact that the researcher asks if the bank is already experimenting with the finalist PQC-algorithms form NIST in the first place may result in that the participants thinks that they should be experimenting. Or that other banks are already experimenting! So, by simply stating, '*yes we are indeed experimenting'*, the participant gives a desired answer, positioning his/her company well, without having to prove him- or herself. Thirdly, the participants could have possibly given untruthful answers because of corporate confidentiality. If bank X would already have a very detailed PQC-implementation strategy in place, and bank Y did not, then bank Y could read this thesis and learn about bank X's strategy. This could be perceived as negatively affecting bank X's competitive advantage over bank Y, which is why some participants might have 'held back' in giving a full answer to certain questions.

All these biases may affect the conclusions from the sub-questions and the TRM. However, the TRM itself has limitations too. The TRM is developed based on this researcher's interpretation of the interview responses and this researcher's perception of the importance of certain elements of the PQC-transition. These interpretations and perceptions might be biased or somewhat subjective, which affects the validity of the TRM. Furthermore, the TRM relies on the information available at the time of its construction. This means that the TRM may not cover all relevant developments and trends that have surfaced since the time of construction. This limitation is inherent to roadmaps in general, as they are limited in their adaptability to circumstance changes. Solving this would require continuous updating and revising of the TRM, which was not feasible in this research. Moreover, the TRM provides banks a general overview of the planning and transitioning phase toward PQC in the payment environment, but does not link this to specific detailed actions that should be taken by certain departments within the bank. This might result in the TRM being too broad to implement. Lastly, the TRM itself is quite a complicated and large diagram, containing many different types of lines and objects. This diagram is not easy to understand if you have never had any experience with constructing or analyzing TRMs, or roadmaps in general. Even though the diagram instruction text in Section 5.8.1 is sufficient for academics to understand how the TRM should be read, it should be noted that in practice (e.g., in decision-making processes) the diagram itself would be most effective if it were completely self-explanatory.

8.2 Future work

Suggestions for further research within this topic can be easily derived from the limitations section, as this points out where the flaws of this research are, and future work could address these flaws. To present the suggestions without becoming too repetitive on the limitations, the suggestions for future work have been summarized in bullet points below:

- Further validate and update the TRM by presenting it to representatives from DNB, NVB, and NIST, to obtain an even broader and more detailed roadmap.
- Extend the TRM by linking the elements to specific organizational action points that are clustered per company department. This would make the TRM easier to implement by the banks.
- Conduct a cost-analysis on the identified processes within the PQC-transition to estimate the cost of the transition.
- Develop a TRM for the PQC-transition in other sectors than the banking sector
- Develop a TRM for the PQC-transition for the international banking sector
- Develop a TRM for the PQC-transition within the banking sector, considering other (secondary) processes besides payments as well.
- Develop system dynamic models in software tool Vensim to simulate processes and decisions within the PQC-transition, to estimate the duration of the transition and identify critical decisions.
- Conduct an extensive literature review and scenario analysis to the development of quantum computing technology, to estimate probabilities of the existence of an LFT quantum computer in the coming years.
- Conduct an exploratory research to the development of other quantum-security related technologies, such as QKD, and analyze the developments and characteristics per technology for a comparative analysis.

9. Reflection on Contribution

This final section of the thesis will reflect on this research's academic contribution and the societal relevance. It will do so by firstly describing the impact this research may have on society, and secondly, by presenting in which academic fields and disciplines this research could be influential, and in which areas it fails to be.

9.1 Societal Relevance

If the PQC-transition has not successfully taken place before Y2Q occurs, an environment will be created wherein malicious cybercriminals may exploit quantum computing's disruptive characteristics to target society's critical infrastructures, such as the payment infrastructure. If the ±14 million payments per day would be facilitated by unsafe digital infrastructures, this would have devastating impacts on lives of ordinary people in terms of safety and economic well-being. This research has addressed this by providing practical guidance and recommendations, regarding the ongoing efforts to mitigate the risks associated with quantum computing technology, ensuring the continued stability and integrity of the Dutch banking sector. This research has provided an evidence-based comprehensive overview with which management of banks can plan and execute the transition towards quantum-safety in their payment infrastructure. As the recommendations may drive decision-making for one of the most critical sectors in the Netherlands, one could argue that the desired impact on society has been largely achieved. However, realistically, this report will probably not find itself on the desks of board-members from Dutch banks, which is not rare for a Master Thesis. A recently published article by the TNO/CWI titled "The PQC Migration Handbook" (Section 9.3), however, is more likely to be read by board members of Dutch banks. This does not mean that this Thesis is less relevant to society, but rather highlights the need for effective collaboration between academic researchers, policymakers, and industry stakeholders. Since this research was conducted in collaboration with EY, such a structure is in place, and the knowledge from this Thesis thereby has the potential to be effectively communicated towards the financial industry. Besides driving decision-making, this research also aimed to inform, which can be seen as societal impact. The research has done this along two axes, these being, (1) informing the public on the negative implications of an emerging disruptive technology (Quantum Computing) of which public knowledge and interest is currently lacking, and (2) emphasizing the importance of the ongoing development of cybersecurity efforts and cryptography research, by presenting the future vulnerabilities in the current payment infrastructure and current cryptography algorithms. This may encourage research to fields related to cryptography and cybersecurity and shows that security in the digital world is an ever-evolving field that continuously faces new threats, as technological development progresses. With more individuals and organizations becoming aware of this, as well as being informed about the potential risks and challenges posed by quantum computing specifically, they may be more likely to support policies or initiatives that promote the development and implementation of cybersecurity initiatives, such as the PQC-transition efforts. Moreover, the societal relevance of this research extends beyond its direct implications for the banking sector. By shedding light on the potential risks of quantum computing on critical digital infrastructures, it raises broader awareness about the need for proactive measures across various industries to prepare for Y2Q, which may ignite conversations among decision-makers to address challenges that go beyond the individual sectors and affect society as a whole.

9.2 Academic Reflection

Research in the field of PQC has seen an incline in the past years. Other research is often technical in nature, while the PQC transition is a complex problem with many socio-technical and organizational components. This research has addressed this by constructing a complete overview on the requirements needed for Dutch banks to transition their payment infrastructures towards safety and security from the quantum threat to cryptography. This has added a unique contribution to PQC research, as prior research in this field has not yet focused the PQC-transition on Dutch banks specifically, and neither on payment processes specifically. While other research had indeed stated that adopting some form of PQC is absolutely critical in facilitating this safety and security for many types of organizations, such as banks (Joseph et al., 2022; Kong et al., 2022), this Thesis has provided a unique overview of *how* this could be executed, in the form of a TRM. However, it should be noted that this overview has several flaws, as Chapter 8 points out. This means that in terms of academic contribution, it does not add a complete solution for all the transitional challenges, but rather serves as a foundation upon which further research can build and refine. The limitations may restrict the immediate applicability of the TRM and call for further research to further extend, refine, and validate the proposed TRM and the associated three-phase transition plan. Furthermore, this research showed that the impact of SNDL is much lower than described in academic literature. The results from the thematic analysis have shown that the impact of SNDL is overall perceived as quite limited and that the implications mainly relate to customer trust, due to privacy concerns. This contradicts various earlier statements in Chapter 1 & 2, in which the severity and urgency of SNDL had been emphasized. What this means is that the importance of SNDL may have been overstated in previous literature, due to theoretical assumptions, instead of industry-expertise-based insights.

The Thesis has contributed an evidence-based overview, based on industry expertise, on what Dutch banks would require for them to transition their critical payment infrastructure to security from the quantum threat to cryptography, with a holistic perspective. What this means is that the research has interdisciplinary implications. “What banks would require” has not been obtained by simply analyzing which technical components are required for the transition, and neither by merely analyzing which governance structures could contribute. On the contrary, this research has integrated these different disciplines by drawing connections between them, which encouraged a more comprehensive understanding of the problem and may lower barriers for decision-making. By considering multiple disciplinary perspectives during the research, the Thesis also promotes the use of a holistic approach to problem-solving and knowledge creation.

Furthermore, this research also has academic value to the field of developing Technology Roadmaps. The approach used to develop the TRM relied on a combination of exploratory research and semi-structured interviews. The thesis gives insights into the advantages and disadvantages of using this method to develop a TRM. A main advantage was that the combination of exploratory research and semi-structured interviews allowed for the collection of scientifically-based and industry-based qualitative data, leading to a very practical roadmap, based on which recommendations could quite easily be presented. However, the disadvantages of this approach include potential bias in the data collected, as it relies heavily on the subjective experiences and opinions of the interviewees (Section 8.1.2). Additionally, the

reliance on qualitative data may limit the generalizability of the findings, as they are specific to the Dutch banking sector, focused on payment processes, and therefore may not be directly applicable to other contexts or industries. Lastly, the TRM displays an absence of a discussion on the potential drawbacks or challenges in implementing PQC and actually executing the transition plan. While the TRM emphasizes the importance of transitioning to PQC, it does not provide an in-depth analysis of the potential challenges, costs, and trade-offs involved in implementation. For instance, the technical resource *Software/hardware compatibility for larger PQC key-sizes,* critical for enabling services/features as *On-site PQC compatible PoS-terminals* and *PQC compatible payment cards,* is merely a resource identified to be necessary in the broad sense of the transition. Meaning that the TRM does not specify how hardware or software can actually become compatible for larger PQC key-sizes, technically speaking. This is often the case in the TRM, which implicates that from an academic perspective it can be concluded that the technical implementation details have been structurally underrepresented in the TRM.

Overall, this Thesis offers a valuable starting point for understanding the complexities of transitioning Dutch banks' payment infrastructures towards PQC. The insights enable Dutch banks to actually start transitioning and it enables academics to further specify. By combining interdisciplinary perspectives and employing a holistic approach, it contributes to the field of PQC, cryptography in payments, the Dutch banking landscape, and the development of Technology Roadmaps. While certain limitations exist, the insights provided serve as a foundation for further academic and practical exploration, facilitating continued refinement and enhancement of the proposed TRM and the associated transition plan.

9.3 Reflection on similar publication

In cybersecurity's rapidly evolving academic landscape, the simultaneous emergence of research studies on similar topics is not uncommon. Ever since this research was initiated in November 2022, other academics have obviously conducted research to PQC as well. Several publications have emerged that address various aspects of PQC, and these may also have implications for the Dutch banking sector. It is impossible to consider all these simultaneously published articles, but one particular article will be reflected on due to its relevance to the PQC transition in the Dutch market. The TNO, CWI, and AIVD published an article titled "The PQC Migration Handbook" (2023). This article (hereafter referred to as 'the TNO report') emerged two weeks before this Thesis was completed and will be briefly discussed.

The TNO report provides comprehensive general guidelines for transitioning towards PQC, addressed to all types of organizations and sectors. Therefore, its focus is more general than this Thesis. However, certain overlaps in recommendations can be found, and since these have been drawn up independently from one another, this might strengthen the validity of these recommendation. Firstly, both the TNO report and this Thesis recognize the importance of PQC algorithms/libraries in mitigating the threat of quantum computers on cryptography, as both papers emphasize the need for organizations to start preparing for the quantum threat as soon as possible. Moreover, both papers recommend organizations to develop and maintain a cryptographic inventory. This Thesis found that banks are already taking steps into this direction and therefore emphasize the need for developing *central* inventories. Furthermore, the

TNO report similarly emphasizes the importance of organizational awareness and collaboration with stakeholders in addressing the quantum threat, but also mention 'cryptographic agility' as a key recommendation. The TNO report defines this as: "*allowing organizations to quickly modify or replace the deployed cryptographic primitives without significantly disrupting the processes in an organization"* (TNO et al., 2023). This Thesis, however, only mentions 'cryptographic agility' when presenting results obtained from P10 and does not further investigate it. Reflecting on this Thesis with this in mind, it could be valuable to further explore the concept of 'cryptographic agility' in the context of the Dutch banking sector. Investigating how Dutch banks can achieve and maintain cryptographic agility in their payment operations could provide additional insights and recommendations for decision-makers, further complementing and strengthening the findings of this Thesis.

Furthermore, the TNO report presents 3 phases to the PQC transition, namely: Diagnosis, Planning, and Execution. The Diagnosis phase relates to the TRM's Phase 1 in terms of assessing current organizational situations and making an inventory of cryptographic protocols. The Diagnosis phase also focusses on identifying the main vulnerabilities, which has already been done in the TRM. The TRM already considers the main vulnerabilities in the payment infrastructure and focusses the roadmap specifically on those processes. The Planning phase from the TNO report involves strategic planning and decision-making, similar to the TRM's Phase 2. However, TNO's Planning phase mainly focusses on deciding on mitigation strategies and the timing of the migration process, while TRM's Phase 2 already looks further ahead, focusing on adopting PQC algorithms in online payment networks and coordinating with external vendors. Lastly, the TNO's Execution phase compares to the TRM's Phase 3 in terms of actual execution of the transition plan. TNO's Execution phase provides strategies and considerations for migrating cryptography, also focused on technical requirement and meaningful insights into several cryptographic protocols. On the other hand, the TRM's Phase 3 focusses on updating hardware, software, and network infrastructures specifically related to payment processes and ensuring compatibility with PQC algorithms, but does not go into great depths on the technical ins and outs. Thus, both approaches have a similar structure, but because this Thesis has a more specific focus, the TRM's transition phases reflect a more tailored approach for the banking sector. Moreover, the TRM is already further ahead than TNO's migration plan, in terms of time in the transitional phases. What is meant by this, is that the TNO Diagnosis phase has already been completed in this Thesis, for a specific sector, on specific sub-processes, making the TRM's starting point later in time than the TNO phases. Therefore, this Thesis may serve the TNO report as a valuable insight on the practicalities of executing their Diagnosis phase, and tailoring the rest of a roadmap specifically based on that.

Although the TNO report and this Thesis differ in focus and depth of technical details, the alignment of their proposed transition phases illustrates the importance of a structured approach to PQC adoption. The similarities between the two approaches in terms of recommendations and transition phases indicate that the findings and conclusions drawn in this Thesis are in line with the current state of research, thus strengthening the validity.

References

Allen, F., & Carletti, E. (2008). *The Roles of Banks in Financial Systems **.

Almeida, R., Pereira, R., & Mira Da Silva, M. (2013). IT governance mechanisms: A literature review. *Lecture Notes in Business Information Processing*, *143 LNBIP*, 186–199. https://doi.org/10.1007/978-3-642-36356-6_14/COVER

Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security . *International Journal of Scientific and Research Publications*, *9*(3), 576. https://doi.org/10.29322/IJSRP.9.03.2019.p8779

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., … Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, *574*(7779). https://doi.org/10.1038/s41586-019-1666-5

Barney, J., Wright, M., & David J. Ketchen, Jr. (2016). The resource-based view of the firm: Ten years after 1991. *Https://Doi-Org.Tudelft.Idm.Oclc.Org/10.1177/014920630102700601*, *27*(6), 625–641. https://doi.org/10.1177/014920630102700601

Berger, A. N., Molyneux, P., & Wilson, J. O. S. (2012). The Oxford Handbook of Banking. *The Oxford Handbook of Banking*, 1–1040. https://doi.org/10.1093/OXFORDHB/9780199640935.001.0001

Bharosa, N., van Wijk, R., de Winne, N., & Janssen, M. (2015). Challenging the Chain: Governing the automated exchange and processing of business information. In *Challenging the Chain: Governing the Automated Exchange and Processing of Business Information*. https://doi.org/10.3233/978-1-61499-497-8-i

BNR. (2019, January 31). Nederlanders wisselen vaker van bank . *BNR Nieuwsradio*. https://www.bnr.nl/nieuws/financieel/10368391/nederlanders-wisselen-vaker-van-bank

Bong, D. (2022, November 15). Symposium Post-Quantum Cryptography - Episode IV. *Keynote 4: Dieter Bong (Utimaco)*.

Bouma, J. J., Jeucken, M., & Klinkers, L. (2017). The Changing Environment of Banks*. In *Sustainable Banking: The Greening of Finance* (1st edition, pp. 12–15). Taylor and Francis. https://doi.org/10.4324/9781351282406

Carlson, A. H., & Sharkey, K. (2022). *Quantum Security Alliance (QSA) NIST Quantum Proof Algorithm Analysis Use of a Venona Style Attack to Determine Block Size, Language, and Attacking Ciphers View project Equivalence of Product Ciphers to Substitution Ciphers, and their Security Implications View project*. https://www.researchgate.net/publication/363611137

Carvalho, M. M., Fleury, A., & Lopes, A. P. (2013). An overview of the literature on technology roadmapping (TRM): Contributions and trends. *Technological Forecasting and Social Change*, *80*(7), 1418–1437. https://doi.org/10.1016/J.TECHFORE.2012.11.008

Castryck, W., & Decru, T. (2022). An efficient key recovery attack on SIDH (preliminary version). *Cryptology EPrint Archive*.

CBS. (2019, February 26). *Minder verhuizingen in 2018*. Centraal Bureau Statistiek. https://www.cbs.nl/nl-nl/nieuws/2019/09/minder-verhuizingen-in-2018

Clarke, V., Braun, V., & Hayfield, N. (2015). Thematic Analysis. In *Qualitative Psychology: A Practical Guide to Research Methods* (pp. 222–248). https://books.google.nl/books?hl=en&lr=&id=lv0aCAAAQBAJ&oi=fnd&pg=PA222&dq=thematic+analysis&ots=eOMJeshmTA&sig=w-T-fDnv511itcOjuAPYIgVqMFo&redir_esc=y#v=onepage&q=thematic%20analysis&f=false

Collaço, N., Wagland, R., Alexis, O., Gavin, A., Glaser, A., & Watson, E. K. (2021). Using the Framework Method for the Analysis of Qualitative Dyadic Data in Health Research. *Qualitative Health Research*, *31*(8), 1555. https://doi.org/10.1177/10497323211011599

Cramer, R., Fehr, S., van Heesch, M., Stevens, M., & Veugen, T. (2022, November 15). Symposium Post-Quantum Cryptography - Episode IV. *Act Now, Not Later: "The Maiden Voyage."*

Csenkey, K., & Bindel, N. (2022). *Post-Quantum Cryptographic Assemblages and the Governance of the Quantum Threat*.

Daim, T. U., Yoon, B. S., Lindenberg, J., Grizzi, R., Estep, J., & Oliver, T. (2018a). Strategic roadmapping of robotics technologies for the power industry: A multicriteria technology assessment. *Technological Forecasting and Social Change*, *131*, 49–66. https://doi.org/10.1016/J.TECHFORE.2017.06.006

Daim, T. U., Yoon, B. S., Lindenberg, J., Grizzi, R., Estep, J., & Oliver, T. (2018b). Strategic roadmapping of robotics technologies for the power industry: A multicriteria technology assessment. *Technological Forecasting and Social Change*, *131*, 49–66. https://doi.org/10.1016/J.TECHFORE.2017.06.006

Das, K., & Sadhu, A. (2022). *Challenges and Trends on Post-Quantum Cryptography*. 271–293. https://doi.org/10.1007/978-981-19-1585-7_12

Dasso, A., Funes, A., Riesco, D., & Montejano, G. (2020). *Computing Power, Key Length and Cryptanalysis. An Unending Battle?* https://doi.org/10.48550/arxiv.2011.00985

de Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology*, *19*(4). https://doi.org/10.1007/s10676-017-9439-z

Doward, J. (2012, June 30). Banking scandal: how document trail reveals global scam . *The Guardian*. https://www.theguardian.com/business/2012/jun/30/banking-scandal-barclays-lawsuits-libor

Dubrawsky, I. (2010). Public Key Infrastructure. *Eleventh Hour Security+*, 153–165. https://doi.org/10.1016/B978-1-59749-427-4.00011-3

Ducas, L. (2022, November 15). Symposium Post-Quantum Cryptography - Episode IV. *(CWI Cryptology Group): Dilithium and Kyber*.

Easttom, W. (2021). Modern Cryptography. *Modern Cryptography*. https://doi.org/10.1007/978-3-030-63115-4

Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J., & Bots, P. (2010). Policy Analysis of Multi-Actor Systems. In *Eleven International Publishing*.

Federal Trade Commission. (2019). *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* . https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach

Forbes Technology Council. (2022, October 17). *Warning: This Product Contains Cyber Bugs*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/10/17/warning-this-product-contains-cyber-bugs/?sh=3d1a185e6d1b

Galazova, S. S., & Magomaeva, L. R. (2019). The transformation of traditional banking activity in digital. *International Journal of Economics and Business Administration*, *7*. https://doi.org/10.35808/ijeba/369

Garcia, M. L., & Bray, O. H. (1997). *Fundamentals of technology roadmapping*. https://doi.org/10.2172/471364

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*. https://doi.org/10.22331/Q-2021-04-15-433

Grimes, R. A. (2020). Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks ... - Roger A. Grimes - Google Books. In *John Wiley & Sons, Inc.* https://books.google.de/books?hl=en&lr=&id=-4uzDwAAQBAJ&oi=fnd&pg=PR21&dq=Grimes+cryptography&ots=lD8Lted0OK&sig=_nlMH1Q2VeYEfB-iUXG3e-ZhMyI&redir_esc=y#v=onepage&q=Grimes%20cryptography&f=false

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Annual ACM Symposium on Theory of Computing*, *Part F129452*. https://doi.org/10.1145/237814.237866

Hülsing, A. (2022, November 15). Symposium Post-Quantum Cryptography - Episode IV. *(TU/e): SPHINCS+*.

Hunt, R. (2001). Technological infrastructure for PKI and digital certification. *Computer Communications*, *24*(14). https://doi.org/10.1016/S0140-3664(01)00293-6

IBM. (2021). *Quantum Decade*. https://www.ibm.com/quantum

Institute for Business Value, I. (2019). *Expert Insights Exploring quantum computing use cases for financial services*. https://www.linkedin.com/in/

Jaques, S., Naehrig, M., Roetteler, M., & Virdia, F. (2020). Implementing Grover Oracles for Quantum Key Search on AES and LowMC. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12106 LNCS*, 280–310. https://doi.org/10.1007/978-3-030-45724-2_10/TABLES/13

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature 2022 605:7909*, *605*(7909), 237–243. https://doi.org/10.1038/S41586-022-04623-2

Kabanov, I. S., Yunusov, R. R., Kurochkin, Y. v., & Fedorov, A. K. (2018). Practical cryptographic strategies in the post-quantum era. *AIP Conference Proceedings*, *1936*. https://doi.org/10.1063/1.5025459

Kar, A. K., & Dey, S. (2014). Cryptography in the Banking Industry. *Researchergate*, *1*(1).

Kemmerich, T., Agrawal, V., & Momsen, C. (2015). Secure migration to the cloud—In and out. *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*, 205–230. https://doi.org/10.1016/B978-0-12-801595-7.00010-0

Kerr, G. (2018). Cybersecurity in Banking and Payments in the United Kingdom. In *The VISIO JOURNAL*. researchgate.net. https://www.researchgate.net/profile/Tanja-Porcnik/publication/330194322_Future_of_Europe_Security_and_Privacy_in_Cyberspace/links/5c3334ac299bf12be3b4cdcf/Future-of-Europe-Security-and-Privacy-in-Cyberspace.pdf#page=44

Khalifa, S. S. M., & Saadan, K. (2013). *The Formal Design Model of an Automatic Teller Machine (ATM)*. https://doi.org/10.12720/lnit.1.1.56-59

Khanam, M., & Daim, T. U. (2017). A regional technology roadmap to enable the adoption of CO2 heat pump water heater: A case from the Pacific Northwest, USA. *Energy Strategy Reviews*, *18*, 157–174. https://doi.org/10.1016/J.ESR.2017.09.019

Khazieva, N. O., Khaziev, A., & Klyushina, E. (2018). Digital Society: The Experience of the Philosophical Understanding of a Problem. *Journal of History Culture and Art Research*, *7*(4). https://doi.org/10.7596/taksad.v7i4.1856

Knudsen, L. R., & Robshaw, M. J. B. (2011). Brute force attacks. In *Information Security and Cryptography* (Vol. 18). https://doi.org/10.1007/978-3-642-17342-4_5

Kong, I., Janssen, M., & Bharosa, N. (2022). Challenges in the Transition towards a Quantum-safe Government; Challenges in the Transition towards a Quantum-safe Government. *ACM Reference Format*, 11. https://doi.org/10.1145/3543434.3543644

Kostoff, R. N., & Schaller, R. R. (2001). Science and technology roadmaps. *IEEE Transactions on Engineering Management*, *48*(2), 132–143. https://doi.org/10.1109/17.922473

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*, 113–122. https://doi.org/10.1016/J.JISA.2014.09.005

Linn, J. (2000). Trust models and management in public-key infrastructures. *RSA Laboratories*.

Martinis, J., & Boixo, S. (2019). *Quantum Supremacy Using a Programmable Superconducting Processor – Google AI Blog*. https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/IJACSA.2018.090354

McGowran, L. (2022, August 19). Quantum apocalypse: Experts warn of 'store now, decrypt later' hacks. *Silicon Republic - Enterprise*. https://www.siliconrepublic.com/enterprise/quantum-apocalypse-store-now-decrypt-later-encryption

Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *218 LNCS*. https://doi.org/10.1007/3-540-39799-X_31

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security and Privacy*, *16*(5). https://doi.org/10.1109/MSP.2018.3761723

Muhammad, A., & Ejiyime, A. S. (2017). Analysis of Ransomware, Origin, Threats and Economic Lost on Victims. *Frontiers of Knowledge Journal Series | International Journal of Pure and Applied Sciences*, *1*(1).

Nationaal Cyber Security Centrum. (2022). *Nederlandse Cybersecuritystrategie 2022-2028* . https://www.ncsc.nl/onderwerpen/nederlandse-cybersecurity-strategie/documenten/publicaties/2022/oktober/10/nlcs-2022

National Fraud & Cyber Crime Reporting Centre. (2021). *Bank account fraud | Action Fraud*. https://www.actionfraud.police.uk/a-z-of-fraud/bank-account-fraud

Nederlandse Vereniging van Banken. (2019). *Persoonsgegevens en uw privacy (AVG)*. https://www.nvb.nl/bank-en-data/persoonsgegevens-en-uw-privacy-avg/

NIST. (2016, December 20). *Public-Key Post-Quantum Cryptographic Algorithms: Nominations | CSRC*. https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms

NIST. (2022a). *Post-Quantum Cryptography | CSRC*. https://csrc.nist.gov/Projects/post-quantum-cryptography

NIST. (2022b, November 1). *Selected Algorithms 2022 | Post-Quantum Cryptography | CSRC*. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022

Pandeya, G. R., Daim, T. U., & Marotzke, A. (2021). *A Strategy Roadmap for Post-quantum Cryptography*. https://doi.org/10.1007/978-3-030-50502-8_4

Pappu, R., & Saranya, G. (2019). Digital Banking Services: Customer Perspectives. *Journal of Emerging Technologies and Innovative Research (JETIR)*, *5*(2).

Prest, T. (2022, November 15). Symposium Post-Quantum Cryptography - Episode IV. *(PQShield): Falcon*.

Priya, N., Nandhini, P., Priya, D. J., & Sharma, N. (2019). Applying cryptography in e-banking security. *International Journal of Innovative Technology and Exploring Engineering*, *8*(9 Special Issue 3), 1159–1162. https://doi.org/10.35940/IJITEE.I3252.0789S319

Probert, D. R., Farrukh, C. J. P., & Phaal, R. (2005). Technology roadmapping—developing a practical approach for linking resources to strategic goals. *Http://Dx.Doi.Org.Tudelft.Idm.Oclc.Org/10.1243/09544050332242011 5*, *217*(9), 1183–1195. https://doi.org/10.1243/095440503322420115

Rabah, K. (2005). Theory and Implementation of Data Encryption Standard: A Review. *Information Technology Journal*, *4*(4), 307–325. https://doi.org/10.3923/itj.2005.307.325

Radonić, M. (2018). *Payment processing in web-based environments-Benchmark of the World's Leading Payment Processors PAYMENT PROCESSING IN WEB BASED ENVIRONMENTS: THE BENCHAMARK OF THE WORDLD'S LEADING PAYMENT PROCESSORS*. https://www.researchgate.net/publication/346107846

Rao, S., Mahto, D., Ali Khan, D., Kumar Rao, S., & Kumar Yadav, D. (2017). The AES-256 Cryptosystem Resists Quantum Attacks. *Article in International Journal of Advanced Computer Research*, *8*(3). www.ijarcs.info

Rawal, B., & Peter, A. (2022). *Quantum-Safe Cryptography and Security*. https://doi.org/10.1007/978-981-16-3412-3_2

Rivest, R. L., Shamir, A., & Adleman, L. (1983). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, *26*(1). https://doi.org/10.1145/357980.358017

Rommer, S., Hedman, P., Olsson, M., Frid, L., Sultana, S., & Mulligan, C. (2020). Architecture extensions and vertical industries. *5G Core Networks*, 431–463. https://doi.org/10.1016/B978-0-08-103009-7.00016-8

Schimpf, S., & Abele, T. (2019). How German Companies apply Roadmapping: Evidence from an Empirical Study. *Journal of Engineering and Technology Management*, *52*, 74–88. https://doi.org/10.1016/J.JENGTECMAN.2017.10.001

Schmidt, J., Drews, P., & Schirmer, I. (2017). *Digitalization of the Banking Industry: A Multiple Stakeholder Analysis Digitalization of the Banking Industry: A Multiple Stakeholder Analysis on Strategic Alignment*.

Schneier, B. (1999). Cryptography: The importance of not being different. *Computer*, *32*(3). https://doi.org/10.1109/2.751335

Seito, T. (2017). *Cryptography and Financial Industry*. 107–115. https://doi.org/10.1007/978-981-10-0962-4_10

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*. https://doi.org/10.1109/SFCS.1994.365700

Shoup, K. (2019). *Quantum Mechanics* (D. McNamara & J. Benson, Eds.; 1st ed.). Cavendish Square Publishing. https://books.google.de/books?hl=en&lr=&id=hvSCDwAAQBAJ&oi=fnd&pg=PP1&dq=quantum+researchers+don%27t+fully+understand+quantum+mechanics&ots=H5sb7xrLkD&sig=vbUXIrdAikFJdckHdnW4KUBEk7g&redir_esc=y#v=onepage&q&f=false

SWIFT. (2023). *Data Protection Policies | Swift*. https://www.swift.com/about-us/legal/compliance/data-protection-policies/frequently-asked-questions

The Frontier Post. (2022, November 2). *'Store now, decrypt later'* . The Frontier Post. https://thefrontierpost.com/store-now-decrypt-later/

The Hill. (2022, November 5). Closing the barn door on 'store now, decrypt later' attacks | The Hill. *The Hill*. https://thehill.com/opinion/cybersecurity/3719786-closing-the-barn-door-on-store-now-decrypt-later-attacks/

TNO, CWI, & AIVD. (2023). *PQC Migration Handbook | TNO*. https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/

Wells, R., Phaal, R., Farrukh, C., & Probert, D. (2004). Technology Roadmapping for A Service Organization. *Http://Dx.Doi.Org.Tudelft.Idm.Oclc.Org/10.1080/08956308.2004.11671619*, *47*(2), 46–51. https://doi.org/10.1080/08956308.2004.11671619

Westerbaan, B. (2022, November 15). Symposium Post-Quantum Cryptography - Episode IV. *Keynote 2: Bas Westerbaan (Cloudflare)*.

Wewege, L., & Thomsett, M. C. (2019). The digital banking revolution: How fintech companies are transforming the retail banking industry through disruptive financial innovation. *The Digital Banking Revolution: How Fintech Companies Are Transforming the Retail Banking Industry Through Disruptive Financial Innovation*, 1–122. https://doi.org/10.1515/9781547401598/MACHINEREADABLECITATION/RIS

White, H. (1968). *Money and Banking Illustrated*. Greenwood Press.

Whiting, L. S. (2008). Semi-structured interviews: guidance for novice researchers. *Nursing Standard (Royal College of Nursing (Great Britain) : 1987)*, *22*(23). https://doi.org/10.7748/ns2008.02.22.23.35.c6420

Willyard, C. H., & McClees, C. W. (1987). Motorola's Technology Roadmap Process. *Https://Doi-Org.Tudelft.Idm.Oclc.Org/10.1080/00345334.1987.11757057*, *30*(5), 13–19. https://doi.org/10.1080/00345334.1987.11757057

World Economic Forum. (2021, May 7). *Is your cybersecurity ready to take the quantum leap? | World Economic Forum*. https://www.weforum.org/agenda/2021/05/cybersecurity-quantum-computing-algorithms/

World Economic Forum. (2022, September 13). *Organizations must protect against quantum threats. Here's how | World Economic Forum*. https://www.weforum.org/agenda/2022/09/organizations-protect-quantum-computing-threat-cybersecurity/

Zamaslo, O., Kovalenko, V., & Lozynska, O. (2021). DIGITAL TRANSFORMATION LEVEL INDICATORS OF BANKS. *Baltic Journal of Economic Studies*, *7*(2). https://doi.org/10.30525/2256-0742/2021-7-2-77-82

Zay Oo, K. (2019). Design and Implementation of Electronic Payment Gateway for Secure Online Payment System the Creative Commons Attribution License (CC BY 4.0). *International Journal of Trend in Scientific Research and Development (IJTSRD) International Journal of Trend in Scientific Research and Development*, *5*, 1329–1334. https://doi.org/10.31142/ijtsrd26635

Appendices

Appendix A

Table 10: A.1:Codes per code group

Code group	Code name	Occurance in interviews
Awareness	Fully aware	11
Capabilities	Collaborative Capabilities	7
	Positive internal capabilities	9
Challenges	Coorperation with many vendors	4
	Future customer needs	1
	Hybrid: In-between phase	1
	Lack of urgency	4
	Memory issues / large key-sizes	5
	Org: perceived as future problem	5
	Public hysteria	1
	Replacing Hardware	6
	Small banks: not worth the costs to transition	2
	Uncertain timelines	6
	Updating internal systems	6
Dependencies	Customer trust	4
	EMVco	3
	Intermeditairy systems	6
	Other banks	6
Governance	Current Crypto Gov	6
	Guidance NVB / DNB	7
	Unaware of governance	2
Impact QT	High impact external communications	1
	High impact online payments	5
	High impact PoS	3
	Limited impact	3
	Limited impact ATM	2
	Severe impact on cryptography	8
	Severe impact on digital signing	2
	Severe impact on privacy	6
Impact SNDL	Limited impact SNDL	9
	Practically no impact, publicly there is impact	1
	Privacy impact SNDL	7

	Trust impact SNDL	3
NIST algorithms	Actively following NIST	4
	Experimenting with NIST	6
	Just interest in NIST	4
Preparedness	Long term preparedness (inventory)	4
	Long term preparedness (organizational)	3
	Not short term prepared (sym)	1
	Short term prepared (symmetric)	4
	Unprepared in wider sense	3
Req. Resources	Alignment/Standards from Industry	8
	Automated PKI deployment	1
	Crypto Inventory	8
	Deep technical knowledge	3
	Internal alignment	2
	Internal risk assessments	1
	Management Priority	2
	Organizational awareness	8
	Push from regulators	4
	Secure TLS channels	4
	Validation from Universities/Consultancies	1
Strategy	Crypto Inventory	8
	Follow others and stay transparant	1
	NIST algorithms	7
	Not roll out already	2
	Plan	2
	Sector Cooperation	4
	Unclear strategy	2

Appendix B

Table 11: B.1: Thematic findings on impact and associated TRM element

Category	Finding	TRM-element	Clarification
Impact	Privacy impact SNDL	Response plan for potential SNDL privacy breach	As respondents indicated that the impact of SNDL is mainly related to customer privacy, a response plan should be drawn up so that there is transparency towards the customer and trust-issues can be avoided
	Severe impact Y2Q on online payments	PQC requirement list for vendors and service providers	The respondents indicated that the impact of Y2Q on online payments is severe. The payment process entails many vendors and service providers for which banks do not directly make decisions.
	Severe impact Y2Q on PoS	On-site PQC compatible PoS-terminals	To mitigate the risks of the severe impact of Y2Q on PoS-terminals, new PQC-compatible PoS-terminals should be in place on the various sale points throughout the Netherlands
	Limited impact on ATMs	PQC compatible ATM Controllers	In order to ensure security of ATM terminals, ATM controllers should be replaced by PQC-compatible ones. Since the impact was perceived as limited, this could be carried out in a later stage than that of the PoS-terminals and online payment network
		PQC compatible ATM processing network	In order to ensure security of ATM terminals, the ATM network should be updated to entail PQC algorithms

Table 12: B.2: Thematic findings on strategy and associated TRM element

Category	Finding	TRM-element	Clarification
Strategy	Experimenting with NIST algorithms	Experimentation with NIST PQC algorithms	As particpants indicated this as being a key strategy, this is implemented as a technical resource in the TRM
	Developing a cryptographic inventory	Local cryptographic inventories	As particpants indicated this as being a key strategy in place, but no yet centralized, this is implemented as a technical resource in the TRM
	Sector cooperation	All governance resources	As sector cooperation is perceived as a key strategy, governance resources in the TRM have an important role. See governance and collaborative capabilities for further explanation

Table 13: B.3: Thematic findings on challenges and associated TRM element

Category		Finding	TRM-element	Clarification
Challenges	Technical	Updating internal systems	Reprogrammed internal software	In order to ensure that all internal systems are quantum-safe, internal software will need to be reprogrammed and updated. Since this is not cricital in providing payment services, this will not have priority over the payment-related systems.
		Replacing ATM hardware	PQC compatible ATM Controllers	In order to ensure security of ATM terminals, ATM controllers should be replaced by PQC-compatible ones. Since the impact was perceived as limited, this could be carried out in a later stage than that of the PoS-terminals and online payment network
		Replacing PoS hardware	On-site PQC compatible PoS-terminals	To mitigate the risks of the severe impact of Y2Q on PoS-terminals, new PQC-compatible PoS-terminals should be in place on the various sale points throughout the Netherlands
		Replacing payment cards	PQC embedded EMV standard	In order to ensure that secure payment cards can be developed, the EMV standard needs to be revised to be compatible with PQC algorithms
			PQC compatible payment cards	In order to ensure security of payment cards, old payment cards need to be replaced with new PQC-embedded EMV standard cards
		Memory issues / large key-sizes	Software/hardware compatibility for larger PQC key-sizes	In order to address the issue of large key sizes of PQC algorithms, banks need to establish the technical resource of compatibility within software/hardware with larger key-sizes. This can be achieved through deep knowledge on the PQC algorithms
	Organizational	Uncertain timelines	Clear transition timelines	Represented in the TRM as a feature. This could also be represented as resouce, but clear transition timelines do not directly support the development of another feature, and is therefore represented as feature itself
		Perceived as future problem	Sector-wide sense of urgency	The perception of the quantum threat being a future problem and the associated lack of urgency call for a sector wide sense of urgency. Sector wide sense of urgency is an endgoal achieved through management priority and is therefore represented as a feature
		Lack of urgency		
		Cooperation with many vendors	Confirmation of software vendors' PQC adoption	As cooperation with many vendors is an organizational challenge, this can be solved by clearly communicating to the vendors which requirements the banks set in terms of PQC adoption in their services.

Table 14: B.4: Thematic findings on capabilities and associated TRM element

Category		Finding	TRM-element	Clarification
Capabilities	Internal	Past experiences with transitions	Past cryptographic transition plans	Past experiences with transitions can be translated into plans, which can act a a supporting guiding resouce for the replacement of all hardware.
		Broad technical knowledge on payment processes and cryptography	Internal process/cryptography expertise	Broad technical knowledge on payment processes and cryptography acts as a technical resource, which supports the development of a central cryptographic inventory and adds to the continous experimentation with PQC algorithms from NIST
	Collaborative	Communications bank-bank	Guidance documents NVB & DNB & Knowledge-sharing sessions NVB & DNB	Guidance documents NVB & DNB & Knowledge-sharing sessions NVB & DNB were sepcifically mentioned as bank-bank communicatinos. These structures facilitate that banks can share knowledge and experiences. These governance resources facilitate sector-wide and features resources such as awareness, hardware replacement strategy and PQC requirement list
		Communications service providers	Communication with service providers and vendors	Represented as a governance resource
		Communications tech companies	Communication with service providers and vendors	Represented as a governance resource

Table 15: B.5: Thematic findings on resources and associated TRM element

Category		Finding	TRM-element	Clarification
Resources	External	Alignment/Standards from industry	NIST PQC algorithm standards	NIST PQC algorithm standards, being a driver for this transition, is also identified by the participants a the most desired external resource.
			PQC embedded EMV standard	Participants indicate that standards from industry are critical. Besides PQC-algorithms for asymmetric encryption, the EMV standard for payment cards is very much desired and anticipated.
		Push from regulators	Guidance documents NVB & DNB & Knowledge-sharing sessions NVB & DNB	Push from regulators, being a driver in the transition, translate into Guidance documents NVB & DNB & Knowledge-sharing sessions NVB & DNB, as the participants mention
		Secure TLS channels	Quantum-safe TLS channels (IETF)	Represented as a feature, externally provided by the Internet Engineering Task Force. It is critical in providing the online payment network quantum-safe communication channels and is dependent on NIST's PQC-algorithms.
		Validation from Universities/Consultancies	Universities, standardization bodies and research institutes	Recognized by participanta aa a relevant external resource, this is a driver for the PQC transition, which may influence organizational awareness.
	Internal	Organizational awareness	Organizational Awareness	Being a governance resource that influences management priority, this is a critical for igniting the PQC-transition
		Central cryptographic inventory	Central cryptographic inventory	As particpants indicated local inventories as being a key strategy in place, but this is no yet centralized, a centralized cryptogrpahic inventory is critical, the particiapnts mentioned.
		Deep technical knowledge	Internal process/cryptography expertise	Internal process/cryptography expertise is a necessary technical resource to facilitate the development of a central cryptogrpahic inventory and add to continous experimentation with NIST's PQC algorithms
		Management priority	Management priority	Indicated in red due to the expert validitations critique on the criticality of it, management priority is a key resource required to start the entire process of the transition.
		Internal alignment	Internal alignment	Through internal aligment, local inventories can be bundled into a central inventory.

Table 16: B.6: Thematic findings on governance and associated TRM element

Category	Finding	TRM-element	Clarification
Governance	Documents NVB & DNB	Documents NVB & DNB	Guidance documents NVB & DNB are sepcifically mentioned as a relevant governance resource. This structure facilitatse that banks can share knowledge and experiences and facilitatse sector-wide and features resources such hardware replacement strategy and PQC requirement lists
	Knowledge-sharing sessions NVB	Knowledge-sharing sessions NVB	Knowledge-sharing sessions NVB & DNB is sepcifically mentioned as a relevant governance resource. This structure facilitate that banks can share knowledge and experiences and facilitates sector-wide awareness
	Current cryptography governance	Current cryptography governance	Current cryptography governance is a governance resource that facilitates the development of a central cryptographic inventory, as existing structures enable internal communication and oversight of cryptographic processes and systems. Expanding on these structures can help organizations create a comprehensive overview of their cryptographic assets
	Involvement with EMV	Involvement with EMVco	As pariticpants indicated that their organizations are involved with the EMVco and hold a chair, this resource can be utilized to push for a new EMV standard for payment cards

Table 17: B.7: Other TRM elements

Category	TRM-element	Clarification
Other	Doubled key-lengths for symmetric algorithms	Derived from the exploratory analysis, this feature can be realized by firstly mapping the symmetric algorithms out of the central cryptographic inventory and enables certain symmetric algorithms to become quantum-safe
	Deployable PQC-updated asymmetric algorithms	This feature can be realized by firstly mapping the asymmetric algorithms out of the central cryptographic inventory and enables the asymmetric algorithms to become quantum-safe once NIST standards are available
	Online payment network -wide PQC adoption	The end-product required to ensure a secure payment network
	Risk-based cost analysis	Recommended by Expert in the validation stage to facilitate actual internal alignment, by firstly allocating resources based on analyses.

Appendix C

This appendix consists of descriptions of the participants' expertise, relating to their function within the organization they represent. Explicit function titles will not be used, since this potentially harms the anonymity of the participants. All participants are employed at Dutch banks. A total of 4 different banks occurs, in which participants from one profile groups originate from at least 3 different banks.

Table 18: C.1: Participant description

Participant	Profile group	Description
P1	Security Architect	Responsible for implementing, maintaining, and monitoring security measures to protect the bank's digital infrastructure, including payment systems.
P2	Security Architect	Develops the security architecture to ensure the bank's digital infrastructure is secure, including payment systems. Collaborates with various teams to design and implement robust security measures.
P3	Security Architect	Manages the IT team responsible for the maintenance and security of the bank's digital infrastructure. Ensures that security protocols are followed and that the team is up to date with the latest security measures, including those related to payments.
P4	Security Architect	Identifies, assesses, and mitigates cybersecurity risks related to the bank's payment systems. Develops policies, procedures, and controls to minimize the impact of potential security breaches.
P5	Payment Security Specialist	Develops and manages the Identity and Access Management (IAM) architecture for the bank, ensuring secure access to digital infrastructure and payment systems.
P6	Payment Security Specialist	Oversees the development and improvement of payment-related products, ensuring compliance with security standards and regulations. Collaborates with security teams to integrate security measures into payment systems.
P7	Payment Security Specialist	Leads the payment domain, ensuring secure and efficient payment processing. Collaborates with various teams to develop and maintain secure payment systems.
P8	Cryptography Specialist	Advises on cryptographic solutions and manages cryptographic services for the bank. Ensures that encryption and decryption mechanisms for digital infrastructure, including payment systems, are secure and up to date.
P9	Cryptography Specialist	Designs and implements the cryptographic infrastructure of the bank, ensuring secure communication and data protection within digital systems, including payment systems.
P10	Cryptography Specialist	Leads the cryptography team responsible for securing the bank's digital infrastructure, including payment systems. Ensures the implementation of the latest cryptographic techniques and manages the cryptographic lifecycle.

P11	Cryptography Specialist	Provides expertise on cryptographic solutions to protect the bank's digital infrastructure, including payment systems. Ensures the secure implementation and maintenance of cryptographic mechanisms, and identifies potential vulnerabilities.