Navigating Through the Unknowns-Organizational Readiness Assessment Model for Quantum-Safe Transition

Kong, I.; Janssen, M.F.W.H.A.; Bharosa, Nitesh

DOI
10.1007/978-3-031-70274-7_27

Publication date
2024

Document Version
Final published version

Published in
Electronic Government

Citation (APA)
Kong, I., Janssen, M. F. W. H. A., & Bharosa, N. (2024). Navigating Through the Unknowns-Organizational Readiness Assessment Model for Quantum-Safe Transition. In M. Janssen, J. Crompvoets, J. R. Gil-Garcia, H. Lee, I. Lindgren, A. Nikiforova, & G. Viale Pereira (Eds.), *Electronic Government* (Vol. 14841, pp. 438-453). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 14841 LNCS). Springer Nature. https://doi.org/10.1007/978-3-031-70274-7_27

Navigating Through the Unknowns-Organizational Readiness Assessment Model for Quantum-Safe Transition

Ini Kong(✉), Marijn Janssen, and Nitesh Bharosa

Delft University of Technology, 2628BX Delft, The Netherlands
{i.kong,m.f.w.h.a.janssen,n.bharosa}@tudelft.nl

Abstract. When implementing and adopting new technologies, knowing the level of organizational readiness is crucial. By assessing the readiness levels, organizations can focus on areas with low readiness levels and prepare for the change processes. Due to the increasing vulnerabilities presented by the advancement of quantum computing technology, today's widely used cryptographic algorithms and encryption methods need to be modified with quantum-safe (QS) ones. However, organizations currently lack tools to understand the complexity of implementing and adopting QS technology, and there is no readiness assessment model available in the context of QS transition. By including different dimensions that organizations should consider when implementing and adopting QS technology, we develop an organizational readiness assessment model for QS transition. The dimensions used in the model include collaboration, governance, policy & regulation, awareness, QS solution standards, hybrid QS solutions, cryptographic agility strategies and knowledge on QS transition. While the organizational readiness assessment model with different dimensions shows the complexity involved in implementing and adopting QS technology, it acts as a guidance tool for organizations to navigate and prepare for uncertainties surrounding QS transition.

Keywords: Quantum-safe · Transition · Organizational Readiness · Assessment

1 Introduction

Today's widely used cryptographic algorithms and encryption methods (e.g., Rivest-Shamir-Adleman (RSA), Diffie-Hellmann key exchange (DHKE), and Elliptic Curve Cryptography (ECC)) that critical infrastructures depend on for digital communication and information sharing will be broken once powerful enough quantum computers become available [1, 2]. As the topic of quantum threats raises alarming concerns, transitioning to a quantum-safe (QS) future is fueled by an ongoing standardization process of QS solution algorithms using Post Quantum Cryptography (PQC) [3, 4]. Many initiatives are being addressed to support modifying existing infrastructures with QS solutions. In Europe, guideline manuals for QS transition have been published by the German Federal Office for Information Security and the Dutch General Intelligence and Security Service [5–8]. Recently, the Dutch government set up the Quantum Secure Cryptography Empire (QvC-Rijk) to provide better preparatory steps for QS transition [9].

M. Janssen et al. (Eds.): EGOV 2024, LNCS 14841, pp. 438–453, 2024.
https://doi.org/10.1007/978-3-031-70274-7_27

While standardization is expected to be completed in 2024, implementation and adoption challenges of QS algorithms remain challenging. It is uncertain which QS technology will be implemented and adopted in the existing infrastructures, and organizations cannot make decisions on their own due to complex technological interdependencies [10, 11]. Despite uncertainties surrounding the direction of the QS transition, organizations may still be held responsible for becoming quantum-safe. According to the NIS 2 Directive, organizations will need to comply with stricter EU-wide requirements to improve their network security and information systems [7]. It would be inevitable for an organization to modify its existing infrastructures and prepare against quantum threats. When the moment arrives for QS transition, organizations need to be ready to move to QS future with the ecosystem. However, organizations currently lack tools to understand the complexity of implementing and adopting QS technology, and no readiness assessment model is available for QS transition.

The following research questions have been formulated to address these gaps:

RQ 1. *What are the different dimensions in the organizational readiness assessment model for QS transition?*
RQ 2. *What are the different readiness levels that we can expect for QS transition?*

By addressing the above research questions, this paper develops a readiness assessment model and identifies a list of dimensions that can address transition challenges that hinder organizations when implementing and adopting QS technology. The paper is structured as follows: Section 2 presents a background on the concept of readiness assessment and QS transition. Section 3 discusses the research approach and section four provides the readiness assessment model for QS transition and further extends the discussions in Sect. 5. Finally, Sect. 6 concludes with an overview of directions for future research.

2 Background

2.1 Concept of Readiness Assessment

While successful integration with evolving technology provides organizations with opportunities for growth and innovation, modifying existing infrastructures for implementing and adopting new technologies can be a complex task [12, 13]. From interoperability, governance, resources, and management, there is a need to understand various dimensions that make up the core elements in the facilitation of existing systems [14, 15]. By recognizing a state of readiness, organizations are able to check whether or not they have the ability to adopt and utilize new technologies [16, 17]. In doing so, organizations can prepare and navigate their processes in accordance with their readiness levels [18, 19].

The concept of readiness has been embedded in various academic disciplines, including but not limited to education, healthcare, sustainability, management and so on [20–23]. The term readiness is a broad multi-level construct which can be present at the individual, group, department, or organizational level [24]. While some literature discusses readiness on the micro level, which focuses on individuals, other literature focuses on the meso level in groups and the macro level, which examines factors at an organizational level [24, 25]. Although we recognize the combination of different levels of readiness, this paper focuses on a macro level and uses organization as a unit of analysis.

Among practitioners, Technology Readiness Level (TRL), which was introduced by the National Aeronautics and Space Administration (NASA) in the 1970s, is widely used to assess the maturity of technologies (Sadin, Povinelli & Rosen, 1989; Straub, 2015). There are also other types of readiness levels, such as Readiness Level (IRL), Regulatory Readiness Level (RRL) and Market Readiness Level (MRL) [26–29]. While the roots of different readiness levels come from diverse fields, these readiness levels are used alongside the TRL to extend understanding and provide insights into the readiness of new technologies [30].

Moreover, from evaluating the compatibility of the existing systems to managing social aspects of transition (e.g., raising a sense of urgency, communicating with stakeholders and providing necessary skill training and knowledge for employees), there are various dimensions that organizations use to assess the readiness levels [31–35]. However, knowing what needs to be assessed is context-dependent, and there is no consensus regarding its definition, the level of analysis, or the dimensions used to measure readiness levels.

Furthermore, there is a lack of research on organizational readiness in the context of QS transition, and there is no organizational readiness assessment model available. Likewise, what needs to be assessed when implementing and adopting QS technology has not yet been identified. Since the topic of QS transition is new, details of which dimensions need to be included in the organizational readiness assessment need to be examined. By doing so, a readiness assessment model can better guide organizations to address challenges that hinder the implementation and adoption of QS technology and act as a communication instrument to prepare for QS transition.

2.2 Readiness for Quantum-Safe Transition

Due to the computation power of quantum computers, their ability to solve complex problems introduces security threats (e.g., using Shor's algorithms) [36]. This means that the cryptographic algorithms and encryption methods that critical infrastructures depend on for secure digital communication and information sharing can potentially break and no longer be reliable. Even today, *store now decrypt later* attack can occur for data that needs a long-term protection [37, 38]. Although data cannot be decrypted without a quantum computer, data can still be harvested, stored and decrypted once quantum computers become available.

As the topic of quantum-safe (QS) future offers new solution areas to protect against quantum threats, the idea of modifying current cryptographic algorithms and encryption methods in the existing infrastructures with ones that are quantum-safe (QS) remains complex [39, 40]. Due to the increasing dependencies on secure digital communication and information exchange, the technical interdependencies with multiple actors allow the facilitation of the existing infrastructures (e.g., standardization bodies, regulatory bodies, service providers, hardware and software vendors, end users) [41–44].

Moreover, the ongoing standardization process of QS solution algorithms is expected to be completed in 2024 [3, 4]. As the standardizations become ready, the technical solution components of QS cryptographic algorithms may need to be validated through testing. However, at the time of writing, organizations do not know yet which QS solutions will be accepted in software and hardware components and when these new products will become available. Many technical uncertainties signal that the development of QS technology is unknown. For organizations, preparation for QS transition remains difficult without much clarity.

From international laws and national regulations to technical standards and protocols, existing critical infrastructures are highly regulated [45–48]. The recent development of the NIS 2 Directive from its initial EU cybersecurity directive (NIS) introduces stricter EU-wide requirements to improve network security and information systems [49]. The ongoing discussions on the EU Cyber Solidarity Act also aim to strengthen cyber resilience [50]. Since non-compliance may lead to negative repercussions, organizations need to be legally obligated to implement appropriate measures to prepare for potential security threats.

With the development of QS technology occurring in parallel, organizations may still be held responsible for preparing and becoming quantum-safe. However, modifying the existing infrastructure is by no means a simple task. Due to technical interdependencies that are inherent to the existing infrastructures, organizations cannot rush QS transition [51–53]. Without considering interoperability and backward compatibility, any disruptions can result in additional issues in data security and affect the business processes of organizations. **As** organizations are looking for ways to become QS-ready, it is crucial that they assess their readiness levels to navigate the development of QS technology and prepare for QS transition**.**

3 Research Methodology

To develop an organizational readiness assessment model, we used a literature review, expert interviews and a series of workshops. Figure 1 shows the flow diagram of the steps taken to develop the model.

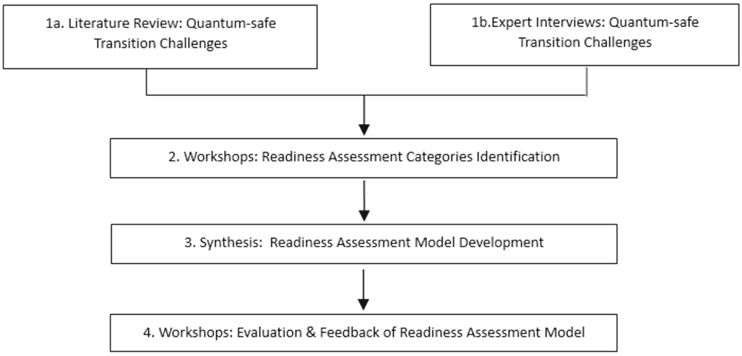
1a. Literature Review: Quantum-safe Transition Challenges
1b.Expert Interviews: Quantum-safe Transition Challenges
2. Workshops: Readiness Assessment Categories Identification
3. Synthesis: Readiness Assessment Model Development
4. Workshops: Evaluation & Feedback of Readiness Assessment Model

Fig. 1. Flow diagram of steps taken to develop the model

3.1 Systematic Literature Review and Expert Interviews: List of Quantum-Safe Transition Challenges

We conducted a Systematic Literature Review (SLR) to identify QS transition challenges that organizations may encounter when modifying their existing infrastructures. The literature was identified using keywords such as "post-quantum cryptography challenge," "quantum-safe cryptography challenge," and "quantum-safe transition challenge" on Google Scholar, Mendeley, ScienceDirect, Scopus, and SpringerLink. From the initial 2266 articles, we chose 154 articles after screening the title and abstract of each paper and excluded 19 duplicate articles. The remaining 135 articles were read, and 93 articles were excluded as irrelevant. As a result, 42 articles were selected for the review.

After evaluating the 42 articles, we identified the list of QS transition challenges. Then, we conducted expert interviews to extend the literature and refine the list of challenges. By validating the results with experts and practitioners, we gain deeper insights into the topic of QS transition and the practical implications of our findings [11]. We used purposive sampling and conducted interviews with 12 industry experts and practitioners in the Netherlands. There were four experts from government agencies, one expert from a bank, two experts from research institutes, one expert from the tax office, two experts from software companies and one expert from a service provider. The respondents were involved in Dutch critical information infrastructure and had prior knowledge of the topic of QS transition.

3.2 Workshops: Dimension Identification and Readiness Assessment Model Development

We conducted Workshop 1 to Workshop 4 (see Table 1) with organizations to identify dimensions that were relevant to QS transition. By extending the discussion at workshops, we gained a common understanding of dimensions that organizations may need to consider when implementing and adopting QS technology [54]. After a series of workshops, the finalized list of dimensions was used to develop the organizational readiness model for QS transition. We conducted Workshop 5 to Workshop 8 (see Table 1) to gather feedback on the organizational readiness assessment model. The participants of the workshops had either a prior technical background or knowledge and experience from industry, government, or academia. The participants provided feedback on the details of the model and discussed whether the list of dimensions in the organizational readiness assessment model for QS transition was relevant. They also examined the usability of the readiness assessment model and checked for any missing information on the topic. The results have been synthesized to further revise the organizational readiness assessment model for QS transition.

Table 1. List of Workshops conducted

# of Workshop	Organizations participated	Date conducted
1	Government Agencies	25/01/2023
2	Government Agencies	14/02/2023
3	Service Providers	14/02/2023
4	Banks	10/05/2023
5	Government Agencies/Service Providers/Software Companies/Research Institutes/Tax Office/Banks	14/06/2023
6	Government Agencies/Service Providers/Software Companies/Research Institutes/Tax Office/Banks	14/06/2023
7	Government Agencies/Service Providers/Software Companies/Research Institutes/Tax Office/Banks	07/11/2023
8	Government Agencies	22/02/2024

4 Results

This section presents the organizational readiness assessment model for QS transition and describes the list of dimensions used in the model. The list of dimensions includes Collaboration, Governance, Policy & Regulation, Awareness, QS solution standards, Hybrid QS solution, Cryptographic Agility Strategies and Knowledge of QS transition. The description of each dimension is explained below, and the organizational readiness assessment model for QS transition is shown in Appendix A.

Collaboration

One of the important dimensions to consider when implementing and adopting QS technology is collaboration. For organizations, the facilitation of critical infrastructures requires multiple actors in the ecosystem, such as regulatory bodies, service providers, software companies, hardware vendors and end users. The underlying technical interdependencies maintain the secure functioning of the existing infrastructures. However, this also means that organizations cannot change the existing infrastructures without affecting other interdependent actors involved in the use and facilitation of the infrastructures. Since QS transition cannot be addressed by one organization, achieving collective action with multiple actors in the ecosystem is crucial.

Governance

Another important dimension to consider when implementing and adopting QS technology is governance. The topic of QS transition is relatively new, and there are no existing guidelines, rules or mechanisms for decision-making and accountability. For organizations, there is a clear institutional void without well-defined roles and responsibilities. Due to many uncertainties regarding the maturity of QS technology, preparation for QS transition remains vague. While some actors may be involved in making external decisions in the ecosystem, other actors may wait for those decisions and follow the lead of frontrunners. Thus, there is a need for a clear governance for organizations to coordinate actions to prepare for QS transition with multiple actors in the ecosystem.

Policy and Regulation

Policy & regulation is another important dimension to consider when implementing and adopting QS technology. Many aspects of QS transition are subject to change due to the ongoing development of QS technology. This also means that if decisions are made in the ecosystem, it may also influence organizations' direction of QS transition. Although having policies and regulations can provide legal mandates and scrutinize uncertainties in standard and compliance requirements, there is currently no policy and regulation available for QS technology. Organizations may need to monitor the regulatory process and identify the requirements for QS transition.

Awareness

Awareness is another important dimension to consider when implementing and adopting QS technology. Since many of the security threats posed by quantum computers are not yet visible (e.g., store now and decrypt later), there is a lack of urgency regarding quantum computing-based threats and risks associated with the technology. Likewise, modifying the cryptographic algorithms in the existing infrastructures is an under-the-hood process where the need for QS transition can go unnoticed by organizations. While many of the decisions regarding QS technology have not yet been crystallized, it is crucial for organizations to raise awareness and stay up-to-date with the development of QS technology so that they become ready for QS transition.

QS Solution Standards

Another important dimension to consider when implementing and adopting QS technology is QS solution standards. Although QS technology with new encryption levels is not yet available, organizations need to conduct technical inventory assessments to identify their vulnerabilities and technical interdependencies. Also, interoperability and backward compatibility are crucial to communicate over networks in the existing infrastructures. Thus, organizations need to evaluate the functionality, performance and resilience of QS solutions. While some actors may be involved in the testing phase of QS solutions to select the right algorithms, other actors may wait on those decisions and technical developments.

Hybrid QS Solution

Hybrid QS solution is another important dimension to consider when implementing and adopting QS technology. The term hybrid provides several definitions, which may involve using either classical cryptographic primitives or quantum-safe cryptographic primitives or employing both of these primitives to secure core processes over networks. Due to the wide implementation of the core processes, there needs to be an assessment of which part of the existing infrastructures requires a hybrid QS solution. While the usability and effectiveness of the solutions are not yet known, organizations need to navigate the development of QS technology and select QS solutions that have been validated in their functionality, performance and resilience.

Cryptographic Agility Strategies
Cryptographic agility strategies is another important dimension to consider when implementing and adopting QS technology. While organizations with defined cryptographic policies and guidelines follow industry-wide accepted cryptographic algorithms and key management, the existing systems are rigid, and changes cannot occur in isolation due to path dependencies. Current cryptographic strategies that organizations have in place do not provide security against quantum threats, and these strategies are not agile enough to adapt to the changing environment of new technologies. Due to many uncertainties surrounding QS transition, it is crucial for organizations to develop cryptographic agility strategies and adopt new cryptographic algorithms, protocols and technologies that become available.

Knowledge on QS Transition
Another important dimension to consider when implementing and adopting QS technology is knowledge on QS transition. There is a lack of knowledge on the scope of QS transition, the impact of quantum threats on existing business processes, and vulnerabilities identified from technical inventory assessments. The selection criteria for QS solutions are not yet known, and organizations do not know which part of the existing infrastructures needs hybrid QS solutions. The lack of knowledge on QS transition creates uncertainties and delays the decisions in the ecosystem. More knowledge sharing and research are needed on the topic of QS transition. Organizations need to stay up-to-date with the development of QS technology and translate insights into their strategic planning to better navigate QS transition.

5 Discussion

This section further discusses several insights regarding the application of the organizational readiness assessment model for QS transition.

5.1 Use of the Model

The model uses the list of dimensions that organizations should consider when implementing and adopting QS technology (mentioned in Sect. 4). For each dimension, the model shows how organization can move towards a higher level of readiness from Level 0 to Level 5. Since organizations may have different readiness levels per dimension, the results of the assessment indicate which of these dimensions the organization may need to improve on. The model is intended to give an overview of what organizations may need to do to navigate the process of QS transition and help communicate the progress of QS transition.

In order to achieve a higher state of readiness, a previous state of readiness needs to be achieved. However, for dimensions such as collaboration, governance and policy & regulations, organizations may not be able to make decisions on their own. Since these dimensions cannot be handled by one organization alone, we assume that external influences may need to be monitored in the ecosystem for organizations to move up to the higher state. It would be crucial for organizations to be up-to-date with the ecosystem in which they are and make decisions with other organizations in the ecosystem.

The limitation of the model is that the list of dimensions used in the model is not completed. This is because there can be other variances of dimensions that could be included to further improve the model. Since the topic of QS transition is now at its early stage, details used in the model are subject to change based on future development. If the standardization of the QS solution is completed, the model will be updated with the changes and development of QS technology. We also assume that organizations have different timelines and resources.

5.2 Demonstration

The readiness assessment model for QS transition is demonstrated to illustrate how the model can be used for organizations. Logius is selected as an example for a demonstration because Logius acts as PA for PKIoverheid (PKIo), managing the digital identities of users for public service provision in the Dutch government. By assessing each dimension, Logius may understand the readiness level for QS transition.

Collaboration: 1.2 Stakeholder Identification

Logius has communication channels in the ecosystem and monitors QS transition. Although there is a unified direction for an ecosystem with a shared vision and common goals for PKIo service provisioning in the public sector, this does not necessarily focus on QS transition. While Logius recognizes the importance of collaboration in the ecosystem, it is not yet clear what a shared vision and common goals are to clarify directions for QS transition. Many questions still need to be asked (e.g. what is our QS transition deadline? What kind of resources do we have? How much time do we have left to go quantum-safe?). Logius is currently monitoring QS transition to negotiate directions for the ecosystem to clarify what direction organizations should proceed to.

Awareness: 2.3 Informed Awareness

Logius has a good overview of stakeholder involvement, and processes are in place to manage changes. However, QS solutions have not yet been tested, and Logius needs to be sure that QS technology is safe and secure. It is also important to clarify what the impact will be on PKIo and what its implications will be for the user base. In 2023, a generic migration manual was published by the Dutch General Intelligence and Security Services. Logius is examining limitations and challenges for the existing infrastructure and monitoring QS transition. Having an awareness of stakeholders is crucial since these stakeholders also need to be aware of situations, and without them, it will only be the point of view of the Logius.

Governance: 3.2 Shared Governance Principle

Logius recognizes the need for governance in the ecosystem and establishes a formal structure. With other organizations in the ecosystem, Logius collaborates with other stakeholders and follows compliance and security requirements for service provisioning in the public sector. There are multiple fixed meetings where they discuss changes with external service providers of PKIo that provide services and products. Logius has a mandate as a PA and is analyzing the implications of QS transition. Although there are no governing bodies, committees or frameworks that define roles, responsibilities and decision-making processes for QS transition, the QvC-Rijk has been recently set up to prepare for QS transition.

Policy and Regulations 4.2 Shared Insights & Discussions

The NIS 2 Directive has been developed to enhance the security of networks and information systems. However, there are many aspects of QS transition that are not yet concrete and are subject to change. If PKIo needs policy changes, this may affect not only hardware but also other parts of the systems. Currently, Logius engages in consultations and participates in various projects to gather insights on QS technologies, guidelines, and informal industry standards. For QS transition, there still needs to be a branch-specific baseline for QS solutions with a set of protocols, security measures and algorithms that are acceptable for organizations to change.

QS Solution Standards: 5.2 Technical Inventory Assessment

In 2022, NIST announced four candidate algorithms for standardization. Logius is conducting cryptographic inventory assessment & impact assessment (e.g. what kind of encryption methods do we use? E.g., RSA or other mechanisms? How quantum resilience are these encryptions?) and is aware of areas that need improvement (e.g., compatibility, security, performance, and scalability etc.). Logius needs to create an environment for tendering and technology implementation since the root structure of PKIo will end in 2028. If the standardization of QS solutions comes later than 2025, the whole root structure may be based on existing technology and standards.

Hybrid QS Solution: 6.2 Technical Inventory Assessment

Logius already has a good overview of their involvement with PKIo (e.g., How are PKI solutions implemented? Where do you use technology? What are their business needs? For Logius, a hybrid QS solution using both classical cryptographic primitives and quantum-safe cryptographic primitives will be issued to secure the core process. All the planning and possibilities are important topics that need to be addressed for Logius. The key features and functionality of hybrid QS solutions still need to be studied. Testing of hybrid QS solution has not yet taken place, and use cases need to be identified.

Cryptographic Agility Strategies: *7.2. Risk-based Approach*

QS transition to secure the existing infrastructure is not just a technical process. It also involves organization, processes, people, finance and other aspects. However, current strategies that organizations have in place do not address quantum safety and security strategies. With defined cryptographic policies and guidelines, industry standards and compliance requirements, Logius has a risk-based approach to security and risk management. Although Logius recognizes the importance of cryptographic agility, the concept still has many aspects to be examined, and it is not yet clear in the organization's security strategy.

Knowledge on QS Transition 8.2 Knowledge of QS solution

Logius is aware of its cryptographic inventory and has knowledge of where hybrid QS solutions may be adopted in its systems. While Logius keeps an eye on the development of QS solutions, Logius finds it crucial to test the limitations and challenges of different

QS solutions. However, there are no test beds available, and it may be too early to already select QS solutions for PKIo. Logius is currently monitoring standardization bodies and other international regulatory bodies to stay-up to date with available QS technology in hardware and software vendors. At the moment, the direction for QS transition remains unclear, and organizations need to extend their scope of knowledge to prepare for QS transition.

While we assume that organizations have different resources and timelines for QS transition, the model provides a conceptual overview with the list of dimensions that organizations should consider when implementing and adopting QS technology. Although dimensions may have different readiness levels, having a low readiness level in one dimension may potentially hinder the readiness in other dimensions. For example, it would be difficult to build knowledge and establish governance for QS transition without recognizing transition efforts and collaboration needed in the ecosystem. While this invites further examination, the model acts as a guidance tool and allows organizations to recognize the complexity involved in implementing and adopting QS technology.

6 Conclusion

With the advancement of quantum computers, it is inevitable that cryptographic algorithms and encryption methods that existing infrastructures depend on will become obsolete. While organizations may still be held responsible for protecting against quantum threats, modifying the cryptographic foundation of existing infrastructures is a complex task that requires preparation. Without it, not only would the implementation and adoption of QS technology be delayed but also the potential security risks in the existing infrastructures would be increased. By developing the first organizational readiness assessment model for QS transition, the paper provides an overview of QS transition and identifies dimensions that are important for organizations to consider.

Moreover, this paper offers the initial exploration in developing an organizational readiness assessment model for QS transition. Depending on the changes that occur in the development of QS technology and how QS transition proceeds in the ecosystem, the readiness assessment model is still subject to change. Since QS transition is at its early stage, there are many uncertainties that may require constant diagnosis and iterations. The identified list of dimensions helps address challenges that hinder organizations when implementing and adopting QS technology. The readiness assessment model not only acts as a guidance tool but also as a communication instrument to discuss and prepare for QS transition.

There are Level 0 to Level 5 in each dimension with a logical sequence on moving from low readiness level to higher level. The list of dimensions includes Collaboration, Governance, Policy & Regulation, Awareness, QS solution standards, Hybrid QS solution, Cryptographic Agility Strategies and Knowledge on QS transition. By fulfilling each state of readiness, the model provides a way for organizations to recognize different areas that need preparation and measure how organizations are progressing toward QS transition. While the model allows organizations to focus on areas that have low readiness levels, it also shows how neglecting one area can also hinder preparation in other areas.

We further conclude this paper with directions for future research. Since the scope of QS transition extends beyond the organizational level, multiple actors in the ecosystem are needed to become quantum-safe. Although many organizations may need to wait on standardization and directions for modifying the existing infrastructures, QS transition cannot be handled by one organization and requires relevant actors and coordinated efforts in the ecosystem. Thus, it is crucial to investigate how changes in the development of QS technology and decisions by relevant actors may affect QS transition. Also, there is much research needed to understand how organizations can better modify cryptographic layers of their existing infrastructures while maintaining business continuities.

In addition, developing the organizational readiness assessment model using a larger data set with more participants could further improve the study. Although we included dimensions such as QS solution standards and hybrid QS solutions, there are different use cases depending on the infrastructure. This may result in different readiness models, and it may also depend on countries and how infrastructures are regulated by policy and sector-specific legislation. While there is much room for improvement, the readiness assessment model presented in this paper can be used as a starting point to explore the applicability and usefulness of an organizational readiness model for QS transition.

Acknowledgments. This publication is part of the HAPKIDO research project with project number NWA.1215.18.002 of the research programme Cybersecurity, which is (partly) financed by the Dutch Research Council (NWO).

Appendix A. Organizational Readiness Assessment Model for QS Transition

	Dimensions							
	1. Collaboration	2. Awareness	3. Governance	4. Policy & Regulation	5. QS solution standards	6. Hybrid QS solution	7. Cryptographic security strategy	8.Knowledge on QS transition
Level 0	**1.0 Disengagement** Organization is disengaged in the ecosystem. Organization is disconnected and not actively involved.	**2.0 Unawareness** Organization lacks awareness on QS transition. Organization is unprepared and has not yet recognized the relevance and benefits of QS solutions.	**3.0 Governance Vacuum** There is a lack of formal governance for transition in the ecosystem. There is no guidelines, rules or mechanisms for decision-making, coordination and accountability.	**4.0 No Formal Policies & Regulations** There is an absence of formal certification process for QS solutions. There is a lack of regulations and policies for QS transition.	**5.0 Limited knowledge of QS solutions** Organization does not have knowledge of key concepts and technology related to QS transition. Organization does not recognize the need for QS technology. .	**6.0 Limited knowledge of QS solutions** Organization does not have knowledge of key concepts and technology related to QS transition. Organization does not recognize the need for QS technology.	**7.0 Reactive & Ad hoc practices** Organization has a reactive approach to security and risk management. Cryptographic algorithms and protocols are implemented on ad hoc basis.	**8.0 Limited Knowledge** Organization has limited knowledge on QS transition. Organization do not know what should be done and what needs to be done. Organization is not aware of quantum threats and benefits of QS technology
Level 1	**1.1 Communication & Monitoring** Organization recognizes the importance of collaboration in the ecosystem. Organization establishes communication channels in the ecosystem and monitors QS transition.	**2.1 Acknowledged awareness** There are emerging discussions on QS transition. Organization recognizes that change is necessary and potential impact of quantum threat on the existing system.	**3.1 Recognition of assessment & planning** Organization recognizes the need for transition governance in the ecosystem. Organization identify a shared objectives of transition.	**4.1 Emerging Insights & Considerations** Organization recognizes the need for some level of policies and regulations.	**5.1 Basic understanding of QS solutions** Organization has a basic understanding of QS transition. However, organization has not yet conducted a technical inventory assessment in the existing system.	**6.1 Basic understanding of QS solutions** Organization has a basic understanding of QS transition. However, organization has not yet conducted a technical inventory assessment in the existing system.	**7.1 Defined Policies & Procedures** Organization has defined cryptographic policies & guidelines outlining acceptable cryptographic algorithms and key management practices. (e.g., basic cryptographic controls based on organizational requirement & industry best practices.)	**8.1 Knowledge of existing infrastructure** Organization has conducted a cryptographic inventory assessment. Organization has knowledge on the existing infrastructure and know areas that are vulnerable and where to implement and adopt QS solutions.
Level 2	**1.2 Stakeholder Identification** Organization identifies potential direction for QS transition. Organization develops a communication plans to shares expectation for QS transition with stakeholders.	**2.2 Growing Awareness** Organization seek information about QS technology. There is a growing awareness of QS technology. However, organization does not understand full scope of QS solutions.	**3.2 Shared Governance Principle** Organization in the ecosystem engage in discussions on shared governance principles. Organization set the foundational values and expectations for QS transition.	**4.2 Shared Insights & Discussions** Organization engages in discussions and shares insights in the ecosystem on QS solution guidelines, and informal industry standards.	**5.2 Technical Inventory Assessment** Organization assesses the existing infrastructure and identify potential areas where QS solutions may be implemented. However, organization does not understand full scope of QS solutions.	**6.2 Technical Inventory Assessment** Organization assesses the existing infrastructure to identify potential areas where hybrid QS solution may be implemented. However, organization does not understand full scope of QS solutions.	**7.2 Risk-based Approach** Organization has a risk-based approach to cryptographic security. Risk assessment are conducted to identify vulnerabilities and threats. The use of cryptographic algorithms is aligned with industry standards & compliance requirements.	**8.2 Knowledge of QS solutions** Organization has knowledge on limitations and challenges of different QS solutions. Organization understand where hybrid QS solution may be implemented and adopted in the existing systems.
Level 3	**1.3 Coordinated efforts** Organization engages with the ecosystem to foster coordination for QS transition. Organization work together to leverage shared vision and collective goals	**2.3 Informed Awareness** Organization looks at different possibilities regarding QS transition. Organization has a deeper understanding of QS technology and areas that need QS technology in the existing system.	**3.3 Governance Structure** Organization establishes a formal structure such as creation of governing committees for QS transition. Organization agrees on roles, responsibilities that facilitates decision-making and QS transition.	**4.3 Gap Analysis & Preparation** Organization identifies policy and regulation gaps on QS transition. Organization evaluates the potential risks and consequences associated with identified gaps in policy and regulations.	**5.3 Testing Specifications & Use Cases** Organization conduct testing of QS solutions. Organization identifies testing scenarios and use-cases of QS solutions. Organization perform interoperability test and validate functionality, performance and resilience.	**6.3 Testing Specifications & Use Cases** Organization conduct testing of hybrid QS solutions. Organization identifies testing scenarios and use-cases of QS solutions. Organization perform interoperability test and validate functionality, performance and resilience.	**7.3 Proactive Approach** Organization takes a proactive approach to cryptographic security. Advanced cryptographic controls are implemented to protect critical data assets. Cryptographic agility is emphasized into the organization's security strategy.	**8.3 Knowledge of selection of QS solutions** Organization has knowledge on selection of different QS solution algorithms. Organization gains understanding and clarifies knowledge needed for implementation and adoption (e.g., roadmap, timeline, goals and resources are defined)
Level 4	**1.4 Collaborative Actions** Organization collaborate in the ecosystem to provide necessary support and resource for QS transition. Organization actively take part in joint projects, initiatives and coordinate efforts to benefit the entire ecosystem.	**2.4 Strategic Awareness** Organization aligns awareness to its strategic goals for QS transition. Organization makes transition plans to achieve a smooth QS transition.	**3.4 Implementation & Enforcement** Established governance structure and principles are put into practice. Organization actively implements and enforces the governance mechanism ensuring compliance, transparency and accountability.	**4.4 Voluntary Guidelines** Voluntary measures and informal guidelines are introduced outlining criteria, procedures and requirements for existing systems to become quantum-safe. These serve as recommendations and are not legally binding. .	**5.4 Piloting & Validation** Organization implement a solution a small scale and conducts pilot deployment of QS solutions. Organization monitor performances, gather feedback on QS solution. Organization collaborates with stakeholders to assess usability and effectiveness.	**6.4 Piloting & Validation** Organization implement a solution a small scale and conducts pilot deployment of hybrid QS solutions. Organization monitor performances, gather feedback on hybrid QS solution. Organization collaborates with stakeholders to assess usability and effectiveness.	**7.4 Continued Enhancement of Cryptographic Measures** Organization improves cryptographic security measures. There is an on-going evaluation and adopting new cryptographic algorithms, protocols and technologies. Cryptographic agility is emphasized into the organization's security strategy.	**8.4 Knowledge of implementation of QS solutions** Organization has strategic planning and implement QS solutions in the existing systems. Organization gains knowledge on implementation and adoption of QS solutions.
Level 5	**1.5 Collaborative Actions Continuous Dialogue** Organization maintain continuous dialogue in the ecosystem. There is ongoing communication, reports feedback, collaboration between leadership to ensure the shared vision and goals are cascaded.	**2.5. Foresighted awareness** Organization looks ahead and stays up-to-date with the latest development of QS technology. Organization is aware of evolving QS environment, and strategically plans for future challenges.	**3.5 Continuous Evaluation & Adaptation** Organization assesses the effectiveness of the governance framework in the ecosystem and make necessary adjustment with evolving needs. Established government undergoes continuous evaluation and adaptation.	**4.5 Mandatory Policy & Regulations** Policy and regulations for QS solutions become mandatory by law. Regulatory bodies introduce legal mandates that require QS solutions for standards, process and compliance requirement that all relevant organizations must adhere to.	**5.5 Scaled deployment** Organization selects QS solutions to implement and adopt in the existing systems. Successful adoption leads to further scaling and integration of QS solutions.	**6.5 Scaled deployment** Organization selects hybrid QS solutions to implement and adopt in the existing systems. Successful adoption leads to further scaling and integration of hybrid QS solutions.	**7.5 Mature & Resilient Cryptographic Security** Organization is highly responsive to cryptographic threats. Agile cryptographic security is a fundamental component of organization's security strategy. Cryptographic agility is scaled across the organization allowing for rapid adaption to emerging cryptographic standards.	**8.5 Knowledge of utilization of QS solutions** Successful adoption leads to further scaling and integration of QS solutions. Organization tracks performance, collect data and gather feedback. Organization shares knowledge and experience with industry best practices.

References

1. del Moral, J.O., et al.: Cybersecurity in Critical Infrastructures: a post-quantum cryptography perspective (2024)
2. Mavroeidis, V., et al.: The impact of quantum computing on present cryptography. Int. J. Adv. Comput. Sci. Appl. (IJACSA), **9**(3) (2018)
3. NIST, Report on Post-Quantum Cryptography, L. Chen, et al., Editors (2016)
4. NIST, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. 2022. p. DF-1.6 %âãÏÓ 5102 0 obj <</Linearized 1/L 781733/O 5105/E 77473/N 102/T 780110/H [897 1293]>> endobj 5119 0 obj <</DecodeParms<</Columns 5/Predictor 12>>/Filter/FlateDecode/ID[<DD696B0DA721BC6F155C55CD1B68CE8B>< 54BC73083A93C34D936B9D263A36AD19>]/Index[5102 175]/Info 5101 0 R/Length 106/Prev 780111/Root 5103 0 R/Size 5277/Type/XRef/W[1 3 1]>>stream hÞbbd‘ “b‘à¨ ‘Œú ’A Ìæ ‘üS@¤ˆd~
5. BSI, Quantum-safe cryptography-fundamentals, current developments and recommendations (2021)
6. Digitale Overheid. Wat is quantumveilige cryptografie? (2023). https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/wat-is-quantumveilige-cryptografie/
7. European Commission. Transition towards Quantum-Resistant Cryptography (2022). https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03
8. TNO, CWI, and AIVD, The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography (2023)
9. Digitale Overheid. Quantumveilige cryptografie: “transitie van een lange adem” (2024). https://www.digitaleoverheid.nl/achtergrondartikelen/quantumveilige-cryptografie-transitie-van-een-lange-adem/
10. Hasan, K.F., et al.: A framework for migrating to post-quantum cryptography: security dependency analysis and case studies. IEEE Access **12**, 23427–23450 (2024)
11. Kong, I., Janssen, M., Bharosa, N.: Realizing quantum-safe information sharing: implementation and adoption challenges and policy recommendations for quantum-safe transitions. Gov. Inf. Q. **41**(1), 101884 (2024)
12. Haber, E., Zarsky, T.: Cybersecurity for infrastructure: a critical analysis. Fla. State Univ. Law Rev. **44**(2), 515 (2017)
13. Janssen, M., et al.: Challenges for adopting and implementing IoT in smart cities. Internet Res. **29**(6), 1589–1616 (2019)
14. de Bruijn, H., Herder, P.M.: System and actor perspectives on sociotechnical systems. IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.Part A: Syst. Hum. **39**(5), 981–992 (2009)
15. Mumford, E.: The story of socio-technical design: reflections on its successes, failures and potential. Inf. Syst. J. **16**(4), 317–342 (2006)
16. Janssen, M., et al.: A framework for analysing blockchain technology adoption: integrating institutional, market and technical factors. Int. J. Inf. Manage. **50**, 302–309 (2020)
17. Uren, V., Edwards, J.S.: Technology readiness and the organizational journey towards AI adoption: an empirical study. Int. J. Inf. Manage. **68**, 102588 (2023)
18. Kiberu, V.M., Mars, M., Scott, R.E.: Development of an evidence-based e-health readiness assessment framework for Uganda. Health Inf. Manage. J. **50**(3), 140–148 (2019)
19. Mittal, S., et al.: A critical review of smart manufacturing & Industry 4.0 maturity models: implications for small and medium-sized enterprises (SMEs). J. Manuf. Syst. **49**, 194–214 (2018)

20. Balasubramanian, S., et al.: A readiness assessment framework for Blockchain adoption: a healthcare case study. Technol. Forecast. Soc. Chang. **165**, 120536 (2021)
21. D'Agostino, A., et al.: Measuring teachers' readiness to use ICT before the COVID-19 pandemic in Italy. Qual. Quant. **57**, 1–27 (2022)
22. Denicolai, S., Zucchella, A., Magnani, G.: Internationalization, digitalization, and sustainability: are SMEs ready? A survey on synergies and substituting effects among growth paths. Technol. Forecast. Soc. Chang. **166**, 120650 (2021)
23. Jansen-Kosterink, S., Broekhuis, M., van Velsen, L.: Time to act mature—gearing eHealth evaluations towards technology readiness levels. DIGITAL HEALTH **8**, 20552076221113396 (2022)
24. Weiner, B.J.: A theory of organizational readiness for change. Implement. Sci. **4**, 67 (2009)
25. Vakola, M.: Multilevel readiness to organizational change: a conceptual approach. J. Chang. Manag. **13**(1), 96–109 (2013)
26. Kobos, P.H., et al.: Timing is everything: a technology transition framework for regulatory and market readiness levels. Technol. Forecast. Soc. Chang. **137**, 211–225 (2018)
27. McGowran, E., Harris, E.: Regulatory readiness level: a tool to enhance early regulatory adoption in academic discovery (2020)
28. Vik, J., et al.: Balanced readiness level assessment (BRLa): a tool for exploring new and emerging technologies. Technol. Forecast. Soc. Change **169**, 120854 (2021)
29. Webster, A., Gardner, J.: Aligning technology and institutional readiness: the adoption of innovation. Technol. Anal. Strateg. Manage. **31**(10), 1229–1241 (2019)
30. Bruno, I., et al.: Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services. In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, pp. 369–380. Association for Computing Machinery: Athens, Greece (2020)
31. Dermott, O., et al.: Motivations, barriers and readiness factors for quality 4.0 implementation: an exploratory study. TQM J. **33**, 1502–1515 (2021)
32. Maganga, D.P., Taifa, I.W.R.: The readiness of manufacturing industries to transit to quality 4.0. Int. J. Qual. Reliab. Manage. **40**(7), 1729–1752 (2023)
33. Miake-Lye, I.M., et al.: Unpacking organizational readiness for change: an updated systematic review and content analysis of assessments. BMC Health Serv. Res. **20**(1), 106 (2020)
34. Shahrasbi, N., Paré, G.: Rethinking the concept of organizational readiness: what can IS researchers learn from the change management field? 2014
35. Yusif, S., Hafeez-Baig, A., Soar, J.: E-Health readiness assessment factors and measuring tools: a systematic review. Int. J. Med. Inform. **107**, 56–64 (2017)
36. Shor, P.W.: Polynomial time algorithms for discrete logarithms and factoring on a quantum computer (1994)
37. Mosca, M.: Cybersecurity in an era with quantum computers: will we be ready? IEEE Secur. Priv. **16**, 38–41 (2018)
38. Mosca, M., Mulholland, J.: A Methodology for Quantum Risk Assessment. Global Risk Institute (2017)
39. AIVD., Bereid je voor op de dreiging van quantum computers (2021)
40. NIST, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, W. Barker, W. Polk, and M. Souppaya, Editors (2021)
41. Christiansen, L.V., Bharosa, N., Janssen, M.: Policy guidelines to facilitate collective action towards quantum-safety. In: Proceedings of the 24th Annual International Conference on Digital Government Research, pp. 108–114 (2023)
42. Lovic, Quantum Key Distribution: Advantages, Challenges and Policy (2020)
43. Tibbetts, J.: Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decision Makers. UC Berkeley: Center for Global Security Research (2019)

44. TNO, Migration to Quantum-safe Cryptography: About Making Decisions on When, What and How to Migrate to a Quantum-safe situation F. Muller and M.P.P. van Heesch, Editors (2020)
45. Lewis, A.M., Travagnin, M.: the impact of quantum technology on the EU's policies part 2: quantum communications from science to policies. European commission (2018)
46. Lewis, A.M., Travagnin, M.: A Secure Quantum Communications Infrastructure for Europe: Technical background for a policy vision. In: JRC Technical Reports. European Commission (2022)
47. Macaulay, T., Henderson, R.: cryptographic agility in practice: emerging user-cases. InfoSec Global (2019)
48. Mashatan, A., Heintzman, D.: The complex path to quantum resistance. Commun. ACM **64**(9), 46–53 (2021)
49. European Commission, Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive) (2023)
50. European Commission, EU Cyber Solidarity Act Factsheet (2024)
51. CCC, Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility. Computing Community Consortium (2019)
52. ISARA, Enabling Quantum-Safe Migration with Crypto-Agile Certificates (2018)
53. Mehrez, H.A.O.O.E.: The crypto-agility properties. In: Proceedings of the 12th International Multi-Conference on Society, Cybernetics and Informatics. Orlando, Florida (2018)
54. Kong, I., Janssen, M., Bharosa, N.: Analyzing Dependencies among Challenges for Quantum-safe Transition. In: EGOV-CeDEM-EPart2023. Corvinus University of Budapest, Hungary (2023)