HAPKIDO

Organizational Readiness Model for Quantum-safe Transition

Ini Kong
Marijn Janssen
Nitesh Bharosa

NWO

Table of Contents

Summary

This report provides an overview of the core concepts on an organizational readiness model for Quantum-safe (QS) transition.

Due to the computation power of quantum computing technology, current Public Key Infrastructure (PKI) will no longer be strong enough to provide secure information sharing and digital communication. This raises the need for quantum-safe (QS) transition where organizations can implement and adopt QS cryptographic algorithms to replace the current cryptographic algorithms that susceptible to quantum threats. As the discussions of QS transition takes place across academia, industry and government, we see that QS transition involves socio-technical challenges that cannot be single-handled by one organization.

The uncertainties of QS technology, and standardization of QS cryptographic algorithms present not only technical challenges, but also organization and ecosystem wide challenges. While NIST is currently working on standardization of QS solution algorithms, it may be insufficient for organizations to start preparing for QS transition. The publication Kong et al. (2024b) reveals that implementation and adoption challenges for QS transition include multiple aspects including complex technological interdependencies, lack of urgency, lack of certified hardware and software and unclear QS direction and governance.

With QS transition challenges being interconnected, a delay in one challenge may lead to delays other challenges. To better address the complex socio-technical challenges of QS transition, the concept of readiness model includes the list of challenges that organization may prioritize when navigating QS transition. While organizations can prepare to tackle QS transition challenges, and the readiness model provides an overview of complex QS transition with uncertainties surrounding QS technologies and how organizations can move towards a QS scenario.

In this report, we introduce the concept of an organizational readiness model for QS transition. By using ISM-MICMAC approach, we gain an understanding of the interrelationship between QS transition challenges and which of these challenges organizations may need to prioritize when preparing for QS transition. We further identified eight dimensions of an organizational readiness model for QS transition which include collaboration, governance, policy & regulation, awareness, QS solution standards, hybrid QS solution, cryptographic agility strategies and knowledge on QS transition (Kong et al., Forthcoming 2024).

1. Introduction

With an on-going standardization process of QS solution algorithms by the National Institute of Standards & Technology (NIST), discussions on the topic of QS transition is taking place (NIST, 2016, 2021, 2022). However, various QS transition challenges signals the complexity of QS transition (Kong et al., 2022). Due to many uncertainties surrounding QS transition, organizations are not yet prepared to implement and adopt QS technology. As organizations are left with unclear transition paths, a delay in one challenge may lead to delays in other challenges (Kong et al., 2023).

We use the concept of organizational readiness model to understand what organization may need to prioritize when preparing for QS transition. Since the topic of QS transition is relatively new, there is no ready-to-use organizational readiness models for QS transition and the existing research on organizational readiness models do not address dimensions that may be relevant for QS transition. By identifying a list of dimensions, we aim to develop an organizational readiness assessment model that may help organizations navigate QS transition (Kong et al., 2023; Kong et al., Forthcoming 2024).

In order to develop an organizational assessment model for QS transition, the following research question has been formulated.

"*What are the different dimensions in the organizational readiness assessment model for QS transition?"*

In this report, we provide an overview of organizational readiness assessment model for QS transition. The report is divided into five sections. Section two presents a brief overview of organizational readiness model and section three discusses methodology used to develop the model. Section four describes a list of QS transition challenges that organizational readiness model is based upon. Section four presents eight dimensions of an organizational readiness assessment model for QS transition. Finally, section five concludes with directions for future research.

We want to highlight that content of this report has been published in several academic papers. (e.g., Kong et al. (2023), Kong et al. (2024b) and Kong et al. (2024a)) and parts of the report also include a forthcoming paper (e.g., Kong et al. (Forthcoming 2024)) that is available in September 2024.

2. Organizational Readiness Model

Section 2 provides an overview of an organizational readiness model and this part of the report is part of the forthcoming paper Kong et al. (Forthcoming 2024).

The term readiness is a broad multi-level construct which can be present at the individual, group, department, or organizational level (Weiner, 2009). 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 (Vakola, 2013; Weiner, 2009). 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) (Kobos et al., 2018; McGowran & Harris, 2020; Vik et al., 2021; Webster & Gardner, 2019). While the roots of different readiness levels come from diverse fields, these readiness levels are used alongside the TRL to provide insights into the readiness of new technologies (Bruno et al., 2020).

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 (Dermott et al., 2021; Maganga & Taifa, 2023; Miake-Lye et al., 2020; Shahrasbi & Paré, 2014; Yusif et al., 2017). 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 has to be further examined. By doing so, a readiness assessment model can better guide organizations to address challenges that hinder the implementation and adoption of QS technology.

3. Methodology Overview

Section 3 provides an overview of methodology used in developing an organizational readiness assessment model for QS transition. Section 3.1 describes ISM-MICMAC approach that was used to developed an organizational readiness assessment model. Section 3.2 further details systemic literature review, semi-structured interviews and workshops conducted in the process of model development.

3.1 ISM-MICMAC Approach

We used integrated Interpretive Structural Modelling (ISM)-Matrice d'Impacts Croisés Multiplication Appliqués à un Classement (MICMAC) approach to examine the contextual relationships among QS transition challenges. The ISM analyzes a set of factors in complex issues and structures them into a comprehensive systemic hierarchical model. Based on matrix theory and graph theory, ISM model enhances group decision regarding elements of a research subject that is generally complex and uncertain (Bashir & Ojiako, 2020).

By involving experts, ISM provides identifying and relating the factors of the issue. It is an interactive process that leads to learning and decision making that shows relationships between various factors. Such identification and association provide information to managers and decision-makers to understand and focus on the core factors and control other factors have a potential effect on the core ones.

However, ISM alone cannot explain the degree of impact that each individual factor. Thus, we integrate the results of ISM with MICMAC analysis which was first developed by Duperrin and Godet (1973). The MICMAC analysis can determine driving power and dependence power of each factor and identify which factor need to be prioritized. In doing so, we use binary relations (0 and 1) to describe the relationship between every two factors (further explained in Step 4 in section 3.1.1) (Krishnan et al., 2021; Sindhwani & Malhotra, 2016).

The integrated ISM-MICMAC approach has been adopted in a variety of research such as supply chain risks, security management, information technology and sustainable construction (Hussain et al., 2023; Khanam et al., 2015; Kim et al., 2018; Pfohl et al., 2011). In the context of QS transition, we use integrated ISM-MICMAC approach to examine the contextual relationships between QS transition challenges and identify dominant challenges that need to be prioritized. The steps used in ISM-MICMAC approach is highlighted in section 3.1.1.

3.1.1 Steps used in ISM-MICMAC approach

The steps used in ISM-MICMAC approach are further described below. This part of the report is also part of the published paper Kong et al. (2023).

Step 1: Identify the list of factors that will be used as input for the ISM-MICMAC approach. The list of QS transition challenges is generated by the literature review and expert interviews.

Step 2: Develop Structural Self-Interaction Matrix (SSIM) to collect data on contextual relationships between the list of QS transition challenges.

Step 3: Examine the contextual relationship between any two factors (i and j) and fill out the SSIM. Start from a yellow box (C1, C2) and indicate one of the four symbols below to represent the relationship between factors.

V: Challenge i will <u>influence</u> Challenge j
A: Challenge j will <u>influence</u> Challenge i
X: Challenge i and Challenge j will <u>influence each other</u>
O: Challenge i and Challenge j are <u>not</u> related

Step 4: Establish Initial Reachability Matrix (IRM) from the SSIM matrix. IRM is a binary matrix with 0's and 1's that is derived in accordance to four symbols following the rules for the substitution.

If the (i,j) in the SSIM is V, then (i,j) in the reachability matrix becomes 1 and the (j,i) becomes 0
If the (i,j) in the SSIM is A, then (i,j) in the reachability matrix becomes 0 and the (j,i) becomes 1
If the (i,j) in the SSIM is X, then (i,j) in the reachability matrix becomes 1 and the (j,i) becomes 1
If the (i,j) in the SSIM is O, then (i,j) in the reachability matrix becomes 0 and the (j,i) becomes 0

Step 5: Test the IRM for transitivity and derive the Final Reachability Matrix (FRM). The transitivity is incorporated to fill the gap and 1* entries are indicated to show the changed relationships for the final reachability matrix. The FRM that is revised from the IRM in accordance with the transitivity. The changes are highlighted in grey boxes and are indicated with 1* entries.

Concept of Transitivity: If factor A influences factor B, and factor B influences factor C, then factor A also influences factor C. If there was no initial relationship between factor A and factor C in IRM, then the concept of transitivity is achieved between factor A and factor C, and 1* entry is indicated in the FRM.

Step 6: Obtain a reachability matrix with reachability set and antecedent set from the entries in rows and columns in FRM. E.g. In the reachability set, factors in the row that are affected by factor C1 are identified. In the antecedent set, factors in the column that are affecting factor C1 are identified. After the reachability set and antecedent set are determined, the intersection set is derived from the list of factors from the intersection of these sets.

Step 7: Once the reachability matrix is determined in Step 6, Step 7 is taken to determine the level of priorities for each QS transition challenge. Partition the reachability matrix and classify the FRM into various levels. The top-level factors (L1) include those factors that will be led by other factors in the lower level (L2, L3.. etc.). Once the top-level factor is identified, it is removed from consideration. Then, the same process is repeated to find out the factors in the next level. This process continues until the level of each factor is found.

Step 8: Organize the ISM-based hierarchy factors using different levels of a partition obtained in Step 7. Develop a visual representation of the ISM-based hierarchy model.

Step 9: Analyze the FRM obtained in Step 5 and calculate the summation of rows and columns based on their driving and dependence power.

Step 10: Classify the factors in a driving and dependence power diagram in accordance with the summation of driving power and dependence power obtained in Step 9. Find out which of the four quadrants each factor belongs to. There are four quadrants in the driving and dependence power diagram:

Autonomous: Factors that have weak drive power and weak dependence power.
Dependent: Factors that have weak drive power but strong dependence power.
Linkage: Factors that have strong drive power as well as strong dependence power.
Independent: Factors that have strong drive power but weak dependence power.

3.2 Dimension Identification & Organizational Readiness Model Development

3.2.1 Systematic Literature Review

We conducted Systematic Literature Review (SLR) to identify the list of QS transition challenges. From the initial 2266 articles, we selected 42 articles for the review and identified the list of QS transition challenges. The details of SLR process and the results of SLR can be found in the published paper Kong et al. (2022) and HAPKIDO project deliverable WP 3.1.

3.2.2 Semi-Structured Interviews

In order to further empirically validate the list of QS transition challenges, we conducted semi-structured interviews with experts and practitioners. The selected 12 experts and practioners from industry and government had relevant work experience with PKI systems and had prior knowledge of organizational and/or technical challenges on QS transition (Kong et al., 2023). The discussion from the semi-structured interviews can be found in the published paper Kong et al. (2024c).

3.2.3 Workshops

Since the workshop provides an opportunity for practitioners to examine the context of the study and share their insights, we conducted Workshop 1 to Workshop 4 to discuss the list of dimensions that organizations may need to consider when implementing and adopting QS technology. After a series of workshops, the finalized list of dimensions was used to develop the organizational readiness model for QS transition. Additionally, we conducted Workshop 5 to Workshop 8 to gather feedback on the organizational readiness model. The participants gave feedback on the details of the model and discussed whether the model can be used and has relevant list of dimensions for QS transition. The results have been synthesized to revise the organizational readiness assessment model for QS transition. The details of the workshops can be found in the forthcoming paper Kong et al. (Forthcoming 2024).

4 QS transition challenges

Section 4 discusses the list of QS transition challenges that an organizational readiness model is based on. The list of QS transition challenges is shown in Table 1 and the list is used as an input for ISM-MICMAC approach described in Section 3.1. The findings of ISM-MICMAC approach are shown in Figure 1 and Figure 2. This part of the report is part of the published paper Kong et al. (2023).

Table 1. QS Transition Challenges

QS Transition Challenges	Code	Description
Legacy System Constraints	C1	The existing system is rigid and only supports a handful of algorithms. The existing system may need changes in the hardware and/ or software depending on the compatibility of new QS solutions.
No Availability of QS Standardization	C2	NIST is currently selecting practical standards and guidelines for QS solutions. Thus, standards for QS cryptographic algorithms are not yet available.
No QS Standards & Selection	C3	Organization has not yet selected which QS solutions will be used and whether or not to have a full substitution of QS solution or a hybrid solution. The selection criteria for QS solutions are not clear. Trade-offs in the performance outcomes and usage context of QS solutions may need to be examined.
No Reliable & Secure QS Solution	C4	The QS solutions have not been tested and currently, there is no testing is available to prove the security of QS solutions.
No Availability of Certified QS Hardware & Software	C5	The suppliers of the current technology are not yet ready to provide the certified technology compartments for the replacement technology. e.g. HSM and certificate issuance software for QS solutions.
Knowledge Needs within Organizations	C6	There is a lack of knowledge on quantum computing-based threats, and risks associated with the technology in organizational assets e.g. cryptographic assets, and vulnerabilities etc.
Lack of Urgency within Organizations	C7	The arrival of a large-scale quantum computer is perceived to be decades away, and there is a lack of urgency for QS transition in organizations.
No Business Case for Organizations	C8	Organization finds it difficult to enter long-term QS transition commitments without clear business benefits and opportunities.
Lack of Technical Skills & Qualified	C9	There is a lack of qualified personnel who can understand QS solutions and make decisions on the implementation process.
Unclear QS Governance within Organizations	C10	Organization does not have transition plans and they do not know what to prioritize for QS transition.
Lack of Urgency in the Ecosystem	C11	There is a lack of collective sense of urgency and it is difficult to achieve inter-agency coordination and collaborations with multiple stakeholders.
Unclear QS Governance in the Ecosystem	C12	Organization does not know which organizations are in the lead and who takes responsibility for what.
Lack of Collaboration in the Ecosystem	C13	The varying levels of interests, needs and expectations contribute to duplication of efforts, limited knowledge sharing and fragmented decision making within the ecosystem.
Lack of Policy & Regulations for	C14	There is a lack of policy and legal implications for the QS transition, and compliances for QS solutions need to be updated.
Complex Technological Interdependency	C15	Changes in the existing system cannot occur in isolation due to its chain of interdependencies including governing bodies, standards bodies, hardware providers, third-party software providers etc.

The dependencies on the critical infrastructure across sectors show that the development of quantum computing technology threatens confidentiality, integrity and availability (CIA). The affect of quantum threats on critical information infrastructure such as public services or telecom affect other critical infrastructure (e.g., healthcare, banking) (Kong et al., 2023; Kong et al., 2024b). While the need to become quantum-safe (QS) remains crucial, the results of ISM-MIMAC analysis show that addressing the QS transition within organizations is much more complicated. The Driving and Dependence Power Diagram in Figure 1 shows that all QS transition challenges were placed in the linkage quadrant. While QS transition challenges are interrelated, it also indicates that the QS transition is complex and not stable in nature.

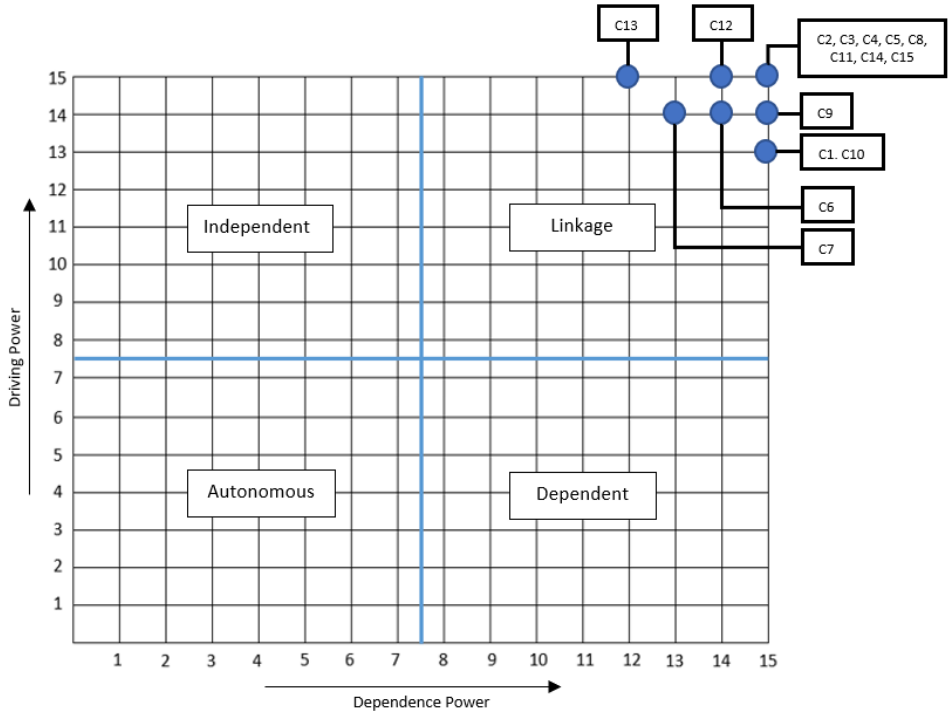

Figure 1. Driving Power & Dependency Power Diagram

As the development of QS technology presents multiple uncertainties, organizations may need to navigate the transition through a constantly changing environment (Kong et al., 2024b). If everyone is just waiting for each other, delays in one challenge can eventually lead to a deadlock for the QS transition (Kong et al., 2023). The ISM-based hierarchy in Figure 2 shows that establishing QS governance and collaboration in the ecosystem have the highest driving power among the QS transition challenges. In order to proceed with the transition, addressing QS transition challenges in the technological context and ecosystem context is crucial. QS transition challenges may need to be addressed synchronously and may need to achieve *collective action* in the PKI ecosystem is viewed as a priority.

Moreover, the results of ISM-MICMAC were used to identify the list of dimensions that need to be prioritized for QS transition. The list of QS transition challenges indicates that addressing QS transition is complex and there is no single solution that can be a single bullet. This highlights that the QS transition cannot be single-handled by one organization and require multiple actors in the PKI ecosystem to be part of the transition (Kong et al., 2023). The dimensions that need to be prioritized for QS transition include Collaboration, Governance, Policy & Regulations, Awareness, QS solution standards, Hybrid QS solution and Cryptographic Agility Strategies. The list of dimensions shows that QS transition is complex and there is no single solution that can address QS transition challenges alone.

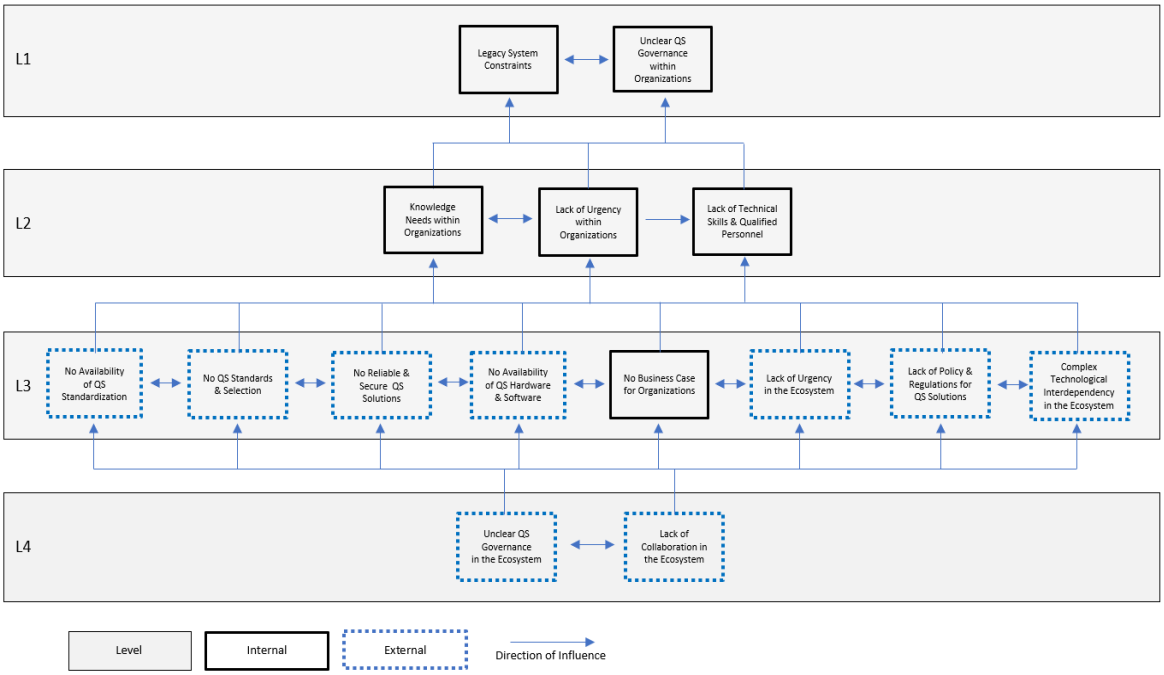

Figure 2. ISM-based Hierarchy for QS transition

5 Organizational Readiness Assessment Model for QS transition

Section 5 provides an overview of an organizational readiness assessment model for QS transition. There are eight dimensions in the model including collaboration, governance, policy & regulation, awareness, QS solution standards, hybrid QS solution, cryptographic agility strategies and knowledge on QS transition. The eight dimensions are further described below and the model is shown in Figure 3. This section of the report is part of a forthcoming paper Kong et al. (Forthcoming 2024) available in September 2024.

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

Governance
Governance is an important dimension to consider when implementing and adopting QS technology. The topic of QS transition is relatively new, and there are no existing guidelines, rules or mechanisms for decision-making and accountability. With a clear institutional void, there are many uncertainties on how to proceed QS transition. 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. However, it would be difficult to coordinate actions without a clear governance.

Policy & Regulation
Policy & regulation is an 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 direction of QS transition. There is currently no policy and regulation available for QS technology and organizations may need to monitor the regulatory process and identify the requirements for QS transition.

Awareness
Awareness is an important dimension to consider when implementing and adopting QS technology. The security threats posed by quantum computers are not yet visible (e.g., store now and decrypt later). 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. Although many of the decisions regarding QS technology are not yet clear, it is crucial for organizations to stay-up-to date and raise awareness regarding quantum computing-based threats and risks.

QS solution standards
QS solution standards is an important dimension to consider when implementing and adopting QS technology. Although QS technology with new encryption levels is not yet available, organizations need to start checking their vulnerabilities and technical interdependencies to better understand the scope of transition and the development of QS solution standards. While some actors may be involved in the testing phase of QS solutions to select the right algorithms, other actors may wait on those technical developments.

Hybrid QS solution
Hybrid QS solution is an important dimension to consider when implementing and adopting QS technology. The term hybrid provides several definitions: 1.using classical cryptographic primitives, 2.

using quantum-safe cryptographic primitives or 3.employing both of these primitives to secure core processes. 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. Organizations may need to navigate the development of QS technology and select QS solutions that are validated through testing.

Cryptographic Agility Strategies

Cryptographic agility strategies is an important dimension to consider when implementing and adopting QS technology. Although there are defined cryptographic policies and guidelines and organizations follow industry-wide accepted cryptographic algorithms, the existing systems are rigid, and changes cannot occur in isolation due to path dependencies. Current cryptographic strategies do not provide security against quantum threats, and these strategies are not agile enough to adapt to the changing environment of new technologies. It may be crucial for organizations to develop cryptographic agility strategies and adopt new cryptographic algorithms, protocols and technologies.

Knowledge on QS transition

Knowledge on QS transition is an important dimension to consider when implementing and adopting QS technology. There is a lack of knowledge on the scope of QS transition, the impact of quantum threats on existing business processes and identified vulnerabilities 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. 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.

	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.

Figure 3. Organizational Readiness Assessment Model for QS Transition

6 Conclusion

In this report, we introduce the concept of the organizational readiness model for QS transition. By using ISM-MICMAC approach, we examine interrelationship between QS transition challenges. The results of driving and dependency power diagram and ISM-based hierarchy for QS transition indicate QS transition challenges in the technological context and ecosystem context need to be addressed. QS governance and collaboration need to be addressed with priority in order for organization to make changes in the existing infrastructure.

Due to technological uncertainties in the ecosystem, organizations may need to navigate the transition in a constantly changing environment. The results of ISM-MICMAC approach shows that many of QS transition challenges are interrelated. Such interdependencies raise the complexity of QS transition and delays in one challenge may potentially lead to delays in other challenges. To better navigate QS transition challenges, we introduce the concept of an organizational readiness model for organizations to prepare for QS transition.

The organizational readiness model show the list of dimensions that need to be prioritized in order to address QS transition challenges such as Collaboration, Governance, Policy & Regulations, Awareness, QS solution standards, Hybrid QS solution and Cryptographic Agility Strategies and Knowledge on QS transition. There are five readiness levels in each dimension and the results of different readiness levels may help organizations better navigate which of the dimensions need to be improved when implementing and adopting QS technology.

We conclude this report with directions for future trajectory of the project. Next steps include assessing the model on its usability, and internal and external validity with actors in the ecosystem. We see that there is much research needed in identifying key actions needed to become quantum-safe. With multiple iterations of an organizational readiness model, we can improve relevance and completeness of the model and further translate the model into an online assessment tool. The online assessment tool can evaluate the readiness levels of different dimensions in the model and provide better guidance on organizations that are preparing for QS transition.

Bibliography

Bashir, H., & Ojiako, U. (2020). An integrated ISM-MICMAC approach for modelling and analysing dependencies among engineering parameters in the early design phase. *Journal of Engineering Design*, *31*(8-9), 461-483. https://doi.org/10.1080/09544828.2020.1817347

Bruno, I., Lobo, G., Covino, B. V., Donarelli, A., Marchetti, V., Panni, A. S., & Molinari, F. (2020). *Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services* Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance, Athens, Greece. https://doi.org/10.1145/3428502.3428552

Dermott, O., Sony, M., Antony, J., & Douglas, J. (2021). Motivations, barriers and readiness factors for Quality 4.0 implementation: an exploratory study. *The TQM Journal*, *ahead-of-print*. https://doi.org/10.1108/TQM-11-2020-0272

Duperrin, J.-C., & Godet, M. (1973). Méthode de hiérarchisation des éléments d'un système : essai de prospective du système de l'énergie nucléaire dans son contexte sociétal.

Hussain, K., He, Z., Ahmad, N., Iqbal, M., & Saeed, M. Z. (2023). Establishing a Green, Lean and Six Sigma implementation model for sustainable construction industry: an analysis of driving forces through ISM-MICMAC approach. *Environ Sci Pollut Res Int*, *30*(11), 30462-30492. https://doi.org/10.1007/s11356-022-24039-9

Khanam, S., Siddiqui, J., & Talib, F. (2015). Modelling the TQM enablers and IT resources in the ICT industry: an ISM-MICMAC approach. *International Journal of Information Systems and Management (IJISAM)*, *1*, 195-218. https://doi.org/10.1504/IJISAM.2015.072290

Kim, D., Kim, Y., & Lee, N. (2018). A Study on the Interrelations of Decision-Making Factors of Information System (IS) Upgrades for Sustainable Business Using Interpretive Structural Modeling and MICMAC Analysis. *Sustainability*, *10*(3). https://doi.org/10.3390/su10030872

Kobos, P. H., Malczynski, L. A., Walker, L. T. N., Borns, D. J., & Klise, G. T. (2018). Timing is everything: A technology transition framework for regulatory and market readiness levels. *Technological Forecasting and Social Change*, *137*, 211-225. https://doi.org/10.1016/j.techfore.2018.07.052

Kong, I., Janssen, M., & Bharosa, N. (2022). *Challenges in the Transition towards a Quantum-safe Government* Proceedings of the 23rd Annual International Conference on Digital Government Research: Intelligent Technologies, Governments and Citizens, DGO 2022

Kong, I., Janssen, M., & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition. EGOV-CeDEM-EPart2023, Corvinus University of Budapest, Hungary.

Kong, I., Janssen, M., & Bharosa, N. (2024a). *Deriving Government Roles for directing and supporting Quantum-safe Transitions* Proceedings of the 25th Annual International Conference on Digital Government Research,

Kong, I., Janssen, M., & Bharosa, N. (2024b). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly*, *41*(1). https://doi.org/10.1016/j.giq.2023.101884

Kong, I., Janssen, M., & Bharosa, N. (2024c). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly*, *41*(1), 101884. https://doi.org/https://doi.org/10.1016/j.giq.2023.101884

Kong, I., Janssen, M., & Bharosa, N. (Forthcoming 2024). Navigating through the Unknowns-Organizational Readiness Assessment Model for Quantum-safe Transition.

Krishnan, S., Gupta, S., Kaliyan, M., Kumar, V., & Garza-Reyes, J. A. (2021). Assessing the key enablers for Industry 4.0 adoption using MICMAC analysis: a case study. *International Journal of Productivity and Performance Management*, *70*(5), 1049-1071. https://doi.org/10.1108/IJPPM-02-2020-0053

Maganga, D. P., & Taifa, I. W. R. (2023). The readiness of manufacturing industries to transit to Quality 4.0. *International Journal of Quality & Reliability Management*, *40*(7), 1729-1752. https://doi.org/10.1108/IJQRM-05-2022-0148

McGowran, E., & Harris, E. (2020). Regulatory Readiness Level: a Tool to Enhance Early Regulatory Adoption in Academic Discovery. https://doi.org/10.21427/qp14-dy42

Miake-Lye, I. M., Delevan, D. M., Ganz, D. A., Mittman, B. S., & Finley, E. P. (2020). Unpacking organizational readiness for change: an updated systematic review and content analysis of assessments. *BMC Health Serv Res*, *20*(1), 106. https://doi.org/10.1186/s12913-020-4926-z

NIST. (2016). *Report on Post-Quantum Cryptography*.

NIST. (2021). *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*.

NIST. (2022). *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*.

Pfohl, H.-C., Gallus, P., & Thomas, D. (2011). Interpretive structural modeling of supply chain risks. *International Journal of Physical Distribution & Logistics Management*, *41*, 839-859. https://doi.org/10.1108/09600031111175816

Shahrasbi, N., & Paré, G. (2014). Rethinking the Concept of Organizational Readiness: What Can IS Researchers Learn from the Change Management Field? https://doi.org/10.13140/RG.2.1.3470.8564

Sindhwani, R., & Malhotra, V. (2016). Modelling and analysis of agile manufacturing system by ISM and MICMAC analysis. *International Journal of System Assurance Engineering and Management*, *8*(2), 253-263. https://doi.org/10.1007/s13198-016-0426-2

Vakola, M. (2013). Multilevel Readiness to Organizational Change: A Conceptual Approach. *Journal of Change Management*, *13*(1), 96-109. https://doi.org/10.1080/14697017.2013.768436

Vik, J., Melås, A. M., Stræte, E. P., & Søraa, R. A. (2021). Balanced readiness level assessment (BRLa): A tool for exploring new and emerging technologies. *Technological Forecasting and Social Change*, *169*. https://doi.org/10.1016/j.techfore.2021.120854

Webster, A., & Gardner, J. (2019). Aligning technology and institutional readiness: the adoption of innovation. *Technology Analysis & Strategic Management*, *31*(10), 1229-1241. https://doi.org/10.1080/09537325.2019.1601694

Weiner, B. J. (2009). A theory of organizational readiness for change. *Implement Sci*, *4*, 67. https://doi.org/10.1186/1748-5908-4-67

Yusif, S., Hafeez-Baig, A., & Soar, J. (2017). e-Health readiness assessment factors and measuring tools: A systematic review. *International Journal of Medical Informatics*, *107*, 56-64. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2017.08.006