Post-Quantum

Cryptography Conference

Online Quantum-safe Readiness Tool

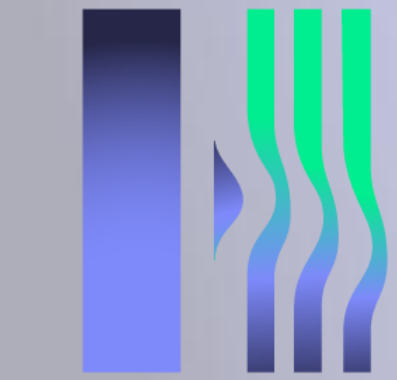
The list of standardization based on Post-Quantum Cryptography (PQC) and the NIST IR 8547 initial public draft signal that organizations should begin preparing for their transitions to PQC standards. While transitions to PQC standards cannot be addressed in isolation due to interdependencies that organizations depend on, there are many uncertainties that prevent organizations from taking actionable steps. In order to navigate the complexities of transitions, an online quantum readiness assessment tool is developed to guide organizations. With a multi-dimensional approach, the tool recognizes various dimensions that organizations should consider when transitioning their existing infrastructures. What sets this tool apart from other available tool is its foundation in the scientific methods, utilizing empirical data and addressing context specific transition challenges relevant to PKIs. Since it remains crucial for organizations to gain an overview of transition progress, the tool allows organizations to focus on areas that have low readiness levels and adjust their strategies with a set of possible recommendations.

Ini Kong

PhD Researcher at Delft University of Technology

January 15 and 16, 2025 - Austin, TX (US) | Online

Online Quantum-safe Readiness Questionnaire Tool



HAPKIDO

Ini Kong

PhD Researcher | Delft University of Technology
Faculty of Technology, Policy & Management

Post-Quantum Cryptography Conference, Austin, Texas, USA, January 15-16, 2025

Table of Content

Development Process of the Tool: Literature

Table 1. Challenges found from the literature

Technological Context	Organizational Context	Ecosystem Context
• Legacy System Constraints • Not-yet achieved standards from NIST • No universal QS algorithm • Implementation flaws and side-channel attacks • Lack of reliability in QS cryptography • Vulnerable Root CA • Complex PKI system & Interoperability • Cost of transition	• Lack of urgency • Knowledge gaps in quantum computing • No one-size-fits-all transition process • Lack of crypto-agility • Unclear QS governance: not knowing how to facilitate • Lack of in-house management support • Unclear QS transition benefits & business case • No technical skills & qualified personnel	• Low level of Investment • Lack of awareness • No clear ownership & operating institution • Different interpretation of QS PKI system • Lack of policy guidance • Various stakeholders: Need for collaboration • Legal issues (eg. laws & legislation) • Bureaucratic process (eg., standards & regulations to follow)

Source: Kong, I., Janssen, M. & Bharosa, N. (2022). Challenges in the Transition towards a Quantum-safe Government.

Development Process of the Tool: Interviews

Table 2. Challenges refined after the Interviews

Technological Context	Organizational Context	Ecosystem Context
• Legacy System Constraints • No Availability of QS Solutions • No QS Standards & Selection • No Reliable & Secure QS Solutions • No Availability of QS Hardware & Software	• Knowledge Needs within Organizations • Lack of Urgency within Organizations • No Business Case for Organizations • Lack of Technical Skills & Qualified Personnel • Unclear QS Governance within Organizations	• Lack of Urgency in the Ecosystem • Unclear QS Governance in the Ecosystem • Lack of Collaboration in the Ecosystem • Lack of Policy & Regulations for QS solutions • Complex Technological Interdependencies

Source: Kong, I., Janssen, M. & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions

Development Process of the Tool: Workshops (ISM-MICMAC analysis)

Structural Self-Interactive Matrix (SSIM)			j													
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
i	Legacy System Constraints	C1															
	No Availability of QS Standardization	C2															
	No QS Standards & Selection	C3															
	No Reliable & Secure QS Solutions	C4															
	No Availability of QS Hardware & Software	C5															
	Knowledge Needs within Organizations	C6															
	Lack of Urgency within Organizations	C7															
	No Business Case for Organizations	C8															
	Lack of Technical Skills & Qualified Personnel	C9															
	Unclear QS Governance within Organizations	C10															
	Lack of Urgency in the *Ecosystem**	C11															
	Unclear QS Governance in the *Ecosystem**	C12															
	Lack of Collaboration in the *Ecosystem**	C13															
	Lack of Policy & Regulations for QS solutions	C14															
	Complex Technological Interdependenc in the *Ecosystem**	C15															

Figure 1. Structural Self-Interactive Matrix (SSIM)

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Development Process of the Tool: Workshops (ISM-MICMAC analysis)

Structural Self-Interactive Matrix (SSIM)			j													
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
i	Legacy System Constraints	C1															
	No Availability of QS Standardization	C2															
	No QS Standards & Selection	C3															
	No Reliable & Secure QS Solutions	C4															
	No Availability of QS Hardware & Software	C5															
	Knowledge Needs within Organizations	C6															
	Lack of Urgency within Organizations	C7															
	No Business Case for Organizations	C8															
	Lack of Technical Skills & Qualified Personnel	C9															
	Unclear QS Governance within Organizations	C10															
	Lack of Urgency in the *Ecosystem**	C11															
	Unclear QS Governance in the *Ecosystem**	C12															
	Lack of Collaboration in the *Ecosystem**	C13															
	Lack of Policy & Regulations for QS solutions	C14															
	Complex Technological Interdependenc in the *Ecosystem**	C15															

Figure 1. Structural Self-Interactive Matrix (SSIM)

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Development Process of the Tool: Workshops (ISM-MICMAC analysis)

Structural Self-Interactive Matrix (SSIM)		j														
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
i	Legacy System Constraints C1															
	No Availability of QS Standardization C2															
	No QS Standar															
	No Reliable &															
	No Availability Software															
	Knowledge Ne															
	Lack of Urgenc															
	No Business C															
	Lack of Techni Personnel															
	Unclear QS Go Organizations															
	Lack of Urgenc															
	Unclear QS Go *Ecosystem**															
	Lack of Collab															
	Lack of Policy & Regulations for QS solutions C14															
	Complex Technological Interdependency in the *Ecosystem** C15															

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

Figure 1. Structural Self-Interactive Matrix (SSIM)

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Development Process of the Tool: Workshops (ISM-MICMAC analysis)

Structural Self-Interactive Matrix (SSIM)		j														
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
Legacy System Constraints	C1		O	O	A	A	A	O	V	O	O	O	O	X	A	A
Lack of Policy & Regulations for QS solutions	C14															A
Complex Technological Interdependency in the *Ecosystem**	C15															

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**

Figure 2. Structural Self-Interactive Matrix (SSIM) with four symbols

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Development Process of the Tool: Workshops (ISM-MICMAC analysis)

Structural Self-Interactive Matrix (SSIM)		j														
		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
Legacy System Constraints	C1	1	0	0	0	0	0	0	1	0	0	0	0	1	0	0
No Availability of QS Standardization	C2	0	1	1	1	1	1	0	1	0	0	1	0	0	1	1
No																1
No																1
No																1
Knc																0
Lac																0
No																1
Lac																0
Unc																0
Lac																1
Unc																1
Lack of Collaboration in the *Ecosystem**	C13	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0
Lack of Policy & Regulations for QS solutions	C14	1	0	1	0	1	1	1	1	1	1	1	1	0	1	0
Complex Technological Interdependency in the *Ecosystem**	C15	1	1	1	1	1	0	0	1	1	1	0	1	1	1	1

i

Test the IRM to get the FRM (Final Reachability Matrix)

Apply the Concept of Transitivity:
If factor A influences factor B, and factor B influences factor C, then factor A also influences factor C.

Figure 3. Initial Reachability Matrix (IRM)

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Development Process of the Tool: Workshops (ISM-MICMAC analysis)

Structural Self-Interactive Matrix (SSIM)			j													
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	C15
i	Legacy System Constraints	C1	1	1	0	0	0	0	1	1	1	1	1	0	1	0	1
	No Availability of QS Standardization	C2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	No QS Standards & Selection	C3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	No Reliable & Secure QS Solutions	C4	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
	No Availability of QS Hardware & Software	C5	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
	Knowledge Needs within Organizations	C6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Lack of Urgency within Organizations	C7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	No Business Case for Organizations	C8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Lack of Technical Skills & Qualified Personnel	C9	1	1	1	1	1	1	0	1	1	1	0	1	0	1	1
	Unclear QS Governance within Organizations	C10	1	1	1	1	1	0	0	1	1	1	0	1	0	1	1
	Lack of Urgency in the *Ecosystem**	C11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Unclear QS Governance in the *Ecosystem**	C12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Lack of Collaboration in the *Ecosystem**	C13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Lack of Policy & Regulations for QS solutions	C14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Complex Technological Interdependency in the *Ecosystem**	C15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Figure 4. Final Reachability Matrix (FRM)

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Development Process of the Tool: Workshops

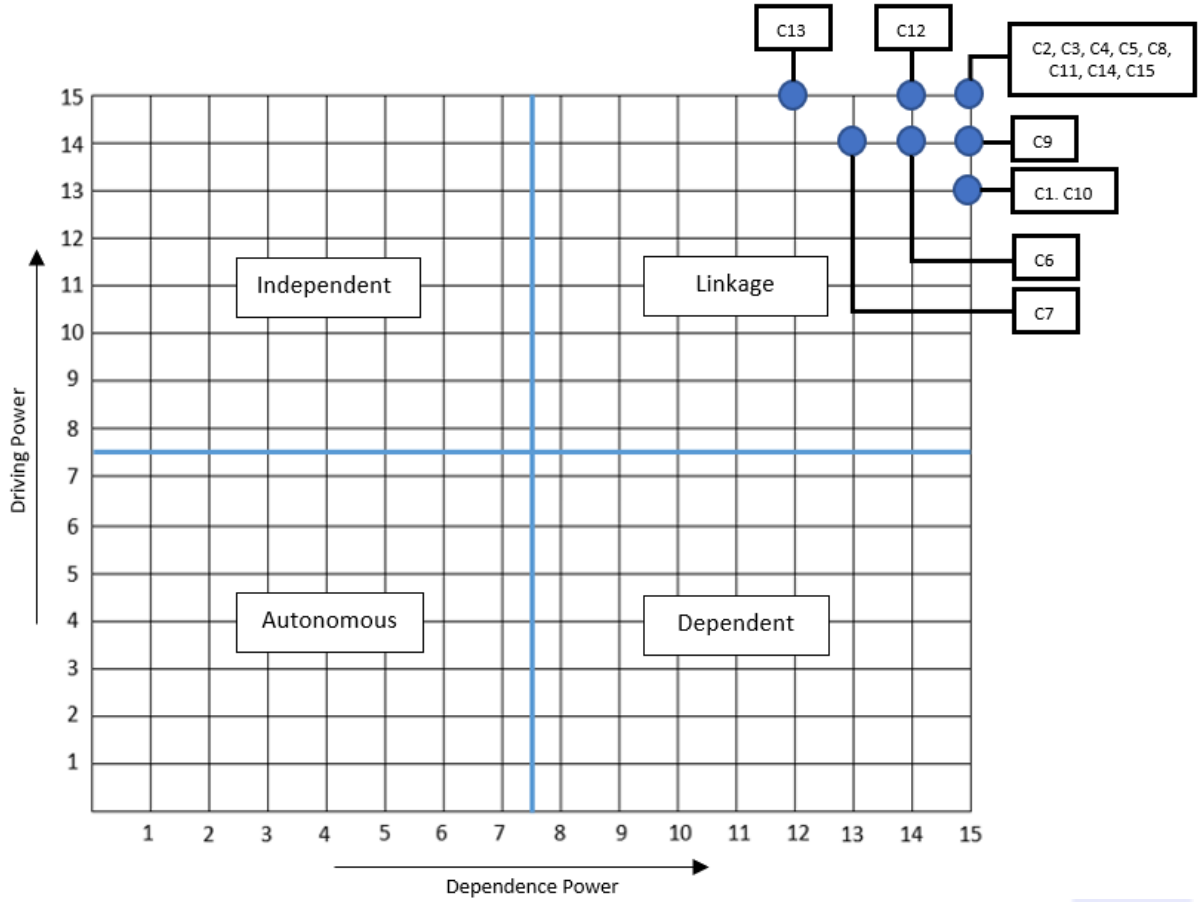


Figure 5. Driving Power & Dependency Power

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

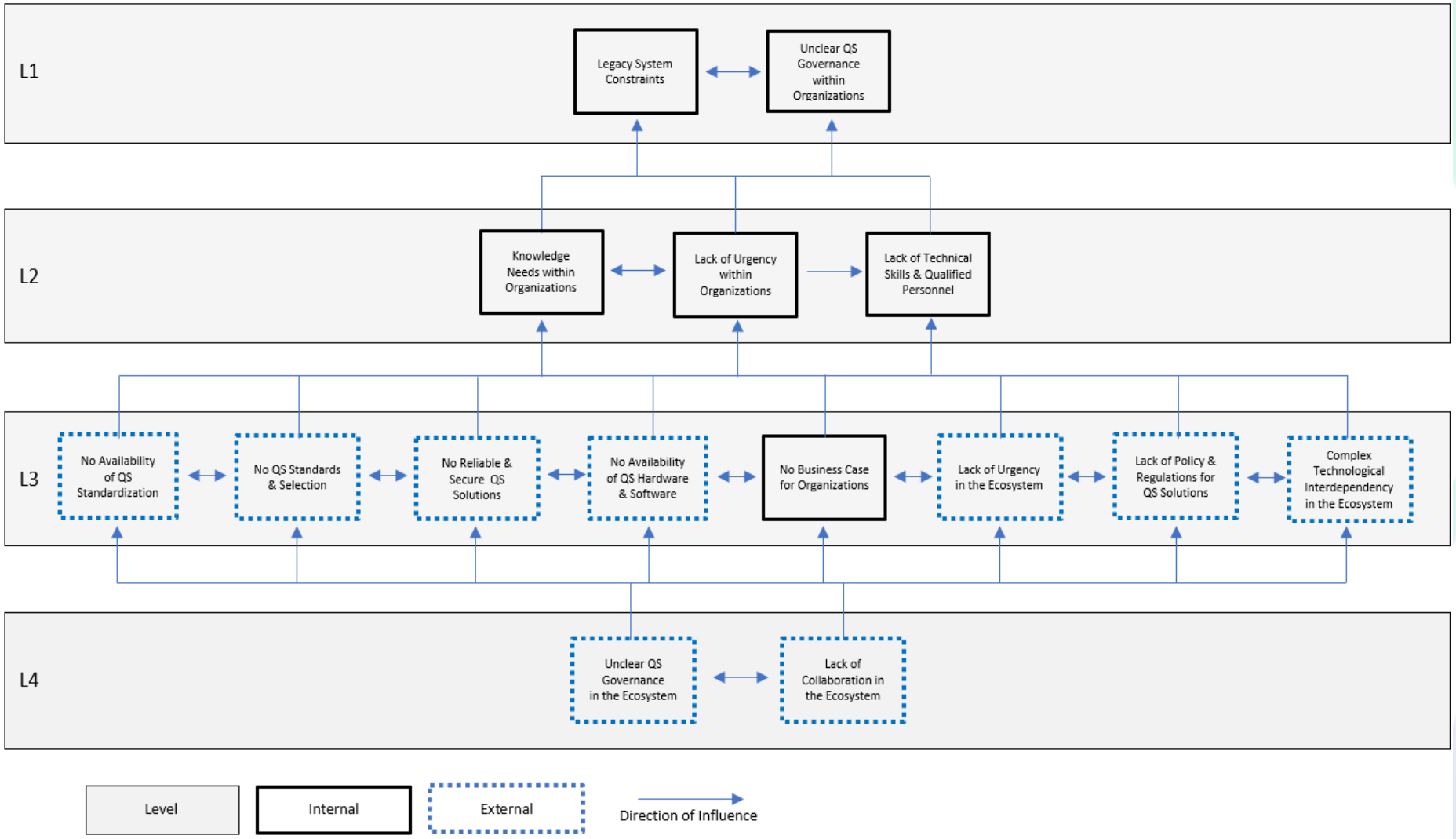


Figure 6. Example of Hierarchical Structural Model

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Development Process of the Tool: Key Takeaways

- No independent challenges with strong driving power and weak dependence power
  - -no single challenge that can act as a key factor for QS transition

- QS transition involves many uncertainties & still at its early stage
  - -changes in the status of the challenges may influence each other
  - -delays in one challenge can result in delays in others

- Ecosystem & Technological challenges influence Organizational challenges
  - -some actors may be involved in making external decisions in the ecosystem
  - -others may wait for those decisions and follow the lead

Source: Kong, I., Janssen, M. & Bharosa, N. (2023). Analyzing Dependencies among Challenges for Quantum-safe Transition.

Why an Organizational QS Readiness Model?

- Organizations may need to navigate QS transition with the changing external environment
  -standardization process, availability of QS technology, selection of QS solution algorithms etc.

- Organizations cannot make decisions on their own (we are part of the ecosystem!)
  -organizations need to be ready to move with the ecosystem

- However, organizations currently lack tools to prepare for QS transition with actionable steps

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

Online QS readiness Questionnaire Tool

Objective of the tool

- To identify dimensions that organization may need to work on
- To assess the level of organizational readiness for QS transition
- To provide the list of possible recommendations to better navigate the specific actions needed

Target audience of the tool

- Information Security Officers, Security managers, Security Awareness Coordinator, CISOs Compliance Analyst, Business Continuity Planner etc.

	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

Figure 7. Organizational Readiness Assessment Model for QS Transition

Source: Kong, I. Janssen, M. & Bharosa, N. 2024. Navigating through the Unknowns-Organizational Readiness Assessment Model for Quantum-safe 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.

Figure 7. Organizational Readiness Assessment Model for QS Transition

Source: Kong, I. Janssen, M. & Bharosa, N. 2024. Navigating through the Unknowns-Organizational Readiness Assessment Model for Quantum-safe 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.

Figure 7. Organizational Readiness Assessment Model for QS Transition

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

Online QS readiness Questionnaire Tool: Dimensions

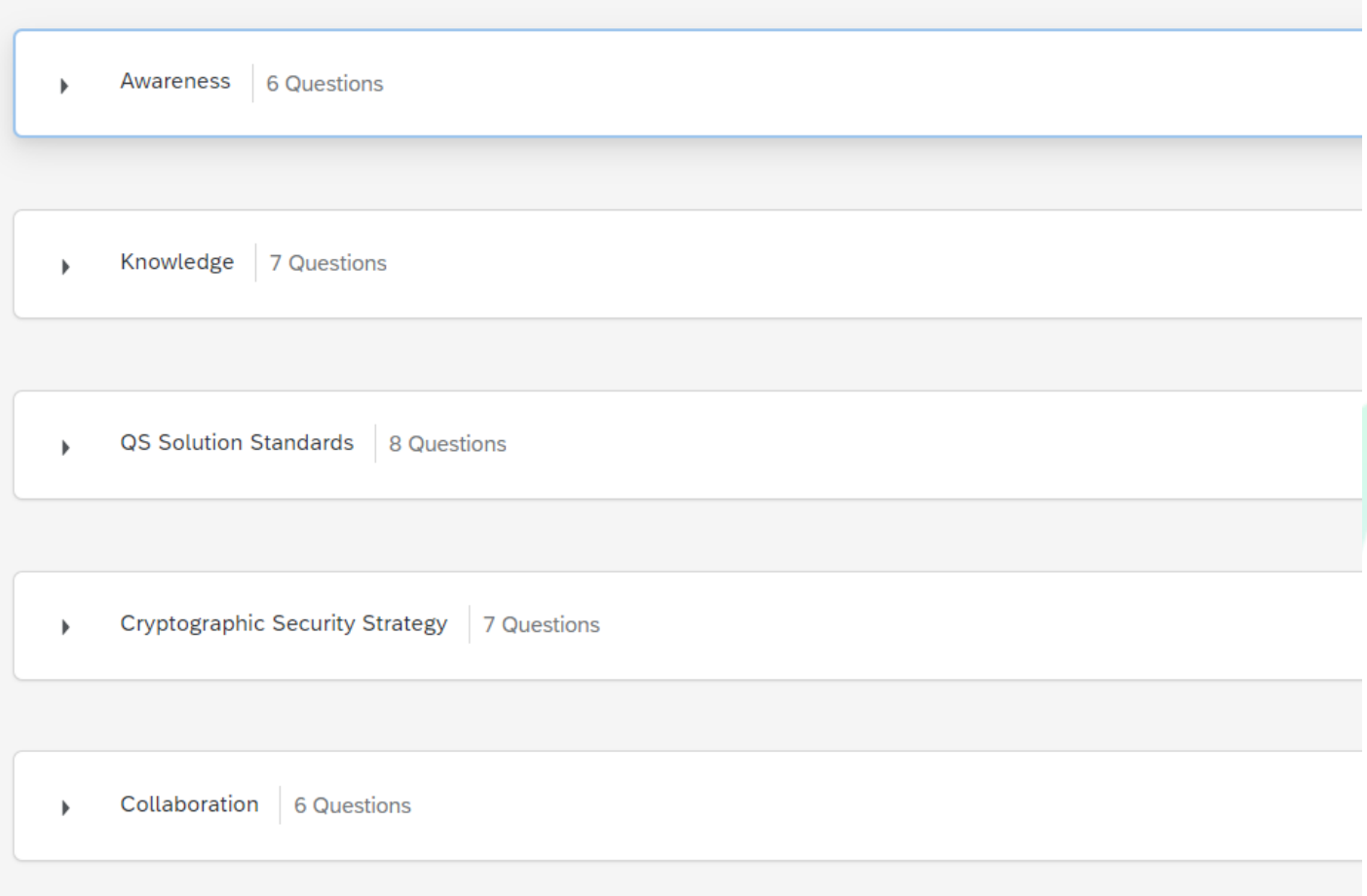


Figure 8. Questions per Dimension in Qualtrics

Online QS readiness Questionnaire Tool: Questions per Dimension

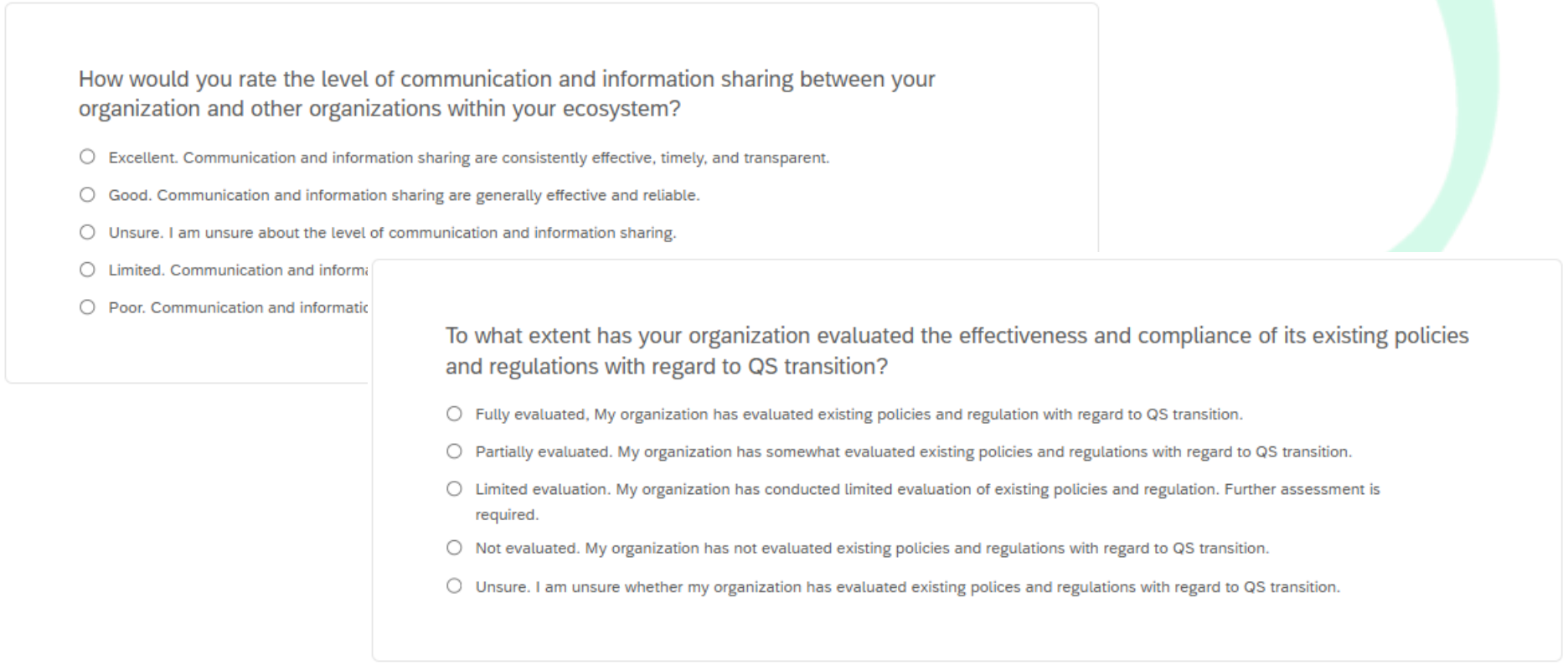


Figure 9. Sample Questions from the Questionnaire Tool

Online QS readiness Questionnaire Tool: Next Steps

- Series of iterations & feedback sessions to improve the tool
- Automated features that offer recommendations based on the results
- Details of the tool may subject to change as QS transition evolves
- MVP online readiness questionnaire tool (2025 Q2)

References

Navigating through the Unknowns-Readiness Assessment Model for Quantum-safe Transition.
Kong, I., Janssen, M. & Bharosa, N. 2024, In: Electronic Government. EGOV 2024. Lecture Notes in Computer Science, vol 14841. Springer, Cham.
Research output: Chapter in Book/Conference proceedings/Edited volume › Conference contribution › Scientific › peer-review

Deriving Government Roles for directing and supporting Quantum-safe Transitions

Ini, K., Marijn, J. & Nitesh, B., 2024, *Proceedings of the 25th Annual International Conference on Digital Government Research, DGO 2024.* Liao, H-C., Cid, D. D., Macadar, M. A. & Bernardini, F. (eds.). Association for Computing Machinery (ACM), p. 507-514 8 p. (ACM International Conference Proceeding Series).
Research output: Chapter in Book/Conference proceedings/Edited volume › Conference contribution › Scientific › peer-review

Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions

Kong, I., Janssen, M. & Bharosa, N., 2024, In: Government Information Quarterly. 41, 1, 101884.
Research output: Contribution to journal › Article › Scientific › peer-review

Analyzing Dependencies among Challenges for Quantum-safe Transition

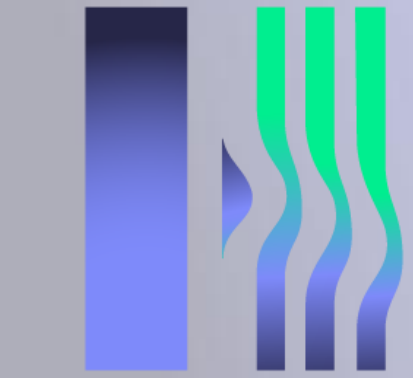
Kong, I., Janssen, M. & Bharosa, N., 2023, In: CEUR Workshop Proceedings. 3449
Research output: Contribution to journal › Conference article › Scientific › peer-review

Transitioning Towards Quantum-Safe Government: Examining Stages of Growth Models for Quantum-Safe Public Key Infrastructure Systems

Kong, I., 2022, *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2022.* Amaral, L., Soares, D. & Zheng, L. (eds.). Association for Computing Machinery (ACM), p. 499-503 5 p. (ACM International Conference Proceeding Series).*Research output: Chapter in Book/Conference proceedings/Edited volume › Conference contribution › Scientific › peer-review*

Challenges in the Transition towards a Quantum-safe Government

Kong, I., Janssen, M. & Bharosa, N., 2022, *Proceedings of the 23rd Annual International Conference on Digital Government Research: Intelligent Technologies, Governments and Citizens, DGO 2022.* Hagen, L., Solvak, M. & Hwang, S. (eds.). Association for Computing Machinery (ACM), p. 282-292 11 p. 82. (ACM International Conference Proceeding Series).
Research output: Chapter in Book/Conference proceedings/Edited volume › Conference contribution › Scientific › peer-review



Thank you!

i.kong@tudelft.nl

Post-Quantum Cryptography Conference, Austin, Texas, USA, January 15-16, 2025