HAPKIDO

Self-Assessment Tool for Quantum-safe Transition

Ini Kong
Marijn Janssen
Nitesh Bharosa

NWO

Table of Contents

Self-Assessment Tool Across Eight Dimensions in Three Categories

The self-assessment tool evaluates organizations across three categories, ***Technology, Organization, and Ecosystem,*** which group together eight key dimensions identified as priorities that organizations should consider when preparing for QS transition. The grouping of these dimensions into three categories was intended to minimize redundancy in assessment questions and to provide a focused and structured evaluation within a clear and manageable structure. The descriptions of the eight dimensions are provided below and are based on the publications referenced on page 5.

Technology

QS Solution Standards

Another important dimension to consider when implementing QS cryptographic solutions 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 QS cryptographic solutions. 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 infrastructure 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 are another important dimension to consider when implementing QS cryptographic solutions. 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.

Organization

Awareness

Awareness is another important dimension to consider when implementing QS cryptographic solutions. 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.

Knowledge on QS Transition

Another important dimension to consider when implementing QS cryptographic solutions 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 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.

Policy and Regulation

Policy & regulation is another important dimension to consider when implementing QS cryptographic solutions 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 or regulation available for QS technology that organizations can follow. Organizations may need to monitor the regulatory process and identify the requirements for QS transition.

Ecosystem

Five QS Transition Challenges in Ecosystem Context are Complex Technical Interdependencies, Lack of Collaboration, Lack of Urgency in the Ecosystem, No QS Governance in the Ecosystem and Lack of Policy & Regulations for QS Solutions. These challenges have been summarized into key dimensions that organizations should consider when implementing QS cryptographic solutions in Organizational context which are Collaboration and Governance.

Collaboration

One of the important dimensions to consider when implementing QS cryptographic solutions 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 QS cryptographic solutions 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 clear governance for organizations to coordinate actions to prepare for QS transition with multiple actors in the ecosystem.

About the Self-Assessment Tool

The objective of this self-assessment tool is to assess the readiness levels for Quantum-safe (QS) transition and provide guidance for progressing through different levels of maturity. There are a total of 60 questions. The results of the assessment indicate the organization's current level of readiness for QS transition. Based on this level, a corresponding list of recommendations is provided, which the organization may consider in preparing for a higher level of readiness.

Quantum-Safe (QS) Transition?

The advancement of quantum computers may introduce new security threats by breaking today's widely used cryptographic algorithms that existing critical infrastructures depend on. There are various motivations across academia, industries, and governments to develop secure alternatives. In 2016, the US National Institute of Standards and Technology (NIST) launched an initiative to evaluate and standardize QS cryptographic algorithms based on post-quantum cryptography (PQC). As of 2024, the NIST has announced a set of PQC-based standards. In this self-assessment, we define *QS transition* as the process of modifying the cryptographic layer of the existing systems with cryptographic solutions based on PQC.

This self-assessment tool is grounded in research and methodologies developed during the PhD study, which is conducted as part of the HAPKIDO project (Hybrid Approach to Quantum-safe Public Key Infrastructure Development for Organizations), funded by Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)

For more details on the underlying methodology and supporting studies, please refer to the publications listed below:

Kong, I. (2026). Moving to the Quantum Era: A Stage-Based Growth Approach for Organizations Navigating the Transition to Post-Quantum Cryptography. PhD Dissertation.

Kong, I. Janssen, M & Bharosa, N. (2024). Navigating through the Unknowns-Readiness Assessment Model for Quantum-safe Transition. Electronic Government: 23rd IFIP WG 8.5 International Conference, EGOV 2024, Ghent-Leuven, Belgium, September 3–5, 2024, Proceedings. p. 438 – 453. https://dx.doi.org/10.1007/978-3-031-70274-7_27

Kong, I. Janssen, M & Bharosa, N. (2024). Organizational Readiness Model for Quantum-safe Transition. TNO. https://hapkido.tno.nl/deliverables/organizational-readiness-model-quantum/

Kong, I. Janssen, M & Bharosa, N. (2022). Challenges in the Transition towards a Quantum-safe Government. In L. Hagen, M. Solvak, & S. Hwang (Eds.), *Proceedings of the 23rd Annual International Conference on Digital Government Research: Intelligent Technologies, Governments and Citizens, DGO 2022* (pp. 282-292). Article 82 (ACM International Conference Proceeding Series). https://doi.org/10.1145/3543434.3543644

Instructions for Completing the Assessment Tool:

There are 60 questions that have been divided into categories such as Technology, Organization, and Ecosystem. For each question, you have three response options: “Yes”, “No”, or “Not Applicable-Need Expert Input”.

- Choose “Yes” if you agree with the statement.
- Choose “No” if you disagree with the statement.
- Choose “Not Applicable-Need Expert Input” if you cannot answer due to lack of knowledge or experience.

Guidance on Handling “Not Applicable-Need Expert Input” Responses:
If you select “Not Application-Need Expert Input” because you do not have the knowledge or experience, someone else with the appropriate knowledge may need to answer the question. Ideally, the total number of questions marked “Not Applicable-Need Expert Input” should not exceed 10 out of 60. If you cannot answer more than this, consider asking someone with the appropriate knowledge to complete the assessment.

Background Questions

Q1. Which of the following statements applies to your organization

- ○ My organization belongs to the public sector.
- ○ My organization belongs to the private sector.
- ○ Other (please specify):

Q2. What is the scope of your organization's influence? Please select all that apply.

- ○ Global: My organization operates across multiple countries beyond national borders.
- ○ National: My organization operates within a specific country, influencing multiple sectors at a national and local level.
- ○ Local: My organization operates within a specific region in a country.

Q3. How would you describe your organization's role in setting industry standards or regulations?

- ○ My organization is involved in creating and establishing standards or regulations that are recognized and adopted globally.
- ○ My organization is involved in shaping and applying standards or regulations in a specific country.
- ○ My organization is not involved in setting or influencing standards or regulations. My organization complies with standards and regulations to service specific customer needs.

Q3. Which of the following best describes your role in the organization? Select all that apply.

- ○ Business & Consulting
- ○ Risk Management
- ○ Legal
- ○ Compliance
- ○ Operations
- ○ Strategy
- ○ Technology/ IT
- ○ Research & Development
- ○ Leadership
- ○ Other (please specify):

Q4. How familiar are you with the topic of QS transition?

- I can discuss various challenges and strategies for QS transition.
- I can explain the need for QS transition and various challenges.
- I have heard about QS transition, but I have limited knowledge.
- I am aware that there are activities going on about QS transition, but I do not know much about them.
- I have not heard of it, and I have no knowledge about the QS transition.

Q5. How urgent do you feel the need for QS transition?

- QS transition needs to happen immediately, and delays could have significant negative consequences.
- QS transition is highly important, and actions should be taken soon to prevent potential issues.
- While QS transition is important, there may be some flexibility in timing, but actions should be taken in the near future.
- QS transition is somewhat important, but there is less urgency, and actions can be taken within a reasonable time frame.
- QS transition is not a pressing concern, and actions can be taken at a later date without significant impact.

Part 1. Organization

Q1. Is your organization aware of the potential quantum threats?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q2. Is your organization aware of the emerging opportunities of QS transition?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q3. Did your organization connect with professionals, experts and other organizations in your industry to inquire about QS transition?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q4. Has your organization reviewed the existing internal policies and other regulations (e.g., NIS 2 Directives) to identify areas of non-compliance?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q5. Is your organization aware of vulnerabilities in current business processes against quantum threats?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q6. Has your organization communicated quantum threats & the need for QS transition across departments?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q7. Is your organization aware of current and regulation gaps for QS transition?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q8. Are you aware if a set of recommendations is available for QS transition (e.g., PQC migration handbook)?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q9. Has your organization contacted vendors to ask about their QS products and services?/ using (hybrid) QS cryptographic solutions?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q10. Has your organization discussed a budget framework for future tendering requirements in the existing system?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q11. Does your organization have defined responsibilities that are responsible for managing QS transition across departments?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q12. Has your organization defined a roadmap, timeline, and goal of QS transition to implement (hybrid) QS cryptographic solutions?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q13. Has your organization addressed the knowledge and skills needed for building awareness, knowledge, and internal policies for QS transition?

- Yes.
- No.
- Not applicable.

Q14. Has your organization developed strategies for managing QS transition across departments?

- Yes.
- No.
- Not applicable.

Q15. Are you aware of any implementation conducted at your organization concerning (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q16. Does your organization have ongoing feedback to monitor the implementation of (hybrid) QS cryptographic solutions and address challenges that arise?

- Yes.
- No.
- Not applicable.

Q17. Has your organization updated its internal knowledge base and policy manual from the implementation of (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q18. Has your organization utilized (hybrid) QS cryptographic solutions in a scaled environment with different business processes?

- Yes.
- No.
- Not applicable.

Q19. Does your organization provide up-to-date resources and training programs to educate employees on awareness, knowledge, and internal policies needed for the emerging security threats & challenges?

- Yes.
- No.
- Not applicable.

Q20. Does your organization have a process in place that addresses awareness, knowledge, and internal policies to enable rapid adaptation to emerging security threats and challenges?

- Yes.
- No.
- Not applicable.

Part 2. Technology

Q21. Does your organization engage in informal chats and discussions across departments to exchange ideas, knowledge and feedback?

- Yes.
- No.
- Not applicable.

Q22. Does your organization follow defined cryptographic policies and practices that are available in the industry?

- Yes.
- No.
- Not applicable.

Q23. Does your organization have on-demand forms of implementing necessary technical measures to address emerging security threats?

- Yes.
- No.
- Not applicable.

Q24. Are you aware if the list of QS cryptographic standards is available?

- Yes.
- No.
- Not applicable.

Q25. Has your organization conducted risk and impact assessments to determine current security vulnerabilities?

- Yes.
- No.
- Not applicable.

Q26. Did your organization identify which areas need to be prioritized to implement (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q27. Does your organization have an up-to-date list of (hybrid) QS cryptographic solutions that are currently being discussed?

- Yes.
- No.
- Not applicable.

Q28. Are these (hybrid) QS cryptographic solutions (validated through testing) available?

- Yes.
- No.
- Not applicable.

Q29. Has your organization defined the list of criteria to select (hybrid) QS cryptographic solutions in products and services when available (e.g., scalability, system requirements, compatibility, etc.)?

- Yes.
- No.
- Not applicable.

Q30. Does your organization have a testing and evaluation process in place to assess the performance of (hybrid) QS cryptographic solutions in the existing system?

- Yes.
- No.
- Not applicable.

Q31. Has your organization developed a pilot plan for a small-scale implementation of the selected (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q32. Has your organization selected available products and services that consist of (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q33. Has your organization implemented (hybrid) QS cryptographic solution in a smaller scale in the existing systems?

- Yes.
- No.
- Not applicable.

Q34. Does your organization have a monitoring mechanism in place to measure and evaluate the success of the deployment of (hybrid) QS cryptographic solutions in the existing systems?

- Yes.
- No.
- Not applicable.

Q35. Is the topic of cryptographic agility included in your organization's security strategy?

- Yes.
- No.
- Not applicable.

Q36. Does your organization have the necessary technology and tools in place to support advanced cryptographic control?

- Yes.
- No.
- Not applicable.

Q37. Did your organization implement (hybrid) QS cryptographic solution in a scaled environment?

- Yes.
- No.
- Not applicable.

Q38. Is cryptographic agility scaled across different business processes of your organization?

- Yes.
- No.
- Not applicable.

Q39. Does your organization provide up-to-date resources and training programs available to educate employees on the deployment of (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q40. Does your organization have a process in place that enables rapid adaptation to change in technologies and compliance requirements for emerging security threats and challenges?

- Yes.
- No.
- Not applicable.

Part 3. Ecosystem

Q41. Has your organization shared initial concerns about quantum threats?

- Yes.
- No.
- Not applicable.

Q42. Does your organization have a good overview of internal stakeholders?

- Yes.
- No.
- Not applicable.

Q43. Does your organization have a good overview of external stakeholders?

- Yes.
- No.
- Not applicable.

Q44. Does your organization have ad-hoc forms of decision-making processes to address QS transition governance?

- Yes.
- No.
- Not applicable.

Q45. Does your organization have a communication channel to stay informed about QS transition?

- Yes.
- No.
- Not applicable.

Q46. Has your organization identified current governance gaps and challenges for QS transition?

- Yes.
- No.
- Not applicable.

Q47. Does your organization have a team that is a point of contact across departments for QS transition?

- Yes.
- No.
- Not applicable.

Q48. Have any collaboration and/ knowledge sharing sessions with the steering committee and working groups on QS transition taken place with your organization?

- Yes.
- No.
- Not applicable.

Q49. Is there a designated team responsible for overseeing regulatory compliance that may be relevant for QS transition?

- Yes.
- No.
- Not applicable.

Q50. Has your organization identified areas where collaboration may be needed for QS transition?

- Yes.
- No.
- Not applicable.

Q51. Has your organization communicated the collaboration needs to internal stakeholders?

- Yes.
- No.
- Not applicable.

Q52. Has your organization communicated the collaboration needs to external stakeholders?

- Yes.
- No.
- Not applicable.

Q53. Has your organization addressed the knowledge and skills needed for collaboration and governance for QS transition?

- Yes.
- No.
- Not applicable.

Q54. Has any collaboration or knowledge sharing with an expertise centre taken place with your organization?

- Yes.
- No.
- Not applicable.

Q55. Does your organization have an established governance structure to manage QS transition?

- Yes.
- No.
- Not applicable.

Q56. Does your organization collaborate with stakeholders to develop QS transition strategies?

- Yes.
- No.
- Not applicable.

Q57. Does your organization have a continuous collaboration structure in place after the implementation of (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q58. Does your organization have a continuous governance structure in place after the implementation of (hybrid) QS cryptographic solutions?

- Yes.
- No.
- Not applicable.

Q59. Does your organization provide up-to-date resources and training programs available to educate employees on collaboration and governance needs for the emerging security threats and challenges?

- ○ Yes.
- ○ No.
- ○ Not applicable.

Q60. Does your organization have a process in place that enables rapid adaptation to change in collaboration and governance for emerging security threats and challenges?

- ○ Yes.
- ○ No.
- ○ Not applicable.

This is the end of the assessment. Thank you for taking the time to fill out the assessment.

Results: Readiness Level of Your Organization

There are five levels of readiness for QS transition. The results of this assessment can be used to determine your organization's current readiness level. To do so, count the number of "Yes" responses to the assessment question. Based on this total, the organization's readiness level can be identified as shown in Table 1.

Table 1: QS Transition Readiness Levels Based on Assessment Response

Number of "Yes" Responses	Readiness Level
0-12	Level 1
13-24	Level 2
25-36	Level 3
37-48	Level 4
49-60	Level 5

Description of Readiness Levels for QS Transition

The readiness levels for QS Transition from level 1 to level 5 are described below in Table 2.

Table 2: Description of Readiness Levels for QS Transition (Level 1-5)

Level 1 Description	
Organization is unprepared and not ready for QS transition. There is lack of planning for QS transition and organization relies on ad-hoc solutions and processes.	
Organization	• Organization has little awareness on quantum threats & the need for QS transition. • Organization has limited knowledge on QS transition. • Organization has emerging insights about QS transition and its implication
Technology	• Organization has a basic understanding of the QS transition (e.g., potential security threats etc.) However, organization has not yet conducted risk and impact assessments. • Organization follows defined cryptographic policies & practices that are available in the industry.
Ecosystem	• Organization has an established communication channel to monitor QS transition. • Organization has informal forms of decision making and coordination to address QS transition governance.
Level 2 Description	
Organization is not ready for QS transition. Assessments have been conducted to identify potential risks and impacts for QS transition. The assessments serve as precursors to enable organization in their transition preparation.	
Organization	• Organization has evaluated the existing infrastructure to identify high risk where in the business processes may be affected. • Organization has identified the need for policy & regulations changes for QS transition. • Organization has identified vulnerable area in the existing systems.
Technology	• Organization has conducted assessments (e.g., risk, readiness, impact etc.) • Organization has identified QS cryptographic solutions requirements needed for the existing systems.
Ecosystem	• Organization has identified where collaboration is needed. • Organization has identified the need for QS transition governance.
Level 3 Description	
Organization is actively allocating resource and knowledge to prepare for QS transition. QS cryptographic solutions have been selected, and implementation strategies are outlined and communicated with stakeholders.	
Organization	• Organization prioritized critical vulnerabilities that require immediate attention for QS transition. • Organization has knowledge on selection of QS cryptographic solutions needed in their existing systems. • Organization has developed internal guidelines to support QS transition.
Technology	• Organization has specified the list of QS cryptographic solutions and developed an implementation plan. • Organization addresses security issues with a proactive approach.
Ecosystem	• Organization has communicated collaboration needs with stakeholders.\ • Organization has communicated the need for QS transition governance with stakeholders.
Level 4 Description	
Organization is ready and in transition. The changes are taking place to implement QS cryptographic solutions in the existing systems. Organization is monitoring their transitions to address emerging demands and challenges.	
Organization	• Organization has implemented QS cryptographic solutions in a smaller scale with the defined scope. • Organization fosters knowledge to utilize QS cryptographic solutions in the existing system. • Organization has adopted mandatory policies & regulations in place.
Technology	• Organization has executed the pilot plan to implement QS cryptographic solutions. • With on-going evaluation and adoption, organization improves cryptographic security measures.
Ecosystem	• Organization has achieved on-going collaborative actions with stakeholders. • Organization has an established governance processes to manage QS transition.
Level 5 Description	
Organization has fully implemented QS cryptographic solution across the existing systems and processes. Crypto-agility is integrated in its security strategies, enabling rapid adaptation to emerging security threats and evolving cryptographic risks	
Organization	• Organization has knowledge on the utilization of PQC in a scaled environment with different business processes. • Organization engages in continuous improvement and has best practices available for policies & regulations on QS transition. • Organization has a proactive approach to monitor future security needs and challenges.
Technology	• Organization has implemented QS cryptographic solutions in a scaled environment • Organization has a mature and resilient cryptographic security strategy with cryptographic agility as a fundamental component.
Ecosystem	• Organization has a continuous collaboration in place to support & receive guidance for QS transition. • Organization has an established governance process responsive to emerging security needs & challenges.

List of Recommendations per Readiness Level

Please see the list of recommendations that corresponds to the readiness level of your organization. Check whether these activities have taken place at your organization. To prepare your organization for a higher level of readiness, you should also review the recommendations for the next level. Based on the description of each readiness level (Table 2), Tables 3 through 7 provide the list of recommendations for organizations to progress from Level 1 to Level 5.

For example, if the level of readiness at your organization is currently assessed at Level 2 and the objective is to achieve Level 4, the organization should first review and confirm the list of recommendations at Level 2. Then, carefully review and apply the recommendations for Level 3 and 4. Ultimately, Level 5 should serve as the long-term target for all organizations.

Table 3: List of Recommendations for Level 1 Readiness

Level 1 Description	
Organization is unprepared and not ready for QS transition. There is lack of planning for QS transition and organization relies on ad-hoc solutions and processes.	
Level 1 Description per Category	
Organization	• Organization has little awareness on quantum threats & the need for QS transition. • Organization has limited knowledge on QS transition. • Organization has emerging insights about QS transition and its implication
Technology	• Organization has a basic understanding of the QS transition (e.g., potential security threats etc.) However, organization has not yet conducted risk and impact assessments. • Organization follows defined cryptographic policies & practices that are available in the industry.
Ecosystem	• Organization has an established communication channel to monitor QS transition. • Organization has informal forms of decision making and coordination to address QS transition governance.
List of Recommendations per Category	
Organization	• Identify emerging challenges & opportunities for QS transition • Establish communication channels to stay up-to-date on QS transition • Discuss potential impact of quantum threats (e.g., business process) and the need for QS transition • Gather knowledge on key concepts and technology related to QS transition • Connect with professionals, experts and organizations in your industry • Identify internal stakeholders & assess cross-departments collaboration opportunities • Ensure compliance with existing policies & regulations • Review current standards for interoperability, data privacy, security etc.
Technology	• Stay informed about PQC updates & industry standards • Discuss potential impact of quantum threats (e.g., business process) and the need for QS transition • Participate in working group & trainings on the topic • Follow defined cryptographic policies & practices • Adopt basic cryptographic measures based on organizations' needs • Identify industry standards & best practices
Ecosystem	• Identify emerging challenges & opportunities for QS transition • Establish communication channels to stay up-to-date on QS transition • Discuss tools, platforms, communication protocols • Identify internal stakeholders & assess cross-departments collaboration opportunities • Address concerns regarding quantum threats & identify (shared) objectives of QS transition • Identify internal stakeholders & assess cross-departments

Table 4: List of Recommendations for Level 2 Readiness

Level 2 Description	
Organization is not ready for QS transition. Assessments have been conducted to identify potential risks and impacts for QS transition. The assessments serve as precursors to enable organization in their transition preparation.	
Level 2 Description per Category	
Organization	• Organization has evaluated the existing infrastructure to identify high risk where in the business processes may be affected. • Organization has identified the need for policy & regulations changes for QS transition. • Organization has identified vulnerable area in the existing systems.
Technology	• Organization has conducted assessments (e.g., risk, readiness, impact etc.) • Organization has identified QS cryptographic solutions requirements needed for the existing systems.
Ecosystem	• Organization has identified where collaboration is needed. • Organization has identified the need for QS transition governance.
List of Recommendations per Category	
Organization	• Identify business processes and systems that could be impacted by quantum threats • Identify high risk areas in organization's assets, operations and critical data • Communicate the impact of quantum threats within organizations • Maintain contact with vendors to ask about their products and services with QS cryptographic solutions • Communicate relevance of QS technology within organizations • Identify current policy and regulation gaps for QS transition • Discuss informal industry standards & recommendations with industry experts, policy makers & regulatory bodies
Technology	• Assess cryptographic assets & data assets (e.g., Create a detailed list of the use of cryptography, both hardware and software, Identify the state of the data asset such as data at-rest, data in-transit, data in-use, location and value of the asset (CIA), Classify the assets into priorities) • Conduct risk and impact assessments • Identify potential implementation areas and requirements for QS cryptographic solutions • Monitor QS cryptographic solutions in the testing environment • Follow defined cryptographic policies & practices • Conduct risk assessment to identify vulnerabilities • Select appropriate cryptographic solutions based on the risk • Review the current security measures, policies, and protocols in place
Ecosystem	• Identify external stakeholders & potential partners for collaboration e.g., vendors • Review vendor contracts & progress of QS cryptographic solutions in their products etc. • Identify areas such as skills, technologies, or resources where collaboration may be needed (e.g., human, technological, financial) • Identify external stakeholders such as service providers, vendors etc. • Ensure that there is a designated point of contact across organizations (e.g., dedicated teams or working group for QS transition) • Identify current governance gaps for QS transition (e.g., roles, responsibilities & decision-making processes between internal and external stakeholder)

Table 5: List of Recommendations for Level 3 Readiness

Level 3 Description	
Organization is actively allocating resource and knowledge to prepare for QS transition. QS cryptographic solutions have been selected, and implementation strategies are outlined and communicated with stakeholders.	
Level 3 Description per Category	
Organization	• Organization prioritized critical vulnerabilities that require immediate attention for QS transition. • Organization has knowledge on selection of QS cryptographic solutions needed in their existing systems. • Organization has developed internal guidelines to support QS transition.
Technology	• Organization has specified the list of QS cryptographic solutions and developed an implementation plan. • Organization addresses security issues with a proactive approach.
Ecosystem	• Organization has communicated collaboration needs with stakeholders. • Organization has communicated the need for QS transition governance with stakeholders.
List of Recommendations per Category	
Organization	• Identify QS cryptographic solution requirements that may be specific to different areas • Assess compatibilities of QS cryptographic solutions in the existing infrastructure • Prepare implementation & adoption planning for QS cryptographic solutions • Participate in the expertise centre to share knowledge and resource • Selected QS cryptographic solutions needed in the existing infrastructure • Define roadmap, timeline, goal for the implementation of QS cryptographic solutions • Participate in consortium, conferences to connect and share knowledge • Monitor changes in external environments (e.g., regulatory changes, geopolitical developments) • Develop internal guidelines • Establish an internal team to follow-up with regulatory changes regarding QS transition • Monitor changes in the regulatory landscape
Technology	• Identify key features & functionalities for QS cryptographic solutions • Communicate tendering requirements for hardware and software in the life cycle management • Develop a plan for implementing QS cryptographic solutions (e.g., Select QS cryptographic solutions & products, Discuss the results of testing and validation, Conduct proof-of-concept) • Monitor QS cryptographic solutions in the testing environment • Establish criteria for acceptable level of risk • Develop a risk management plan • Create an overview of cryptographic inventory • Implement (new) security controls, policies and procedures to prevent security issues
Ecosystem	• Discuss QS transition and address collaboration need to relevant stakeholders • Maintain up-to-date contact with vendors • Define a shared vision, set common goals & targets for collaboration • Outline roles, responsibilities and decision making to monitor and manage QS transition • Communicate governance needs with stakeholders on roles, responsibilities and decision-making processes for QS transition • Discuss the need to allocate resource and coordinate QS transition with both internal and external stakeholders

Table 6: List of Recommendations for Level 4 Readiness

Level 4 Description	
Organization is ready and in transition. The changes are taking place to implement QS cryptographic solutions in the existing systems. Organization is monitoring their transitions to address emerging demands and challenges.	
Level 4 Description per Category	
Organization	• Organization has implemented QS cryptographic solutions in a smaller scale with the defined scope. • Organization fosters knowledge to utilize QS cryptographic solutions in the existing system. • Organization has adopted mandatory policies & regulations in place.
Technology	• Organization has executed the pilot plan to implement QS cryptographic solutions. • With on-going evaluation and adoption, organization improves cryptographic security measures.
Ecosystem	• Organization has achieved on-going collaborative actions with stakeholders. • Organization has an established governance processes to manage QS transition.
List of Recommendations per Category	
Organization	• Adopt & integrate new technology with QS cryptographic solutions in different areas of the systems • Provide necessary training to employees to foster knowledge across departments • Discuss areas where collaborations are needed • Have strategies in place for managing new technology with QS cryptographic solutions • Execute the transition plan to implement QS cryptographic solutions in the existing system while monitoring the progress • Provide trainings and resource needed to share knowledge via. workshops, seminars etc. • If available, join an expertise centre to share knowledge & develop expertise • Review and update internal policies and regulations that support QS transition • Build awareness on new policies and regulations on QS transition • Monitor changes in the regulatory landscape
Technology	• Pilot QS cryptographic solutions (with available products that support these solutions) • Monitor the performance and security of QS cryptographic solutions • Identify potential security concerns associated with QS cryptographic solutions & gather feedback on performance, security incidents and usability etc. • Recruit & train personnel with necessary skills and expertise on QS transition • Review cryptographic policies and practices • Emphasize cryptographic agility is emphasized in organization's security strategy • the organization's security strategy. • Engage with stakeholders to ensure that cryptographic practices are up-to-date • Provide regular security training for employees and stakeholders • Monitor potential threats & vulnerabilities in the existing infrastructure
Ecosystem	• Address lacking skills, technologies & resources within organization • Develop QS transition strategies with stakeholders involved • If available, join an expertise centre to share knowledge & develop expertise • Establish a framework for decision-making to ensure clear guidance and accountability etc. • Incorporate inputs & feedback from stakeholders • Provide training and support to ensure that skills and knowledge related to QS transition are fostered across the organization • Monitor and manage QS transition

Table 7: List of Recommendations for Level 5 Readiness

Level 5 Description	
Organization has fully implemented QS cryptographic solution across the existing systems and processes. Crypto-agility is integrated in its security strategies, enabling rapid adaptation to emerging security threats and evolving cryptographic risks	
Level 5 Description per Category	
Organization	• Organization has knowledge on the utilization of PQC in a scaled environment with different business processes. • Organization engages in continuous improvement and has best practices available for policies & regulations on QS transition. • Organization has a proactive approach to monitor future security needs and challenges.
Technology	• Organization has implemented QS cryptographic solutions in a scaled environment • Organization has a mature and resilient cryptographic security strategy with cryptographic agility as a fundamental component.
Ecosystem	• Organization has a continuous collaboration in place to support & receive guidance for QS transition. • Organization has an established governance process responsive to emerging security needs & challenges.
List of Recommendations per Category	
Organization	• Monitor and forecast market, regulatory change and emerging QS technology • Prepare for possible futures and action plans for different scenarios • Provide trainings and tools to stay-up-date and share knowledge on security & innovation • Track performance & collect data and gather feedback • Share knowledge and experience with industry best practices • Stay informed about industry trends, best practices, new developments etc. • Update internal knowledge base or policy manual, accessible to all stakeholders • Establish monitoring mechanisms to review and update policies & regulations • Provide additional training and share best practices available.
Technology	• Assess whether QS cryptographic solutions implemented in the systems meet KPIs • Identify areas of improvement & lessons learned • Plan a full rollout across organizations • Document findings and share knowledge • Follow compliance requirements & industry standards • Prepare trainings during and after the scaled deployment • Conduct regular security assessments • Integrate cryptographic agility as part of organization's security strategy • Provide real-time feedback & share lesson-learned with employees and stakeholders • Allocate organization's resource to support changing organizational needs based on new threats, insights, regulatory and technology changes
Ecosystem	• Share industry best practices & collaborate in initiatives on security & innovation • Build a continuous collaboration to maintain and integrate cryptographic agility across organizations • Evaluate organization's governance framework & identify areas for improvement • Establish a process that can adapt to changes in future security needs & challenges