(DRAFT FOR PUBLIC CONSULTATION)

QUANTUM READINESS INDEX

2025

CSA SINGAPORE
Cyber Security Agency of Singapore

10 YEARS OF SECURING OUR CYBERSPACE

Table of Contents

Developed in consultation with

This document is published by the Cyber Security Agency of Singapore, in consultation with partners across the quantum-safe communities listed in alphabetical order:

- A*STAR
- Accenture
- Deloitte
- evolutionQ
- SGTech
- SpeQtral
- World Economic Forum

Disclaimer

Users should use this document in conjunction with the Quantum-Safe Handbook as a resource. This document is intended for informational purposes only and is not mandatory, prescriptive nor exhaustive.

The information provided in this document does not, and is not intended to, constitute legal advice. All information is for general informational purposes only. These organisations provided views and suggestions on the framing, descriptions of the objectives, and recommendations included in this document. CSA and its partners shall not be liable for any inaccuracies, errors and/or omissions contained herein nor for any losses or damages of any kind (including any loss of profits, business, goodwill, or reputation, and/or any special, incidental, or consequential damages) in connection with any use of this document. Organisations are advised to consider how to apply the recommendations within the document to their specific circumstances, in addition to other measures relevant to their needs. This document contains links to other third-party references. Such links are informational and do not represent endorsement of content from these third-party references.

Preface

The quantum technology landscape is evolving rapidly and much remains uncertain. The exact timeline for "Q-day" – when a quantum computer capable of breaking today's cryptography becomes available – cannot be predicted with precision. Nor can we be fully certain about how the technology will develop or which quantum safe implementation approaches will prove most effective. The issue is complex, dynamic, and subject to scientific breakthroughs and geopolitical shifts.

Despite this uncertainty, the collective assessment is that preparation must begin now, especially for critical systems where the risks of inaction are greatest. Governments around the world are starting to take steps, experimenting with different approaches and refining methods as experience is accumulated.

At the same time, rushing ahead indiscriminately or in isolation is not encouraged. Some actions are "no-regrets" steps that can and should be taken immediately. Others are less well understood and require more monitoring and careful evaluation, as early movement could bring unintended costs or first-mover disadvantages.

The publications by CSA therefore seek to provide guidance and a set of practical measures. They reflect the collective stance: to begin readiness in a measured, deliberate way whilst staying adaptive to emerging knowledge and standards.

Executive Summary

Quantum computers are poised to revolutionise computing by solving some computational problems exponentially faster than classical computers. While their transformative potential is immense, quantum computers can also pose significant cybersecurity threats. In anticipation of the availability of quantum computers, threat actors can launch harvest now, decrypt later (HN-DL) attacks where encrypted data is stolen in anticipation of a quantum computer to decrypt it in the future.[1] The threats may not just compromise confidentiality through HN-DL attacks but could also undermine integrity and authenticity through the forgery of digital signatures. Recognising these impending quantum-enabled threats, international bodies have been advocating the importance of planning for quantum safe migration through guidance, strategies and standards.

The journey towards quantum safe migration is resource intensive and may take organisations many years to fully migrate their systems. Organisations grapple with the challenge of contextualising international guidance to their current state of readiness. In particular, organisations do not know where they stand in the quantum safe migration journey and what the next steps are. Having a self-assessment of preparedness through the Quantum Readiness Index (QRI) can help organisations address quantum-enabled threats and enable them to plan, prioritise and execute quantum-safe migration effectively.

The QRI allows organisations to understand their levels of readiness and enables them to prioritise quantum-safe migration action areas. It also facilitates conversations with organisational leaders and the Board about the state of readiness to address quantum-enabled threats and can be used to seek buy-in on the recommended steps to strengthen their readiness. The QRI is intended for organisations that lack the awareness of the quantum threats and are keen to undertake immediate “no-regrets moves” towards quantum safety. The primary users of the QRI are leaders and decision-makers who have responsibilities for managing technology and mitigating cybersecurity risks within an organisation. The QRI is intended to be a voluntary resource for organisational use and is not mandatory or compliance based.

The QRI is consistent with the five principles outlined in the World Economic Forum (WEF)’s Quantum Readiness Toolkit, with readiness levels adapted from the Capability Maturity Model Integration (CMMI) of the Information Systems Audit and Control Association (ISACA). The QRI was developed in collaboration with experts from the industry listed in an earlier section.

[1] https://www.ietf.org/archive/id/draft-ietf-pquip-pqc-engineers-02.html

The QRI has been designed using the constructs of domains, objectives, levels and recommendations. A domain refers to an organisational aspect to address the quantum-enabled threat. It comprises various quantum safe objectives that manifest the intent of the domain. The domains are namely **Governance, Risk Assessment, Training and Capability, External Engagement** and **Technology**. The levels indicate the readiness of organisations for each objective. Understanding the levels enables the identification of recommended next steps to improve the security posture for each objective.

To use the QRI, organisations answer a series of questions aligned with objectives under the domains. Upon completion of all questions in the QRI, the readiness level for each objective and recommendations on the next steps are shown. Organisations can subsequently develop action plans based on suggested recommendations by referring to guidance in the **Quantum-Safe Handbook** and implementing these plans. This process is repeated periodically to assess progress after the implementation of the plans and to reflect developments in the operating environment.

https://go.gov.sg/qri

1. Introduction

Quantum computing offers opportunities for transformation in applications and environments where fast and efficient calculations are required. Quantum computers can solve some computational problems exponentially faster than classical computers leading to advances such as optimised routing, better pharmaceutical designs, and faster and more granular financial models. While quantum computers will enable some types of calculations to be done exponentially faster than classical computers, such capabilities can be used by threat actors to compromise existing cryptographic algorithms that rely on hard mathematical problems. Although a Cryptographically Relevant Quantum Computer (CRQC) does not exist today, there is an attack known as harvest now, decrypt later (HN-DL) where an attacker steals encrypted data in anticipation of a CRQC to decrypt it. Quantum-enabled threats may not be limited to HN-DL attacks through compromised confidentiality but could also undermine integrity and authenticity through the forgery of digital signatures. Recognising these impending quantum-enabled threats, international bodies have been advocating the importance of planning for quantum safe migration through guidance, strategies and standards.

To address the HN-DL and other quantum-enabled threats, the cryptographic community has been developing Post Quantum Cryptographic (PQC) standards and protocols. These standards, coupled with existing cybersecurity controls, uplift readiness to address quantum-enabled threats. Quantum cryptographic technologies, such as Quantum Key Distribution (QKD) complements PQC to safeguard information and the digital communication infrastructure.

While quantum safe technologies are nascent and evolving, international bodies and governments have put forth guidance on quantum safe readiness and migration in anticipation of the arrival of the CRQC. For example, the cryptographic community has been developing Post Quantum Cryptographic (PQC) standards and protocols. These standards, coupled with quantum safe guidance and controls, uplift readiness to address quantum-enabled threats. In the midst of such a landscape where a plethora of sources is available, organisations still find it a challenge to understand where they stand in terms of quantum readiness and navigate towards quantum safety.

The journey towards quantum safe migration is resource intensive and may take organisations many years to fully migrate their systems. Organisations grapple with the challenge of contextualising international guidance to their current state of readiness. In particular, organisations do not know where they stand in the quantum safe migration journey and what the next steps are. The QRI addresses this challenge by helping organisations self-assess their preparedness against quantum-enabled threats, enabling them to plan, prioritise and execute quantum-safe migration.

2. Purpose and Objectives of the QRI

The QRI provides a self-assessment of an organisation's preparedness to address quantum-enabled threats. It allows organisations to understand their levels of readiness and enables them to prioritise quantum-safe migration action areas. It also facilitates conversations with organisational leaders and the Board about the state of readiness to address quantum-enabled threats and can be used to seek buy-in on the recommended next steps to strengthen their readiness.

As organisations vary in size, industry and maturity, the guidance and recommendations provided through the QRI is suggestive rather than exhaustive. Each organisation needs to develop its own quantum security migration action plan, with the QRI serving as a starting point for organisations to develop their quantum readiness strategy and action plan. As a voluntary self-assessment questionnaire, the QRI does not prescribe minimum readiness levels and is intended to help organisations track their progress in their journey towards quantum safety.

The QRI is consistent with the five principles of the World Economic Forum (WEF)'s Quantum Readiness Toolkit (QRT), with readiness levels adapted from the Capability Maturity Model Integration (CMMI) of the Information Systems Audit and Control Association (ISACA).

3. Target Audience

The QRI is intended to be used by organisations that want to raise their awareness of the quantum-enabled threats and undertake "no-regrets moves" in their journey towards quantum safety. The primary users of the QRI are leaders and decision-makers who have responsibilities for managing technology and mitigating cybersecurity risks within an organisation. Examples of key users include the C-suite and other senior leaders responsible for leading quantum-safe migration for the organisation:

- Chief Information Officers,
- Chief Information Security Officers,
- Chief Data Officers,
- Chief Technology Officers,
- Chief Risk Officers, and
- Other senior leaders responsible for leading quantum-safe migration for the organisation.

4. Constructs of the QRI

The QRI is based on the constructs of **domains, objectives** and **levels**. In-depth details of the domains, objectives, levels and recommendations can be found in **Annex A**.

4.1 Domains and Objectives

The domains of the QRI are consistent with the five principles of the World Economic Forum (WEF)'s Quantum Readiness Toolkit, which are organisational aspects to address quantum-enabled threats. Each domain comprises various objectives relevant to the intent of the domain. The domains are namely **Governance, Risk Assessment, Training and Capability, External Engagement** and **Technology**. Table 1 provides the descriptions for each QRI domain.

WEF Quantum Readiness Toolkit Principle	QRI Domain	Description
Ensure the organisational governance structure institutionalises quantum risk	**Governance**	Governance structures institutionalise quantum risk management and enable systematic implementation through appropriate policies, procedures, organisational champions and resources.
Treat and prioritise quantum risk alongside existing cyber risks	**Risk Assessment**	Risk assessment relates to identifying crown jewels and prioritising critical business functions for quantum-safe migration that is supported by cryptographic asset management.
Raise quantum risk awareness throughout the organisation	**Training and Capability**	Training and capability relate to educating stakeholders on quantum risks and quantum-safe migration, as well as develop essential competencies for quantum-safe migration.
Encourage collaboration across ecosystems	**External Engagement**	External engagement is essential to understand organisational risk exposure of products/services from third party vendors, as well as to leverage the ecosystem on information regarding identified risks, experiences and insights in implementing quantum safe migration.
Make strategic decisions for future technology adoption	**Technology**	Technology involves organisations to think ahead and conduct technology experimentation and proof of concept projects to assess quantum safe technologies.

Table 1. Descriptions of QRI domains

The **domains** and their respective **objectives** of the QRI are illustrated below in Figure 1.

Figure 1: Domains and Objectives of the QRI

4.2 Levels

The **levels** of the QRI are adapted from maturity levels in the Capability Maturity Model Integration (CMMI) framework from Information Systems Audit and Control Association (ISACA). The levels indicate the degree of readiness in meeting the objectives and enables the identification of organisational gaps and recommendations to improve the readiness for each objective. Each **objective** has four **levels** (L0, L1, L2 and L3), with the description of each level found in Table 2.

CMMI Maturity Levels	QRI Level	Description of QRI Level
Maturity Level 0: Incomplete Ad hoc and unknown	**L0 - Not started**	The organisation has not begun the quantum-safe migration journey and does not have capabilities to meet the intent of the objective.
Maturity Level 1: Initial Unpredictable and reactive. **Maturity Level 2: Managed** Managed on the project level.	**L1 - Initial**	The organisation has begun exploring the quantum threat and has started work on meeting the intent of the objective.
Maturity Level 3: Defined Organisation-wide standards provide guidance across projects, programs, and portfolios.	**L2 - Defined**	The organisation has defined an organisational wide approach to meet the intent of the objective.
Maturity Level 4: Quantitatively Managed Measured and controlled. Organisation objectives are predictable and align to meet the needs of stakeholders. **Maturity Level 5: Optimising** Stable and flexible. Organization continuously improves, pivots and responds to opportunity and change.	**L3 -Operational**	The organisation's capabilities in the objective have been deployed operationally and are continuously improved.

Table 2: Description of each QRI level

4.3 Assessment results and recommendations

The assessment results are automatically computed per objective after submitting the responses to all the questions and are reflected as **current level**. Based on the current level, the QRI provides **recommendations** as next steps an organisation can take to progress in the quantum-safe migration journey (i.e. **next level** after the current level). These recommendations serve as informative guidance rather than prescriptive requirements, with references to the relevant portions of the Quantum-Safe Handbook where possible.

An illustrative example of assessment results and suggested recommendations is shown in Table 3 below.

Domain/Objective	Current Level	Next Level (+1)	Suggested Recommendations to improve to Next Level
Governance			
Objective 1	0	1	Identify and appoint organisation champions for quantum readiness....
Objective 2	0	1	Initiate discussions....
Objective 3	1	2	Include quantum risk....
Objective 4	3	-	Keep up the continuous effort towards quantum-safety!
Risk Assessment			
Objective 1	0	1	Perform a preliminary quantum risk assessment.....
Objective 2	1	2	Perform a comprehensive inventorisation of all high value....
Training & Capability			
Objective 1	1	2	Establish a quantum-safe migration information programme....
Objective 2	2	3	Develop a matrix on competencies....
External Engagement			
Objective 1	1	2	Perform an in-depth, risk-based evaluation....
Objective 2	2	3	Contribute experiences and insights....
Objective 3	0	1	Establish a watchlist....
Objective 4	3	-	Keep up the continuous effort towards quantum-safety!
Technology			
Objective 1	0	1	Identify use cases as a basis....
Objective 2	1	2	Define cryptographic agility considerations....

Table 3: Illustrative assessment results and recommendations for an organisation using the QRI

4.4 Report

Upon submission of the responses to questions at https://go.gov.sg/qri, the assessment results and suggested recommendations will be compiled in a pdf report and automatically sent as an attachment via the indicated email (see Figure 3 for an example of a sample QRI report).

Quantum Readiness Index (QRI) Report for Quantumania

Dear **Scott Lang**,

Based on your responses, the QRI readiness levels for your organisation are shown in the table below.

The table below also provides some recommendations for your organisation to improve your quantum-safe posture.

For further guidance, please refer to CSA's Quantum-Safe Handbook.

Legend

Level	
0	Not started
1	Initial
2	Defined
3	Operational

Governance

Objectives	Current Level	Next Level	Recommendations
Objective 1: Establish formal governance structure for mandate on migrating to quantum safety	1	2	**Establish a formal governance body led by an organisational champion** • Create a Quantum-Safe Governance Committee or integrate the function into an existing risk/technology committee. • Define formal roles and responsibility of the governance body
Objective 2: Establish a strategic quantum-safe roadmap for implementation of initiatives	1	2	**Develop a strategic quantum safe roadmap** • Define key building blocks of the strategic quantum safe roadmap such as but not limited to: o Vision and objectives o Timeline and milestones o Resourcing needs o Roles and responsibilities o Quantum safe initiatives
Objective 3: Integrate quantum risks into existing cyber risk management programme	2	3	**Review the effectiveness in managing quantum risk as part of the cybersecurity risk management programme** • Regularly review the effectiveness in managing quantum risk to inform updates to quantum-safe migration timelines and dependencies • Refine quantum risk tolerance based on changing business needs and evolving ecosystem developments
Objective 4: Develop and implement policies and frameworks that guide the migration to quantum safety	1	2	**Develop quantum-safe policy** • Develop and document formal policy including but not limited to: o Cryptographic policy o Key management policy o Data protection policy

Figure 3. Sample QRI Report

5. Process flow of using the QRI

The organisation starts the self-assessment process by accessing https://go.gov.sg/qri and answering assessment questions organised according to objectives. The organisation is shown the readiness level and recommended next steps for each objective. The organisation then develops action plans leveraging the guidance in the Quantum-Safe Handbook and implements these plans. This process is repeated periodically after the plans are implemented and to reflect developments in the operating environment (see Figure 4 for the flow of using the QRI).

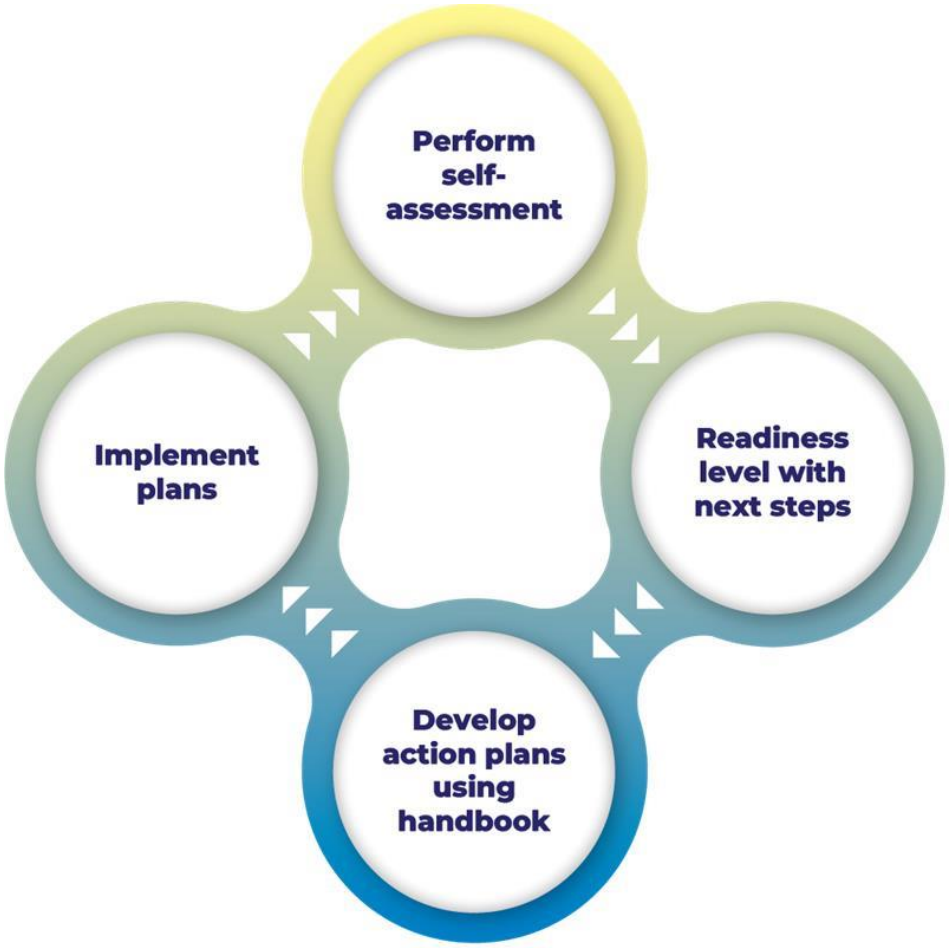

Figure 4. Flow of using the QRI

6. Conclusion

Achieving quantum readiness is a progressive journey that requires multi-year planning, preparation and execution. The QRI enables organisations to measure their readiness as they prepare to embark on the migration towards quantum safety and provide recommended next steps in the domains of Governance, Risk Assessment, Training and Capability, External Engagement and Technology. As a self-assessment resource, organisations can use it as a first step to understand where they are in the journey towards quantum readiness and subsequently develop its own quantum safe action plan using guidance in the Quantum-Safe Handbook as a resource.

Glossary of Key Terms

Terms and Definitions	
Asymmetric key algorithm	A cryptographic algorithm that uses a public-private key pair for encryption and is sometimes referred to as a public key algorithm.
Symmetric key algorithm	A cryptographic algorithm that uses the same key for both encryption and decryption.
Cryptographically relevant quantum computers (CRQC)	A quantum computer that is powerful enough to break a cryptographic algorithm, especially an asymmetric cryptographic algorithm.
Domain	A specific organisational aspect to address the quantum-enabled threat.
Harvest Now Decrypt Later (HN-DL) attack	A strategy where an attacker steals encrypted data now and waits for a quantum computer to decrypt it.
Post Quantum Cryptographic (PQC) algorithm standards	New cryptographic algorithm standards that are theoretically resistant to threats by quantum computers.
Quantum Key Distribution (QKD)	A secure communication method that uses quantum mechanics to create and exchange encryption keys.

References

Accenture. (November 2023). *Moving Toward a Quantum Security Maturity Index*.

AIVD Netherlands. (June 2023). *The PQC Migration Handbook*.

BSI Germany. (May 2022). *Quantum Safe Cryptography*.

CFDIR. (June 2023). *Canadian National Quantum-Readiness, Best Practices and Guidelines*.

Deloitte. (April 2025). *Cryptographic Resilience Community Profile (Initial Draft)*.

ETSI. (July 2020). *Migration to Quantum Safety*.

evolutionQ. (January 2017). *A Methodology for Quantum Risk Assessment*.

FS-ISAC. (2023). *Preparing for a Post-Quantum World by Managing Cryptographic Risk*.

HAPKIDO. (2024). *Organisational Readiness Model for Quantum-safe Transition*.

ISACA. (2022). *Cybersecurity Capability Maturity Model v2.1*.

NIST. (December 2016). *PQC Standardization Process*.

NIST. (March 2019). *NIST SP-800-131: Transitioning the Use of Cryptographic Algorithms and Key Lengths*.

NIST. (May 2023). *NICE Framework for Workforce Cybersecurity*.

NIST. (September 2020). *NIST SP.800-53 rev 5: Security and Privacy Controls for Information Systems and Organisations*.

Quantum Insider. (February 2023). HNDL, The Truth Behind This Common Quantum Theory.

US White House. (November 2022). *M-23-02 Migrating to Post-Quantum Cryptography*.

World Economic Forum. (June 2023). *Quantum Readiness Toolkit*.

Annex A – QRI Domains, Objectives, Levels and Recommendations

The objectives, levels and recommendations within each domain are described below:

Governance (GV)

Governance structures institutionalise quantum risk management and enable systematic implementation through appropriate policies, procedures, organisational champions and resources.

Objective 1. Establish formal governance structure for mandate on migrating to quantum safety *Formal governance structures institutionalise the mandate for migration to quantum safety through clear accountability and decision making, led by an organisational champion.*	
Rationale: A formal governance structure enables a strong organisational mandate for migrating to quantum-safety by defining organisational responsibilities and decision-making processes.	
Level	**Descriptors**
L0	The organisation has not identified a champion or cross-functional team to institutionalise the migration to quantum safety. No formal governance structure exists to address these areas.
L1	The organisation has identified a champion or cross-functional team to institutionalise the migration to quantum safety. However, their roles and responsibilities remain informal, and activities are conducted on an ad-hoc basis.
L2	The organisation has established a formal governance structure led by an organisational champion, such as a dedicated committee, with clearly defined roles and responsibilities to institutionalise the migration to quantum safety.
L3	The organisation has convened the governance structure and is continuously evaluating the roles, responsibilities and processes of the governance structure and refining them in tandem with evolving requirements.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Identify and appoint organisation champions for quantum readiness**

	• Assign senior personnel with domain knowledge in data management, cryptography, risk or infrastructure as the initial point of contact for quantum readiness. **Establish functional team to coordinate quantum-safe initiatives** • Form a cross-functional team comprising of stakeholders such as security officers, engineers, IT managers and legal representatives to support the champion in coordinating quantum-safe initiatives.
L1	**Establish a formal governance body led by an organisational champion** • Create a Quantum-Safe Governance Committee or integrate the function into an existing risk/technology committee • Define formal roles and responsibility of the governance body.

L2	**Establish a review cycle for governance effectiveness**
	• Assess on a regular basis:
	  ○ Governance objectives versus outcomes
	  ○ Relevance of definitions of roles and responsibilities
	  ○ Engagement levels of cross-functional teams
	• Refine governance process through feedback and evolving requirements

L3	Keep up the continuous effort towards quantum-safety!

Objective 2: Establish a strategic quantum-safe roadmap for the implementation of initiatives *A comprehensive implementation plan with clear objectives, resource requirements and timelines for quantum-safe initiatives.*	
Rationale: A comprehensive implementation plan ensures effective planning, prioritisation and execution of quantum-safe initiatives through clear milestones and resource allocation. This provides the ability of organisations to measure their progress over time.	
Level	**Descriptors**
L0	The organisation has not developed plans or allocated resources for quantum safe initiatives.
L1	The organisation has initiated discussions about quantum safe initiatives, but formal plans await finalisation and approval for integration into broader organisational strategies.
L2	The organisation has developed a strategic roadmap for quantum-safe initiatives, outlining objectives, resource requirements and implementation timelines.

L3	The organisation is executing its strategic roadmap for quantum safe initiatives with allocated resources and defined timelines. Progress is continuously monitored, and the roadmap is regularly updated to align with organisational priorities.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Initiate discussions to estimate migration costs and timelines** • Identify budgetary needs and identify the timeframe the budget is needed • Develop a cost-benefit analysis to support early investment requests.
L1	**Develop a strategic quantum safe roadmap** • Define key building blocks of the strategic quantum safe roadmap such as but not limited to: o Vision and objectives o Timeline and milestones o Resourcing needs o Roles and responsibilities o Quantum safe initiatives
L2	**Operationalise the planned initiatives according to the roadmap** • Begin rolling out the initiatives in phases and track execution **Update the roadmap on a regular basis** • Update planned initiatives on the roadmap periodically
L3	Keep up the continuous effort towards quantum-safety!

Objective 3: Integrate quantum risks into existing cyber risk management programme *Treatment of quantum risks alongside other cyber risks under the organisation's cyber risk management programme.*	
Rationale: Addressing quantum risks alongside other existing cybersecurity risks as part of an organisation's risk management approach enables organisations to make holistic and informed decisions in risk mitigation.	
Level	**Descriptors**
L0	The organisation does not view quantum risks as risks to be addressed.
L1	The organisation acknowledges that quantum risks need to be addressed and has taken initial steps to address them. However, the risks are treated separately from existing cybersecurity risks.
L2	The organisation has integrated quantum risks into its cybersecurity risk management programme, treating quantum risks alongside existing cybersecurity risks.
L3	The organisation continuously evaluates and tracks the effectiveness in managing quantum risks.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Seek leadership buy-in for quantum risks to be addressed** • Explain that quantum risks are long-tail risks and why planning to address the risks is crucial for business continuity • Conduct executive briefings on quantum threats, highlighting potential business areas that process data which are sensitive and with long shelf life (e.g. customer PII, trade secrets, financial records).
L1	**Include quantum risks into the enterprise cybersecurity risk management programme** • Treat quantum risks alongside existing cybersecurity risks. • Determine how quantum risks can affect other identified enterprise risks.
L2	**Review the effectiveness in managing quantum risks as part of the cybersecurity risk management programme** • Regularly review the effectiveness in managing quantum risks to inform updates to quantum-safe migration timelines and dependencies. • Refine quantum risk tolerance based on changing business needs and evolving ecosystem developments.
L3	Keep up the continuous effort towards quantum-safety!

Objective 4: Develop and implement policies and frameworks that guide the migration to quantum safety *Policies and frameworks guide the organisation's migration to quantum safety.*	
Rationale: Well-structured policies and frameworks provide clear direction and guidance for quantum-safe initiatives while ensuring alignment with organisational strategy.	
Level	**Descriptors**
L0	The organisation has no established policies or frameworks for data, cryptography and quantum risk management.
L1	The organisation has no formal policies or frameworks, but has implemented basic measures for data, cryptography and quantum risk management, including preliminary key storage practices and data classification procedures.
L2	The organisation has developed formal policies and frameworks for data, cryptography and quantum risk management, but these are not fully implemented yet.
L3	The organisation implements and maintains comprehensive policies and frameworks for data, cryptography and quantum risk management. These undergo regular review and updates to align with evolving requirements, including post-quantum cryptography adoption.
Recommendations	
For level	**Suggested recommendations to progress to next level**

L0	**Implement basic practices**
	• Introduce fundamental practices such as:
	  ○ Ad-hoc cryptographic key protection guidelines
	  ○ Classification of sensitive data

L1	**Develop quantum-safe policy**
	• Develop and document formal policy including but not limited to:
	  ○ Cryptographic policy
	  ○ Key management policy
	  ○ Data protection policy

L2	**Establish policy review cycles**
	• Review policy outcomes on a regular basis:
	  ○ Determine the need for policy updates in response to industry, technology and/or regulatory developments
	  ○ Adjust controls based on policy updates

L3	Keep up the continuous effort towards quantum-safety!

Risk Assessment (RA)

Risk assessment relates to identifying crown jewels and prioritising critical business functions for quantum-safe migration enabled through cryptographic asset management.

Objective 1: Perform quantum risk assessment and prioritise affected assets and data *Systematic assessment of quantum risks enables prioritisation of affected assets and data and facilitates decision-making for quantum safe migration.*	
Rationale: Performing systematic quantum risk assessments enables the organisation to make informed decisions on the priority areas for quantum safe migration. It helps quantify exposure to quantum risks, assess the value and shelf life of data and identify critical systems that should be prioritised for protection.	
Level	**Descriptors**
L0	The organisation has not begun assessing quantum risks or evaluating potential impact on its data and cryptographic assets.
L1	The organisation has begun preliminary quantum risk assessments to understand and quantify potential business impact, but such assessments are informal and limited in scope.
L2	The organisation has conducted an organisation-wide quantum risk assessment using a systematic methodology that is based on the value and shelf life of data, understanding of cryptographic vulnerabilities and asset prioritisation.
L3	The organisation regularly conducts quantum risk assessments, continuously refining the process to address evolving needs.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Perform a preliminary quantum risk assessment for a subset of key systems** • Perform an initial risk assessment for a subset of key systems to estimate business impact if cryptography is compromised

L1	**Perform a comprehensive quantum risk assessment for all key systems**
	• This is conducted across the entire organisation, with the following formally documented in the enterprise cyber risk register:
	  ○ Risk Scenarios
	  ○ Impact on organisation
	  ○ Likelihood of occurrence
	  ○ Risk level
	  ○ Risk appetite

	○ Remediation and mitigation • Prioritise remediation or treatment based on the risk level
L2	**Continuously refine the quantum risk assessment methodology** • Refine assessments based on updates and feedback, including new NIST PQC standard updates and evolving business priorities.
L3	Keep up the continuous effort towards quantum-safety!

Objective 2: Implement cryptographic asset management *Identify key systems that handle high-value data and document their associated cryptographic modules (such as hardware security modules, PKI, cryptographic libraries), sensitivity and confidentiality levels of the data. This will provide the basis for understanding the cryptographic assets for these systems (e.g. keys, certificates, algorithms, protocols).*	
Rationale: The understanding of key systems that handle high-value data and their associated cryptographic assets enables the organisation to evaluate the risk exposure to quantum threat. This approach allows organisations to focus on key areas that should be prioritised for quantum-safe migration.	
Level	**Descriptors**
L0	The organisation has not begun identifying key systems that handle high-value data nor documented their associated cryptographic assets and cryptographic dependencies.
L1	The organisation has taken initial steps to identify a subset of key systems that process high-value data and their associated cryptographic assets and cryptographic dependencies.
L2	The organisation has a comprehensive inventory of all key systems that handle high-value data and associated cryptographic assets and cryptographic dependencies. Inventories include fields such as data classification, system criticality and cryptographic details.
L3	The organisation's cryptographic inventory is regularly updated to inform quantum-safe migration planning.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Identify a subset of high-value business systems and cryptographic assets** • List key systems that process high-value data such as but not limited to: ○ Personally Identifiable Information (PII)

	○ Regulated financial/health data ○ Intellectual property or trade secrets • For each high-value system, include data classification (e.g. public, confidential, secret) and estimated data shelf-life. • For identified systems, begin capturing cryptographic assets such as: ○ Cryptographic Modules and Application (Library, HSM, VPN) ○ Certificates (e.g. used by TLS, S/MIME) ○ Keys (e.g. RSA, ECDH) ○ Protocols (e.g. TLS, SSH, IPSEC) **Understand cryptographic dependencies** • Begin mapping cryptographic dependencies such as products, applications, processes that rely on cryptography.
L1	**Perform a comprehensive inventorisation of all high-value systems and cryptographic assets through automated cryptographic discovery** • Deploy or pilot tools to augment cryptographic discovery • Include asset inventory of remaining high-value systems and cryptographic assets
L2	**Monitor asset changes and update asset inventory** • Monitor and update changes to inventory of high-value systems and cryptographic assets regularly
L3	Keep up the continuous effort towards quantum-safety!

Training and Capability (TC)

Training and capability relate to educating stakeholders on quantum risks and quantum-safe migration as well as develop essential competencies for quantum-safe migration.

Objective 1: Educate organisational stakeholders on quantum risks and importance of quantum-safe migration *Awareness and education on quantum computing risks and the importance of quantum safe migration gives the organisation the impetus to address quantum-enabled threats.*	
Rationale: Educating organisation stakeholders on quantum-safe migration ensures the awareness of quantum computing risks and provides the impetus to drive quantum safe initiatives. This would minimise the spread of fear, uncertainty and doubt about quantum-enabled threats.	
Level	**Descriptors**
L0	The organisation has no awareness of quantum computing risks and its impact on critical digital assets.
L1	The organisation recognises the importance of quantum safety, with initial steps taken to educate themselves on quantum-safe migration.
L2	The organisation has established an awareness programme to educate stakeholders of quantum risks and what quantum-safe migration entails and aligns these activities to the organisation's strategic goals and priorities.
L3	The organisation has implemented an awareness programme to educate stakeholders of quantum risks and what quantum safe migration entails, with regular evaluation of its effectiveness and enhancement of the programme based on feedback. The organisation looks ahead and stays up to date with the latest development of quantum-safe migration approaches.
Recommendations	
For level	**Suggested recommendations to progress to next level**

L0	**Obtain C-level and senior management support**
	• Raise the awareness among C-level and senior management by:
	  ○ Outlining what quantum computing is and explaining why it is a business risk
	  ○ Highlighting risks such as "harvest now, decrypt later" and the lifespan of current data
	
	Conduct ad-hoc information sessions across all organisational levels
	• Develop introductory materials such as:

	○ One-pagers or infographics on quantum threats ○ Internal blog posts or newsletters ○ Short videos or email explainers
L1	**Establish a quantum-safe migration information programme** • Customise content for different audiences (strategic, operational, technical): ○ Strategic risk, timing and resource allocation to address quantum-enabled threats for strategic ○ Dependency mapping and interlinkages across systems and processes for operational ○ Technical readiness and limitations of existing systems
L2	**Establish metrics and feedback mechanisms to track programme effectiveness** • Track information programme effectiveness by measuring metrics such as: ○ Completion rates of training modules ○ Surveys (e.g. post-training quizzes) **Improve the programme through monitoring and feedback** • Regularly review the programme: ○ Training content relevance and clarity ○ Incorporate latest regulatory, technological, and threat updates
L3	Keep up the continuous effort towards quantum-safety!

Objective 2: Develop the necessary competencies to effectively drive quantum-safe migration *Essential competencies that enable the organisation to implement quantum safe initiatives.*	
Rationale: Building competencies in quantum computing risks and quantum safe technologies enable the organisation to effectively assess, plan and implement quantum safe measures.	
Level	**Descriptors**
L0	The organisation has not identified essential competencies needed for quantum-safe migration, including cryptography and key management.
L1	The organisation has identified key areas of competency required for quantum-safe migration but has not yet started developing it.
L2	The organisation has developed a matrix on the required competencies for specific roles to enable quantum-safe migration.
L3	The organisation has developed and is maintaining a matrix for all relevant roles, updating competency requirements for each role based on evolving needs.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Identify and build competencies** • Build knowledge base from authoritative sources such as NIST, WEF and CFDIR for quantum-safe guidance or by attending relevant quantum security webinars, workshops, or industry panels for competency development

L1	**Develop a matrix on competencies for specific roles**
	• Describe competencies according to roles or team functions. For example,
	  ○ Cryptographers/Engineers → PQC primitives, configuration, cryptographic security levels
	  ○ GRC teams → cryptographic and policy requirements
	  ○ Procurement → vendor cryptographic posture assessments
	
	Establish a training plan
	• Structure the plan to include:
	  ○ Internal briefings or targeted training sessions
	  ○ Certification opportunities (if available)
	  ○ Access to public resources (e.g. ETSI, NIST webinars)

L2	**Develop a matrix on competencies for all relevant job roles and update the matrix to address evolving needs**
	• Periodically review and revise:
	  ○ Role requirements as the organisation progresses through quantum-safe migration
	  ○ Training materials based on evolving needs

L3	Keep up the continuous effort towards quantum-safety!

External Engagement (EE)

External engagement is essential to understand organisational risk exposure of the products/services from third party vendors, as well as to leverage the ecosystem on information regarding identified risks, experiences and insights in implementing quantum safe migration.

Objective 1: Evaluate and manage vendors and other third parties to address supply chain risks *Evaluation of quantum risk exposure from vendors and third parties based on data access, business criticality and quantum readiness.*	
Rationale: Vendors and other third parties often have access to sensitive systems and data, making them potential weak links in the organisation's quantum-safe migration efforts. Evaluating third-party risks enables holistic quantum-safe migration planning and strengthens supply chain security.	
Level	**Descriptors**
L0	The organisation has not assessed the quantum risk of vendors and other third parties.
L1	The organisation recognises the quantum risks posed by vendors and other third parties and has initiated risk evaluations.
L2	The organisation has assessed third-party quantum risk based on data access, business impact and quantum readiness but has not integrated it into vendor governance frameworks.
L3	The organisation has integrated third-party quantum risk assessments into vendor governance frameworks and translated mitigating measures into security requirements during procurement.
Recommendations	
For level	**Suggested recommendations to progress to next level**

L0	**Identify high-risk third parties**
	• Identify vendors and other third parties service with:
	  ○ Access to sensitive or regulated data
	  ○ Cryptographically dependent systems (e.g. HSMs, VPNs, PKIs, firmware) that has critical business impact
	• Request relevant information from high-risk vendors, such as but not limited to:
	  ○ Cryptographic algorithms used
	  ○ Use of asymmetric cryptography
	  ○ Existing plans towards PQC or hybrid approaches
	
	Perform preliminary quantum risk assessment of key vendors
	• Factor in considerations related to quantum risks in the assessment of key vendors

L1	**Perform an in-depth, risk-based evaluation of key vendors**
	• Map business criticality and data access level
	• Determine cryptographic dependencies
	• Evaluate whether their products rely on vulnerable cryptography
	
	Request asset inventory and quantum-safe roadmaps from vendors
	• To support organisational quantum-safe migration planning, request key vendors to provide details such as but not limited to:
	  o Cryptographic Bill of Materials (CBOMs)
	  o Migration timelines to PQC
	  o Support for hybrid implementations

L2	**Integrate quantum risk into the enterprise's vendor governance framework**
	• Vendor risk evaluation and their mitigation plans should be tracked and reviewed periodically.
	
	Include quantum-safe requirements into procurement policies
	• RFP templates, vendor contracts, and renewal documents should be updated to include requirements such as but not limited to:
	  o PQC and hybrid implementation support clauses
	  o Considerations for cryptographic agility
	  o CBOM submission templates

L3	Keep up the continuous effort towards quantum-safety!

Objective 2: Connect with ecosystem stakeholders to collectively address quantum risks
Connect and engage with ecosystems stakeholders, including vendors, industry groups, academia and regulators, to address quantum computing risks collaboratively.

Rationale: Quantum risks are systemic and cannot be mitigated by individual organisations alone. Collaboration across organisations and the ecosystem enables shared risk understanding, align quantum-safe migration planning objectives and access to collective expertise for an effective and unified response.

Level	**Descriptors**
L0	The organisation has not initiated any engagements with external stakeholders on quantum risk issues.
L1	The organisation has an understanding of relevant ecosystem stakeholders, industry groups, ISACs and other stakeholder partners to address quantum-enabled threats.

L2	The organisation is learning from ecosystem stakeholders on their identified quantum risks, experiences and insights on quantum safe migration.
L3	The organisation is contributing its perspective on quantum risks, its experiences and insights on quantum safe migration to the ecosystem stakeholders.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Understand relevant ecosystem stakeholders** • Monitor existing events and platforms that spread knowledge relevant to quantum safe migration • Examples of relevant stakeholders could be industry groups, Information Sharing and Analysis Centres (ISACs) and other professional groups

L1	**Engage and learn from relevant ecosystem stakeholders**
	• Start by attending and networking in events such as but not limited to:
	  ○ Quantum-safe migration related conferences
	  ○ Technical roundtable hosted by standards bodies or industry associations
	  ○ Public consultation on quantum-safe guidelines (e.g. NIST, ETSI, AiSP, FS-ISAC)
	  ○ Industry-specific (e.g. FS-ISAC, AiSP Quantum SIG, SCS Quantum SIG)
	• Engage stakeholders to learn about identified quantum risks, their experiences and insights on quantum-safe migration.

L2	**Contribute experiences and insights to ecosystem stakeholders** • Present insights and lessons learnt from implementing quantum-safe migration to the ecosystem through local and international events and platforms
L3	Keep up the continuous effort towards quantum-safety!

Objective 3: Promote the adoption of common quantum-safe standards and guidelines for interoperability *Promote the adoption of common quantum-safe standards and implementation guidelines for interoperability across the ecosystem.*	
Rationale: Quantum-safe standards and guidelines facilitate interoperability and reduce future implementation costs.	
Level	**Descriptors**

L0	The organisation is not involved in the promotion of the use of quantum-safe standards and guidelines.
L1	The organisation is monitoring national or international developments in quantum-safe standards and guidelines and acknowledges the importance of adopting relevant standards and guidelines.
L2	The organisation is actively promoting the use and adoption of relevant standards and guidelines.
L3	The organisation is recognised as a leader in adopting quantum-safe standards and guidelines and regularly shares lessons learnt across the ecosystem.
Recommendations	
For level	**Suggested recommendations to progress to next level**

L0	**Establish a watchlist and its relevance to organisation**
	• Monitor updates in standards such as but not limited to:
	  ○ NIST PQC algorithm standardisation
	  ○ ETSI Quantum-Safe Cryptography (QSC) series
	  ○ Regional and sector-specific developments
	• Review relevance of standards to organisation's existing cryptographic practices

L1	**Promote the use and adoption of standards and guidelines through the organisation's quantum-safe journey** • Promote adoption of standards and guidelines through industry events (e.g. ISACA)
L2	**Establish thought leadership on the use and adoption of standards and guidelines groups with the ecosystem** • Present insights and lessons learnt from the adoption with entire ecosystem through international fora and renowned publication outlets
L3	Keep up the continuous effort towards quantum-safety!

Objective 4: Contribute to the ecosystem's future talent pool *Organisation's collaboration with the ecosystem and academia to expand the future talent pool.*	
Rationale: Collaborating with the ecosystem and academia to support the pipeline of future-ready quantum security talent can help grow the collective knowledge base, aid innovation speed and obtain insights on latest research.	
Level	**Descriptors**
L0	The organisation has no engagement with the ecosystem and academia related to talent pipeline development.

L1	The organisation is exploring collaboration opportunities with the ecosystem and academia for talent pipeline development.
L2	The organisation has established collaborations with the ecosystem and academia for talent pipeline development.
L3	The organisation has contributed significantly to building the quantum safe talent pipeline, with these initiatives aligned with the organisation's strategy and their effectiveness tracked.
Recommendations	
For level	**Suggested recommendations to progress to next level**

L0	**Exploring collaboration opportunities with ecosystem and academia**
	• Understand ongoing initiatives from ecosystem and academia such as but not limited to:
	  o University-hosted initiatives on PQC or cryptographic trends
	  o Quantum safe related innovation and R&D projects
	  o Quantum talent programmes

L1	**Establish collaboration with ecosystem and academia**
	• Form partnerships with local or international academia such as but not limited to:
	  o University-hosted initiatives on PQC or cryptographic trends
	  o Quantum-safe related innovation and R&D projects
	  o Quantum talent programmes

L2	**Lead or co-sponsor impactful ecosystem talent initiatives**
	• Lead or co-sponsor initiatives such as but not limited to:
	  o Academic-industry conferences
	  o Joint university labs or fellowships in post-quantum cryptography
	
	Track and review outcomes
	• Integrate quantum readiness into long-term talent strategies such as but not limited to:
	  o Graduate hiring pipelines
	  o Talent upskilling roadmaps
	• Regularly assess talent acquisition (e.g. internship placement rates and conversion to hires)

L3	Keep up the continuous effort towards quantum-safety!

Technology (TE)

Technology involves organisations to think ahead and conduct technology experimentation and proof of concept projects to assess quantum safe technologies.

Objective 1: Conduct technology experimentation and proof-of-concepts (PoCs) to assess implications of adoption with regards to use cases *Technology exploration to assess implications of adopting quantum-safe technology and concepts.*	
Rationale: Conducting technology experimentation and PoCs for quantum-safe migration will help organisations to gain better understanding of the challenges and resources involved. In turn, this will help to inform the quantum safe migration journey. Such technology exploration will also provide insights into the viability, operational impact and challenges to facilitate a smoother migration to real-world implementation.	
Level	**Descriptors**
L0	The organisation has not initiated any technology experimentation or PoCs related to quantum-safe technologies or concepts for assessing the impact of quantum-safe technologies on existing systems.
L1	The organisation has embarked on technology experimentation and PoCs on quantum-safe technologies or concepts, with initial efforts to identify use cases.
L2	The organisation's technology experimentation and PoCs are based on its use-cases and are aligned with the strategic quantum safe roadmap.
L3	The organisation has adopted quantum-safe technologies and monitors the effectiveness of adoption in use cases.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Identify use cases as a basis for technology experimentation** • Identify use cases involving vulnerable cryptographic algorithms (such as VPN or webserver authentications) that will eventually be replaced with PQC or hybrid methods. **Establish a technology experimentation track as part of the quantum-safe migration plan** • Designate a workstream to explore and experiment with quantum-safe technologies. • Allocate budget and infrastructure for technology experimentation activities • Launch small-scale PoC pilots based on organisation's use-cases

L1	**Determine technology experimentation and PoC projects based on use cases**
	• Develop each project based on use cases such as but not limited to:
	  ○ Secure email/signature workflows
	  ○ Authentication and identity infrastructure
	  ○ Third-party APIs, browser and cloud communications
	
	Align quantum safe initiatives with strategic quantum safe roadmap
	• Timelines for cryptography migration
	• Milestones for system upgrades
	• Dependencies across applications and third-party services
	• Quantum-safe cryptographic requirements:
	  ○ PQC algorithm selection
	  ○ Performance, latency, resource constraints and considerations of PQC algorithms on selected use cases

L2	**Adopt quantum-safe technologies in operational environment** • Share findings of pilots with key stakeholders • Plan for adoption of quantum-safe technologies with regards to their use cases in the wider operational environment • Monitor the effectiveness of quantum-safe technologies with regards to threat landscape
L3	Keep up the continuous effort towards quantum-safety!

Objective 2: Instill agility considerations to enable timely replacement of cryptographic algorithms

Agility considerations facilitate the timely replacement of vulnerable cryptographic algorithms to alternative quantum safe cryptographic algorithms.

Rationale: It takes a long time and significant resources for organisations to replace vulnerable cryptographic algorithms. Considering cryptographic agility upfront in quantum-safe migration will enable timely replacement to other quantum safe cryptographic algorithms as needed.

Level	**Descriptors**
L0	The organisation has not considered cryptographic agility in its quantum-safe migration plans.
L1	The organisation acknowledges the importance for cryptographic agility and has begun exploring its implementation for quantum-safe migration planning.
L2	The organisation has developed an approach to include cryptographic agility considerations into its quantum-safe migration plans.

L3	The organisation continuously refines the approach to implement cryptographic agility based on developments arising from quantum enabled threats and evolving business needs.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0	**Educate stakeholders on the importance of cryptographic agility** • Initiate efforts to plan ahead and use quantum-safe cryptographic algorithms • Conduct a sharing with stakeholders on topics such as but not limited to: o The history of cryptographic algorithm failures o Risks of hardcoded cryptography o How long and costly it takes to replace compromised cryptography
L1	**Define cryptographic agility considerations** • Define cryptographic agility considerations in the quantum-safe migration plan such as but not limited to: o Identification of quantum-safe cryptographic algorithms and planning for their implementation o Use of modular cryptographic APIs/libraries o Capacity to support hybrid cryptography (e.g. classical and post-quantum algorithms) o Validation for future algorithm switching in case of PQC or other algorithm deprecation
L2	**Monitor quantum-safe algorithm landscape and update cryptographic agility considerations** • Regularly monitor the landscape for quantum-safe cryptographic algorithms and updates identified algorithms based on changing threat landscape and technology developments. • Update cryptographic agility considerations to: o Updates from authoritative sources (e.g. NIST) o Use-case changes o Business priorities and risk tolerance levels
L3	Keep up the continuous effort towards quantum-safety!

Annex B – QRI Questions

The questions can also be accessed at go.gov.sg/qri or the QR code.

https://go.gov.sg/qri

S/N	Domain	Objective Ref	Question	A (L0)	B (L1)	C (L2)	D (L3)
1	Governance	1	How has your organisation established leadership and oversight to institutionalise the migration to quantum safety?	The organisation has not identified a champion or cross-functional team to institutionalise the migration to quantum safety. No formal governance structure exists to address these areas.	The organisation has identified a champion or cross-functional team to institutionalise the migration to quantum safety. However, their roles and responsibilities remain informal, and activities are conducted on an ad-hoc basis.	The organisation has established a formal governance structure led by an organisational champion, such as a dedicated committee, with clearly defined roles and responsibilities to institutionalise the migration to quantum safety.	The organisation continuously reviews the roles, responsibilities and processes of the governance structure and refines them in tandem with evolving requirements.
2	Governance	2	How does your organisation plan and allocate resources for quantum safe initiatives?	The organisation has not developed plans or allocated resources for quantum safe initiatives.	The organisation has initiated discussions about quantum safe initiatives, but formal plans await finalisation and approval for integration into broader organisational strategies.	The organisation has developed a strategic roadmap for quantum-safe initiatives, outlining objectives, resource requirements and implementation timelines.	The organisation is executing its roadmap for quantum safe initiatives with allocated resources and defined timelines. Progress is continuously monitored, and the roadmap is regularly updated to align with organisational priorities.
3	Governance	3	How does your organisation view quantum risks vis-à-vis existing cybersecurity risks?	The organisation does not view the quantum risks as a risk to be addressed.	The organisation acknowledges that the quantum risk needs to be addressed and has taken initial steps to address it. However, the risk is treated separately from existing cybersecurity risks.	The organisation has integrated quantum risks into its broader cybersecurity risk management programme, treating quantum risks alongside existing cybersecurity risks.	The organisation continuously evaluates and tracks the effectiveness in managing quantum risk as part of the cybersecurity risk management programme on a regular basis.

S/N	Domain	Objective Ref	Question	A (L0)	B (L1)	C (L2)	D (L3)
4	Governance	4	What is the progress of your organisation in developing policies and frameworks for data, cryptography and quantum risk management?	The organisation has no established policies or frameworks for data, cryptography and quantum risk management.	The organisation has no formal policies or frameworks, but has implemented basic, informal measures for data, cryptography and quantum risk management, including preliminary key storage practices and data classification procedures.	The organisation has developed formal policies and frameworks for data, cryptography and quantum risk management, but these are not yet fully implemented.	The organisation implements and maintains comprehensive policies and frameworks for data, cryptography and quantum risk management. These undergo regular review and updates to align with evolving requirements, including post-quantum cryptography adoption.
5	Risk Assessment	1	How does your organisation assess quantum risks to data and cryptographic assets?	The organisation has not begun assessing quantum risks or evaluating potential impact on its data and cryptographic assets.	The organisation has begun preliminary quantum risk assessments to understand and quantify potential business impact, but such assessments are informal and limited in scope.	The organisation has conducted an organisation-wide quantum risk assessment using a systematic methodology that is based on the value and shelf life of data, understanding of cryptographic vulnerabilities and asset prioritisation.	The organisation regularly conducts quantum risk assessments, continuously refining the process to address evolving needs.
6	Risk Assessment	2	What is the extent of your organisation's inventory of its **key systems that handles high-value data?**	The organisation has not identified key systems and their high-value data assets.	The organisation has taken initial steps to identify key systems that process high-value data and has identified a subset of key systems.	The organisation has a comprehensive inventory of all key systems and their high-value data assets.	The organisation regularly updates its inventory of all key systems and their high-value data assets.

S/N	Domain	Objective Ref	Question	A (L0)	B (L1)	C (L2)	D (L3)
7	Risk Assessment	2	What is the extent of your organisation's inventory of its **cryptographic assets** (e.g. keys, certificates, algorithms, protocols)?	The organisation has not identified their cryptographic assets.	The organisation has taken initial steps to identify its cryptographic assets and has identified a subset of cryptographic assets.	The organisation has a comprehensive inventory of all its cryptographic assets.	The organisation regularly updates its inventory of all cryptographic assets
8	Risk Assessment	2	How are your organisation's **cryptographic dependencies in key systems** (products, applications, processes that rely on cryptography) included in cryptographic inventories?	The organisation has not identified cryptographic dependencies in key systems.	The organisation has taken initial steps to identify its cryptographic dependencies in key systems and has identified a subset of cryptographic dependencies.	The organisation has a comprehensive inventory of all its cryptographic dependencies.	The organisation regularly updates its inventory of all cryptographic dependencies.
9	Training and Capability	1	What is the extent of organisation's awareness of the quantum threat and its impact on critical digital assets?	The organisation is not aware of the quantum threat and has not yet recognised the relevance and benefits of quantum safe migration.	The organisation recognises the importance of quantum safety and potential impact of quantum threat on critical digital assets.	The organisation aligns awareness of the quantum threat and quantum safe migration to its strategic goals and priorities.	The organisation looks ahead and stays up to date with the latest development of quantum safe migration. It is aware of evolving quantum safe environment and strategically plans for future challenges

S/N	Domain	Objective Ref	Question	A (L0)	B (L1)	C (L2)	D (L3)
10	Training and Capability	1	What is your organisation's progress in building awareness for quantum risks and quantum safe migration?	The organisation has not initiated any initiatives on educating stakeholders on quantum risks and the need for quantum -safe migration.	The organisation has begun discussions to develop awareness sessions on quantum risks and what quantum -safe migration entails.	The organisation has established an awareness programme to educate stakeholders on quantum risks and what quantum safe migration entails through targeted communications and training across business units.	The organisation has implemented an awareness programme to educate stakeholders on quantum risks and what quantum safe migration entails, with regular evaluation of its effectiveness and enhancement of the programme based on feedback.
11	Training and Capability	2	How does your organisation identify and develop the competencies needed for quantum-safe migration?	The organisation has not identified essential competencies needed for quantum-safe migration, including cryptography and key management.	The organisation has identified key areas of competency required for quantum-safe migration but has not yet started developing it.	The organisation has developed a matrix on the required competencies for specific roles to enable quantum-safe migration.	The organisation has developed and is maintaining a matrix for all relevant roles, updating competency requirements for each role based on evolving needs.
12	External Engagement	1	How does your organisation evaluate and manage quantum risks from vendors and other third parties?	The organisation has not assessed the quantum risk of vendors or other third parties.	The organisation recognises the quantum risks posed by vendors and other third parties and have initiated risk evaluations.	The organisation has assessed quantum risks of vendors and other third parties based on data access, business impact and quantum readiness but has not integrated it into vendor governance frameworks.	The organisation has integrated third-party quantum risk into vendor governance frameworks. Risk mitigating measures inform procurement requirements.

S/N	Domain	Objective Ref	Question	A (L0)	B (L1)	C (L2)	D (L3)
13	External Engagement	2	How does your organisation engage with external stakeholders to collectively address quantum risks?	The organisation has not initiated any engagements with external stakeholders on quantum risk issues.	The organisation has an understanding of relevant ecosystem stakeholders, industry groups, ISACs and other stakeholder partners to address quantum-enabled threats.	The organisation is learning from ecosystem stakeholders on their identified quantum risks, experiences and insights on quantum safe migration.	The organisation is contributing its perspective on quantum risks, its experiences and insights on quantum safe migration to the ecosystem stakeholders.
14	External Engagement	3	How does your organisation promote the adoption of common quantum-safe standards and guidelines?	The organisation is not involved in the promotion of the use of quantum-safe standards and guidelines.	The organisation is monitoring national or international developments in quantum-safe standards and guidelines and acknowledges the importance of adopting relevant standards and guidelines.	The organisation is actively promoting the use and adoption of relevant standards and guidelines.	The organisation is recognised as a leader in adopting quantum-safe standards and guidelines and regularly shares lessons learnt across the ecosystem.
15	External Engagement	4	How does your organisation engage with ecosystem and academia to support talent pipeline development?	The organisation has no engagements with ecosystems and academia related to talent pipeline development.	The organisation is exploring collaboration opportunities with ecosystem and academia for talent pipeline development.	The organisation has established collaborations with ecosystem and academia for talent pipeline development.	The organisation has contributed significantly to building the quantum safe talent pipeline, with these initiatives aligned with the organisation's strategy and their effectiveness tracked.

S/N	Domain	Objective Ref	Question	A (L0)	B (L1)	C (L2)	D (L3)
16	Technology	1	To what extent has your organisation conducted experimentation and PoCs for quantum-safe technologies to inform quantum-safe migration efforts?	The organisation has not initiated any technology experimentation or PoCs related to quantum-safe technologies or concepts for assessing the impact of quantum-safe technologies on existing systems.	The organisation has embarked on technology experimentation and PoCs on quantum-safe technologies or concepts, with initial efforts to identify use cases.	The organisation's technology experimentation and PoCs are based on its use-cases and aligns with the strategic quantum safe roadmap.	The organisation has adopted quantum-safe technology and monitors the effectiveness of adoption in use cases.
17	Technology	2	Does your organisation plan ahead based on quantum-safe cryptographic algorithms?	The organisation has not planned ahead based on quantum safe cryptographic algorithms.	The organisation has initiated efforts to plan ahead to be quantum-safe and is considering the use of quantum safe cryptographic algorithms.	The organisation has identified quantum safe cryptographic algorithms for use in the quantum-safe migration plan.	The organisation regularly monitors the landscape for quantum safe cryptographic algorithms and updates identified algorithms based on changing threat landscape and technology developments.
18	Technology	2	How does your organisation incorporate cryptographic agility considerations into its quantum-safe migration planning?	The organisation has not considered cryptographic agility in its quantum-safe migration plans.	The organisation acknowledges the importance for cryptographic agility and has begun exploring its implementation for quantum-safe migration planning.	The organisation has developed an approach to include cryptographic agility considerations into its quantum-safe migration plans.	The organisation continuously refines the approach to implement cryptographic agility based on developments arising from quantum enabled threats and evolving business needs.