QUANTUM READINESS INDEX

2026

CSA SINGAPORE

Cyber Security Agency of Singapore

Table of Contents

Developed in consultation with

This document is published by the Cyber Security Agency of Singapore, in close consultation with the following partners listed in alphabetical order:

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

Disclaimer

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.

CSA and its partners contributed views and suggestions on the framing, objective descriptions, 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 should consider how to apply the recommendations in light of their specific circumstances, alongside other relevant measures.

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.

Version History

VERSION	DATE RELEASED	REMARKS
0.1 – PUBLIC CONSULTATION	23 Oct 2025	Release of draft for public consultation
1.0	16 Jul 2026	This version represents the formal release of the QRI following the public consultation. Feedback received was reviewed and, where appropriate, incorporated into the document. Key changes: Objectives were refined to enhance clarity, ensure clearer distinction across domains, and improve interpretability for organisations. In addition, each domain now includes a “no-regrets” objective to provide a clear and practical starting point for organisations to begin their quantum-safe migration journey.

Preface

The quantum computing landscape is evolving rapidly and much remains uncertain. The exact timeline for "Q-day" – when a quantum computer capable of breaking widely deployed cryptography becomes available – cannot be predicted with precision, nor can we be certain how the technology will develop. The field is complex, dynamic, and subject to scientific breakthroughs and geopolitical shifts.

Despite this uncertainty, there is broad consensus that preparation should begin now, particularly for critical systems where the risks of inaction are greatest. Governments worldwide are taking steps to prepare, experimenting with different approaches and refining them as experience is gained.

At the same time, indiscriminate or isolated action is not encouraged. Some measures are "no-regrets" steps that can and should be taken immediately, while others require further monitoring and careful evaluation, as early adoption can lead to unintended costs or ineffective or premature investment.

The Quantum Readiness Index helps organisations assess their readiness for quantum-safe migration, identify capability gaps, and prioritise actions. Its results and recommendations facilitate management discussion and enable buy-in for quantum-safe migration.

It complements CSA's Quantum-Safe Handbook, which covers what is at stake, where to focus efforts on, and practical steps to start building quantum-safe readiness now.

For enquiries or feedback on the Quantum Readiness Index, please contact: Quantum-Safe@csa.gov.sg

Executive Summary

Quantum computers are poised to revolutionise computing by solving certain computational problems exponentially faster than classical computers. While their transformative potential is immense, quantum computers can also pose significant cybersecurity threats, often termed the quantum threat. In particular, sufficiently powerful quantum computers could break the cryptographic systems that secure today's digital infrastructure. This could impact core business functions such as financial transactions, secure communications, and identity management, potentially disrupting operations, exposing sensitive data, and eroding trust.

To address this, organisations need to transition to quantum-safe solutions, a process commonly referred to as quantum-safe migration. Migrating cryptography at such scale is complex and will require significant time and effort. Recognising this, governments worldwide have emphasised the importance of planning for quantum-safe migration.

Despite this, organisations lack clarity on what is required to plan and execute the migration, as well as their current level of readiness. The Quantum Readiness Index (QRI), a self-assessment questionnaire developed to help organisations assess their readiness for quantum-safe migration. In this context, readiness refers to the processes and expertise required to plan and execute the transition. More broadly, these elements are also fundamental to strengthening organisations' ability to respond to an evolving cybersecurity landscape.

The QRI is organised around five key domains: **Risk Assessment**, **Governance**, **Technology**, **Training and Capability**, and **External Engagements**, each with a set of objectives that describe the core areas organisations need to address when preparing, planning, and executing the migration. Each domain consists of one "no-regrets" objective to provide organisations with a clear and accessible starting point.

To perform the self-assessment, organisations answer a series of questions aligned with the objectives within each domain. Upon completion, a readiness level is determined for each objective, together with recommended next steps based on the responses. Organisations can use these results to ascertain their readiness levels, identify gaps, and prioritise action areas.

https://go.gov.sg/qri

1. Introduction

Quantum computing has the potential to deliver transformative benefits across sectors, enabling faster and more efficient solving of complex problems in areas such as logistics, pharmaceuticals, and financial modelling. However, these capabilities also herald what is commonly referred to as the quantum threat. In particular, sufficiently powerful quantum computers could compromise widely deployed cryptographic systems that underpin today's digital infrastructure.

In response, the cryptographic community has been developing Post-Quantum Cryptography (PQC) to replace cryptography vulnerable to quantum computers. With the conclusion of NIST's PQC competition, new PQC algorithms have been standardised, and protocols and systems are beginning to incorporate these algorithms. Addressing this threat will require organisations to adopt these quantum-safe solutions.

However, translating these developments into practice is far from straightforward. Quantum-safe migration is a complex, resource-intensive undertaking that requires significant time and coordination. Drawing from past cryptographic transitions, such efforts involve resolving deep dependencies across systems and infrastructures and often require long lead times. As such, planning and preparation must begin now to ensure a coordinated and timely transition.

Organisations also face challenges in translating guidance into actionable steps. In particular, many organisations lack clarity on what is required to prepare for, plan, and execute quantum-safe migration. To address this, the QRI was developed to help organisations assess their readiness for quantum-safe migration and provide a structured starting point for their migration.

2. Purpose and Objectives of the QRI

The Quantum Readiness Index (QRI) is a self-assessment questionnaire, designed to help organisations understand their readiness to address quantum threats. In this context, readiness refers to the organisational processes and expertise required to plan and execute the migration.

The QRI provides a common basis for organisations to consider the implications of quantum computing on their business functions and systems, and to inform strategic planning for quantum-safe migration.

The QRI is intended as a **guidance resource** and not as a compliance framework. It does not prescribe specific solutions or minimum levels of readiness, recognising that organisations vary in size, sector, and maturity. Instead, it provides a consistent approach for organisations to assess their current state and inform decision-making on quantum-safe readiness.

The key objectives of the QRI are to:

- **Establish a baseline understanding of organisational readiness** to address quantum threats
- **Provide a structure for identifying and considering relevant areas** required for quantum-safe migration
- **Enable engagement with senior leadership** by facilitating a clear and consistent articulation of organisational readiness to inform strategic planning and decision-making
- **Complement existing guidance**, including CSA's Quantum-Safe Migration Handbook, by supporting organisations in navigating and contextualising relevant recommendations

3. Target Audience

The QRI is primarily designed for leaders and decision-makers responsible for technology, cybersecurity, and risk management within an organisation. Typical users include:

- Chief Information Officers (CIOs)
- Chief Information Security Officers (CISOs)
- Chief Data Officers (CDOs)
- Chief Technology Officers (CTOs)
- Chief Risk Officers (CROs)
- Other senior leaders overseeing quantum-safe migration

4. Quantum Readiness Cycle - Using the QRI for Quantum-Safe Migration Planning

Organisations begin by conducting a self-assessment using the QRI, accessible at https://go.gov.sg/qri, by answering questions across the five domains and associated objectives to determine their current readiness levels. Based on the assessment results, organisations review the recommendations and identify priority gaps that require attention.

Organisations then develop and implement action plans to address these gaps, referencing *the Quantum-Safe Migration Handbook* for detailed guidance and practical considerations. Progress should be regularly reviewed, and plans updated as necessary. The QRI can then be used to reassess readiness, enabling organisations to track improvements and adapt to changes in the operating environment. This cycle is intended to be repeated periodically to support continuous improvement in quantum-safe readiness (see Figure 1).

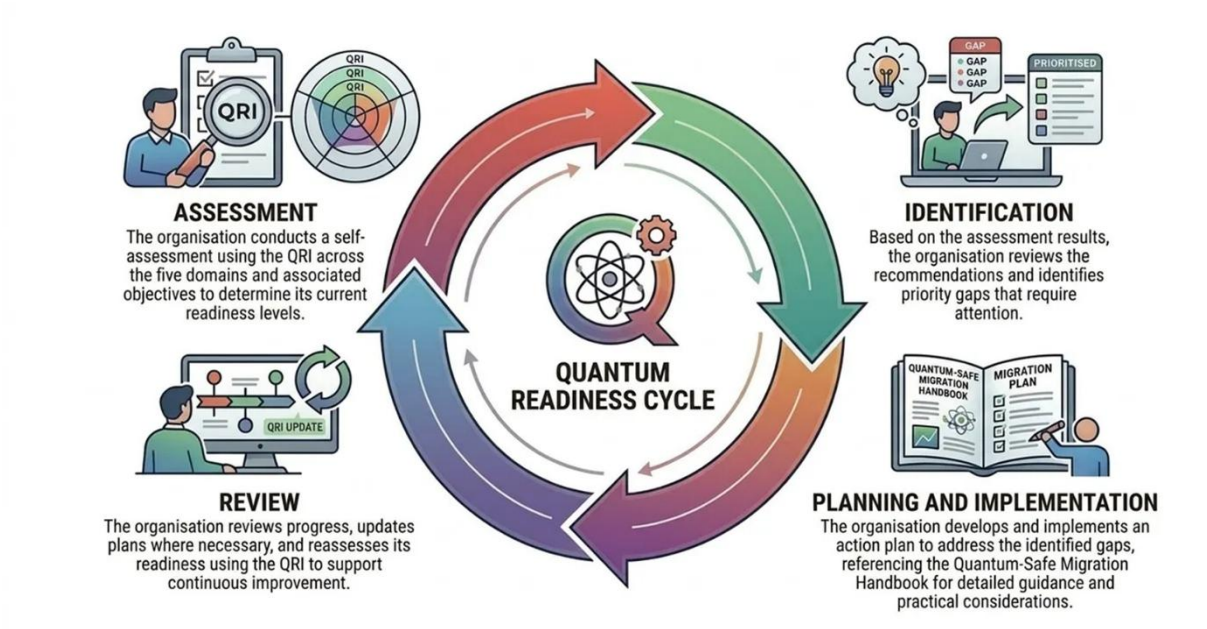

Figure 1: Flow of using the QRI

5. Constructs of the QRI

5.1 Domains and Objectives

The QRI is organised around **five key domains**, each with a set of **objectives** that describe the core areas organisations need to address when preparing for quantum-safe migration. These domains are consistent with those set out in the *Quantum-Safe Migration Handbook* and are aligned with established international frameworks and best practices, including the principles of the World Economic Forum's (WEF) *Quantum Readiness Toolkit*. Each domain includes a **"no-regrets"** objective that represents a foundational starting point for organisations to begin progressing in quantum-safe migration, regardless of their current level of readiness. Details of the domains and objectives can be found in **Annex A**. The **objectives** of each domain are illustrated below in Figure 2.

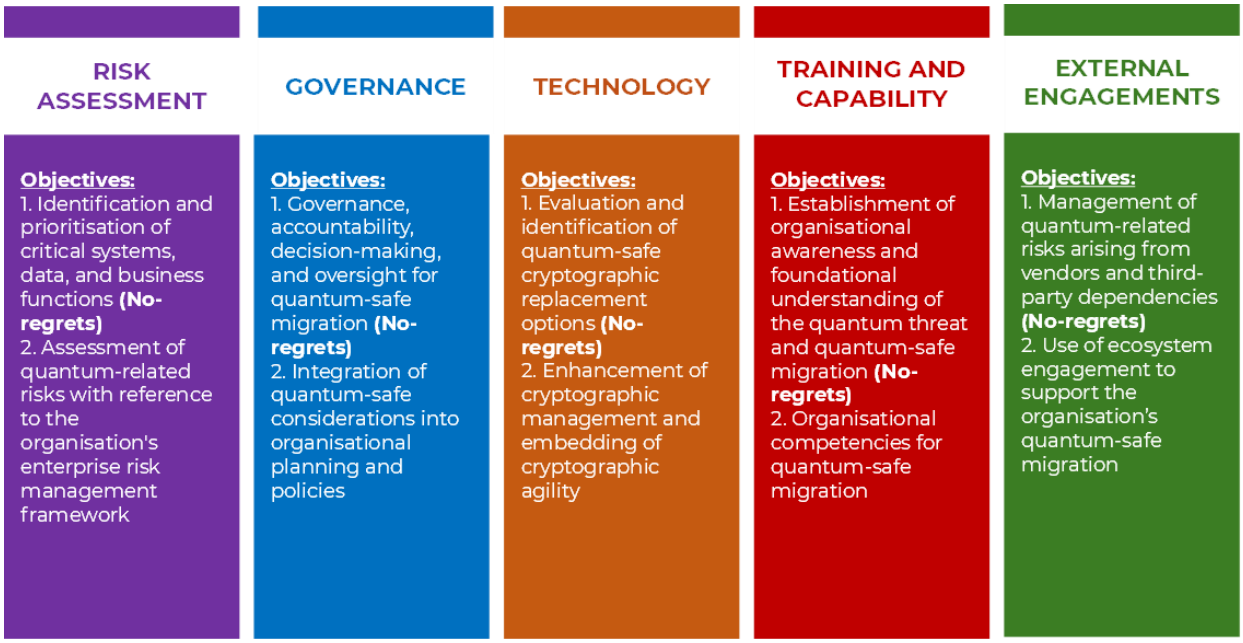

Figure 2: Domains and Objectives of the QRI

5.2 Levels

Each objective is assessed across four defined levels, adapted from the Capability Maturity Model Integration (CMMI) framework developed by the Information Systems Audit and Control Association (ISACA). These levels indicate the degree of organisational readiness and enable the identification of priority areas for improvement. Descriptions of each level are provided in Table 1.

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 its 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 initiated efforts to meet 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 and documented an organisation-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. Organisation continuously improves, pivots and responds to opportunity and change.	**L3 - Operational**	The organisation's capabilities for the objective are operationalised and continuously improved.

Table 1: Description of each QRI level

5.3 Assessment results and recommendations

Evaluation results are automatically computed upon submission of responses at https://go.gov.sg/qri and are reflected as the current level for each objective. A PDF report containing the **assessment results and recommended next steps** is automatically generated and sent to the indicated email address.

Based on the current level, the QRI provides recommended next steps that organisations can take to progress in their quantum-safe migration journey (i.e. to the next level). These recommendations are intended as guidance rather than prescriptive requirements and, where applicable, reference relevant sections of the *Quantum-Safe Migration Handbook* for further detail and practical considerations.

6. Conclusion

Achieving quantum readiness is a progressive, multi-year undertaking that requires sustained planning, preparation, and execution. Given the scale and complexity of transitioning cryptographic systems, organisations should begin taking steps early to ensure a structured and timely migration.

The Quantum Readiness Index (QRI) supports this effort by providing a structured self-assessment to help organisations understand their current state of readiness across key domains, including Risk Assessment, Governance, Technology, Training and Capability, and External Engagements. It enables organisations to establish a baseline, identify areas for improvement, and take informed steps towards strengthening their quantum-safe posture.

As a guidance resource, the QRI is intended to be used alongside the *Quantum-Safe Migration Handbook*. While the QRI helps organisations assess their readiness and identify priority areas, the Handbook provides detailed guidance and practical considerations to guide the development and implementation of migration plans.

Organisations are encouraged to adopt an iterative approach, using the QRI to periodically reassess their readiness, track progress, and refine their plans over time. Through this continuous cycle of assessment, planning, and review, organisations can progressively build the capabilities required to address quantum threats and transition towards quantum-safe systems in a measured and adaptive manner.

Glossary of Key Terms

Terms and Definitions	
Cryptographic Agility	The ability of systems to efficiently replace or update cryptographic algorithms, protocols, or keys in response to emerging threats or evolving standards.
Crown Jewels	An organisation's most critical systems, data, and business functions that require prioritised security due to their high value or sensitivity.
Post-Quantum Cryptography (PQC)	Public-key cryptographic algorithms designed to be secure against attacks from both classical and quantum computers.
Q-Day	The point in time when a quantum computer becomes practically capable of breaking commonly used cryptographic systems.
Quantum Computing	A computing paradigm that leverages quantum mechanical principles to solve certain computational problems significantly faster than classical computers.
Quantum Readiness	The state of an organisation's preparedness, across structures, processes, and expertise, to plan and execute quantum-safe migration.
Quantum Threat	The potential for advances in quantum computing to compromise widely deployed cryptographic systems that secure digital infrastructure.

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

Risk Assessment (RA)

Addresses the identification and prioritisation of organisational "crown jewels" and the structured assessment of quantum-related risks with reference to the organisation's existing enterprise risk management frameworks, to inform prioritisation and decision-making for quantum-safe migration.

Objective 1: Identification and prioritisation of critical systems, data, and business functions (No-regrets)
Assesses the extent to which the organisation has identified and prioritised systems, data, and business functions (collectively referred to as organisational assets) that may be exposed to quantum-related risks, based on factors such as business criticality, data sensitivity and longevity, system exposure, and cryptographic dependencies.

Rationale: Organisations should begin quantum-safe preparation by scoping the problem, identifying and prioritising their most critical business functions, systems and information assets rather than attempting organisation-wide migration prematurely. Identifying and prioritising what matters most is a no-regrets step that supports informed planning, risk assessment, efficient allocation of resources, and targeted migration efforts. Without this foundation, organisations risk fragmented initiatives and misaligned priorities.

Level	Descriptors
L0	The organisation has not identified or prioritised organisational assets in relation to quantum-related risks. Prioritisation is absent or ad hoc.
L1	The organisation has identified a preliminary set of organisational assets that warrant attention based on business importance or data sensitivity, and longevity. Prioritisation remains largely qualitative and informal, and cryptographic dependencies are not yet systematically examined.
L2	The organisation has applied defined criteria to prioritise organisational assets based on factors such as business criticality, data sensitivity and longevity, system exposure, and known or suspected cryptographic dependencies. Targeted cryptographic discovery is conducted for prioritised assets to improve visibility into cryptographic dependencies, and a cryptographic inventory is established for these areas.
L3	The organisation maintains a comprehensive and documented prioritisation of assets, supported by a cryptographic inventory. The prioritisation and cryptographic inventory are periodically reviewed and updated as systems evolve, data usage changes, or business context shifts.

Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• At the organisational level, acknowledge quantum-related risk as a relevant consideration for long-lived or sensitive data and critical systems. • Identify an initial set of organisational assets that warrant further attention based on business importance or sensitivity.

L1→L2	• Define clear criteria for prioritisation, based on factors such as:
	  ○ business criticality,
	  ○ data sensitivity, and longevity,
	  ○ system exposure (e.g. internet-facing systems)
	  ○ known or suspected cryptographic dependencies.
	• Apply these criteria consistently to identify priority assets.
	• Begin targeted cryptographic discovery for priority assets to improve visibility into key cryptographic dependencies and establish a cryptographic inventory for these assets.

L2→L3	• Formalise asset-level prioritisation as a maintained and documented artefact, supported by a cryptographic inventory that records key cryptographic mechanisms and dependencies for prioritised systems. • Periodically review the cryptographic inventory to ensure it remains accurate and up to date. • Establish review mechanisms to periodically update both the cryptographic inventory and asset prioritisation as systems evolve, data usage changes, or business context shifts.
L3 (Sustain)	• Ensure that asset prioritisation and the associated cryptographic inventory are actively used to inform risk assessment, migration planning, and decision-making.

Objective 2: Assessment of quantum-related risks with reference to the organisation's enterprise risk management framework
Assesses the extent to which the organisation conducts structured quantum risk assessments using established risk assessment frameworks. This includes whether quantum-related risk scenarios are defined, evaluated using threat modelling where appropriate, and documented as risk outputs to inform migration planning.

Rationale: Conducting structured quantum risk assessments using established frameworks enables organisations to define risk scenarios, evaluate likelihood and impact, and produce documented risk outputs to inform migration planning. Quantum-related risks shall be assessed within the organisation's broader enterprise risk context, rather than treated as isolated or purely technical concerns.

Level	**Descriptors**
L0	Quantum-related risk is not recognised or considered by the organisation. No discussions have taken place and no assessment of quantum-related risks has been conducted.
L1	Quantum-related risk is recognised as relevant to the organisation and initial discussions have taken place beyond purely technical contexts. However, quantum-related risk scenarios have not been defined, and no structured assessment has been conducted.
L2	Quantum-related risks are formally assessed with reference to the organisation's existing enterprise risk management frameworks or established standards. Threat modelling is used, where appropriate, to inform the development of quantum-related risk scenarios. Defined quantum-related risk scenarios are documented, with likelihood, impact, and risk level evaluated.
L3	Quantum-related risk assessments are conducted on a regular and repeatable basis. Risk scenarios and assessments are reviewed and updated to reflect changes in systems, data characteristics, and the threat landscape. Documented risk outputs are produced consistently to inform migration planning and decision-making.

Recommendations

For level	**Suggested recommendations to progress to next level**
L0→L1	• Recognise quantum-related risk as relevant to the organisation, beyond purely technical handling, and acknowledge its potential impact on critical systems, data, and business functions. • Initiate preliminary discussions on quantum-related risk at the organisational level to build shared understanding.
L1→L2	• Identify and document quantum-related risk scenarios relevant to the organisation, with reference to existing risk assessment frameworks or established standards.

	• Use threat modelling to inform and refine quantum-related risk scenarios, where appropriate. • Evaluate risk scenarios by assessing likelihood, impact, and risk level.
L2→L3	• Establish a regular and repeatable cadence for reviewing and updating quantum-related risk assessments as systems, data characteristics, and the threat landscape evolve. • Ensure documented risk outputs are consistently produced and used to inform technology risks and how they align to business objectives.
L3 (Sustain)	• Periodically review the quantum risk assessment process to ensure it remains current and effective as technologies, standards, and the threat landscape evolve.

Governance (GV)

Covers the establishment of accountability, decision-making authority, and oversight structures to guide quantum-safe migration, and the translation of these decisions into organisational planning, policies, and roadmaps to ensure alignment with broader business and cybersecurity objectives.

Objective 1. Governance, accountability, decision-making, and oversight for quantum-safe migration (No-regrets)
Assesses the extent to which governance, accountability, decision-making, and oversight are established for quantum-safe migration. The focus is on whether quantum-safe migration is governed within the organisation's existing governance and technology decision structures, rather than treated as a standalone or parallel initiative.

Rationale: Quantum-safe migration is a multi-year organisational transition that requires clear accountability, effective decision-making, and sustained oversight. Establishing governance early is a no-regrets action that clarifies ownership, decision pathways, and oversight mechanisms across functions, enabling coordinated and timely progress. Where quantum-safe requirements are not embedded within existing governance and technology decision structures, organisations risk fragmented and uncoordinated migration efforts downstream.

Level	Descriptors
L0	Governance for quantum-safe migration is absent or not clearly defined. Accountability, decision-making processes, and oversight are not discussed or defined. Quantum-safe migration, if undertaken, occurs on an ad hoc basis or as standalone activities at the project or system level, without coordination or visibility at the organisational level.
L1	Roles, decision authority, and oversight for quantum-safe migration remain informal or loosely defined. Accountability may rest with individuals or project teams without clear mandates, and decision-making is reactive or fragmented. Quantum-safe migration is discussed within the organisation but is not yet embedded within existing governance or technology decision structures.
L2	Clear governance for quantum-safe migration is established, with defined accountability, decision-making authority, and oversight. Quantum-safe migration is governed within existing organisational governance and technology decision structures, with responsibilities assigned to appropriate organisational functions. Decisions related to quantum-safe migration are coordinated and traceable through established governance processes.
L3	Governance for quantum-safe migration is operating effectively and sustained over time. Accountability, decision-making, and oversight are applied in practice, and governance processes support ongoing

	coordination, monitoring, and adjustment as organisational priorities, technologies, and external developments evolve.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• Recognise that quantum-safe migration requires governance, accountability, and oversight, even if these remain informal initially. • Begin articulating, at a high level, who is involved in quantum-safe migration decisions and how such decisions are currently made.
L1→L2	• Define and document clear accountability, decision-making authority, and oversight for quantum-safe migration within existing organisational governance and technology decision structures. • Assign responsibilities to appropriate organisational functions and clarify decision pathways and escalation mechanisms. • Ensure decisions related to quantum-safe migration are recorded and traceable through established governance processes.
L2→L3	• Ensure that defined governance structures for quantum-safe migration are applied in practice, with accountability, decision-making, and oversight functioning as intended across the organisation. • Embed quantum-safe migration into existing governance activities and decision processes, so that it is routinely addressed as organisational priorities, technologies, and external conditions evolve.
L3 (Sustain)	• Periodically review governance structures for quantum-safe migration to ensure accountability, decision-making authority, and oversight remain effective and appropriate as organisational context and external developments change.

Objective 2. Integration of quantum-safe considerations into organisational planning and policies

Assesses the extent to which governance decisions for quantum-safe migration are translated into organisational planning and policy artefacts. This includes the development of a quantum-safe roadmap to guide sequencing and prioritisation over time, and the integration of quantum-safe considerations into enterprise risk management, cryptographic, data governance, procurement and contractual policies. The focus is on whether these artefacts provide coherent and consistent direction for planning, decision-making, and resource allocation across the organisation.

Rationale: Governance decisions for quantum-safe migration must be translated into organisational planning and policy artefacts to guide coordinated action over time. Planning artefacts, such as a quantum-safe roadmap, help organisations sequence and allocate resources. Additionally, supporting frameworks or policies, such as enterprise risk management, cryptographic, data governance, procurement and contractual policies, ensure that these decisions are applied consistently in operations and external engagements, reducing the risk of misalignment between governance intent, operational decisions, and long-term migration objectives.

Level	Descriptors
L0	Quantum-safe considerations are not reflected in organisational planning or policy artefacts. There is no quantum-safe roadmap, and existing supporting policies do not address quantum-safe migration. Governance decisions, if any, are not translated into planning or policy guidance.
L1	Initial consideration of quantum-safe migration is reflected in planning or policy discussions, but coverage is partial or informal. A quantum-safe roadmap is conceptually initiated but remains high-level and does not yet inform the sequencing or execution of migration. There are plans to review and update supporting policies to reflect quantum-safe considerations. References to quantum-safe considerations may appear in some policies or procurement activities, but these are limited in scope and not applied consistently across the organisation.
L2	Organisational planning and policy artefacts explicitly incorporate quantum-safe considerations. A defined quantum-safe roadmap exists to guide the execution of migration across prioritised systems, providing structure for sequencing and coordination over time. Relevant policies are aligned with governance decisions and provide consistent direction for planning, decision-making, and the allocation of resources to support migration activities across functions.
L3	Planning and policy artefacts that reflect quantum-safe considerations are actively used in practice. The quantum-safe roadmap and supporting policies inform routine planning, resource allocation, procurement, and decision-making, and are periodically

	reviewed and updated to reflect changes in organisational priorities, technologies, and external developments. This enables sustained, coordinated execution of quantum-safe migration over a multi-year transition.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• Initiate consideration of quantum-safe migration within organisational planning or policy discussions, even if informally. • Begin articulating the need for a quantum-safe roadmap to guide future sequencing and execution of migration. • Discuss how quantum-safe migration affects organisational planning, enterprise risk management, resource allocation, procurement, cryptographic management, data governance, and contractual arrangements, without yet formalising policies or planning artefacts.
L1→L2	• Translate governance decisions into relevant supporting policies, such as enterprise risk management, cryptographic, data governance, procurement and contractual policies, to provide clear and consistent planning guidance. • Develop and document a defined quantum-safe roadmap to guide the sequencing, resource allocation, and execution of migration across prioritised systems. • Ensure these planning and policy artefacts are aligned and communicated across relevant organisational functions.
L2→L3	• Apply the quantum-safe roadmap and supporting policies in practice to inform routine planning, procurement, and contractual decisions. • Establish mechanisms to periodically review and update the roadmap, planning, and policy artefacts so they continue to reflect quantum-safe considerations as organisational priorities, technologies, and external developments evolve.
L3 (Sustain)	• Maintain the effective use of planning and policy artefacts by routinely reviewing their relevance, coherence, and alignment with governance decisions, ensuring they continue to support coordinated execution of quantum-safe migration.

Technology (TE)

Examines suitable quantum-safe cryptographic replacement options, alongside the strengthening of cryptographic management practices and agility to enable timely adaptation, updating, or replacement of cryptographic implementations as technologies and standards evolve.

Objective 1. Evaluation and identification of quantum-safe cryptographic replacement options (No-regrets)
Assesses the extent to which the organisation has evaluated and identified suitable quantum-safe cryptographic replacement options for prioritised systems and use cases. The focus is on determining appropriate replacement approaches based on known cryptographic dependencies, operational requirements, interoperability needs, performance considerations, and implementation constraints. Evaluation can be informed by testing, experimentation, proofs-of-concept, or early adoption activities, as appropriate to the organisation's context.

Rationale: Certain cryptographic mechanisms in use are vulnerable to compromise by future cryptographically relevant quantum computers (CRQCs) and will need to be replaced in due time. Organisations should therefore begin identifying and assessing quantum-safe replacement options for prioritised systems as a no-regrets action. Early and informed identification supports realistic planning, reduces uncertainty, and enables phased transition over a multi-year migration. This approach strengthens preparedness while allowing organisations flexibility in how and when they adopt appropriate solutions.

Level	Descriptors
L0	The organisation has not considered or evaluated quantum-safe cryptographic replacement options for prioritised systems. No assessment has been conducted to determine the appropriate replacements for vulnerable cryptographic mechanisms.
L1	The organisation has begun exploring potential quantum-safe cryptographic replacement options at a conceptual level. Assessment is limited in scope and typically consists of literature reviews or high-level discussions. Evaluation is ad hoc and does not yet systematically consider known cryptographic dependencies, operational requirements, interoperability needs, performance implications, or implementation constraints.
L2	The organisation has defined a systematic approach to evaluate and identify suitable quantum-safe cryptographic replacement options for prioritised systems and use cases. Replacement approaches are assessed based on known cryptographic dependencies, operational requirements, interoperability needs, performance considerations, and integration constraints. Evaluation activities inform documented findings on feasibility, limitations, and implementation considerations that support migration planning.

L3	Evaluation outcomes are used to inform organisational migration planning. Identified alternatives and associated constraints are incorporated into technical planning, architecture considerations, and implementation strategies for prioritised systems. Organisation uses evaluation results to address identified challenges, sequence migration activities accordingly, and periodically review decisions as technologies, standards, and system contexts evolve.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• Begin exploring quantum-safe cryptographic alternatives relevant to the organisation's prioritised systems and use cases. • Conduct literature reviews to build an initial understanding of available approaches and solutions. • Initiate internal discussions on how quantum-safe replacement options affect system architectures, operational requirements, and future technology planning.
L1→L2	• Establish a structured approach to evaluate and identify suitable quantum-safe cryptographic alternatives for prioritised systems. • Assess candidate replacement options against relevant factors such as interoperability requirements, performance implications, operational constraints, and system dependencies. • Conduct evaluation activities, such as testing, experimentation, proofs-of-concept, or technical assessments, to validate feasibility and identify potential limitations. • Document evaluation findings and recommended replacement approaches to support organisational migration planning.

L2→L3	• Use evaluation outcomes to inform organisational migration planning and technical decision-making for prioritised systems.
	• Incorporate identified replacement options and associated constraints into system architecture considerations, technical planning, and migration roadmaps.
	• Address identified implementation challenges, and sequence migration activities where dependencies or technology readiness require a phased approach.
	• Explore mitigating measures where limitations prevent immediate replacement, and consider interim strategies such as:
	  ○ implementing cryptographic wrapper solutions or enabling forward secrecy,
	  ○ isolating affected systems, or
	  ○ plan staggered migration as vendor support becomes available.

L3 (Sustain)	• Periodically review evaluation outcomes and decisions to ensure continued alignment with evolving technologies, standards, system architectures, and organisational priorities. • Update replacement approaches and technical planning as new solutions mature or as operational conditions change.

Objective 2. Enhancement of cryptographic management and embedding of cryptographic agility

Assesses the extent to which the organisation has strengthened its cryptographic management practices and embedded cryptographic agility across systems and supporting processes. The focus is on whether cryptographic mechanisms and their dependencies are managed with sufficient governance and lifecycle control, and whether systems and architectures are designed to allow cryptographic mechanisms to be introduced, replaced, or retired over time with minimal disruption.

Rationale: Robust cryptographic management improves the resilience, security, and manageability of systems by ensuring that cryptographic mechanisms and their dependencies are properly governed and maintained throughout their lifecycle. At the same time, cryptographic agility is necessary because algorithms need to be updated as new threats, vulnerabilities, or standards emerge. Organisations therefore require the ability to replace or reconfigure cryptographic mechanisms in a controlled and minimally disruptive manner. Together, strong cryptographic management and embedded agility enable organisations to respond effectively to technological changes, newly discovered weaknesses, and evolving compliance obligations.

Level	Descriptors
L0	There are no defined cryptographic management practices. Cryptographic mechanisms and their dependencies are not subject to formal governance or lifecycle controls. Cryptographic agility is not considered, and replacing or modifying cryptographic mechanisms is therefore difficult and potentially disruptive.
L1	The organisation recognises the need for both stronger cryptographic management and cryptographic agility. Some cryptographic management practices exist, and basic lifecycle controls are in place. However, practices remain fragmented and are not consistently applied across systems. The need for cryptographic agility is acknowledged, but the organisation has not yet examined how agility considerations should be embedded into system architecture or supporting processes.
L2	The organisation has established defined cryptographic management practices that provide governance over cryptographic mechanisms and their dependencies across relevant systems. Cryptographic mechanisms are managed through documented lifecycle practices and appropriate oversight. Cryptographic agility requirements are defined for the organisation, and the organisation has identified the architectural, system, and process considerations necessary to support cryptographic agility.
L3	Cryptographic management practices are operationalised across the organisation, with cryptographic mechanisms and their dependencies governed through established lifecycle management

	processes. Cryptographic agility considerations are applied in practice, for example during technology refresh, system upgrades, or migrations, and are reflected in systems, architectures, and supporting processes, enabling cryptographic mechanisms to be introduced, replaced, or reconfigured with minimal disruption. Cryptographic management practices and agility considerations are periodically reviewed and refined to maintain resilience and alignment with evolving technologies, standards, and threats.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• Recognise the need to strengthen cryptographic management practices and begin considering cryptographic agility as an organisational capability, acknowledging that cryptographic algorithms and mechanisms need to be updated or replaced over time as new threats, vulnerabilities, or standards emerge. • Begin introducing basic organisational practices for managing and maintaining cryptographic mechanisms within systems, including assigning responsibility for oversight and considering how systems need to accommodate future cryptographic updates or replacements.
L1→L2	• Define and establish cryptographic management practices, including documented processes for governing and maintaining cryptographic mechanisms throughout their lifecycle (e.g. introduction, maintenance, replacement, and retirement). • Identify and define architectural, system, and process considerations necessary to support cryptographic agility, including how systems should accommodate future cryptographic mechanism updates or replacements.
L2→L3	• Operationalise cryptographic management practices across systems through consistent lifecycle governance and oversight. • Apply cryptographic agility considerations in practice, for example during technology refresh, system upgrades, migrations, or responses to cryptographic vulnerabilities or standards updates.
L3 (Sustain)	• Periodically review and refine cryptographic management practices and agility considerations to maintain resilience and alignment with evolving technologies, standards, and threats. • Ensure cryptographic agility considerations remain embedded in system architecture, engineering practices, and technology governance processes.

Training and Capability (TC)

Builds organisational awareness of the quantum threat and develops the competencies required to plan, govern, and implement quantum-safe migration, including ensuring that relevant stakeholders possess the knowledge and skills needed to guide decision-making and execution.

Objective 1. Establishment of organisational awareness and foundational understanding of the quantum threat and quantum-safe migration (No-regrets)
Assesses the extent to which the organisation has established awareness and training initiatives to develop organisational understanding of the quantum threat and quantum-safe migration. The objective focuses on whether such initiatives are established, and whether relevant stakeholders are equipped with the necessary knowledge of the quantum threat and key migration considerations through these initiatives.

Rationale: Preparing for quantum-safe migration requires stakeholders across relevant organisational functions to understand the nature of the quantum threat and the considerations involved in quantum-safe migration. Establishing awareness and training initiatives enables organisations to equip stakeholders with the knowledge needed to recognise the implications of the quantum threat and understand migration considerations. Developing this understanding early supports organisational readiness and helps ensure stakeholders remain informed as developments in quantum computing, cryptographic standards, and quantum-safe technologies evolve.

Level	Descriptors
L0	The organisation has no established awareness or training initiatives related to the quantum threat or quantum-safe migration. Stakeholders generally have little or no understanding of the quantum threat or the considerations involved in quantum-safe migration.
L1	Initial awareness efforts are introduced to educate stakeholders about the quantum threat and quantum-safe migration, such as briefings, informal knowledge-sharing sessions, or brown-bag talks. These efforts are ad hoc and not systematically organised. As a result, stakeholder understanding remains uneven and limited across the organisation.
L2	The organisation has defined a structured awareness or training programme, such as structured training modules or curated learning resources, to develop understanding of the quantum threat, key migration considerations, and emerging quantum-safe technologies among relevant stakeholders. Stakeholders participating in these initiatives demonstrate foundational understanding that supports informed organisational discussions and planning.
L3	Awareness and training programmes on the quantum threat and quantum-safe migration are sustained across the organisation. These

	programmes are periodically reviewed and updated to reflect developments in quantum computing, cryptographic standards, and quantum-safe technologies. Stakeholders across relevant organisational functions maintain an up-to-date foundational understanding of the quantum threat and key migration considerations.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• Introduce initial awareness activities to familiarise stakeholders with the quantum threat and the concept of quantum-safe migration. • Conduct introductory briefings or knowledge-sharing sessions explaining the impact of quantum computing on current cryptography.

L1→L2	• Develop a defined awareness or training programme to build foundational understanding of the quantum threat and quantum-safe migration among relevant stakeholders.
	• The programme can include topics such as:
	  ○ Developments in quantum computing and their potential impact on cybersecurity, including confidentiality, integrity, and availability
	  ○ An overview of quantum-safe cryptography
	  ○ Operational considerations for quantum-safe migration, such as prioritisation, cryptographic discovery, threat modelling, and evaluation
	• Training can be delivered through structured modules, internal workshops, or external training courses.
	• Identify relevant organisational functions and ensure stakeholders from these functions participate in the programme to build foundational understanding.

L2→L3	• Integrate awareness and training activities into regular organisational learning or professional development programmes. • Periodically review and update training content to reflect developments in quantum computing, cryptographic standards, and quantum-safe technologies. • Ensure that relevant stakeholders continue to participate in awareness and training activities to maintain an up-to-date foundational understanding.
L3 (Sustain)	• Maintain ongoing awareness and training initiatives by periodically reviewing programme effectiveness and ensuring learning materials remain current with developments in technology, standards, and guidance related to quantum-safe migration.

Objective 2. Organisational competencies for quantum-safe migration
Assesses the extent to which the organisation possesses the technical and organisational competencies necessary to manage quantum-safe migration. This includes competencies across functions such as cybersecurity, enterprise architecture, risk management, and programme coordination. The objective focuses on whether relevant organisational functions have the competencies to evaluate and implement quantum-safe technologies, and to coordinate migration activities across systems and organisational processes.

Rationale: Quantum-safe migration is a complex endeavour requiring competencies across governance, technical, and operational functions. Beyond awareness of the quantum threat, organisations must be able to assess risks, evaluate suitable technologies, manage cryptographic dependencies, and plan and coordinate migration activities effectively. Possessing relevant competencies enables organisations to translate strategic intent into practical implementation, ensuring that quantum-safe migration can be carried out in a coordinated and sustainable manner.

Level	Descriptors
L0	The organisation lacks the competencies required to plan, govern, support, or execute quantum-safe migration. Relevant functions do not possess the knowledge, skills, or experience to contribute effectively to migration activities, and there is minimal organisational understanding of what is required to coordinate a migration.
L1	The organisation has identified the competencies needed across relevant functions, such as cybersecurity, enterprise architecture, risk management, and programme coordination. However, stakeholders still have limited capability to support quantum-safe migration, and competencies remain unevenly distributed, typically concentrated within a small number of individuals or teams.
L2	The organisation has recognised competency gaps and taken steps to address them. Training initiatives, formal processes, and documented guidance are established to equip relevant teams with the knowledge and skills necessary to plan, govern, support, and execute quantum-safe migration.
L3	Competencies are actively applied across governance, technical, and operational functions. Relevant teams demonstrate the ability to coordinate and carry out migration activities across systems and organisational processes. Training initiatives, formal processes, and documented guidance are periodically reviewed to reflect evolving technologies, standards, lessons learned, and best practices, ensuring organisational competencies are sustained.

Recommendations	
For level	**Suggested recommendations to progress to next level**

L0→L1	• Identify key organisational competencies required to support quantum-safe migration, such as:
	  ○ Cybersecurity
	  ○ Enterprise architecture
	  ○ Risk management
	  ○ Programme management
	• Map these competencies to the relevant organisational functions or teams responsible for migration-related activities.
	• Conduct a gap assessment to determine whether existing teams possess the required competencies.

L1→L2	• Develop targeted initiatives to address identified competency gaps, such as structured training programmes, external courses, or workshops. • Establish documented guidance, processes, playbooks, or internal reference materials to support activities such as migration planning, risk assessment and management, technology evaluation, and programme coordination.
L2→L3	• Apply the developed competencies in practice to support migration planning, risk management, technology evaluation, and programme coordination. • Integrate competency development into regular organisational training or professional development programmes to ensure skills remain current.
L3 (Sustain)	• Periodically review organisational competency requirements and update training programmes, guidance, and processes accordingly. • Capture lessons learned from migration activities and incorporate them into organisational knowledge bases or playbooks to strengthen institutional expertise.

External Engagements (EE)

Addresses the management of quantum-related risks arising from vendors and third parties, including dependencies on external products and services, as well as engagement with the broader ecosystem to stay informed of developments, access expertise, and support migration efforts.

Objective 1. Management of quantum-related risks arising from vendors and third-party dependencies (No-regrets)
Assesses the extent to which the organisation understands and manages quantum-related risks arising from vendors and third-party dependencies. The focus is on whether organisations consider readiness of vendors and third-party solutions during migration and technology planning, and whether they have sufficient visibility into how these dependencies affect their migration.

Rationale: Organisations often rely on vendors and third-party providers for critical technologies. An organisation thus has limited visibility into or control over cryptographic mechanisms used within these solutions. Progress in quantum-safe migration depends on vendors updating their products or services. If vendors are slow or unable to transition, this could introduce security, operational, or compliance risks, and affect the organisation's migration timeline. Understanding and managing vendor-related quantum risks is therefore an important no-regrets step to ensure that these dependencies do not hinder quantum-safe migration.

Level	Descriptors
L0	The organisation has not considered quantum-related risks arising from vendors or third-party dependencies. There is little or no visibility into the technologies provided by external vendors, and the organisation does not consider vendor quantum-safe readiness when planning its own migration.
L1	The organisation has begun identifying technologies and dependencies provided by vendors or third parties and has an initial overview of these components. Initial engagement with vendors may take place to understand their quantum-safe readiness, but efforts remain limited in scope and are conducted on an ad hoc basis.
L2	The organisation has established a structured overview of technologies and dependencies provided by vendors and third-party solutions. Assessment processes are defined to obtain information from vendors on their quantum-safe readiness, including their migration roadmap, implementation approach, support capabilities, and potential impact on the organisation's migration planning.
L3	The organisation actively applies established assessment processes to engage vendors and third parties on their quantum-safe readiness and their ability to support the organisation's migration plans.

	Insights from these engagements inform organisational migration planning, and identified limitations or dependencies are considered and addressed as part of the migration strategy.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• Identify key technologies and services provided by vendors or third parties that support organisational systems (e.g. cloud platforms, IAM, enterprise applications, security products, and network infrastructure). • Develop an initial overview of vendor-provided technologies and dependencies that affect quantum-safe migration. • Initiate discussions with key vendors to understand their awareness of quantum-safe migration and their plans for it.

L1→L2	• Develop a structured approach to assess vendor quantum-safe readiness and its potential impact on organisational migration planning.
	• Request information from vendors on topics such as:
	  o their quantum-safe migration roadmap
	  o the cryptographic mechanisms used in their products or services (e.g. libraries, protocols, and algorithms)
	  o their ability to facilitate cryptographic algorithm updates in future releases
	  o the expected timeline, cost, and operational implications of quantum-safe upgrades.
	• Identify vendor dependencies that affect organisational migration planning (e.g. systems that cannot be upgraded until vendor support becomes available).
	• Document vendor responses and incorporate the findings into organisational migration planning and risk assessments.

L2→L3	• Integrate vendor quantum-safe readiness assessments into regular vendor engagement and technology planning activities.
	• Work with vendors to align migration timelines, implementation approaches, and support arrangements with the organisation's quantum-safe migration plans.
	• Explore mitigating measures where vendor limitations prevent immediate replacement, and consider interim strategies such as:
	  o implementing cryptographic wrapper solutions or enabling forward secrecy,
	  o isolating affected systems, or
	  o plan staggered migration as vendor support becomes available.

L3 (Sustain)	• Maintain ongoing engagements with vendors to monitor developments in product support for quantum-safe cryptography.

	• Update organisational migration planning and risk assessments to reflect changes in vendor capabilities, dependencies, and relevant technology developments.

Objective 2. Use of ecosystem engagement to support the organisation's quantum-safe migration

Assesses the extent to which the organisation leverages ecosystem engagement to support its quantum-safe migration. The focus is on whether organisations draw on external guidance, industry practices, peer engagement, and standards to inform migration planning and implementation approaches.

Rationale: Quantum-safe migration is a complex and evolving undertaking, and many organisations may not possess all the expertise or experience required internally. Engaging with the broader ecosystem, including industry peers, standards bodies, research communities, and consulting firms, allows organisations to learn from emerging practices, leverage external expertise, and stay informed about developments in quantum-safe cryptography and migration strategies. Such engagement can help organisations identify practical approaches, tools, and lessons learned from others facing similar migration challenges, while retaining control over their own migration decisions.

Level	Descriptors
L0	The organisation does not consider engaging with the broader ecosystem on quantum-safe migration. External guidance, industry practices, and standards are not considered when planning or implementing quantum-safe migration.
L1	The organisation has begun engaging with the ecosystem to understand developments related to quantum-safe migration. This can include attending industry briefings, participating in forums, or reviewing external publications and guidance. Engagement remains informal, and insights gained are not yet systematically incorporated into organisational migration planning.
L2	The organisation actively leverages ecosystem engagement to inform its quantum-safe migration. This can include working with industry peers, expert communities, or technology providers to identify emerging practices, understand common migration challenges, and explore potential solutions. Opportunities for collaborative activities, including experimentation, evaluation, or validation of approaches, are explored to generate practical insights that inform migration planning.
L3	Ecosystem engagement is embedded within the organisation's migration approach. The organisation maintains ongoing engagement with relevant stakeholders to stay informed about evolving practices and developments. Collaborative initiatives are

	carried out with ecosystem partners, and insights gained are applied to refine the organisation's migration planning and implementation approaches over time.
Recommendations	
For level	**Suggested recommendations to progress to next level**
L0→L1	• Identify relevant ecosystem stakeholders that can support organisational understanding of quantum-safe migration, such as industry peers, research communities, standards bodies, and technology providers. • Participate in industry briefings, seminars, or forums to stay informed about developments in quantum computing, quantum-safe cryptography, and migration strategies. • Review external guidance, industry publications, migration frameworks, and available resources (e.g. open-source tools or industry best practices) to build awareness of emerging practices and challenges.
L1→L2	• Establish more regular engagement with ecosystem stakeholders to deepen understanding of practical quantum-safe migration considerations. • Leverage ecosystem knowledge to understand common migration challenges and technical dependencies (e.g. cryptographic discovery, PKI migration, or system interoperability). • Explore opportunities for collaborative initiatives to assess potential solutions and identify implementation considerations.
L2→L3	• Conduct collaborative activities with ecosystem stakeholders, such as joint experimentation, proof-of-concepts, evaluation of quantum-safe technologies, or validation of migration approaches. • Work with industry peers or technology providers to address shared migration challenges or technical dependencies. • Use insights gained from these activities to refine the organisation's migration planning and implementation strategies.
L3 (Sustain)	• Maintain ongoing engagement with relevant ecosystem stakeholders to stay informed about evolving standards, technologies, and migration practices. • Continue participating in collaborative initiatives and knowledge-sharing communities to exchange lessons learned and strengthen collective readiness for quantum-safe migration.