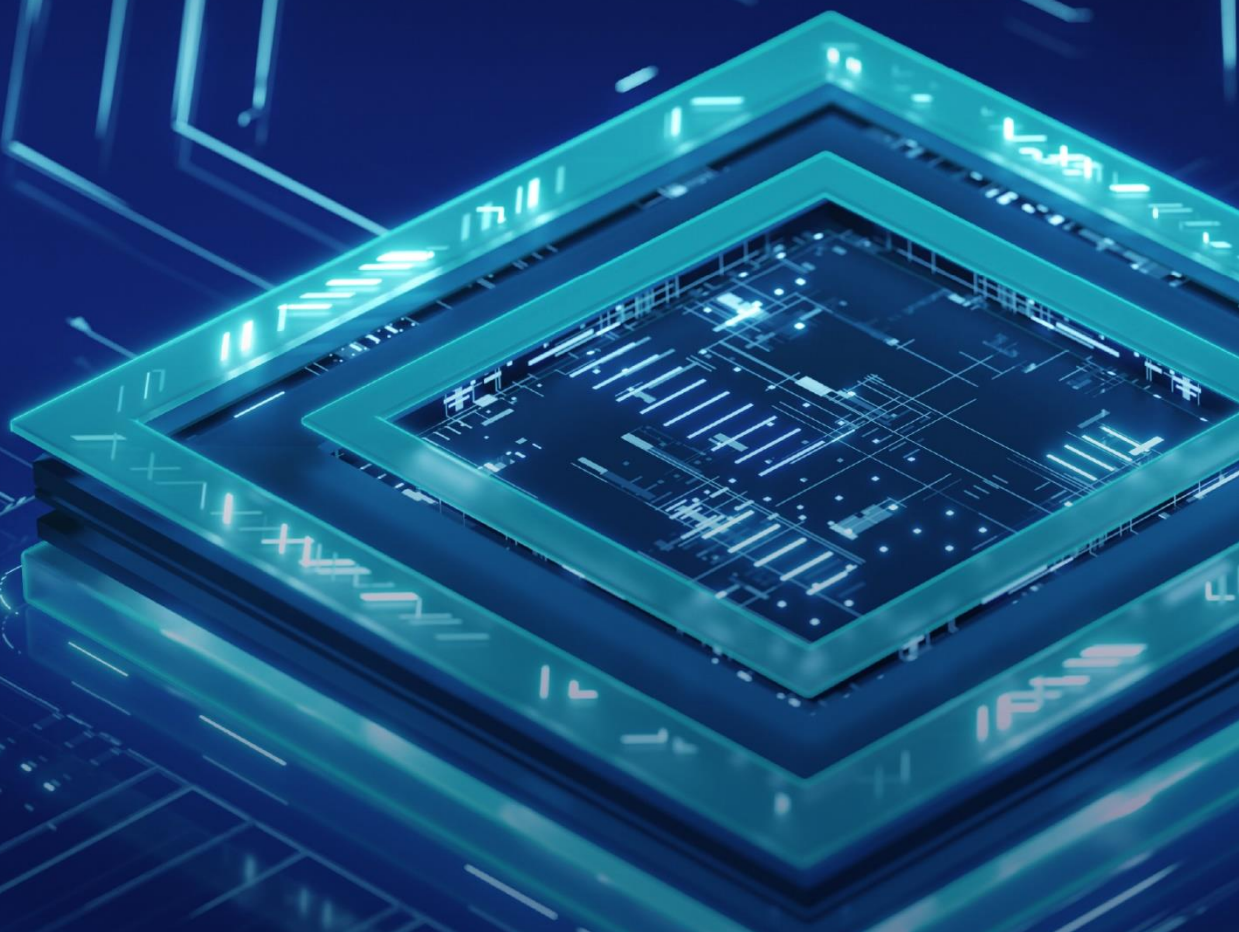
(Draft for Public Consultation)

QUANTUM-SAFE MIGRATION HANDBOOK



CSA SINGAPORE
Cyber Security Agency of Singapore

GOVTECH SINGAPORE

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

This document was developed based on contributions, or publicly-available material, from private and public -sector organisations. We thank those organisations for their valuable contributions. The handbook provides practical advice on preparing and planning for quantum-safe migration. This document is intended for informational purposes only and is not mandatory, prescriptive or exhaustive.

Developed by CSA, GovTech, IMDA, based on contributions, or publicly-available material, from industry partners, including:

- Accenture
- Amazon Web Services
- Deloitte & Touche LLP
- IBM
- PQStation
- The Association of Information Security Professionals (AiSP)

DISCLAIMER

The information provided in this document is voluntary and does not, and is not intended to, constitute legal advice. All information is for general informational purposes only. Not all the considerations or measures listed in this document will be applicable to all organisations or environments. Organisations may also be at different stages of cybersecurity maturity or readiness, and are advised to consider how to conduct the quantum-safe migration measures within their specific circumstances, in addition to other measures relevant to their needs.

The information has been gathered across public and private collaborators, referencing existing understanding and deployment of quantum-safe solutions. Technology advancements may render the information in this document inaccurate and outdated. 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 handbook. This document contains links to other third-party websites. Such links are informational and do not represent endorsement of content from these third-party sites.

VERSION HISTORY

VERSION	DATE RELEASED	REMARKS
0.1	23 OCT 2025	Release of Draft Quantum-safe Handbook for Public Consultation

Preface

The 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 at this point about how technology will develop or which approaches will prove most effective. The issue is complex and dynamic, and will continue to evolve quickly with scientific breakthroughs and geopolitical shifts.

Despite this uncertainty, there is increasing consensus that organisations should start preparation as soon as practically possible, especially for critical systems where the risks of inaction are the greatest. This is because quantum-safe migration is likely to be a non-trivial effort, and will require resources, funding and time to complete. At the same time, organisations need not rush into implementation. There can be first-mover disadvantages given that the quantum-safe field continues to evolve. Some actions are “no-regrets” and can be taken immediately. Other techniques and solutions are less well understood and require further monitoring and careful evaluation, to avoid unintended costs or abortive efforts.

This handbook therefore aims to strike a practical balance: to seed readiness for quantum-safe migration in a considered way, while staying adaptive to emerging developments and solutions.

Table of contents

Purpose

This handbook provides guidance for organisations, in particular Critical Information Infrastructure (CII) owners and government agencies, in preparing for the transition to quantum-safe. It explains what is at stake, highlights key areas of focus, and sets out practical considerations and resources for organisations to begin building readiness.

The advice in this handbook is voluntary, and not all the considerations or measures listed in this document will be applicable to all organisations or environments. Organisations may also be at different stages of cybersecurity maturity or readiness, and should consider relevance to their use cases as well.

Understanding the Quantum Threat

Key takeaways:

1. The threat of breaking cryptography is not new, but quantum computing will amplify the likelihood, scale and impact.
2. The quantum threat affects the confidentiality, integrity and availability of your organisation's systems and data. These have implications for your organisation's risk posture, business continuity and reputation.

Cryptography underpins the security of our digital communications and data, forming the foundation of trust in today's digital world. It secures the messages we exchange, online transactions conducted, and the systems we depend on – from online banking and cloud applications to government platforms and critical services. The threat of breaking cryptography is a long-standing one, and there are significant security (and downstream economic) risks. However, computational problems underpinning cryptography continue to be intractable for classical computers, even supercomputers, today. The arrival of powerful enough quantum computers will upend this paradigm assumption, as it is expected that threat actors will misuse quantum computing to break encryption, placing sensitive data and digital trust at significantly higher risk.

Cryptography is used for a variety of use cases.

Public Key Cryptography

<u>Key Establishment</u>

Key establishment is a cryptographic process that allows two parties to establish a shared secret key. This shared secret can subsequently be used to facilitate the encryption of communication between the two parties. This can be achieved via *key encapsulation*, where the secret is generated and encrypted by one party and sent to the other, or via *key exchange*, where public keys are exchanged between the two parties allowing them to derive the same secret based on their own private keys.

Key establishment is used in secure communication protocols, such as TLS, SSH, IPSEC, and S/MIME, prior to confidential data being sent between the two parties. Key establishment may also be used in file encryption solutions, where an entity wants to encrypt many files with different keys but does not wish to keep track of numerous secret keys. Examples of key establishment algorithms commonly used are Rivest-Shamir-Adleman (RSA), Elliptic Curve Diffie-Hellman (ECDH), DSA, and Diffie-Hellman (DH).

Digital Signatures

A digital signature, analogous to a physical signature, is a cryptographic algorithm where a party signs a piece of data. This allows another party to verify that the signature is authentic, the data has not been modified, and the signer cannot repudiate the signature.

Digital signatures are used primarily for authentication, to prove that a party is who they claim to be, or that the data received did indeed originate from the sender. Solutions where digital signatures are used include solutions for identity management, access control, electronic signatures, as well as secure communication protocols where authentication of the communicating party is needed. Examples of digital signature algorithms commonly used are RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), Digital Signature Algorithm (DSA).

Symmetric Ciphers

A symmetric cipher is a cryptographic algorithm used to encrypt data using a secret key, so that it can be decrypted later with the same key. While encryption was the original motivation for cryptography, it must often be used alongside many different types of cryptography to achieve the spectrum of logical security functionalities we use daily.

In secure communication, symmetric ciphers are used to encrypt the data to be communicated, while the secret key is established through a separate key establishment mechanism. An example of a commonly used symmetric cipher is Advanced Encryption Standard (AES).

Hash Functions

A hash function is a cryptographic algorithm used to produce a pseudorandom digest of fixed length from an input of any size. It is based on the difficult problem of finding a suitable input that results in a specific output. As hash functions can be used with or without cryptographic keys, it is a very versatile algorithm that is combined with different types of cryptographic algorithms for many protocols. Examples of hash functions commonly used are Secure Hash Algorithm (SHA)-1, SHA-2, and SHA-3.

Hash functions can be found in many security mechanisms, including:

- Password protection – the hash value of a password is stored, instead of the password itself;
- Digital signatures – the data to be signed may be hashed prior to signing;

- Key derivation – the hash of specific data or password, sometimes including a master key, is used as a secret key;
- Message authentication codes – the message is hashed, together with a secret key, to obtain a means to verify the authenticity of the message as well as its integrity.
- Post Quantum Cryptography (PQC) – hash functions can be used not just with but also used to construct PQC. Examples of hash-based PQC are SLH-DSA, XMSS and LMS.

The exact timeline for "Q-day" – when a Cryptanalytically Relevant Quantum Computer (CRQC) is capable of executing algorithms that can break or significantly weaken today's widely deployed cryptography – cannot be predicted with precision. Expert estimates generally place this horizon within the next 5-10 years. However, this could shorten considerably due to unforeseen scientific advances, algorithmic optimisations, or covert developments by sophisticated actors.

Q-day can come much earlier than expected. This could be due to unforeseen scientific advances, algorithmic optimisations, or covert developments by sophisticated actors.

There are currently two quantum computing algorithms that have been shown to break encryption.

- Shor's algorithm can solve the mathematical problem of large prime factorisation and discrete logarithm, with an exponential speed up over classical methods. As such, public key cryptography used today that relies on the difficulty of solving this problem for their security cannot be relied on. Examples include:
    - Integer factoring-based: RSA;
    - Discrete logarithm-based: ECDSA, ECDH, DSA, DH

- Grover's algorithm can solve unstructured search problems and has demonstrated quadratic reduction in the time needed for brute force key search attacks. There is currently debate as to what the effective reduction in cryptographic security is, due to the significant tradeoffs in terms of memory and hardware needed to implement such an attack. Nevertheless, Grover's can be used to improve brute force attacks on all cryptography even if its impact on their security is not as drastic as that of Shor's. Examples of cryptography that may need to be upgraded or replaced due to the threat from Grover's algorithm, but not Shor's, include:

- Symmetric Ciphers: AES
- Hash Functions: SHA (including SHA1, SHA2, SHA3)

The vulnerable cryptography algorithms listed here serve as most of the public-key cryptography in use today and will need to be replaced. Other than public key cryptography, cryptography like symmetric ciphers and hash functions are also affected by the quantum threat, albeit to a lesser degree. These may still be used, depending on the use case and security level needed. We continue to observe new advancements in algorithms, including optimisation for speed and performance, that will further affect how fast the quantum threat manifests. The reality is further complicated by limited visibility into quantum computing developments, given that the field is subject to commercial competition and geopolitical sensitivities.

A CRQC can be misused to undermine the confidentiality, integrity and availability of your organisation's systems and data.

	Confidentiality *Exposure of sensitive information at rest or in transit*	**Integrity** *Manipulation of transactions and processes*	**Availability** *Disruption of essential services*
Examples	• Exfiltration and decryption of sensitive or confidential data, such as Personally Identifiable Information (PII), medical records, organisational secrets, eroding trust and violating privacy • Exfiltration and decryption of security or system-related data, such as passwords, credentials, and system configuration parameters, that can be used to gain access to and exploit systems	• Compromised authenticity of controls (e.g. forged signatures) that enable manipulation of transactions or modification of data	• Compromised authenticity of controls (e.g. forged signatures) that enable the manipulation of ICS and SCADA commands that halt functionality of essential services (e.g. water filtration)

If unaddressed, the quantum threat can hence lead to data breaches, operational disruption, and potential financial loss as well. It can also expose organisations to legal and compliance risks such as privacy law violations and intellectual property theft, ultimately leading to loss of stakeholder confidence and reputation damage that can be difficult to recover from.

Quantum-safe Migration

Key takeaways:

1. Q-day is a when and not an if – organisations should start preparing and planning now as it will take significant effort and time to migrate.
2. However, there is no need to rush into implementation too quickly, as the quantum-safe solution space is still developing. Use the time to seed readiness and build capability.

Quantum-safe migration aims at ensuring that digital systems and cryptography assets are resistant to attacks from CRQCs, by removing vulnerable cryptography and putting in place quantum-safe solutions. While quantum-safe solutions may be new, the threat and mitigation processes involved are not. In practice, the associated efforts will cover 5 key domains:

5 Key Domains for Quantum-Safe Migration

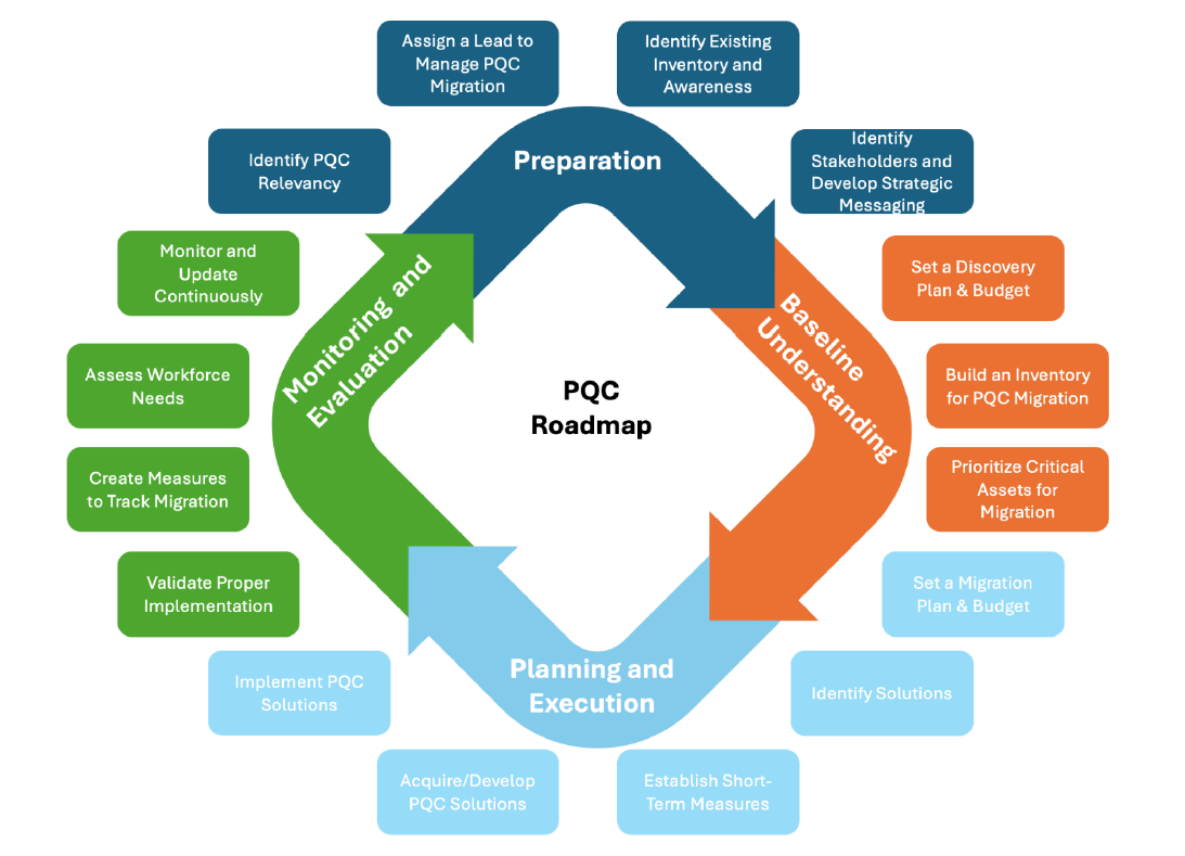
Risk Assessments	Identify and prioritise your key assets
Governance	Establish a coordinated and sustainable plan across the organisation
Technology	Guide the implementation steps and considerations to execute migration
Training & Capability	Develop the knowledge and competencies needed for migration
External Engagements	Work with vendors and ecosystem partners to drive migration

Quantum-safe migration is likely to be a multi-year endeavour, given the complexity and scale of the efforts required. Organisations should also note that migration of systems is likely to be executed in phases.

Developing a roadmap with a multi-year planning horizon can be helpful to track what needs to be done to prepare now, and what can wait while solutions and standards continue to mature. There are different resources that may be useful in helping your organisation to break down the quantum-safe migration process into discrete, more

manageable tasks. For example, the Post-Quantum Cryptography Coalition recommends a roadmap implementation per the figure below.

PQC Roadmap Categories (from PQCC)



Organisations may also refer to the following resources for examples of quantum-safe roadmaps:

- PQC Migration Roadmap, PQCC (2025)
- SP 1800-38B (Prelim.) - Migration to PQC: Cryptographic Discovery, NIST NCCoE (2023)
- TR 103 619 v1.1.1 - Migration Strategies & Recommendations to Quantum-Safe Cryptography, ETSI (2020)
- Preparing for a Post-Quantum World by Managing Cryptographic Risk, FS-ISAC (2023)
- The PQC Migration Handbook (2nd ed.), TNO/CWI/AIVD (2024)
- IBM Quantum Safe

While there is uncertainty over the Q-day timeline, preparation and planning for quantum-safe migration should start as soon as practically possible. This is especially so for critical systems where the risks of inaction are the greatest. Cryptography can be deeply embedded

in infrastructural components such as software libraries, and discovering and replacing vulnerable cryptography are likely to be a non-trivial effort. Experts also assess that the harvest-now-decrypt-later threat is ongoing, particularly for high-value data. As such, migration is a risk management measure – the later it is conducted, the wider the risk exposure window for your organisation's systems and data.

Harvest-Now-Decrypt-Later refers to a tactic where attackers capture and store encrypted data today, with the intent to decrypt it in the future when a CRQC is available. High value data with long shelf-life will be most vulnerable, as future decryption could yield significant advantage or information. Examples of such data include intellectual property, and personal financial and health records.

Migration should not be seen only about addressing the quantum threat. For some organisations, the primary motivator may be the direct risk from the quantum threat; for others, the quantum threat can be seen as a catalyst to review and "spring clean" and strengthen your organisation's cybersecurity hygiene, and value-add to your organisation's competitiveness and ability to better conduct business and serve your customers.

The quantum-safe solution space continues to evolve, and standards are still in development. There can be first mover disadvantages given that the quantum-safe field continues to evolve. This handbook therefore aims to strike a practical balance: to seed readiness for quantum-safe migration in a considered way, while maintaining space for emerging developments and solutions.

We cannot be fully certain at this point about how technology will develop or which approaches will prove most effective. The field will continue to evolve quickly with scientific breakthroughs and geopolitical shifts.

As such, this document will be kept live and updated to account for material developments as necessary. Organisations should continue to monitor developments, consider their operating context to guide their quantum-safe migration plans and incorporate cryptographic agility where practical (refer to Domain 3: Technology on cryptographic agility).

Domain 1: Risk Assessment

Key takeaways:

1. Leverage risk assessments to inform how your organisation prioritises preparation and planning. This helps to scope the problem down and focus efforts and resources, rather than tackle organisation-wide migration at once.

Cybersecurity risk assessment is an integral part of an organisation's enterprise risk management process and continues to be relevant in dealing with quantum-related risks.

- Given the diversity of systems and operating context across organisations, there is no one-size-fits-all solution to quantum-safe migration. Effective migration starts with conducting a risk assessment, which will help your organisation to identify priorities, potential risks, and the appropriate risk management strategies. Taking a risk-based approach will enable prioritisation of efforts where it matters most.

- This assessment enables organisations to determine the level and area of exposure, and to inform how to effectively allocate resources and implement appropriate actions to address these risks.

Risk assessments can be conducted based on best practices or your organisation's existing Enterprise Risk Assessment/Management Framework. Organisations can refer to established frameworks for business impact analysis, continuity planning, and quantitative risk assessment (e.g. ISO/TS 22317 (Business Impact Analysis), ISO 22301 (Business Continuity Management Systems, NIST SP 800-34 (Contingency Planning), or FAIR (Factor Analysis of Information Risk)). Organisations can also refer to CSA's published guides, if applicable:

- Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure
- Guide to Cyber Threat Modelling

We highlight three considerations to guide organisations' risk assessments.

Identifying which systems, data, or assets to prioritise

Organisations can first identify and prioritise their most critical business functions, systems, and information assets - so-called 'crown jewels'.

This can help to break down migration into risk-based, more digestible steps, than addressing the whole-of-organisation at once, which can be very complex and challenging. Such systems could be where compromise could result in significant operational, financial, or reputational impact. These can take the form of data breaches compromising sensitive information, operational interruptions affecting essential service delivery or key business services to customers, non-compliance with regulatory requirements, financial losses impacting business sustainability, and/ or reputational damage.

Identifying these critical assets will help your organisation understand where the risk impact is highest, and where to focus migration efforts as a start.

Examples of adverse business consequences

Data breaches	Exposure of sensitive customer, partner, and proprietary information
Operational disruption	Compromised systems and service interruptions due to broken security mechanisms
Legal and compliance risk	Violation of privacy laws, intellectual property theft, and contractual breaches
Financial loss	Costs arising from breach response, regulatory penalties, and legal liabilities
Reputational damage	Loss of stakeholder trust, brand harm, and the public fallout of large-scale incidents

Cryptographic asset discovery

For the identified critical systems, conduct cryptographic asset discovery to determine where and what could be vulnerable cryptography. This refers to the process of identifying and cataloguing cryptographic resources within your organisation's systems to understand and manage their security posture.

Cryptographic asset discovery involves locating assets such as cryptographic algorithms, protocols and digital certificates within system components such as Hardware Security Modules (HSM), smart cards or cryptographic tokens and Trusted Platform Modules. Such discovery can be daunting as cryptographic assets can be deeply embedded within such components or even managed externally. For a single function, different cryptographic assets may be in place (e.g. email content might use end-to-end S/MIME encryption while its client-server communication channel relies on separate TLS protection), raising complexity of discovery efforts. As such, prioritising such efforts for critical assets can help to manage the resources and efforts involved, as opposed to a comprehensive discovery effort across the organisation.

Organisations may refer to the following examples of system components that may contain cryptographic assets to support their asset discovery activities.

S/N	Category	Components
1	Cryptographic Modules	• Hardware Security Modules • Smart Cards/Cryptographic token • Trusted Platform Modules • Cryptographic libraries
2	Cryptographic Application	• Secure email • File and Folder encryption • VPN Clients • TLS Clients/Servers • SSH Clients/Servers • Database encryption
3	Cryptographic System	• Public Key Infrastructure (PKI)/Certificate Authorities • Identity and Access Management • Email exchange server • Key Management System • Certificate Management System

Asset discovery can be done in a phased and incremental way.

- First, use what you already have and know. By starting with existing documentation and technical artefacts, you can gain meaningful initial insights with minimal disruption. For example, logs from components such as Hardware Security Module (HSM), Key Management Systems (KMS) and Certificate Management Systems (CMS) can offer visibility into active keys and certificates. Configurations applied on load balancers, and web servers can provide insights into the protocols and cipher suite used in external facing network paths. Network monitoring tools can provide visibility to the network protocols used in internal network traffic. Similarly, network diagrams, system inventories, and penetration testing reports may already highlight where cryptographic controls are applied. By starting with these readily available resources, organisations can take a practical and less effort-intensive approach to begin mapping out their cryptographic assets.

- Second, leverage Automated Cryptographic Discovery and Inventory (ACDI) tools. These have emerged as a promising way to enhance cryptographic discovery efforts, and use automation to provide central visibility, streamlining and reducing the

manual workload involved in cryptographic asset discovery. However, many tools are still in the early stages of development, and vendors continue to expand their roadmaps to support more cryptographic use cases, asset types, and deployment models. As a result, these tools are unlikely to be able to fully execute the asset discovery process at this point.

Currently, ACDI tools scan for cryptographic assets based on three approaches.

- Code scanning – Involves examining source code to identify cryptographic libraries, APIs, and functions that are imported and used during development. If the organisation has in-house development capabilities, it is advisable to integrate code scanning tools into the Continuous Integration/Continuous Deployment (CI/CD) pipeline. This enables automated and consistent detection of cryptographic usage, potential vulnerabilities, and policy violations early in the software development lifecycle.

- Network analysis – Involves analysing network traffic to detect the use of cryptographic protocols (e.g. TLS, SSH) and their configurations. This helps identify non-quantum safe or insecure implementations, weak cipher suites, expired certificates, or unencrypted traffic traversing the network.

- Host scanning – Examining endpoints, servers, and devices to detect stored cryptographic assets and usage.

When selecting and deploying ACDI tools, organisations should consider:

- Your operating environment. For example, are your systems deployed on-premise, or via the cloud? Do you have access to source code?

- Your needs and scope. What type of assets do you have limited existing visibility over, where tools are needed to support assets discovery? What type of infrastructure needs to be scanned (e.g. endpoints, code repositories)?

- Integration with your current enterprise environment. Many ACDI tools now feature built-in integration capabilities with existing enterprise security solutions, eliminating the need for additional agents or sensors. These native integrations commonly include firewalls, Endpoint Detection and Response (EDR) systems, Extended Detection and Response (XDR) platforms, Configuration Management Databases (CMDB) and Vulnerability management platforms.

- Maturity and effectiveness of the solution. Ask the vendor for references of previous applications of their ACDI tool to determine if it is relevant for your needs.

As the ACDI tooling space continues to evolve, organisations should continue to work with solution providers and vendors to understand what options are relevant to their use cases and systems before making significant investments in such tooling.

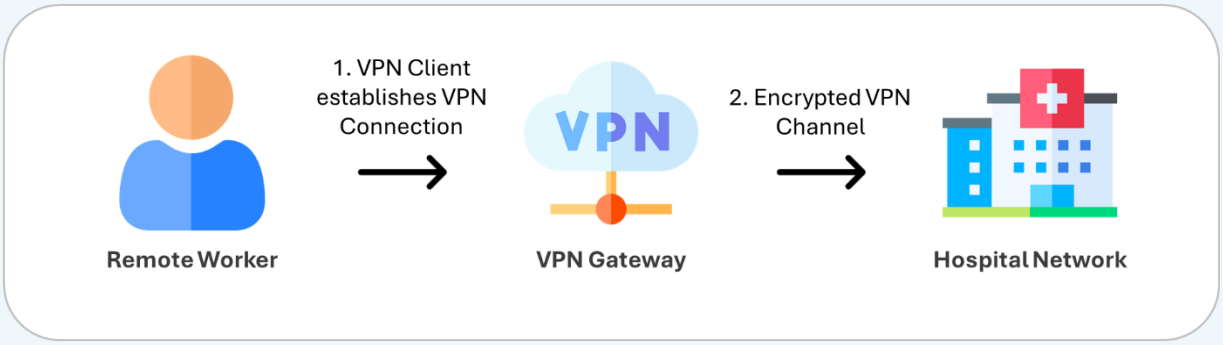
Leverage threat modelling

Threat modelling can help to further supplement the risk assessment and inform where efforts should be prioritised. Threat modelling involves taking the perspective of an attacker to identify potential weaknesses and key attack vectors that should be addressed early.

We illustrate two threat modelling examples to show how it can be applied to better understand quantum-related risks.

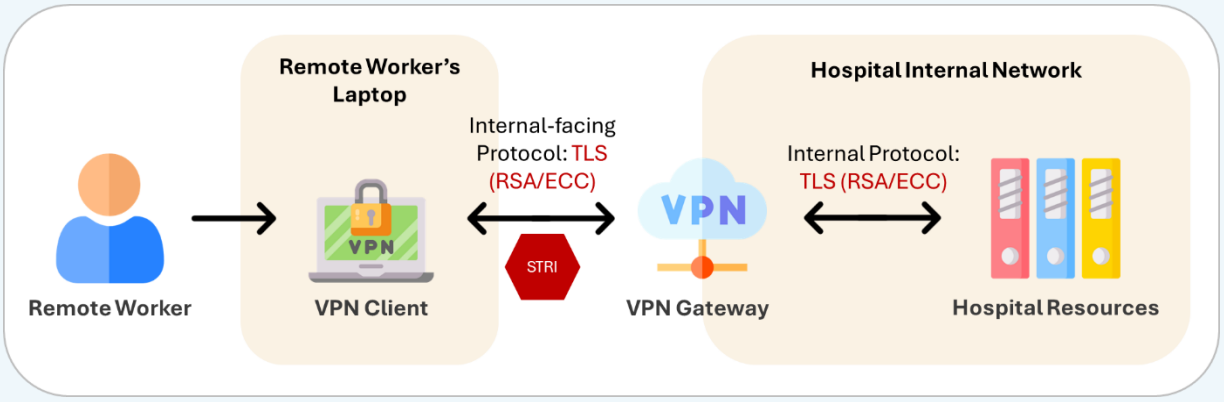
Example 1: Enterprise system accessed remotely by an employee
This example highlights the scenario of a healthcare worker working remotely, accessing the hospital network over the internet.

The diagram below shows the simplified process flow of a healthcare worker remotely accessing the hospital network.

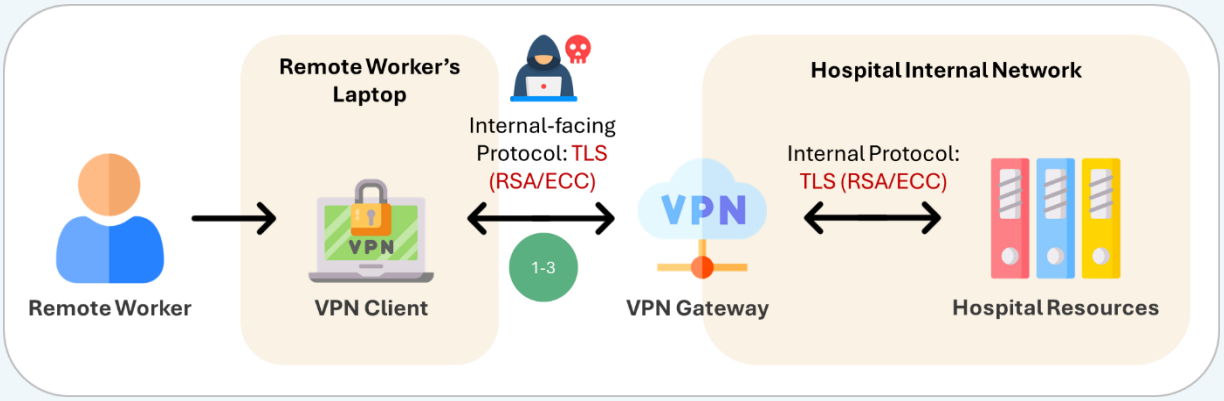


A closer look at the components and connections reveals potential vulnerabilities. Transport Layer Security (TLS) is used to provide end-to-end security for communications with the hospital network. However, the underlying asymmetric cryptography (RSA, ECC) used by TLS is quantum-vulnerable. [Note: At this juncture, versions of TLS older than 1.3 do not support PQC] In this scenario, the remote worker accesses the hospital network via the internet.

Using the STRIDE-LM threat modelling framework, the hospital's VPN infrastructure that secures internet-facing communications using RSA/ECC is at the highest risk of Spoofing, Tampering, Repudiation and Information Disclosure (STRI) by a quantum-enabled threat actor.



Based on the above, and referencing the MITRE ATT&CK framework, a hypothetical attack path and threat scenario might look something like this:



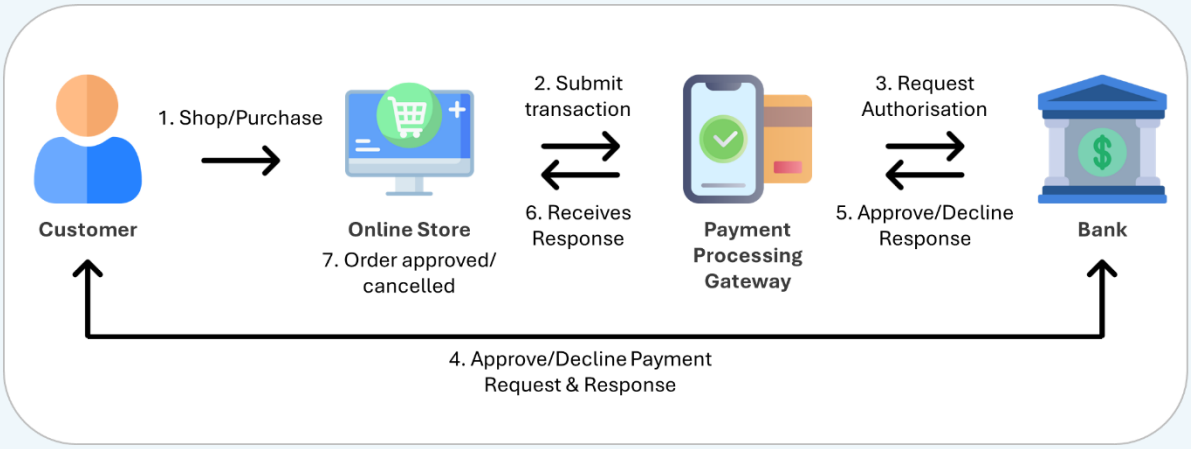
Step	Action	Threat Scenario
1	**[Collection] T1557: Adversary-in-the-Middle** A quantum-enabled threat actor breaks the encryption used by the remote worker's VPN and positions themselves between the communication of the customer and the hospital network.	A quantum-enabled threat actor may successfully intercept and decrypt internet-facing communications between remote workers and the hospital containing
2	**[Exfiltration] T1020: Automated Exfiltration**	

	The threat actor automatically exfiltrates any sensitive data that the remote worker accesses.	sensitive patient data, leading to sensitive information disclosure. The threat actors may threaten to release the information publicly or use the information for blackmail.
3	**[Impact] T1657: Financial Theft** The threat actor may use the sensitive data to extort the hospital by threatening to release the data and impact the hospital's reputation.	

In this scenario, the hospital should focus on understanding the external connectivity of their systems, such as how its VPN clients connect to the VPN gateway, and assess how PQC can be incorporated to secure the communication channels.

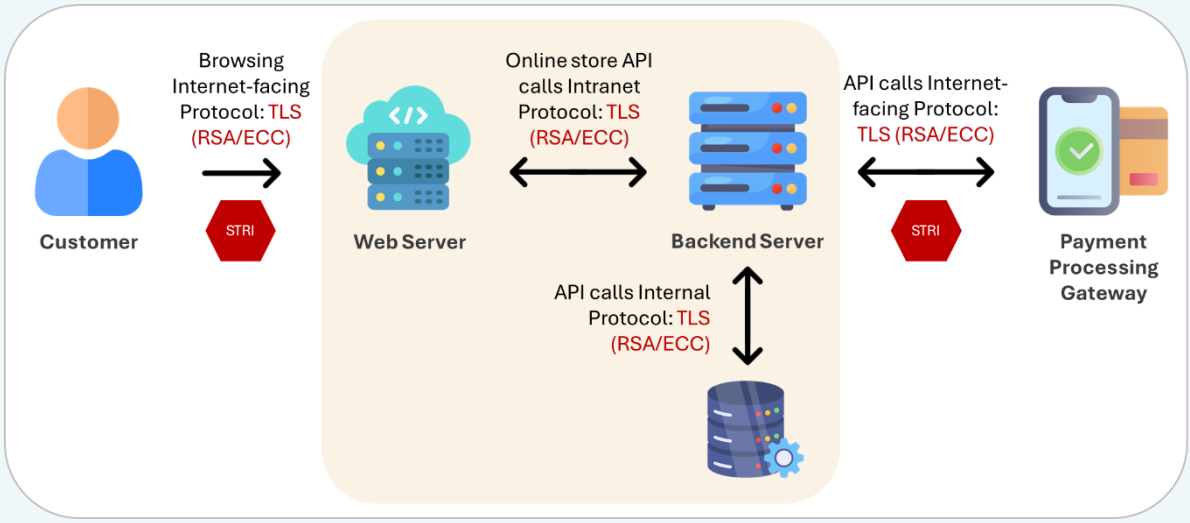
Example 2: Customer makes online purchase with a retailer
This example highlights the scenario of a customer making an order with an online retailer.

The diagram below shows the simplified process flow of a customer making an order with an online retailer.

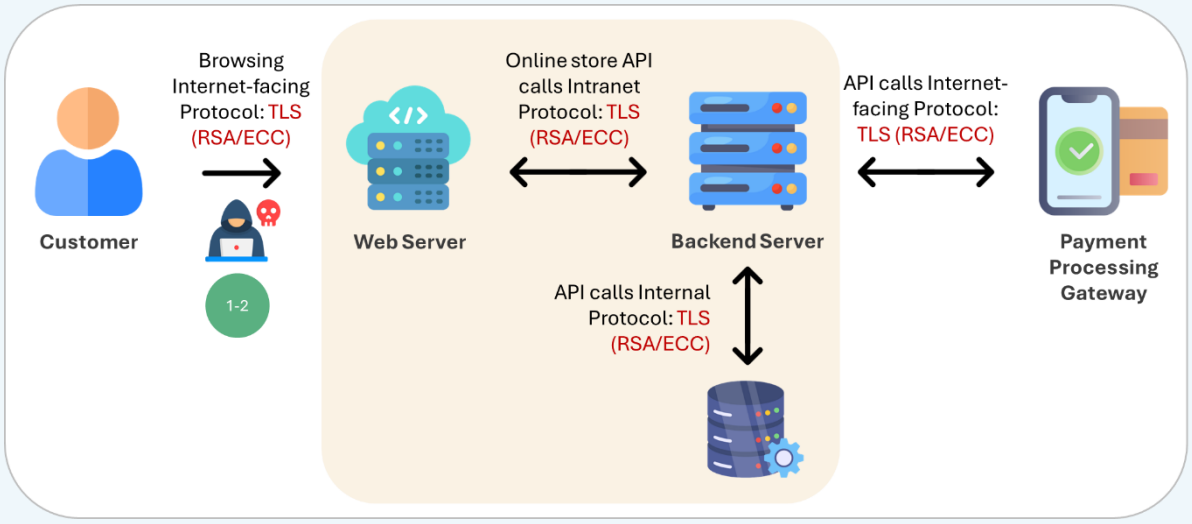


A closer look at the components and connections reveals potential vulnerabilities. In this scenario, the customer, online store and payment processing gateway communicate via the internet. Generally, internet-facing connections are at higher-risk and system owners have less control over external communication channels. Hence, securing external connectivity should be prioritised.

Using the STRIDE-LM threat modelling framework, the identified threat areas show that the internet-facing communications using RSA/ECC are at the highest risk of Spoofing, Tampering, Repudiation and Information Disclosure by a quantum-enabled threat actor.



Based on the above, and referencing the MITRE ATT&CK framework, a hypothetical attack path and threat scenario might look something like this:



Step	Action	Threat Scenario
1	**[Collection] T1557: Adversary-in-the-Middle** A quantum-enabled threat actor breaks the encryption used by the secure channel between the customer and online store and positions themselves between the communication of the customer and online store.	A quantum-enabled threat actor may successfully intercept and decrypt internet-facing communications and possibly modify the

2	**[Impact] T1565.002: Transmitted Data Manipulation** The threat actor manipulates the transaction data between the customer and online store, possibly making fraudulent orders that may have adverse impacts on the customer and online store.	information being transmitted, leading to fraudulent or inaccurate transactions if not detected.

In this scenario, the retailer should focus on understanding the external connectivity of their systems, particularly the connections between the customer and the web server hosting the online store, and between the backend server and payment processing gateway. This can then inform how PQC can be incorporated to secure these communication channels.

After conducting a risk assessment and prioritising areas to address based on the risk, organisations can then identify and implement actions to secure the system. This is detailed in the subsequent sections on governance, technology, external engagements and training and capability.

Domain 2: Governance

Key takeaways:

1. Being clear on the stakeholders involved, and their roles and responsibilities, as well as timelines and key milestones, will help to ensure coordinated execution, with accountability and measurable progress.
2. Quantum-safe migration should be incorporated into existing governance and risk management structures, to streamline access to systems, data, and policy/ other levers.
3. Review your policies and strategies regularly to ensure relevance, given the evolving quantum threat.

Governance entails ensuring there are framework(s) and/ or policies in place that set out the organisation's strategy and approach for quantum-safe migration, and the roles and responsibilities of stakeholders.

Rather than conducting governance for quantum-safe migration as an isolated workstream, organisations should embed it within their existing governance frameworks. This will help to maintain alignment with established risk management and compliance structures across critical organisational functions.

Establishing clear roles and responsibilities to support quantum-safe migration

There are four key stakeholder groups within your organisation that are likely to be involved in quantum-safe migration:

- Senior management and decision makers. This can include your executive boards, C-suite. This group will need to approve and support quantum-safe migration plans, especially where they involve resources and efforts.

- Cybersecurity teams. This can entail the teams that report to the Chief Information Security Officer, or equivalent teams that are responsible for protecting your organisation's data and IT systems from cyber threats. This group will identify, recommend and evaluate security solutions to address the quantum threat.

- IT and technology strategy teams. This can entail the teams that report to the Chief Information Officer, or equivalent teams that are in charge of the organisation's overall IT infrastructure and systems to meet business goals. This group will need to identify systems that are business-critical and should be prioritised for the quantum threat, and will need to update the IT policies, infrastructure and systems to address the quantum threat with support of the cybersecurity teams.

- Business units. This entails the different teams and units that operate and execute their specific business functions and manage their own operations and resources. This group will work with the security and technology strategy teams to align its goals and needs for quantum-safe migration, including to ensure that business needs continue to be addressed and that any potential downtime and disruption are minimised.

Establishing roles and responsibilities for quantum-safe migration based on these existing stakeholder groups will enable you to tap on established strengths and competencies, as well as existing lines of communication and reporting. In turn, this will ensure that quantum-safe migration is addressed in a sustainable and effective way. It is possible to set up a separate team dedicated to execute quantum-safe migration, but that team would still need to interact with these stakeholder groups, and may incur trade-offs in terms of clarity of roles and responsibilities, as well as delays in starting work due to the need to establish new structures and capabilities.

For each of these stakeholder groups, defining clear roles and responsibilities between teams, as well as timelines and key milestones will help to ensure coordinated execution, with accountability and measurable progress.

Organisations can consider frameworks like the RACI model to assign clear roles for tasks and deliverables in quantum-safe migration. This can also help to ensure accountability.

- Responsible (does the work)
- Accountable (owns the work and approves it)
- Consulted (provides input)
- Informed (receives updates)

Example of a RACI model for quantum-safe migration

Based on PQC Migration Roadmap | Post-Quantum Cryptography Coalition

Task / Responsibility	IT Steering Committee	CISO	CIO	Business Owner
Stage 1: Preparation				
1. 1 Identify PQC Relevancy	A	R	R	C
1.2 Assign a Lead to Manage PQC Migration	A	C	R	I

1.3 Establish migration vision & governance	A	C	R	R
1.4 Identify Existing Inventory	I	C	R	A
Stage 2: Baseline Understanding				
2.3 Prioritise high-value systems and data	I	R	R	A
2.1 Set a Cryptographic Discovery Plan	I	R	A	I
2.2 Build and maintain an up-to-date cryptographic inventory	I	R	A	I
Stage 3: Planning and Execution				
3.1 Set a Migration Plan and Budget	I	R	A	C
3.2 Identify Solutions a. Select PQC algorithms and migration strategies b. Implement and test PQC in systems c. Upgrade crypto libraries and configurations	I	R	A	C
3.3 Coordinate vendor and third-party assessments	I	R	A	C
Stage 4: Monitoring and Evaluation				
4.1 Validate Proper Implementation a. Oversee compliance, policy, and assurance alignment b. Manage project milestones and reporting	I	R	A	C
4.3 Assess Workforce Needs a. Conduct training and awareness activities	A	R	R	C
4.4 Continuous Monitoring	I	R	A	I

Reviewing and adapting organisational policies and strategies

Review your organisation's existing policies to understand how to integrate quantum-safe requirements, as the quantum threat presents a long-term risk with strategic and operational implications.

- Update your organisations' cryptographic policies to keep track of the cryptography inventory, and timely disallowing of vulnerable cryptography and/or integrating newer encryption algorithms.

- Integrate quantum-related risks as part of your broader enterprise risk management frameworks and business continuity planning. The risk description should be guided by your assessments of the quantum-related risks to your business-critical systems and data. Accordingly, integrate quantum-safe migration as part of risk treatment action plans. This includes developing your multi-year roadmap or strategy for quantum-safe migration. Establish processes for monitoring progress across your organisation. This can be measured against key performance indicators (KPIs) and metrics, including cryptographic inventory completion rates, system migration milestones or percentages.

- Update your procurement policies and frameworks to explicitly address quantum-safe requirements. This includes specifying cryptographic specifications in line with your cryptographic policies, regulatory requirements or standards, and cryptographic agility capabilities, and requiring vendors to submit post-quantum roadmaps as part of the evaluation process. Contractual clauses should also be reviewed; where relevant, clauses that address PQC support, cryptographic algorithm update mechanisms, service level agreements for quantum-safe transitions, and escalation procedures for addressing emerging quantum-related vulnerabilities can be included.

- Third party risk management policies can also be updated to reflect evaluation criteria for assessing vendors' quantum readiness or maturity (e.g. current cryptographic implementations and PQC adoption timelines), and their ability to support future cryptographic transitions without significant system overhauls. More information on engaging vendors is in Domain 5: External Engagements.

Migration should also be seen as an iterative process – rather than a one-off effort - as quantum computers continue to grow more powerful, and existing quantum-safe solutions may eventually become vulnerable to attacks. As such, organisations should review their policies and strategies regularly to ensure that they continue to be relevant. Organisations should also keep abreast of evolving standards, guidance and regulatory requirements in this space, such as by establishing the necessary processes or engagements to do so. For standards, the relevant bodies include the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and ETSI. For Singapore,

organisations should consult the CSA, as the national cybersecurity authority, or sectoral regulators for advice.

International governments like the US and EU have issued guidelines outlining timelines and requirements for quantum-safe migration, such as the US Commercial National Security Algorithm Suite (CNSA) 2.0 that provides requirements for national security systems, and the EU's Quantum-Safe Cryptography Roadmap on the timelines for transition to PQC for EU Member States. This reflects growing international momentum and interest to drive quantum-safe migration efforts.

For Singapore, we recognise the value of such guidance in supporting organisations' quantum-safe migration journey. We are engaging key stakeholders across industry and the government to develop practical and relevant guidance for our local context.

Domain 3: Technology

Key takeaways:

1. Evaluate existing quantum-safe solutions that are relevant to your quantum-safe migration strategy, while maintaining space to adapt to new threats and solutions, as technology continues to advance.
2. Choose, test, validate and monitor your technology implementations to ensure that they address your migration goals.

Technology refers to the technical solutions that your organisation will put in place as part of quantum-safe migration. This can include classical solutions, such as AES at sufficiently large key sizes that continue to be considered quantum-safe. It also includes new techniques designed to be more resilient against quantum-enabled attacks such as Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD).

Understanding the technology options

Quantum-safe cryptography (QSC) refers to cryptographic methods that are believed to be secure against both classical and quantum computing attacks. These include existing symmetric ciphers and hash functions that are quantum-resistant, PQC, as well as quantum technologies such as QKD. QSC can also be used in hybrid or combination implementations.

Post Quantum Cryptography

PQC was developed as a response to the quantum threat to public-key cryptography. The primary goal of PQC is to be an in-place replacement for classical public-key cryptography that can run on classical computing hardware, with suitable options for every existing use case of public-key cryptography. It is designed to resist attacks by classical adversaries and quantum algorithms such as Shor's algorithm, and is designed to replace vulnerable classical encryption schemes such as asymmetric public-key cryptographic systems (e.g. RSA, ECDSA, Diffie-Hellman). Since 2016, there has been a concerted global effort to develop PQC, led by the US National Institute of Standards and Technology (NIST).

PQC Standardisation

In 2024, following eight years of review and study by international cryptographers, NIST published their first three PQC standards, namely:

- FIPS 203: ML-KEM, Module-Lattice Key Encapsulation Mechanism, based on algorithm CRYSTALS-Kyber;
- FIPS 204: ML-DSA, Module-Lattice Digital Signature Algorithm, based on algorithm CRYSTALS-Dilithium;
- FIPS 205: SLH-DSA, Stateless Hash-Based Digital Signature Standard, based on algorithm SPHINCS+

NIST has also announced two further PQC algorithms that are pending standardisation:

- FALCON, a lattice-based digital signature scheme;
- Hamming Quasi-Cyclic (HQC), a code-based key encapsulation mechanism as a backup to ML-KEM

- The security of PQC is based on the assumption that the underlying mathematical problems are too computationally complex for both quantum and classical computers to solve.

- There are different PQC algorithm families such as lattice-based, code-based, hash-based, isogeny-based, and multivariate algorithms. These descriptions refer to the underlying mathematical problems their security is based on.

- While PQC is ascertained to be quantum-safe against attacks based on known quantum algorithms, future improvements in quantum and classical cryptanalysis may necessitate an upgrade of key sizes or a change in algorithms.

PQC offers a comprehensive suite of cryptographic functionalities, including digital signatures, key exchange, and encryption, making it well-suited for integration into existing digital infrastructures with minimal disruption. PQC can be implemented in software or hardware. It can also be deployed into existing infrastructure and cryptographic libraries, making it relevant for many existing use cases.

- Some common use cases for PQC include network security (e.g. TLS, VPN, SSH, IPSEC), secure emails and messaging (e.g. S/MIME, PGP), signing of software and firmware, public key infrastructure (PKI), authentication and access control (e.g. smart cards, security tokens), encryption of storage (e.g. HSM).

- Deployment needs to account for performance overhead and impact due to increased PQC key sizes, signature lengths, and computation time compared to classical algorithms. Other requirements may include communication bandwidth and data storage, as PQC may require larger public keys and signatures which can affect scenarios like TLS handshake, network/ resource-constrained environments, and certificate chains.

Quantum Key Distribution

QKD is a quantum technology technique that uses the principles of quantum mechanics to enable two parties to generate a shared secret. QKD-generated and communicated keys are considered highly secure as any attempt at eavesdropping attacks can be automatically detected by the sender and receiver given that it disturbs the quantum states of the photons involved.

For specific use cases, e.g. where long-term confidentiality, high assurance, and critical infrastructure security are paramount, QKD may serve as a complementary security mechanism.

- There are different types of QKD network architectures such as point-to-point networks (requiring direct links between communicating parties), trusted node-based networks (that enable secure key exchange without direct point-to-point links between each party), and satellite-based networks (that extend distances for long-range QKD).

- Some notable use cases of QKD adoption include secure communication between geographically-separated locations (e.g. data centres), enhancing network security protocols and encryption (e.g. AES) using QKD-generated keys, and securing backbone networks (e.g. finance, energy, healthcare, telecommunications services, government, and defence).

- QKD does not replace digital signatures – it does not provide authentication unless combined with pre-shared keys or PQC signatures.

- While QKD itself is theoretically secure, robust implementation is needed to ensure that the physical setup is not vulnerable to side-channel attacks. The current state of technology also requires trusted nodes to be implemented to relay keys across longer distances. These trusted nodes also need to be individually secure in order to maintain the security of the entire system.

Use of QKD continues to move from lab environments into real-world deployment. However, given the potential vulnerabilities arising from real-world implementation (e.g. to side channel attacks), more testing and validation are needed to increase confidence in the use of QKD in wider adoption.

Nonetheless, standards bodies such as ISO and ETSI continue to develop standards for QKD security and testing. These will support deployment and testing when ready.

It is generally considered more expensive and complex to implement QKD.

- Physical infrastructure and integration are required for implementation, including specialised QKD hardware (as source of keys that are encoded in quantum states), quantum and classical channels (for transmission and distillation of keys), and quantum key management systems (to store and deliver QKD-generated keys). Other potential factors affecting deployment include the cost of QKD devices, scalability, coverage distance, and cross-vendor interoperability.

- Organisations may reduce the costs and complexity of owning specialised hardware and physical infrastructure by tapping on QKD solutions from service providers (e.g. QKD-as-a-service).

Organisations need to understand which of the existing cryptography they use today is vulnerable, as well as the potential quantum-safe replacement options. There may be performance and other operational trade-offs. For example, larger keys and stronger hashing may impact latency and computational performance, particularly in constrained environments (e.g. IoT and mobile).

Key Establishment

Key establishment may be accomplished using a pre-shared key (used with a symmetric cipher) or public-key cryptography. The quantum-safe options include continuing to use a pre-shared symmetric key of a suitably large size (e.g. AES-256), a PQC key establishment mechanism (ML-KEM), or QKD. Note that a pre-shared key scheme assumes the existence of a secure mechanism to share this initial key, so it does not by itself solve the problem of distributing keys between the two parties.

Digital Signatures

Digital signatures rely on public-key cryptography, and the only quantum-safe options are PQC (e.g. ML-DSA and SLH-DSA). There are other older quantum-safe options for digital signatures based on stateful hash constructions, namely XMSS and LMS, but as the secure implementation and usage of these algorithms are tricky, they are not expected to be widely adopted. To complement the PQC options for digital signatures, the search for more quantum-safe digital signatures is still ongoing to offer a greater variety of size and performance options.

Symmetric Ciphers

As the security of symmetric ciphers is not dependent on the factoring problem nor the discrete logarithm problem, they are not vulnerable to Shor's algorithm. However, given

that Grover's algorithm can impact their security, the security of symmetric ciphers with smaller key sizes may potentially be broken with advancements in CRQCs. Thus, organisations need to consider using AES with key sizes larger than 128 bits to reduce the quantum risk for systems using the symmetric cipher.

Hash Functions

Like symmetric ciphers, many existing hash functions are quantum-safe. Hash functions with output smaller than 256 bits are deemed as not quantum-safe and should no longer be used. This applies to all use cases for hash functions.

Enhancing cryptographic management practices

Quantum-safe migration also presents an opportunity for organisations to review their cryptographic management practices. While these do not directly mitigate the quantum threat, these are well-established, cost-effective practices that can be implemented now to improve the resilience, security, performance, and manageability of existing systems. Organisations can consider:

- Using stronger entropy sources for cryptographic schemes (e.g. true random number generator (TRNG)). These will introduce more unpredictability and randomness in the generation of cryptographic keys or values, thereby strengthening the security of the scheme.

- Strengthening key management practices across the key lifecycle, from generation to destruction. In practice, this can include key rotation policies (e.g. more frequent rotations limit the amount of data that could be exposed if a key is compromised), audit logs to track and verify security across the key lifecycle, and revocation mechanisms in case keys are found to be compromised. Organisations can also plan for PQC-enabled certificates, dual-key usage, and key management across trust chains.

- They also enable systems to be crypto-agile during quantum safe migration to PQC and/ or QKD, acting as fallback or backup cryptography during transition.

Hybrid cryptography implementations

Hybrid cryptography approaches refer to the combined use of multiple cryptographic mechanisms. This may involve classical cryptography algorithms, PQC, and/ or QKD protocols to provide defence-in-depth.

While often discussed as interim solutions on a complete quantum-safe migration, organisations can also consider hybrid implementations as part of the longer-term approach to optimise performance while raising quantum resistance. Hybrid implementations allow organisations to hedge against algorithmic uncertainty while maintaining interoperability with existing systems. Nonetheless, such approaches may introduce performance and complexity trade-offs, and require careful planning prior to implementation.

PQC-Classical and PQC-PQC Hybrid

This section discusses two hybrid types:

- PQC-Classical hybrid scheme, in which a classical algorithm and a PQC algorithm are used in parallel for key exchange or digital signatures. The combined result is used to perform functions like to secure a session, authenticate a message, verify a certificate, or encrypt data. The main goal is to integrate quantum-resistant algorithms while maintaining compatibility with existing systems. Such a hybrid scheme also offers a fail-safe mechanism for continued security and functionality even if the newly adopted PQC algorithm(s) encounters unexpected vulnerabilities or implementation issues.

- PQC–PQC hybrid, in which two or more PQC algorithms are used within a single cryptographic operation. This provides algorithmic diversity, to avoid single points of cryptographic failure due to potential vulnerabilities in any single class of PQC algorithms (e.g. lattice-based, hash-based).

Use cases include:

- Hybrid key exchange, in which multiple key exchange algorithms are used to derive a shared session key.

- Hybrid signatures, to sign a digital message using both a classical signature algorithm (e.g. RSA) and a PQC signature algorithm (e.g. ML-DSA), followed by the independent verification of both signatures by the recipient.

- Hybrid certificates contain multiple public keys and dual signatures, enabling clients to authenticate using either classical and/ or post-quantum methods.

Such hybrid approaches typically require interoperability and support. This may involve complexity in terms of support from cryptographic libraries and protocols, certificate authorities, endpoint software and libraries, and key management systems. Organisations should consider operational and practical factors in choosing a hybrid scheme and the component algorithms, including performance overhead (e.g. computation time, memory

usage), complexity of implementation, compatibility with existing and legacy systems (e.g. protocols like TLS and IPsec, libraries and software stacks, PKI), and fallback options (i.e. fail-safe mechanism in case of PQC failure).

We continue to observe developments in hybrid PQC-Classical and PQC-PQC approaches:

- IETF is developing the standard for hybrid key exchange in TLS 1.3 [draft-ietf-tls-hybrid-design-14], such that even if one algorithm becomes compromised, the other can still provide a secure foundation for the session key.
- NIST is developing standards [NIST SP 1800-38C] on testing for performance and interoperability of PQC algorithms.
- There are other international standards developments, such as the IETF's RFC 9794 (Terminology for Post-Quantum Traditional Hybrid Schemes) and the ISO/IEC 14888-4 (Stateful Hash-based Mechanisms).

As understanding of the benefits and potential trade-offs of such hybrids continues to evolve, organisations should weigh these against their operational context and use cases to inform adoption, if at all.

QKD-PQC Hybrid

QKD-PQC cryptography combines both technologies to strengthen cryptographic systems with a defence-in-depth strategy, leveraging both quantum-safe algorithmic security and quantum physics-based secrecy. The goal behind this hybrid model is to ensure that even if one layer is compromised, the other can still uphold security assurance for the system.

Implementation would encompass requirements from both technologies, where new infrastructure is needed for QKD (e.g. quantum devices, channels, key management), and software/ system upgrades are necessary for PQC. Other implementation factors could include additional support at protocol levels and interfaces to integrate both QKD and PQC-derived keys. As such, given the implementation complexity and potential performance implications (e.g. computational latency, increased communications bandwidth), organisations should define their security goals and use case requirements to assess if such a hybrid is meaningful or necessary. This can in turn inform the appropriate deployment architecture. Possible hybrid deployments include:

- Overlay PQC in a QKD network, where PQC handles authentication and access control over a QKD backbone.

- QKD generates a shared secret key through quantum channels and authenticated classical communication, while PQC is used to perform a separate key exchange.

The secure authentication of classical channels for QKD can be done via PQC or pre-shared keys. The two keys (exchanged through QKD and PQC respectively) are then combined to form a final hybrid session key.

- QKD-generated keys are distributed across satellites in intercontinental links, and integrated with PQC algorithms for terrestrial interconnects, and vice versa.

Cryptographic agility

Cryptographic agility refers to the capability of an organisation to rapidly adapt its cryptographic assets quickly and with minimal disruption. Theoretically, it should enable seamless replacement or reconfiguration of algorithms, protocols, keys and supporting cryptographic libraries in response to technological shifts, newly identified weaknesses, or compliance obligations. This is a valuable characteristic in quantum-safe migration given the expectation that algorithms that are considered quantum-safe today may become vulnerable as quantum computers grow more powerful.

Cryptographic agility is an umbrella concept that relies on visibility, flexible architectures, automation, as well as fit-for-purpose governance approaches. It should be seen as part of the organisation's wider digital transformation agenda. It supports initiatives such as IT modernisation, cloud adoption, automation, and compliance management by embedding flexibility and control into the cryptographic layer. Designing cryptographic services with centralised control and well-defined interfaces allows consistency across diverse platforms and simplifies integrations when new protocols or algorithms are required.

- Comprehensive visibility: Fundamentally, agility requires clear visibility into where and how cryptography is used. Organisations should establish processes to identify, locate, and understand their cryptographic assets, as well as their interconnections within systems and supply chains. This allows organisations to systematically pinpoint dependencies on outdated or vulnerable components, rather than discovering risks reactively during incidents or audits or relying on ad-hoc inventorisation efforts.

- Flexible and modular architecture: Agility requires software and systems to be designed for the modular and interchangeable implementation of cryptography. Applications should avoid embedding cryptographic parameters directly into code. Instead, cryptographic functions can be externalised through secure APIs, abstraction layers, or cryptographic service providers, so algorithms can be replaced or upgraded without extensive redevelopment.

- Automation: Automation is essential for maintaining agility at scale. Integrating cryptographic management within DevSecOps pipelines enables controlled testing, validation, and rollout of algorithm or configuration updates without manual

intervention. Automated monitoring and configuration management tools can detect deprecated algorithms or misconfigurations early.

- Fit for purpose governance: Sound governance ensures that cryptographic changes occur in a controlled and accountable manner. Organisations should define clear policies specifying how cryptographic mechanisms are selected, updated, and retired, along with approval and review processes to manage these transitions. Effective governance also requires coordination between security, engineering, compliance, and risk management teams to ensure that updates align with regulatory requirements, internal risk tolerances, and business continuity objectives.

However, the concept of cryptographic agility is still maturing across the global cybersecurity community and there is no comprehensive out-of-the-box solution. Standards bodies, regulators, and industry groups are actively developing frameworks, models, and reference architectures to define and operationalise agility in practice. These efforts aim to establish shared terminology and practical methodologies that help organisations assess their readiness and embed agility as a core element of their quantum-safe transition strategy. As these frameworks continue to evolve, organisations should keep a close watch on emerging developments and align their approaches accordingly.

Implementation, testing and validating quantum-safe solutions

Organisations should consider the following when identifying technology solutions for their quantum-safe migration.

- Choose quantum-safe solutions to best fit operational, security, risk, and performance requirements. Organisations can also design hybrid implementations between classical and PQC algorithms to support the transition phase, or for the long term. Refer to Domain 3: Technology for more information on the different technology options.

- Prepare for integration and interoperability between quantum-safe and classical systems. This can span several OSI layers, including the physical, network and protocol levels.

- Leverage automation to integrate cryptographic changes into DevSecOps pipelines where possible to reduce human error.

- Plan for phased deployment to facilitate coexistence and gradual migration without disrupting existing services. Backward compatibility and integration with existing systems are important to enable gradual migration while maintaining system operations. Implement contingency options to revert systems to a stable state in case of issues.

- Understand the impact of implementing quantum-safe technologies through proof-of-concept and pilot projects, towards eventual deployment and transition. These should leverage controlled but realistic environments, before full deployment to operational systems.

Comprehensive validation ensures that the implementation is robust, compatible, and secure, preventing operational disruptions and the introduction of new security vulnerabilities. Key practices include to:

- Verify cryptographic operations: Test encryption, decryption, signing, and verification to ensure expected behaviour across all systems.

- Assess system stability: Ensure migrated systems continue to support critical business processes and can recover safely from errors.

- Evaluate performance under realistic conditions: Measure processing time, resource consumption, and response under normal and peak workloads to identify bottlenecks.

- Check interoperability across systems: Confirm that implementation works seamlessly with other remaining systems, applications, and third-party integrations.

- Identify vulnerabilities early: Conduct penetration testing to uncover implementation weaknesses.

Quantum-safe migration may introduce both business and technical risks due to the complexity of replacing foundational cryptographic components. Without proper management, these risks can lead to service disruption, degraded security, or increased operational burden. A structured risk management approach helps ensure migration proceeds in a controlled and resilient manner. Key practices include to:

- Conduct migration-specific risk assessments: Evaluate potential business impacts (e.g. service downtime, compliance gaps, reputational harm) alongside technical risks (e.g. interoperability failures or dependency issues).

- Assess interdependencies and cascading risks: Map upstream, downstream, and third-party connections to prevent disruptions that may propagate across systems or business units.

- Embed continuous risk review: Reassess and update risk registers as migration progresses, incorporating new technical findings, emerging PQC standards, and operational lessons.

- Plan for contingencies: Develop fallback options, rollback procedures, and recovery playbooks to mitigate the impact of migration failures or unexpected performance issues.

Quantum-safe migration is an iterative process. Continuous monitoring and reviews will ensure that the implementation progresses according to plan and that systems remain secure and compliant. It enables organisations to identify and address issues promptly while maintaining operational reliability and align with evolving standards and developments. Key practices include:

- Compliance oversight: Verify ongoing alignment with regulatory and organisational standards as standards evolve.

- Stakeholder communication: Keep business and technical teams informed about migration progress, operational impact, and value of PQC adoption.

Example: Post-Quantum Migration for Endpoint Device File Encryption

This case study examines an enterprise laptop equipped with software-based file encryption, designed to safeguard sensitive corporate data stored locally on the device. The current encryption model employs elliptic curve cryptography (ECC) for key management, with files stored in the standard Cryptographic Message Syntax (CMS) format. In this model:

- AES-256 is used for file content encryption.
- The AES key is encrypted to the user's X.509 public-key certificate.
- Files are digitally signed to ensure both authenticity and integrity.

With the advent of quantum computing threats, the organisation intends to migrate from classical cryptography to PQC, using algorithms such as ML-KEM for key encapsulation and ML-DSA for digital signatures. This transition aims to preserve the confidentiality and integrity of data against future quantum-capable adversaries.

Migration Strategy

File encryption on enterprise laptops is typically managed internally by the organisation and may not require interoperability with external parties. In this specific context, encryption is intended solely to protect a user's own files, rather than to facilitate secure sharing with other recipients. The recommended approach is to adopt PQC directly for all new encryption operations, avoiding hybrid or phased transitions.

Engineering and Implementation

Establish a PQC-Capable PKI

- Deploy an enterprise PKI supporting ML-KEM and ML-DSA, with updated X.509 certificate profiles for PQC keys.
- Integrate certificate issuance, distribution, and revocation processes into existing device management workflows.
- Treat the PQC-based PKI as a core anchor for the migration, as the encryption software will rely on it for all PQC operations.

Develop PQC-Enabled File Encryption Software

The endpoint file encryption application must retain the ability to decrypt and verify legacy ECC-encrypted files, allowing users continued access to pre-existing encrypted content. However, once a file is modified or newly created, it should automatically be signed and encrypted exclusively with PQC algorithms.

The key design considerations are:

- Architect a secure workflow for decrypting ECC-encrypted files (by authorised users) and re-encrypting them with PQC.
- Maintain legacy ECC decryption and signature verification capability.
- Implement CMS support for ML-KEM and ML-DSA in line with emerging PQC standards.
- Ensure crypto-agility and precise object identifier tagging in accordance with IETF CMS specifications to avoid ambiguity in cryptographic structure handling.

Develop Supporting Tools for PQC Migration

While files will naturally migrate to PQC as users modify and save them, it is advisable to proactively convert all existing encrypted files to PQC to eliminate any residual content vulnerable to quantum attack. This can be achieved through dedicated migration tools that:

- Scan for ECC-encrypted files.
- Decrypt them (with authorisation) using ECC.
- Re-sign and re-encrypt content with PQC.
- Operate unobtrusively in the background as low-priority processes to minimise user disruption.

Such tools mitigate the risk of harvest-now, decrypt-later (HNDL) attacks by ensuring no legacy ECC-encrypted files remain on the device.

Challenges

Standards and Interoperability
PQC support in CMS and X.509 is still evolving, and some cryptographic libraries may lag in adopting the standards. Migrating data before standards are finalised risks producing large volumes of files that may require complex and costly reprocessing. It is therefore prudent to defer large-scale data migration until CMS standards are formally established.

Performance Considerations
While ML-KEM and ML-DSA generally offer comparable computational performance to ECC on modern enterprise-grade CPUs, their larger key sizes and signatures increase CMS payload sizes. This may marginally affect storage efficiency and performance, particularly on systems handling large volumes of small files.

The re-encryption of large files can be time-consuming. Performance may be optimised by retaining the existing AES key and re-wrapping it with PQC rather than generating a new one.

Summary

For enterprise laptop file encryption, a secure and operationally efficient strategy is to migrate in a single step to PQC for all new encryption, while preserving compatibility with existing ECC-protected files.

By combining robust PKI planning, the development of PQC-enabled applications and migration tools, and the adoption of standards-compliant cryptographic structures, organisations can carry out a smooth, well-governed transition to PQC-based file encryption.

Domain 4: Training and Capability

Key takeaways:

1. Your organisation's stakeholders and people need to have the necessary information and skills to support quantum-safe migration.
2. Organisations will need to identify if, where and how to build internal capabilities to support migration.

Training and building capability seek to ensure that your organisation and people have the necessary skills and information to support your quantum-safe migration journey. This entails education and awareness of the risks and migration strategies, as well as technical competencies to support eventual execution.

Based on the stakeholder groups indicated in Domain 2: Governance, we identify competencies that could be useful to aid their quantum-safe migration-related roles and responsibilities, as well as potential reference resources.

Stakeholder group	Related competencies/skills	In order to...	References/ Resources
Senior management and decision makers	• Understanding the quantum threat and potential implications on business/ operations • Understanding regulatory requirements and contractual obligations	• Establish migration vision and goals for quantum-safe migration, and approve resources, efforts and timelines	OMB Memorandum M-23-02 Migrating to Post-Quantum Cryptography Commission Recommendation (EU) 2024/1101 Report on Post-Quantum Cryptography (US Federal Action Plan) NIS Cooperation Group - A Coordinated Implementation Roadmap for the Transition to PQC Canadian Quantum-Readiness Best Practices & Guidelines v.04
Cybersecurity teams	• Threat modelling and risk assessment in relation to the quantum-threat	• Develop and manage the migration plan for	NIST SP 1800-38C (Prelim.) Migration to PQC: Interoperability Compatibility & Performance

	• Identify, test and evaluate potential quantum-safe solutions and standards to meet security requirements • Configuration and upgrades of cryptographic and software libraries • Verify and validate implementation	systems of interest, including budget and resources required, with the IT/tech team • Execute the migration steps, including implementing solutions (e.g. PQC, QKD), working with vendors as necessary • Monitor progress	FS-ISAC Preparing for a Post-Quantum World by Managing Cryptographic Risk ETSI TR 104 016 v1.1.1 Quality of PQC Implementation & Migration Assessment NIST CSWP Getting Ready for Post-Quantum Cryptography FS-ISAC Risk Model
IT and technology strategy teams	• Identify and prioritise systems for migration, in consultation with the security team • Identify existing cryptographic assets, and build and manage inventory, working with vendors and identifying appropriate tools to do so • Configuration and upgrades of cryptographic and software libraries • Verify and validate implementation, especially with a view to functionality and interoperability	• Develop and manage the migration plan for systems of interest, including budget and resources required, with the security team • Conduct cryptographic asset discovery, and create and manage an inventory • Monitor progress	NIST SP 1800-38B (Prelim.) Migration to PQC: Discovery & Architecture FS-ISAC Current State (Crypto Agility) Technical Paper TNO/CWI/AIVD The PQC Migration Handbook (2nd ed.) ETSI TR 103 619 v1.1.1 Migration Strategies & Recommendations
Business units	• Understand the quantum threat and potential implications on business/ operations • Understand regulatory requirements and contractual obligations	• Sign off and shape the quantum-safe migration strategy/ approach, in alignment with business operations and needs (e.g. to manage downtime)	WEF Quantum Readiness Toolkit (2023) TNO/CWI/AIVD _PQC Migration Handbook (2nd ed.) EU NIS Cooperation Group PQC Roadmap

Domain 5: External Engagements

Key takeaways:

1. Work with your third-party vendors to understand their quantum-safe roadmaps and your risk exposure based on the products and services that you rely on.
2. Leverage expertise within the ecosystem to guide and drive migration efforts.

Working with third-party solution providers and vendors

Many organisations depend on third-party solution providers and vendors for operational capabilities like cloud computing and enterprise applications, to security solutions. This creates complexity in quantum-safe migration, as organisations may not have full visibility or control over their technology components, and in turn, cryptographic assets. This means that:

- A significant part, or all, of quantum-safe migration can only be executed by the solution provider/ vendor, which has implications on an organisation's migration timeline and success; and

- If the solution provider/ vendor is slow to, or unable to, migrate to a quantum-safe solution, they may present vulnerabilities or compliance risks for your organisation's cybersecurity risk posture.

As such, organisations that leverage such third-party solution providers should proactively engage vendors and partners early to confirm product readiness and PQC roadmap compatibility. Relatedly, procurement and contractual requirements for such solution providers should align with your organisation's goals for quantum-safe migration. Organisations should:

- Communicate the importance of quantum-safe readiness to vendors and establish clear expectations for quantum-safe migration, including developing contingency strategies such as hybrid approaches for legacy systems that cannot be updated quickly or at all.

- Evaluate the solution provider's current cryptographic practices and future migration plans to ensure alignment with your organisation's goals.

- Request a cryptographic inventory of algorithms and components for the products and services that you procure/ acquire from the solution provider.

- Work with vendors to understand their ability to update algorithms as new quantum-safe developments emerge.

- Per Domain 2: Governance, assess the vendor's quantum-safe capabilities and use these assessments to inform procurement processes, contract renewals, and risk management activities.

We have compiled a list of questions that may be useful to ask solution providers/ vendors when engaging them as part of your quantum-safe migration journey.

Roadmap and Transition

- What is your roadmap for integrating PQC into your products and services?
- Which cryptographic algorithms are being prioritised for migration, and what standards (e.g. FIPS 203, 204, 205) do they comply with?
- What is your expected timeline for PQC-enabled product releases or updates?
- What is your expected timeline for PQC-enabled product certifications, e.g. NIST FIPS or Common Criteria?

Implementation and Costs

- Can you provide an inventory of cryptographic algorithms, protocols, schemes, and components used across your products and services?
- Will quantum-safe integration require software, firmware, or hardware changes for the organisation, and what are the associated costs?
- How will you ensure interoperability and backward compatibility during the transition?
- How will you support and validate the cryptographic implementation in your solutions?
- What is your process for maintaining, updating, and replacing cryptographic components across different protocols as cryptography evolves?

Experience and Case Studies

- Can you share examples or success stories of quantum-safe migration that you have supported?
- What are the potential challenges that my organisation should be aware of? Will there be downtime or operational disruption?

Leveraging the broader ecosystem to support your quantum-safe migration journey

The post-quantum transition will take place over many years. Organisations can leverage the existing talent, experience, and expertise within industry and other relevant expert bodies to support their migration efforts. It is therefore useful to build long-term partnerships and identify where you can leverage external capacity, while preserving internal expertise and retaining control over your organisation's critical decisions.

Risk assessment	Potential references/ resources
• Companies and consultancies have started to develop quantum readiness frameworks and can be engaged to support organisations across different industry sectors in their migration planning and assessments.	FS-ISAC Risk Model EY's Improving tomorrow's security by decoding the quantum computing threat Deloitte's Quantum Cyber Readiness services
• Vendors and open-source projects have started to develop automated discovery tools and scanners that can scan applications, APIs, and data flows to support cryptographic asset discovery, even for niche environments.	NIST SP 1800-38B, Quantum Readiness: Cryptographic Discovery
Governance	
• Industry and non-governmental organisations have developed resources on governance templates, roadmaps and best practices.	WEF Quantum Readiness Toolkit (2023) TNO/CWI/AIVD PQC Migration Handbook (2nd ed.) BSI Migration to Post Quantum Cryptography
Technology	
• The open-source community and post-quantum cryptographic providers have made available source code and implementation libraries for experimentation and integration. Test harnesses and benchmark routines are also provided to compare the performance of PQC algorithm implementations in a common framework.	Open Quantum Safe (OQS) project aims to support the development and prototyping of quantum-resistant cryptography and is part of the Linux Foundation's Post-Quantum Cryptography Alliance.

	PQ Code Package is a collection of open-source projects that aim to build high-assurance implementations of standards-track PQC algorithms.
• International standards organisations and working groups including NIST and IETF are defining and specifying PQC standards for PKI. ETSI and ISO/IEC are also spearheading initiatives to standardise QKD, focusing on interoperability, interface definitions, and security assurance frameworks.	IETF LAMPS – Limited Additional Mechanisms for PKIX and SMIME, is an IETF working group that aims to define extensions and algorithm identifiers to incorporate post-quantum primitives into existing X.509 and CMS structures. IETF Hackathon – PQC Certificates. The project provides repositories for X.509 data structures and also provides a comprehensive compatibility matrix. ETSI Quantum-Safe Cryptography Working Group ETSI Industry Specification Group QKD ISO/IEC 23837 Security requirements, test and evaluation methods for QKD. https://www.iso.org/standard/77097.html https://www.iso.org/standard/77309.html
• Standards organisations, independent laboratories, and industry consortia are collaborating to support functional validations and facilitate plug-fests for integration and interoperability testing.	The NIST Cryptographic Algorithm Validation Program (CAVP) provides validation testing of FIPS-approved PQC algorithms. PQC algorithm implementations successfully validated by NIST are also added to the validation list. The NIST SP 1800-38C led by the NCCoE in collaboration with industry and academic partners, conducts lab-based testing of PQC to assess interoperability and performance. It provides a public report that documents findings, lessons learned, and practical guidance. The PKI Consortium manages a PQC Capability Matrix (PQCCM), listing software applications, libraries and hardware with post-quantum support.

Training and Capability	
• Industry associations are creating collaborative learning communities that bring together industry, academia, and government to strengthen trust and interoperability in public key infrastructures and prepare for the post-quantum era.	The PKI Consortium provides a collaborative platform for members to share migration experiences, tools and best practices for quantum-safe PKI deployment. It promotes knowledge exchange in conferences and technical hands-on workshops. The Cloud Security Alliance's Quantum-Safe Working Group supports the global community in the development and deployment of a framework to protect data in the post-quantum era. It also offers a range of publications and resources.

Unknowns, assumptions and moving forward

Key takeaways:

1. We may never know when Q-day is. It cannot form a reliable reference point for quantum-safe migration, and organisations should start as soon as practically possible to start preparing and seeding changes.
2. Quantum-safe solutions available today can become obsolete in the future. Plan upfront to make changes to adapt to new technology options and developments.
3. Making investments in R&D and working closely with international and industry partners to monitor the quantum computing landscape and raise awareness, will support the ecosystem in being quantum-safe.

Collectively, cybersecurity industry leaders, regulatory bodies, and academic experts should consider how to work together to raise public awareness about the threat quantum computers pose to cryptographic security – and the profound impacts it may have on the economy and society. Right now, public understanding is low due to a focus on the mechanics of quantum computing, rather than the real-world implications for digital privacy, secure communications, and the reliability of essential operations. While the technology itself is complex, the message of the risk is simple: the systems and processes that underpin daily life could become vulnerable to attack.

Despite the ubiquity of digital communication and widespread digital literacy, most people remain unaware of how quantum advancements threaten this way of life. We can explore coordinated awareness campaigns and align our communications internationally to address this gap – not only to drive awareness and support for necessary investments, but also to establish a channel for communicating updates on quantum developments and evolving cryptographic standards. Regulators and industry leaders have a role to play to advise the public on these emerging threats, and in turn help to build public trust and prevent misinformation or unnecessary panic.