QUANTUM-SAFE MIGRATION HANDBOOK

CSA SINGAPORE
Cyber Security Agency of Singapore

GOVTECH SINGAPORE

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

ACKNOWLEDGEMENT

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.

Developed by CSA, GovTech, IMDA, in collaboration with the following industry partners:

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

This document has also benefited from the valuable feedback shared by the following organisations:

- Ensign InfoSecurity Pte Ltd
- Google
- NCS
- PQCee
- Singtel

DISCLAIMER

This document is intended for informational purposes only and is not mandatory, prescriptive or exhaustive. It is not intended to, and does not, constitute legal advice. Not all considerations or measures listed will be applicable to all organisations or environments. Organisations 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 references 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 Technology advancements may render the information in this document inaccurate and outdated.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
1	16 JUL 2026	Release of Version 1 of the Quantum-safe Handbook, incorporating feedback received during the public consultation period. Revisions have been made to address comments from stakeholders and to align with the latest developments in quantum-safe cryptography standards. Key updates to the No-Regret Moves [page 12], RACI table [page 21], Algorithm Recommendations [page 25].

Purpose

This handbook helps Singapore organisations — especially CII owners and government agencies — prepare for the quantum-safe transition. It covers what's at stake, where to focus, and practical steps to start building readiness now.

Preface

The exact date when a quantum computer can break today's encryption, i.e. "Q-day", is unknown. Expert consensus place it within 5–10 years, with some more conservative estimates at 10-20 years. More critically, adversaries are likely to already be harvesting encrypted data today to decrypt later. Migration is not a future problem but a present risk management issue.

The window to act is narrowing. For critical systems, the cost of inaction is highest. Quantum-safe migration is a multi-year effort that may need significant resources. While there are concerns of first-mover disadvantages given that the quantum-safe solution and standards space continues to develop, organisations must start now with planning. There are also "no-regrets" actions that can be taken immediately, while managing migration over a longer timeline. **Start now, prioritise, and build in flexibility to adapt as the field evolves.**

CSA's Quantum Readiness Index (QRI) complements this handbook as a self-assessment tool to help organisations evaluate their quantum-safe readiness, identify capability gaps, and prioritise next steps. Organisations can revisit the QRI over time to track progress and refine their migration strategies.

> Given the pace of scientific and geopolitical change, no approach to quantum-safe technology can be considered settled. This document will be updated as the field evolves. Organisations should monitor developments, assess their own operating context, and build in cryptographic agility where practical (refer to Domain 3: Technology on cryptographic agility).

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

Table of contents

Understanding the Quantum Threat

> The threat of breaking cryptography is not new, but quantum computing will amplify the likelihood, scale and impact of such attacks. These have implications for your organisation's risk posture, business continuity and reputation.

Cryptography is the backbone of digital trust — securing communications, transactions, and critical systems from banking to government platforms. While today's encryption remains beyond the reach of even the most powerful classical computers, sufficiently advanced quantum computers will change this. Threat actors are expected to exploit quantum computing to break encryption, putting sensitive data and digital trust at risk.

Cryptography is used in a variety of use cases.

Public Key Cryptography

Key Establishment
Key establishment allows two parties to securely agree on a shared secret key used to encrypt their communications. This is done either via key encapsulation (one party generates and encrypts the secret, then sends it) or key exchange (both parties share public keys and independently derive the same secret). It underpins protocols such as TLS, SSH, IPSec, and S/MIME. Common algorithms today include RSA, ECDH, and DH.

Digital Signatures
A digital signature, analogous to a physical signature, is a cryptographic mechanism that binds a party's identity to a piece of data. This can prove authenticity of communications, ensure that data hasn't been tampered with, and prevent the signer from denying the action. Examples of digital signature algorithms commonly used are RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), Digital Signature Algorithm (DSA).

Symmetric Ciphers

A symmetric cipher encrypts and decrypts data using the same secret key. In secure communications, it handles data encryption while a separate key establishment mechanism handles key exchange. The most widely used example is AES.

Hash Functions

A hash function takes an input of any size and produces a fixed-length output (digest). They are versatile building blocks used across many security mechanisms, including:

- Password protection — stores a password's hash rather than the password itself
- Message digest — hashes data before signing to improve efficiency
- Key derivation — derives secret keys from passwords or other data
- Message authentication codes (MACs) — hashes a message with a secret key to verify both authenticity and integrity
- Digital signatures — hash-based signatures such as SLH-DSA, XMSS, and LMS are also post-quantum compatible
- Trust anchors — hash functions like SHA-256 create cryptographic fingerprints of device components and code, embedded in tamper-resistant modules to verify integrity at boot. Quantum attacks that can forge signatures or tamper with boot artifacts would compromise the entire chain of trust.

Most public-key cryptography (e.g. RSA, ECDH, DH) relies on the computational hardness of two problems: factoring large integers and solving discrete logarithms. These are effectively unsolvable for classical computers at scale. Quantum algorithms change this.

Two quantum computing algorithms have been shown to break encryption. More may be developed.

- Shor's algorithm can solve the mathematical problem of large prime factorisation and discrete logarithm, at an exponential speed up over classical methods. Public key cryptography that relies on the difficulty of this problem for security are vulnerable and **should be prioritized for replacement**.
    - Integer factoring-based: RSA;
    - Discrete logarithm-based: ECDSA, ECDH, DSA, DH

- Grover's algorithm can solve unstructured search problems. This is effective in reducing the time needed for brute force key search attacks against cryptography like symmetric ciphers and hash functions. Its effectiveness is currently debated due to the memory and hardware needed to implement such attacks. As such, based on risk appetite and use case, organisations should consider the need to upgrade cryptography such as:
    - Symmetric Ciphers: AES, TDES
    - Hash Functions: SHA (including SHA1, SHA2, SHA3)

The confidentiality, integrity and availability of your organisation's systems and data is at risk.

	Confidentiality *Exposure of sensitive information at rest or in transit*	**Integrity** *Manipulation of transactions and processes*	**Availability** *Disruption of essential services*
Examples	Sensitive data e.g. medical records, financial data, credentials, decrypted and exposed	Forged digital signatures enabling fraudulent transactions or manipulated data	Forged control commands disrupting industrial systems, power grids, water treatment

Harvest-Now-Decrypt-Later (HN-DL) is the immediate threat. It refers to a tactic in which attackers capture and store encrypted data today, with the intent to decrypt it in the future when a Cryptographically Relevant Quantum Computer (CRQC) is available.

- There remains skepticism over the extent of HNDL attacks as it requires adversaries to intercept and indiscriminately store large volumes of encrypted traffic and maintain that data for years or decades until a CRQC becomes available. The storage, infrastructure, and operational overhead are substantial, placing this capability primarily within reach of motivated, well-resourced actors.
- Nonetheless, this does not mean no attacks. Adversaries will focus collection of data where the long-term payoff is highest. Harvesting such data can be done via network interception, supply chain compromise, or third-party services. Critical infrastructure (configuration data, authentication traffic) and systems dealing with long-life data (e.g. identify and biometric data, legal archives) are prime targets.

But resource intensity does not mean selectivity — it means prioritisation. Adversaries will focus collection efforts where the long-term payoff is highest: data that retains sensitivity well beyond the arrival of a CRQC. This makes CII sectors — energy, water, transport, finance, healthcare, and government — prime targets. The operational data, authentication traffic, and sensitive communications these organisations generate today could be weaponised years from now to disrupt services, compromise national security, or undermine public trust.

Existing cybersecurity practices make such attacks more challenging, such as the use of pre-shared keys, or rapid and regular rotation of encryption keys in public key cryptography. However, these can only slow down advanced attackers, and quantum-safe migration is the most effective long-term solution.

The quantum threat carries tangible consequences: data breaches, operational disruption, regulatory non-compliance, financial loss, and reputational damage. Left unaddressed, it also creates legal exposure through privacy violations and intellectual property theft.

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

The financial stakes are real.

1. A Citi Institute report[1] from Jan 2026 estimates that about $500-600 billion of cryptocurrency is ‘quantum-exposed’.
2. The Hudson Institute[2] reported in Apr 2023 that a quantum-enabled cyberattack on the US Federal Reserve’s interbank payment service could put $2.0–$3.3 trillion of U.S. GDP at risk.
3. We can also use data breach incidents to proxy the potential losses of a data attack, such as by CRQCs. IBM reports that the global average cost of a data breach in 2025 is $4.4 million USD[3], even without accounting for quantum capability.

Sources:
[1] “Quantum Threat”, Citi Institute, dated Jan 2026, accessed at link
[2] “Prosperity at Risk: The Quantum Computer Threat to the US Financial System”, Hudson Initiative, dated Apr 2023, accessed at link
[3] “Cost of a Data Breach Report 2025”, IBM, dated Aug 2025, accessed at link

Quantum-safe Migration

Why act now, not later:

1. Migration will take years. Starting late means rushing, missing critical steps, or competing for support.
2. Every day without migration extends your HN-DL exposure window.

Quantum-safe migration is also an opportunity to modernise your organisation's legacy cryptographic practices, improve governance, and improve overall cybersecurity.

Quantum-safe migration removes vulnerable cryptography, and/or replaces those with quantum-safe solutions to provide resilience against the quantum threat. Migration is not a new issue. Cryptographic systems have always had finite lifespans and organisations should have best practices in place to identify, assess, and rotate cryptographic primitives in a controlled and timely manner. However,

- We observe structural fragility in cryptographic implementations that make migration an urgent problem. Cryptography is deeply embedded across software libraries, hardware modules, and protocols. Such dependencies are poorly inventoried, deeply embedded in critical systems, and rarely reviewed.
- Rapid digitalisation has expanded the attack surface enormously. and spread across a sprawling ecosystem of vendor-supplied platforms, outsourced infrastructure, and third-party integrations that organisations do not fully control or even inventory. Dependencies are inherited, opaque, and often undocumented. Discovering and replacing vulnerable cryptography are non-trivial efforts that will likely take years.

As such, migration can be challenging for many organisations today. However, it is also an opportunity. Organisations operating legacy or on-premises infrastructure should see quantum-safe migration as a catalyst to modernise. This means not simply to patch cryptographic vulnerabilities, but to retire technical debt and rebuild on architectures that are more performant, more secure, and easier to maintain. Modern infrastructure will be faster, more resilient, and lower cost to operate and secure over the long term.

Modernised infrastructure delivers tangible benefits:

- **Performance gains.** Cloud-native and software-defined architectures offer greater compute capacity, lower latency, and scalable resource allocation compared to legacy on-premise systems.

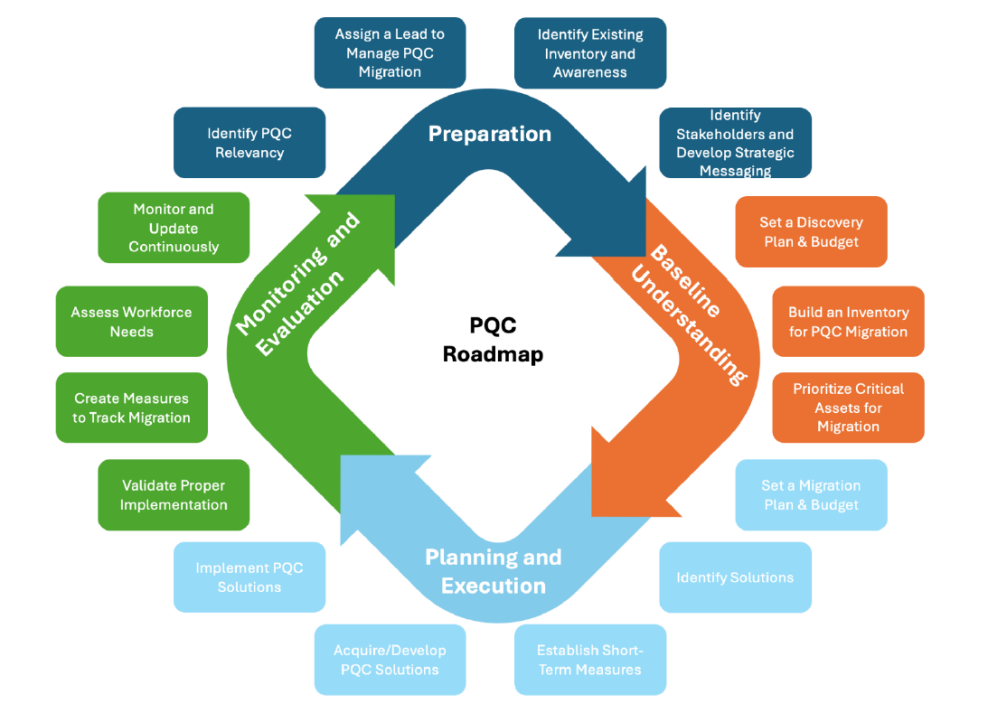
- **Smaller attack surface.** Replacing firmware-dependent appliances and end-of-life hardware eliminates legacy vulnerabilities.
- **Reduced operational overhead.** Centralised TLS termination, cloud-native key management services, and software-defined networking reduce the complexity of managing cryptography at scale.
- **Cryptographic management and visibility**. Modern architectures centralise cryptographic management — reducing the burden of discovery, enabling continuous inventory, and ensuring cryptographic assets are visible, auditable, and updatable at scale.
- **Stronger cryptoagility by design**. Modern architectures support algorithm updates centrally, without requiring firmware changes or hardware replacements across distributed systems. Cryptographic transitions beyond quantum, as standards continue to evolve, become significantly easier.

We identify five domains of efforts:

5 Key Domains for Quantum-Safe Migration

Quantum-safe migration is likely to be a multi-year endeavour, given the complexity and scale of the efforts required. Planning early helps to identify what needs to be done to prepare now, versus what can wait while solutions and standards continue to mature. There are many resources that break the quantum-safe migration process down into discrete, more manageable tasks, incl. the example from the Post-Quantum Cryptography Coalition 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

To support organisations in kickstarting your efforts, we have identified no-regret moves across each domain that can be first stepping stones.

No-Regret Moves	
Risk Assessment	**Identify your most critical systems and run cryptographic asset discovery on those first**. This helps to scope down the problem, rather than spend effort and resources inventorising across all systems at the outset.

Governance	**Identify who is *accountable* for quantum-safe migration decisions**. This is the person who owns the outcome and approves the plan. Clear ownership upstream will facilitate execution later.
Technology	**For your priority systems, identify which quantum-safe algorithms can replace the vulnerable ones currently in use**. Understand performance trade-offs before committing.
Training & Capability	**Brief senior leadership on the quantum threat now.** This will help them to understand and approve the resources and timelines.
External Engagement	**Contact your key vendors now and ask for their post-quantum roadmaps.** This will inform your migration timelines and approaches.

Domain 1: Risk Assessment

> **No-regret move**: Identify your most critical systems and run cryptographic asset discovery on those first. Do not attempt to inventory everything at once — scope down to where the risk is highest.

Quantum risk sits within your broader cybersecurity risk process.

There is no universal migration path. Each organization has different systems, priorities and constraints. The starting point must be a clear-eyed risk assessment: what matters most, where are you exposed, and what actions must apply? This focus ensures efforts and resources go where they are needed.

Conduct a risk assessment using your organisation's existing Enterprise Risk Assessment/Management Framework, or established standards. These include 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). CSA's published guides are also available, if applicable:

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

1. Identify what to prioritise

Start with your 'crown jewels': your most critical business functions, systems, and information assets. Compromises of these could cause the greatest operational, financial, or reputational impact. These include:

- IT systems with long-lived and/or highly sensitive data such as financial and medical records; these are the primary HN-DL targets; and/or
- OT systems with long operational lifespans, such as power grids system and satellite control infrastructure, where replacement cycles are slow.

As a supplementary factor, assess your attack surface and exposure profile. Threat modelling can be a useful technique to understand the threat exposure (i.e. likelihood of being attacked). Prioritise systems that are:

- Internet-facing or broadly networked (e.g. hosted in cloud environments), which are more accessible to attacks.
- Highly interconnected, or serve as critical nodes (e.g. identity providers, authentication hubs and privileged access gateways) can become single points of failure.

Mapping both impact and likelihood allows you to scope and sequence migration efforts effectively.

2. Cryptographic asset discovery

Once priority systems are identified, map what cryptographic assets they use. This is harder than it sounds: cryptography is often deeply embedded, and a single function may use multiple cryptographic mechanisms (e.g. email content encrypted with one standard, the transmission channel secured with another).

Cryptographic algorithms can be embedded in a variety of components incl.

- Network and transport layer: load balancers, web servers, API gateways
- Identity and authentication components: PKI/certificates, secrets, password and credential storage
- Applications and code: source code, application logic, packages and libraries
- Hardware and firmware: Hardware Security Modules (HSM), embedded & IoT devices, smart cards

Take a phased approach:

- Start with what you already have and know. Existing documentation and technical artefacts can give meaningful initial insights, without much effort. Existing logs from HSMs, key management systems, and certificate management systems reveal active keys and certificates. Load balancer and web server configurations show which protocols and cipher suites are used in external facing network paths. Network monitoring tools can show protocols used in internal network traffic. Network diagrams and penetration testing reports often already flag where cryptographic controls sit.

- Supplement with Automated Cryptographic Discovery and Inventory (ACDI) tools. These tools are still maturing and will not catch everything, but significantly reduce the manual effort required for cryptographic asset discovery. When evaluating tools, consider whether they fit your environment (on-premise vs. cloud, access to source code), what gaps they address, and how well they integrate with your existing security stack to eliminate the need for additional agents or sensors (firewalls, endpoint detection systems, vulnerability management platforms). Ask the vendor for

references of how their ACDI tool has been used to assess its maturity and relevance, before making significant investments in such tooling.

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

- Code scanning – Examines source code for cryptographic libraries, APIs, and functions that are used during development. For organisations with in-house development, integrating such tools into the Continuous Integration/Continuous Deployment (CI/CD) pipeline enables automated, early and consistent detection of cryptographic usage, vulnerabilities, and policy violations.

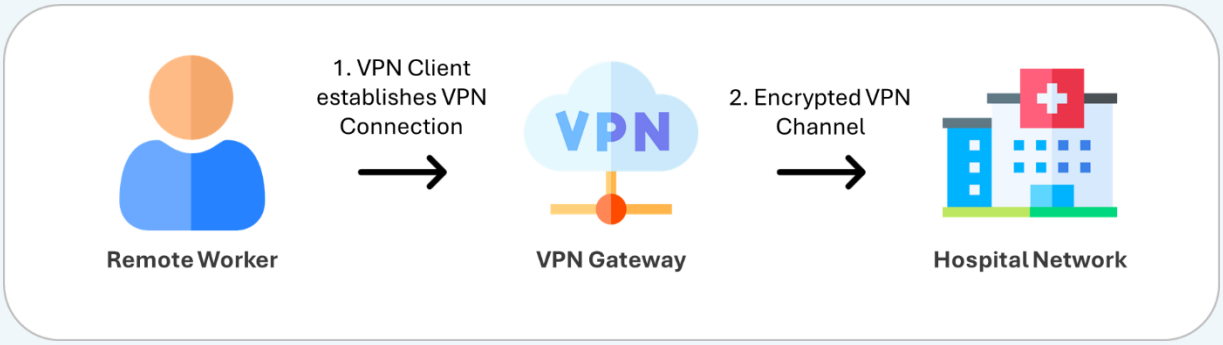
- Network analysis – Analysing network traffic to detect the use of cryptographic protocols (e.g. TLS, SSH, IPSEC) and their configurations. This helps identify non-quantum safe or insecure implementations, weak cipher suites, expired certificates, or unencrypted traffic traversing the network.

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

Leverage threat modelling

Use threat modelling to test your risk assessment. Threat modelling takes the perspective of an attacker to identify weaknesses and key attack vectors that should be addressed early. We illustrate two worked threat modelling examples to show how it can be applied to quantum-related risks.

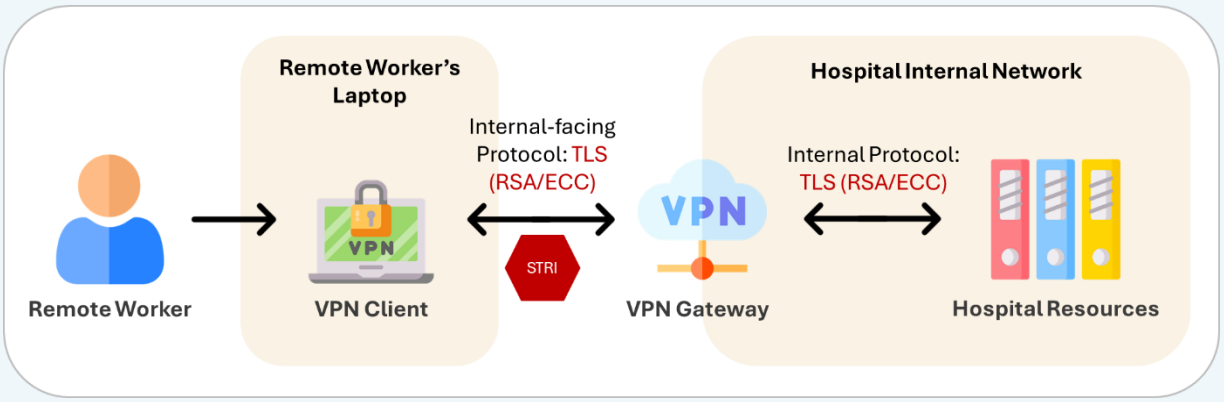
Example 1: Remote healthcare worker accessing a hospital network
The diagram shows the simplified process flow:



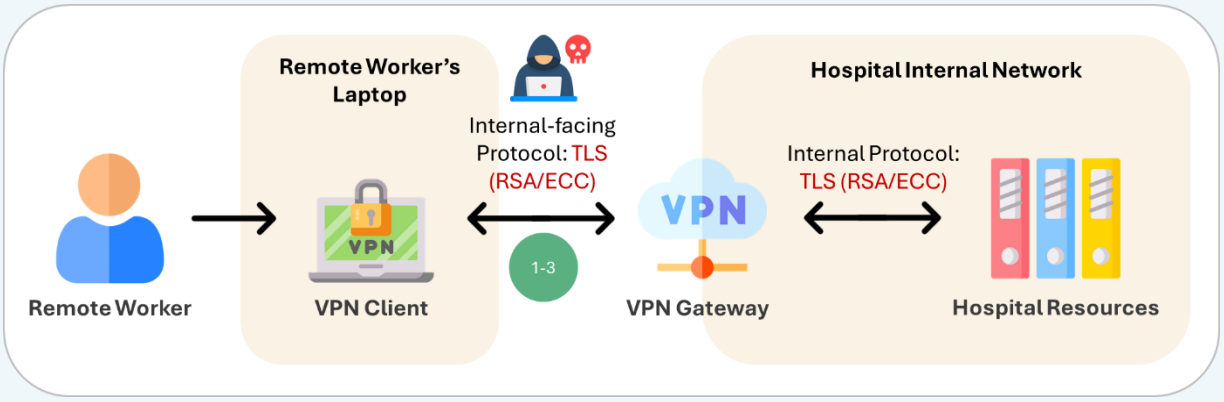
In this scenario, the remote worker accesses the hospital network via a Virtual Private Network (VPN). This VPN uses RSA/ECC-based TLS. RSA/ECC are quantum-vulnerable asymmetric cryptography. Only TLS 1.3 has the extensibility to support post-quantum key exchange; earlier versions do not.

Applying the STRIDE-LM* threat modelling framework, this internet-facing connection is the highest-risk point: a quantum-capable adversary could Spoof credentials, Tamper with data in transit, or intercept communications for Information Disclosure.

* More details on STRIDE-LM here: https://isomer-user-content.by.gov.sg/36/cc960d15-3bc3-4431-a2ce-5a5feeabbbc7/Guide-to-Cyber-Threat-Modelling.pdf.

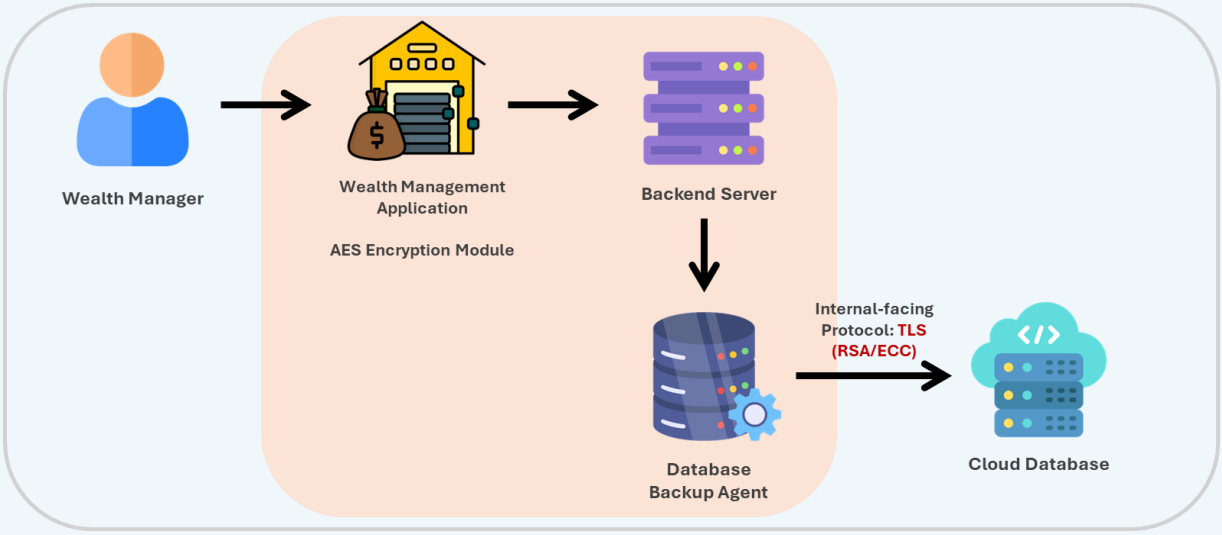


Referencing the MITRE ATT&CK framework, a hypothetical attack path might look like:



The hospital's priority is to map its external connectivity — how VPN clients connect to the gateway — and assess where PQC can be introduced to secure those channels.

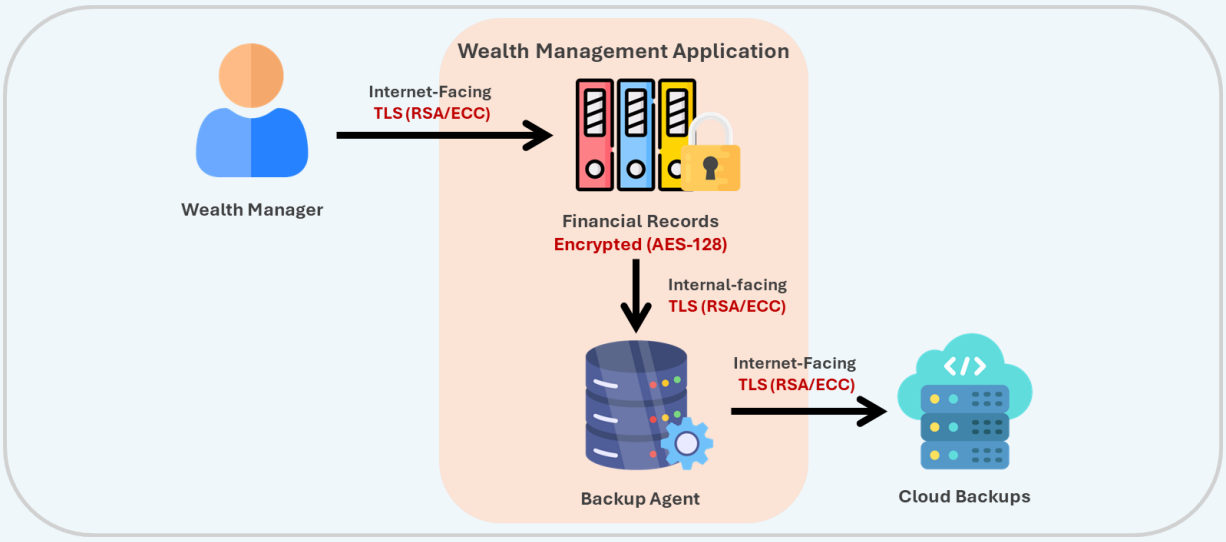
Example 2: Family office wealth management platform
The diagram below illustrates a simplified system architecture of a wealth management platform used by a family office for ownership records, trust structures and asset allocation documents.



Data at rest is encrypted with the industry standard AES-128 symmetric key. Nightly backups transfer via Transport Layer Security (TLS) using RSA/ECC, to a cloud database.

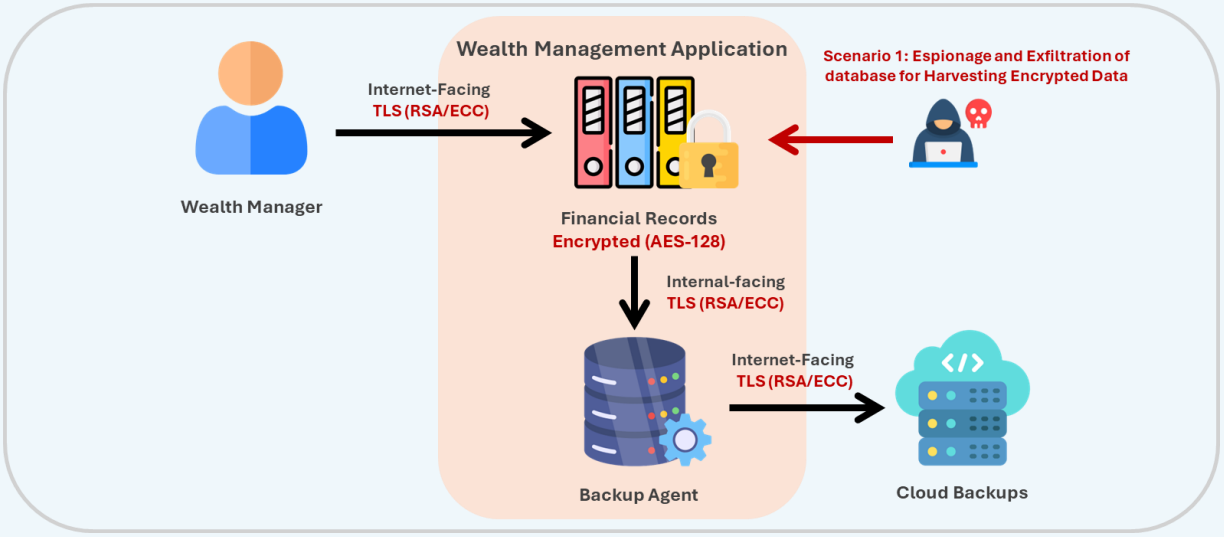
Two quantum algorithms compound the risk: Grover's reduces AES-128 to roughly 64-bit effective security, which makes it more feasible for attackers to conduct brute force attacks, and Shor's breaks the RSA/ECC key exchange entirely. This makes migration a priority on both fronts — data at rest and data in transit.

Applying the STRIDE-LM framework, the cloud database store faces the risk of Tampering, Repudiation and Information Disclosure by a quantum-enabled threat actor.

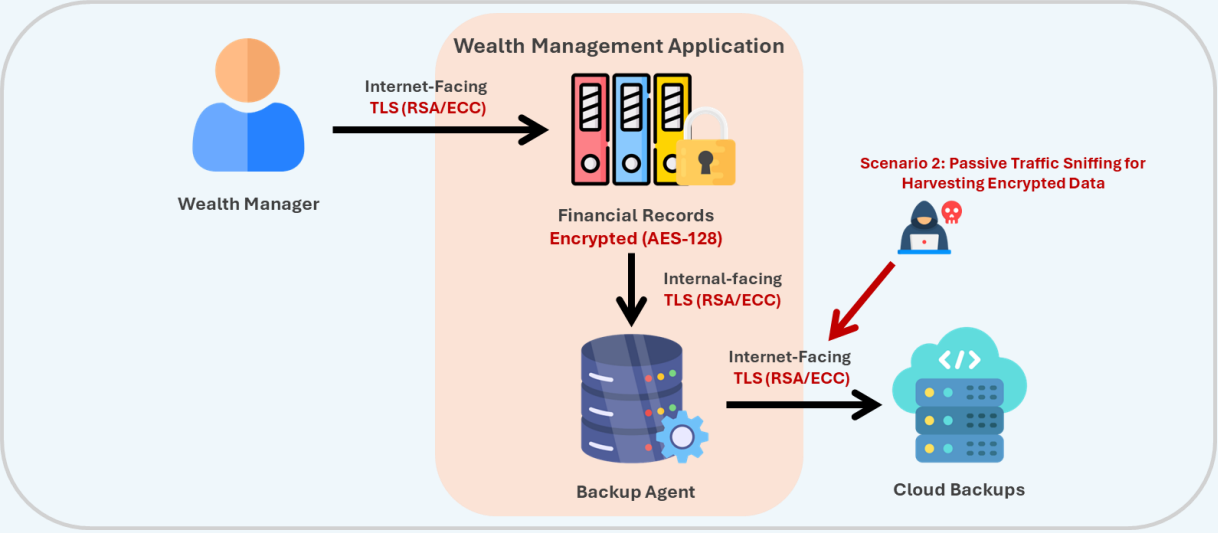


Based on the MITRE ATT&CK framework, a hypothetical attack path might look like:

Scenario 1: Espionage and Exfiltration



Scenario 2: Passive network sniffing



The family office should prioritise migration to PQC to protect data at rest and in transit.

Domain 2: Governance

> **No-regret move:** Identify who is *accountable* for quantum-safe migration decisions — the person who owns the outcome and approves the plan. Without clear ownership, nothing moves.
>
> Next,
> 1. Use the RACI model to also Identify “Responsible”, “Consulted”, and “Informed” stakeholders to ensure coordinated execution
> 2. Incorporate quantum-safe requirements into natural technology upgrades and new procurement, to manage the effort/resources involved and minimise technical debt
> 3. Update existing governance structures given its long-term strategic and operational impact

Establish clear roles and responsibilities to support quantum-safe migration

Four internal stakeholder groups are likely to be involved in quantum-safe migration:

- Senior management and executive board. Accountable for approving migration plans and committing the necessary resources to execute them.
- Cybersecurity teams. Led by or reporting to the Chief Information Security Officer, responsible for identifying the quantum threat's impact on security posture and recommending appropriate solutions.
- IT and technology strategy teams. Led by or reporting to the Chief Information Officer, responsible for identifying business-critical systems, prioritising them for migration, and updating IT infrastructure and policies accordingly.
- Business units. Responsible for aligning operational needs with migration plans, ensuring business continuity and minimising disruption throughout the transition.

There are two approaches to managing migration:

- Working within such existing structures has clear advantages: established expertise, communication channels, and reporting lines make migration more sustainable over time. An integrated approach requires upfront coordination effort, but avoids silos and embeds cryptographic best practices across the organisation efficiently.

- A dedicated migration team offers focused accountability and agility, which is useful for urgent, time-sensitive migrations. The trade-off is sustainability: quantum-safe migration spans technical and non-technical domains (budgeting, procurement, compliance), and a siloed team is poorly placed to manage these cross-cutting responsibilities over the long term.

Whichever structure is chosen, define clear roles, timelines, and milestones for each stakeholder group to ensure coordinated execution and measurable progress. Quantum-safe migration is an iterative process. Keep business and technical teams informed about migration progress, operational impact, and value of PQC adoption.

Frameworks like the RACI model can be applied to assign clear roles and deliverables

- 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 Prioritise high-value systems and data	I	R	R	A
Stage 2: Baseline Understanding				
2.1 Identify Existing Inventory	I	C	R	A
2.2 Set a Cryptographic Discovery Plan	I	R	A	I
2.3 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

Incorporate quantum-safe requirements into technology upgrades and new procurement

As far as possible, align migration with planned technology refreshes so quantum-safe requirements are built in from the outset. This is more cost-effective and less disruptive than ad-hoc migration, which typically requires additional investment to replace or re-engineer systems outside their natural replacement cycle, and risks operational downtime.

Update procurement policies to explicitly require:

- Cryptographic specifications in line with your cryptographic policies, regulatory requirements and relevant standards
- Cryptographic agility capabilities, to facilitate downstream adjustments
- Post-quantum roadmaps from vendors as part of the evaluation process.
- Where applicable, modernisation consideration for on-premises infrastructure with legacy components or little to no quantum-safe migration pathways

Review contractual clauses to address PQC support, cryptographic algorithm update mechanisms, service level agreements for quantum-safe transitions, and escalation procedures for addressing emerging quantum-related vulnerabilities.

Updating organisational policies

The quantum threat presents a long-term risk with strategic and operational implications. Embed quantum-safe requirements into existing governance structures rather than running a parallel process. This will help to maintain alignment with established policies and processes across critical functions.

- Cryptographic policies: maintain a live cryptography inventory. Set timelines for retiring and replacing vulnerable cryptography.

- Interdependency mapping: Identify upstream, downstream, and third-party connections to prevent cascading disruptions.

- Enterprise risk management: Add quantum-related risks to your risk register. Use clear risk descriptions as guided by your risk assessments, set out migration as part of treatment action plans. Add progress metrics to track readiness, including inventory completion rates, percentage of priority systems migrated. Update risk registers as migration progresses, incorporating new findings, emerging standards and operational lessons. Verify ongoing alignment with regulatory and organisational standards as standards evolve.

- Third party risk management: Assess vendors' maturity in quantum-safe implementation (e.g. current cryptographic practices, and migration timelines). A vendor that cannot migrate is a vulnerability in your supply chain. More information on engaging vendors is in Domain 5: External Engagements.

- Contingency planning: Maintain fallback options, rollback procedures, and recovery playbooks.

Migration is iterative, not a one-time project. Existing quantum-safe solutions may eventually become vulnerable. Review your policies and approaches regularly as standards (e.g. from the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), and European Telecommunications Standards Institute (ETSI)), guidance and regulatory requirements change, and quantum computers grow more capable. In Singapore, consult the CSA, as the national cybersecurity authority, or sectoral regulators for advice.

International governments have moved decisively on quantum-safe migration timelines. The US CNSA 2.0 sets requirements for national security systems, and the EU's Quantum-Safe Cryptography Roadmap establishes transition deadlines for EU Member States.

Singapore is aligning with this momentum with requirements for Critical Information Infrastructure (CII) owners as part of their quantum-safe migration planning:

- **By 31 Mar 2027:** Submission of CII owner's quantum-safe migration plan to CSA.
- **From 1 Jan 2028:** Procurement and implementation of new CII computer and computer systems that have a digital component should either (a) support quantum-safe algorithms/ technologies; and/or (b) be quantum-safe ready.
- **By 31 Dec 2031:** Completion of quantum-safe migration across CII computer and computer systems, i.e. vulnerable cryptography should no longer be used.

CSA, GovTech, and IMDA are developing detailed guidance to support CII owners in meeting these milestones.

Domain 3: Technology

No-regret move: For your priority systems, identify which quantum-safe algorithms can replace the vulnerable ones currently in use. Understand the performance trade-offs before committing to implementation.

Next,

1. Enhance your organisation's cryptographic management best practices and implement interim architectures or solutions to reduce risk exposure.
2. Incorporate crypto agility to adapt to new threats and solutions (e.g. evolving standards), as technology continues to advance
3. Continue to test, validate and monitor your technology implementations to ensure that they address your migration goals, as solutions evolve.

Algorithm Recommendations

PQC and quantum-safe classical algorithms remain the primary recommended options. QKD should be considered for layered defence or niche use cases where its specific security properties are warranted.

The standards below are widely accepted, and can support a comprehensive range of cryptographic functions. This list will be updated as new options emerge.

	Deprecated	Recommended
Asymmetric cryptography	RSA, DH, ECC (all key sizes)	ML-KEM, ML-DSA, SLH-DSA Firmware signing only: LMS, XMSS
Symmetric cryptography	AES with key sizes below 128-bit;	AES-256
Hash functions	SHA with output sizes below 256-bit (e.g. SHA-224)	Hash functions ≥256-bit

Understanding the technology options

Technical solutions that are secure against both classical and quantum computing attacks include classical solutions, such as AES at sufficiently large key sizes, and new tecnbiques like Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD).

Post Quantum Cryptography

Post-Quantum Cryptography (PQC) is the primary migration path for most organisations. PQC algorithms are designed to withstand quantum attacks (e.g. Shor's algorithm). They

replace vulnerable public-key cryptography such as RSA, ECDSA, and Diffie-Hellman, and run on existing classical hardware, making them practical for broad deployment.

PQC covers the full range of cryptographic functions and can be deployed in software or integrated into existing cryptographic libraries, making it practical for most use cases. Some common use cases for PQC include network security (e.g. TLS, 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).

The main operational consideration is that PQC keys and signatures are larger than their classical equivalents, which can affect bandwidth, storage, and latency. Deployment needs to account for performance overhead and impact due to increased PQC key sizes, signature lengths, and computation time compared to classical algorithms. This can affect use cases like TLS handshake, network/ resource-constrained environments, and certificate chains. This is most pronounced in constrained environments such as IoT devices or high-throughput network paths.

PQC security relies on mathematical problems considered computationally intractable for both classical and quantum computers, spanning algorithm families such as lattice-based, code-based, and hash-based constructions. These descriptions refer to the underlying mathematical problems that their security is based on.

In 2024, NIST published three PQC standards following eight years of international review:

- FIPS 203: ML-KEM (Module-Lattice Key Encapsulation Mechanism), based on the CRYSTALS-Kyber algorithm, for key encapsulation. Replaces RSA, ECDH key exchange.
- FIPS 204: ML-DSA (Module-Lattice Digital Signature Algorithm), based on the CRYSTALS-Dilithium algorithm. Replaces RSA, ECDSA.
- FIPS 205: SLH-DSA (Stateless Hash-Based Digital Signature Standard), based on SPHINCS+ algorithm. For hash-based digital signatures.

Two further PQC algorithms (FN-DSA, lattice-based digital signatures; and HQC, code-based key encapsulation as a backup to ML-KEM) are pending standardization, as below. Cryptographers continue to develop algorithms with better performance, smaller key sizes, or different mathematical foundations.

Quantum Key Distribution

QKD uses quantum mechanics to enable two parties to generate a shared secret key. When correctly implemented, QKD is considered highly secure as any eavesdropping attempt

disturbs the quantum states involved and is automatically detected. It is not a replacement for PQC: QKD does not provide digital signatures or authentication unless combined with pre-shared keys or PQC signatures. QKD is best suited as a complementary solution for high-security, point-to-point links where physical infrastructure investment is justified.

QKD supports three network architectures: point-to-point (direct links between parties), trusted node-based (enabling key exchange without direct links), and satellite-based (for long-range QKD). Common use cases include securing communication between geographically separated data centres, enhancing encryption protocols such as AES with QKD-generated keys, and securing government and CII backbone networks.

QKD is more expensive and complex to deploy than PQC. It requires specialised 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). Additional factors include the cost of QKD devices, scalability, coverage distance, and cross-vendor interoperability. Organisations can reduce the costs and complexity of using QKD by tapping on QKD-as-a-service offerings.

While QKD itself is theoretically secure, QKD cannot operate in isolation. It requires an authenticated classical channel alongside the quantum channel. Otherwise, man-in-the-middle attacks can compromise key exchange. Robust implementation is needed to ensure that the physical setup is not vulnerable to side-channel attacks. Trusted relay nodes are required to extend range, and must be individually secured to maintain the security of the entire system. Testing and validation are needed to increase confidence for wider adoption of QKD. Standards bodies such as ISO and ETSI continue to develop testing and security standards for QKD, which will provide a more robust basis for wider deployment when ready.

Quantum-safe replacements for different cryptographic functions:

Key Establishment

Three quantum-safe options exist: a pre-shared symmetric key of suitable large size (256-bit), ML-KEM, or QKD. Pre-shared keys (PSK) require secure out-of-band distribution (e.g. via HSM, smart card, or secured courier). These are operationally demanding but highly secure, with no reliance on mathematical problems vulnerable to quantum attack. PSK with AES-256 is among the strongest options for CII operators with existing secure distribution infrastructure. Where PSK distribution at scale is impractical or operationally challenging, ML-KEM is a practical alternative that does not require out-of-band distribution.

Digital Signatures

All classical digital signature algorithms are quantum-vulnerable. The only quantum-safe replacements are PQC algorithms, primarily ML-DSA and SLH-DSA. XMSS and LMS are stateful hash constructions that are technically quantum-safe. However, they are tricky to implement securely and are not expected to be widely adopted.

Symmetric Ciphers

Not vulnerable to Shor's algorithm, but Grover's algorithm effectively halves key strength. Organisations should migrate to AES-256.

Hash Functions

Hash functions with output sizes below 256 bits may not sufficiently secure against quantum attacks. Use hash functions with an output size of 256 bits or larger.

Random Number Generation

Random numbers are fundamental to the security of cryptographic mechanisms. These are typically the output of two phases of generation:

- True Random Number Generators (TRNG), also referred to as Non-Deterministic Random Number Generators (NDRNG). These extract entropy from physical phenomena (e.g. computer mouse movement, CPU fan noise, quantum vacuum fluctuations) and are not quantum-vulnerable, but produce insufficient volume for most applications.
- (Cryptographically-Secure) Pseudo Random Number Generators (PRNGs or CSPRNGs), also referred to as Deterministic Random Number Generators (DRNG). These deterministic algorithms expand TRNG output into a much larger entropy pool to meet the needs of cryptographic algorithms. While they do not add natural randomness, these can be seen as practically random. These are mostly based on hash functions, and are as quantum-safe as the hash functions used to build them.

<u>Interim enhancements, before migration is executed</u>

While preparing for migration, organisations can consider the measures below to strengthen existing cryptographic practices. They do not directly mitigate the quantum threat, but improve resilience and manageability now, and support cryptographic agility.

- Stronger entropy sources for cryptographic schemes: Use TRNGs to introduce greater unpredictability and randomness in key generation, thereby strengthening the security of cryptographic schemes.

- Apply Key Derivation Functions (KDFs): Use KDFs to separate access and limited exposure of key material. KDFs can derive downstream keys from raw key material, ensuring keys are properly sized, domain-separated across applications, and not directly exposed if compromised. During hybrid key establishment, KDFs also allow classical and quantum-safe secrets to be cryptographically combined into a single key, rather than relying on either source alone.

- Key lifecycle management, from generation to destruction: Strengthen practices including frequent key rotation to limit data exposure per compromised key, audit logs to track key usage and integrity, and revocation mechanisms for compromised keys. Organisations should also plan for PQC-enabled certificates, dual-key usage, and key management across trust chains.

- Middleware and proxy architectures: Deploy middleware and cipher-translation proxies to bridge current and future cryptographic standards, facilitating gradual transition.

- Monitoring: Implement data exfiltration detection systems and tools to identify cryptographic anomalies that may indicate quantum-related threats.

Hybrid cryptography implementations

Hybrid cryptography approaches refer to the combined use of multiple cryptographic mechanisms, including classical algorithms, PQC, and/ or QKD. During the transition period, this provides a fail-safe: if the PQC algorithm has an unexpected vulnerability, the classical algorithm still holds; if the classical algorithm is broken by a quantum computer, the PQC algorithm still holds. Hybrid approaches add some performance overhead and implementation complexity but can be a sound interim strategy for systems that cannot migrate fully in one step.

- PQC-Classical hybrid: a classical and a PQC algorithm run in parallel for the same operation (e.g. key exchange or digital signatures). This enhances quantum resistance while maintaining compatibility with existing systems.

- PQC–PQC hybrid: Two or more PQC algorithms from different families (e.g. lattice-based and hash-based) are used together for a single operation. This provides algorithmic diversity to avoid single points of cryptographic failure.

Common use cases include:

- Hybrid key exchange, deriving a shared session key from multiple algorithms;

- Hybrid signatures, to sign with both a classical signature algorithm (e.g. RSA) and a PQC algorithm (e.g. ML-DSA), with the recipient independently verifying each

- Hybrid certificates, which contain multiple public keys and dual signatures for classical and/ or post-quantum authentication.

Hybrid schemes require broad support across cryptographic libraries, certificate authorities, endpoint software, and key management systems. Organisations should assess performance overhead, implementation complexity, compatibility with existing protocols (e.g. TLS, IPSec) and fallback options (i.e. fail-safe mechanism in case of PQC failure) before adoption.

Standards and industry developments for hybrid implementations are ongoing:

- 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.
- Major browsers (Chrome, Edge, Safari) and CDNs (Cloudflare, AWS Cloudfront) have implemented support for hybrid PQC-Classical key establishment (e.g. X25519 + MLKEM768) under TLS 1.3.
- 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).

Cryptographic agility

PQC migration will not be "one and done". Plan for the reality that today's quantum-safe algorithms may need to be replaced in the future as quantum computers grow more capable. There is no comprehensive out-of-the-box solution. Cryptographic agility means building systems so that algorithms can be swapped out with minimal disruption. This requires:

- Visibility: A live, accurate inventory of all cryptographic assets and their dependencies. 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: Cryptographic functions should be exposed through well-defined interfaces or APIs, and not hardcoded into applications. This allows algorithm replacement without extensive redevelopment.

- Automation: Cryptographic management should be integrated into development and deployment pipelines so that updates can be tested, validated, and rolled out consistently and at scale. Automated monitoring and configuration management tools can detect deprecated algorithms or misconfigurations early. 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.

- Fit for purpose governance: Clear policies specifying how cryptographic mechanisms are selected, updated, and retired, with defined approval and review processes. Cross-functional coordination between security, engineering, compliance, and risk management teams will ensure that updates align with regulation, internal risk tolerances, and business continuity objectives.

Implementing, testing and validating quantum-safe solutions

Organisations should:

- Choose solutions that best fit operational, security, risk, and performance requirements. Hybrid classical-PQC implementations are a viable option during or beyond the transition period.

- Plan for phased deployment to enable gradual migration with minimal disruption to existing services. Maintain backward compatibility and implement rollback procedures in case of issues.

- Test in controlled environments before full deployment. Proof-of-concept and pilot projects should use realistic conditions to surface integration issues early.

- Automate cryptographic changes into DevSecOps pipelines where possible to reduce human error.

- Address interoperability across relevant OSI layers — physical, network, and protocol levels — between quantum-safe and classical systems.

Validation should confirm that the implementation is robust, compatible, and secure across five areas:

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

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

- Performance: Measure processing time, resource consumption, and response under normal and peak workloads to identify bottlenecks.

- Interoperability: Verify seamless implementation with remaining systems, applications, and third-party integrations.

- Security: Conduct penetration testing to uncover implementation weaknesses.

Worked Example: Enterprise laptop file encryption

A organisation uses software-based file encryption on enterprise laptops to protect sensitive corporate data stored locally. The current setup uses elliptic curve cryptography (ECC) to manage encryption keys, with files stored in Cryptographic Message Syntax (CMS) format. Specifically:

- File contents are encrypted using AES-256.
- The AES key is encrypted with the user's public-key certificate (X.509).
- Files are digitally signed to ensure both authenticity and integrity.

ECC-based key management is quantum-vulnerable and must be replaced with post-quantum cryptography (PQC), specifically ML-KEM for key encapsulation and ML-DSA for digital signatures, to protect the confidentiality and integrity of the information.

Migration Approach

Unlike network-facing systems, enterprise laptop file encryption is managed internally and does not require interoperability with external parties. This makes it practical to make a clean migration, with all new encryption operations using PQC immediately, while maintaining the ability to read/ decrypt legacy ECC-protected files. This can be combined with background tools to proactively convert legacy ECC-protected files. Built on a PQC-capable PKI and standards-compliant cryptographic structures, this is an operationally efficient approach that minimises user disruption while eliminating quantum vulnerabilities.

Implementation Steps

1. Establish a PQC-Capable Public Key Infrastructure (PKI)

PKI is the system that issues and manages the digital certificates used to secure encryption keys. The existing PKI must be updated as below. It will form the foundation for all subsequent PQC operations across the organisation's devices.

- Support 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.

2. Update the File Encryption Application

The endpoint file encryption application must be updated to:

- Encrypt and sign all new or modified files exclusively using PQC algorithms
- Retain the ability to decrypt and verify legacy ECC-protected files, ensuring users do not lose access to existing content
- Re-encrypt ECC-protected files with PQC keys when those files are modified or saved
- Implement CMS support for ML-KEM and ML-DSA in line with emerging PQC standards.
- Ensure the system can identify and handle different cryptographic algorithms unambiguously — each encrypted file must be clearly tagged with the specific algorithm used, so the correct decryption method is applied. This follows IETF CMS specifications and is essential for crypto-agility, where systems need to support multiple algorithms during the transition period..

3. Build and deploy migration tools

Files will gradually migrate to PQC as users modify and save them. However, legacy ECC-protected files that remain untouched are still vulnerable to HNDL attacks. To eliminate this risk, dedicated migration tools should:

- Scan for remaining ECC-protected files.
- Decrypt them using the authorised user’s ECC-protected keys.
- Re-encrypt and re-sign them using PQC.
- Run as background, low-priority processes to minimise user disruption.

Challenges

- Standards maturity: PQC support for CMS and X.509 is still evolving. Some cryptographic libraries may lag in standards adoption. Migrating large volumes of data before standards are finalised risks costly reprocessing later. Large-scale data migration should be deferred until CMS standards are formally established.

- Performance: ML-KEM and ML-DSA perform comparably to ECC on modern enterprise-grade hardware, but their larger key and signature sizes increase file

payload sizes. In turn, this affects storage efficiency and performance, particularly on systems handling large volumes of small files. Performance can be improved by retaining the existing AES content encryption key and re-wrapping it with PQC, although this does not mitigate the risk of the ECC-secured AES key being harvested.

Domain 4: Training and Capability

> **No-regret move:** Brief senior leadership on the quantum threat now. They need to understand the risk before they can approve the resources and timelines required.
>
> Next,
> 1. Equip "Responsible" and "Accountable" stakeholders with the expertise and skills needed to plan, direct and execute the organisation's migration efforts.

Successful migration depends on people having the right knowledge and skills. This section maps the competencies required across each stakeholder group (as indicated in Domain 2: Governance) with reference resources to support capability development.

Stakeholder	What they need to know	In order to	References/ Resources
Senior management and decision makers	The business implications of the quantum threat; regulatory requirements and contractual obligations	Approve migration plans, allocate budget, and set organisational direction	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	How to • Conduct threat modelling and risk assessment	• To develop and execute the migration plan, including budget and resources	NIST SP 1800-38C (Prelim.) Migration to PQC: Interoperability Compatibility & Performance

	for quantum risks • Identify, test and evaluate quantum-safe solutions • Configure and upgrade cryptographic libraries • Verify and validate implementation	required, with the IT/tech team • Working with vendors • 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	How to: • Identify and prioritise systems, in consultation with the security team • Discover cryptographic assets, and manage inventory • Configure and upgrade cryptographic libraries • Verify and validate implementation, especially for functionality and interoperability	• Identify what needs to be migrated, with the security team • Build and maintain the inventory • Ensure systems work correctly post-migration	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	Business implications of the quantum threat; regulatory and contractual obligations	Shape migration plans around business/ operational needs and 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

> **No-regret move:** Contact your key vendors now and ask for their post-quantum roadmaps. Their migration timelines directly constrain yours. If a critical vendor has no roadmap, that is a risk you need to manage.
>
> Next,
>
> 1. Engage consultancies or service providers for new quantum-safe capabilities or services that can support your organisation's migration.

Working with third-party solution providers and vendors

Many organisations cannot execute quantum-safe migration independently. They depend on third-party vendors for cloud infrastructure, enterprise applications, and security tooling. This creates two risks: the vendor controls the migration timeline and execution, and a vendor that fails to migrate becomes a vulnerability in your supply chain.

Proactively engage vendors and partners to confirm product readiness and PQC roadmap compatibility:

- Set clear expectations: Communicate quantum-safe requirements to vendors explicitly. For legacy systems that cannot be updated quickly or at all, establish contingency plans strategies such as hybrid cryptography.
- Assess the vendor's cryptographic practices: Evaluate current implementations and future migration plans for alignment with your organisation's timeline and goals.
- Request a cryptographic inventory (e.g. in the form of a Cryptographic Bill of Materials, CBOM): Obtain the inventory or cryptographic algorithms and components used in the products and services that you procure/ acquire from the solution provider.
- Confirm cryptographic agility: Verify that vendors can update algorithms as standards evolve.
- Embed vendor assessments into governance: Per Domain 2: Governance, use quantum-safe capability assessments to inform procurement processes, contract renewals, and supply chain risk management.

Key questions to ask solution providers/ vendors when engaging them as part of your quantum-safe migration journey.

Roadmap and Transition

- What is your timeline for PQC-enabled product releases and certifications?
- Which cryptographic algorithms are you prioritising, and what standards (e.g. FIPS 203, 204, 205) do they comply with?

Implementation and Costs

- Can you provide a full inventory of cryptographic algorithms and components used in your products and services?
- What changes (e.g. software, firmware, or hardware) will be required on our side, and what will they cost?
- 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 of quantum-safe migration that you have supported?
- What operational disruptions or challenges should we expect?

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

Quantum-safe migration is a long-term effort. Build partnerships with industry bodies, specialist vendors, and external experts to supplement internal capacity — while retaining internal oversight and control over 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

> Three things remain true regardless of how the quantum landscape evolves::
> 1. There is no reliable timeline for Q-day. Organisations should not wait for certainty. Preparation and early action is the only response.
> 2. Today's solutions may not be permanent. Build in cryptographic agility from the outset so that systems can adapt to new technologies and standards.

Public understanding of the quantum threat remains low. This is not because the risk is obscure, but because discussion has focused on the mechanics of quantum computing rather than its real-world consequences. The core message is straightforward: the cryptographic systems underpinning digital communications, financial transactions, and critical infrastructure could become vulnerable to attack.

Cybersecurity leaders, regulators, and academics should collaborate to close this gap through coordinated awareness campaigns, educational initiatives, and internationally aligned communications. This serves two purposes: building public support for the investments migration requires, and establishing trusted channels for communicating developments as standards evolve. Clear, measured communication from credible institutions will also help prevent misinformation and unnecessary alarm.