HONG KONG MONETARY AUTHORITY
香港金融管理局

Quantum Preparedness of Hong Kong's Banking Sector

July 2026

Supported by

KPMG

QUINLAN &ASSOCIATES

Contents

Foreword p.3

Executive Summary p.4

01 Quantum Computing p.6

02 Post-Quantum Cryptography p.13

03 Current Hong Kong Landscape p.22

04 Way Forward p.40

05 Appendix p.50

Foreword

The financial services industry is entering a new phase of technological transformation. Advances in data, computing power and artificial intelligence are reshaping how financial services are delivered, managed, and supervised. For Hong Kong to maintain its status as an international financial centre, it must not only embrace new technologies but also develop the capacity to manage the risks that may accompany their adoption.

Quantum computing represents a development of strategic significance. Although the technology remains in an evolving stage, its long-term implications for financial services are profound. On one hand, quantum computing may eventually unlock new possibilities in risk analysis, modelling and optimisation. On the other hand, it may also undermine the cryptographic foundations that underpin trust and security in banking systems, payment networks, and financial market infrastructure (FMI).

The banking sector must therefore approach quantum developments with both strategic foresight and disciplined execution. The implications of the quantum era extend beyond future technological opportunities. They encompass operational resilience, cybersecurity, third-party dependencies, and long-term transition planning. In particular, the shift to Post-Quantum Cryptography (PQC) will require sustained effort over many years, given the deep integration of cryptographic functions across systems, processes, and external interfaces.

The Hong Kong Monetary Authority (HKMA) has identified this as a key priority within Hong Kong's broader fintech agenda. Under "Fintech 2030"[1], one of the strategic objectives is to strengthen business, technology, and quantum resilience. This underscores a clear intent: to support responsible innovation while safeguarding the resilience, integrity, and trust that are fundamental to the banking system. In preparation for the quantum era, the HKMA's approach is to encourage the industry to begin early, act in an orderly fashion, and build the capabilities necessary to navigate the transition ahead.

Quantum preparedness is not merely a technical challenge. It demands senior management engagement, institutional planning, capability development, and coordinated action across the ecosystem. It also calls for collaboration among Authorized Institutions (AIs), technology providers, academic institutions, and other relevant stakeholders. A well-prepared banking sector will be better equipped to manage quantum-related risks while remaining poised to harness the benefits of technological advancement over time.

The HKMA will continue to support the industry through practical guidance, active engagement, and capacity-building initiatives. As the landscape evolves, the objective remains to promote a measured, forward-looking, and coordinated approach to quantum preparedness across the banking sector.

Preparing for the quantum era is a shared responsibility. It requires sustained commitment and close collaboration across the entire financial ecosystem. By acting early and working together, we can enhance Hong Kong's readiness for the future and support the continued evolution of a resilient, trusted, and innovative financial system. As innovation accelerates, resilience and trust must keep pace. That is how Hong Kong will remain future-ready in the next phase of financial transformation.

[1] HKMA. 2025. *The HKMA Unveils "Fintech 2030" at the Hong Kong FinTech Week 2025.* (https://www.hkma.gov.hk/eng/news-and-media/press-releases/2025/11/20251103-3/).

Executive Summary

Quantum computing represents a significant advancement in computing technology with transformative potential for the financial services sector, particularly in areas such as portfolio optimisation, risk modelling, fraud detection, product pricing, stress testing and complex simulation. Concurrently, the emergence of Cryptographically Relevant Quantum Computers (CRQC) poses a potentially significant cyber risk to the traditional cryptography that safeguards secure communications, customer data, payments, authentication and FMI. Although the timing of this threat remains uncertain, the migration to PQC is expected to be a multi-year effort. Early preparation is therefore essential to address both the operational complexity of migrating interconnected systems and the "Harvest Now, Decrypt Later" (HNDL) risk to long-lived confidential data.

To assess the current state of readiness within Hong Kong's banking sector, the HKMA invited all AIs operating in Hong Kong to participate in a survey. The findings reveal that while awareness of quantum computing is growing, practical adoption remains limited. Most AIs possess at least some awareness of quantum computing, and a smaller group has begun exploring or piloting applications. However, adoption is still in its early stage, with many AIs identifying the technology's low implementation readiness given its nascent nature, uncertain commercial value and a lack of internal expertise as key challenges. Therefore, quantum computing is generally perceived as a long-term strategic opportunity. However, quantum-related cyber risk and PQC readiness demand immediate attention.

Assessment of PQC readiness across the dimensions of Awareness, Planning, Pilots and Practical Preparedness indicates that the sector remains at an early stage of transition. Across the majority of AIs, formal governance, dedicated funding, workforce training, quantum-risk assessments, cryptographic inventories, migration planning, testing protocols and progress monitoring are not yet fully established. A small but notable group of AIs has made more advanced progress, including formal governance frameworks, structured planning, pilot activity and more mature operational practices. Nonetheless, the overall landscape reflects uneven readiness, with a clear gap between leading institutions and the broader sector.

AIs have identified several common barriers to advancing PQC readiness. These include the absence of established risk assessment methodologies and industry-standard frameworks, the technical complexity and scale involved in building cryptographic inventories, legacy infrastructure and accumulated technical debt, uncertainty around standards and regulatory timelines, and a shortage of internal expertise. External dependencies further complicate progress. AIs often rely on input from vendors, FMIs, common utility providers and counterparties to assess risks, understand embedded cryptography, define migration pathways and coordinate interoperability testing. These dependencies underscore that PQC readiness cannot be achieved in isolation by individual institutions.

This paper outlines a practical action plan for AIs adopting the same four-stage approach: from Awareness, Planning, Pilot to Practical Preparedness. AIs may begin by establishing board and senior management engagement, assigning clear ownership, building workforce capability, developing a cryptographic inventory, assessing quantum-related exposure, prioritising migration based on data sensitivity and system criticality, engaging vendors, and establishing a documented roadmap. Subsequently, controlled pilots can be conducted to validate interoperability and rollback mechanisms, while embedding PQC readiness into business-as-usual (BAU) processes, such as cyber risk management, operational resilience, third-party risk management and change governance.

The paper also identifies areas where external support can accelerate sector-wide readiness. AIs have expressed

strong demand for supervisory clarity, practical guidance, industry knowledge sharing and facilitated testing environments. In response, the HKMA will support the sector through initiatives such as providing supervisory guidance, training and workshops, developing PQC toolkits in collaboration with academic partners, and facilitating industry collaboration and engagement through platforms including Hong Kong FinTech Week, FiNETech events and other targeted forums. These efforts aim to help AIs translate PQC concepts into tangible actions, promote consistency across the sector and encourage coordinated engagement with vendors and other external stakeholders.

In the immediate term, AIs can take several practical steps to advance their PQC readiness.

- **Engage the board**, framing quantum risk as an enterprise risk and establishing it as a standing item in risk governance
- **Identify an accountable owner for quantum readiness**, with senior sponsorship and a mandate that crosses functional lines
- **Commission a cryptographic inventory**, accepting that it will be imperfect at first and improve with iteration
- **Engage critical vendors**, requesting their post-quantum roadmaps and embedding quantum readiness requirements in new contracts

These actions do not require AIs to wait for full maturity in quantum technology or finalised PQC implementation guidance, and can lay a stronger foundation for subsequent planning, piloting and migration efforts.

The Quantum Preparedness Index shows that building upon the initial foundations, the next stage of the transition journey will require stronger capability development, more structured planning, and greater progress in testing and implementation. The transition to quantum-safe banking will require sustained commitment over a number of years. By acting now, building foundational visibility, developing cryptographic agility, conducting early testing and coordinating across the ecosystem, AIs in Hong Kong can enhance customer trust, strengthen operational resilience and uphold financial stability in the emerging quantum era.

01 Quantum Computing

1.1 Introduction to Quantum Computing

Today we are familiar with the concept of machines that compute. These machines, called classical computers, take the shape of laptops, phones, watches and other digital devices. At the heart of each of these machines are semiconductor devices that are commonly built on silicon and provide the microscopic switches and circuits that enable computation. Over the last 60 years, as silicon manufacturing technologies have developed, these computing devices have shrunk in size and increased in capability, delivering more computational power in a smaller package.

Meanwhile, in the early 1980s, the foundational theories of quantum computation were being established through the independent works of physicists Paul Benioff, Richard Feynman and David Deutsch, who proposed quantum mechanical models of computation that could be used to simulate quantum systems and process multiple computational states at the same time.

The further development of these ideas and the physical development of materials, often using the advanced manufacturing capabilities from the semiconductor and photonics industries, has led to the implementation of these concepts at an atomic scale. Hardware suppliers can now design and build new computing architectures where quantum mechanics are at the heart of their operation.

Over time, quantum computers are expected to help solve certain classes of problems that are difficult for today's largest classical supercomputers. While classical computers store information as bits, which can be understood as being in one of two states, quantum computers encode information using qubits. Qubits can represent a combination of states until they are measured, a property known in quantum physics as superposition.

In addition to superposition, another quantum mechanical property used in quantum computation is entanglement. This is the ability to connect different qubits such that they can increase the probability of correct solutions being output. This is important because, while for classical computers that are deterministic, where a given calculation typically produces the same output for the same input, quantum computing is probabilistic. This means that the same quantum computation can produce different results, and each result is output with a certain probability.

These properties of superposition and entanglement allow quantum computers to represent and manipulate information in ways that differ fundamentally from classical computing. For certain computational tasks, many researchers believe that sufficiently large-scale quantum computers may eventually outperform classical computers.[2]

For financial services, quantum computers are expected to offer potential benefits over time, including more accurate simulations of markets, better optimisation of asset use and enhanced analytical capabilities in areas such as fraud detection. However, a significant risk associated with quantum computers is their theoretical capability to break common encryption methods. Section 2 provides more details on quantum cyber risk and PQC.

1.2 Quantum Use Cases for Financial Services

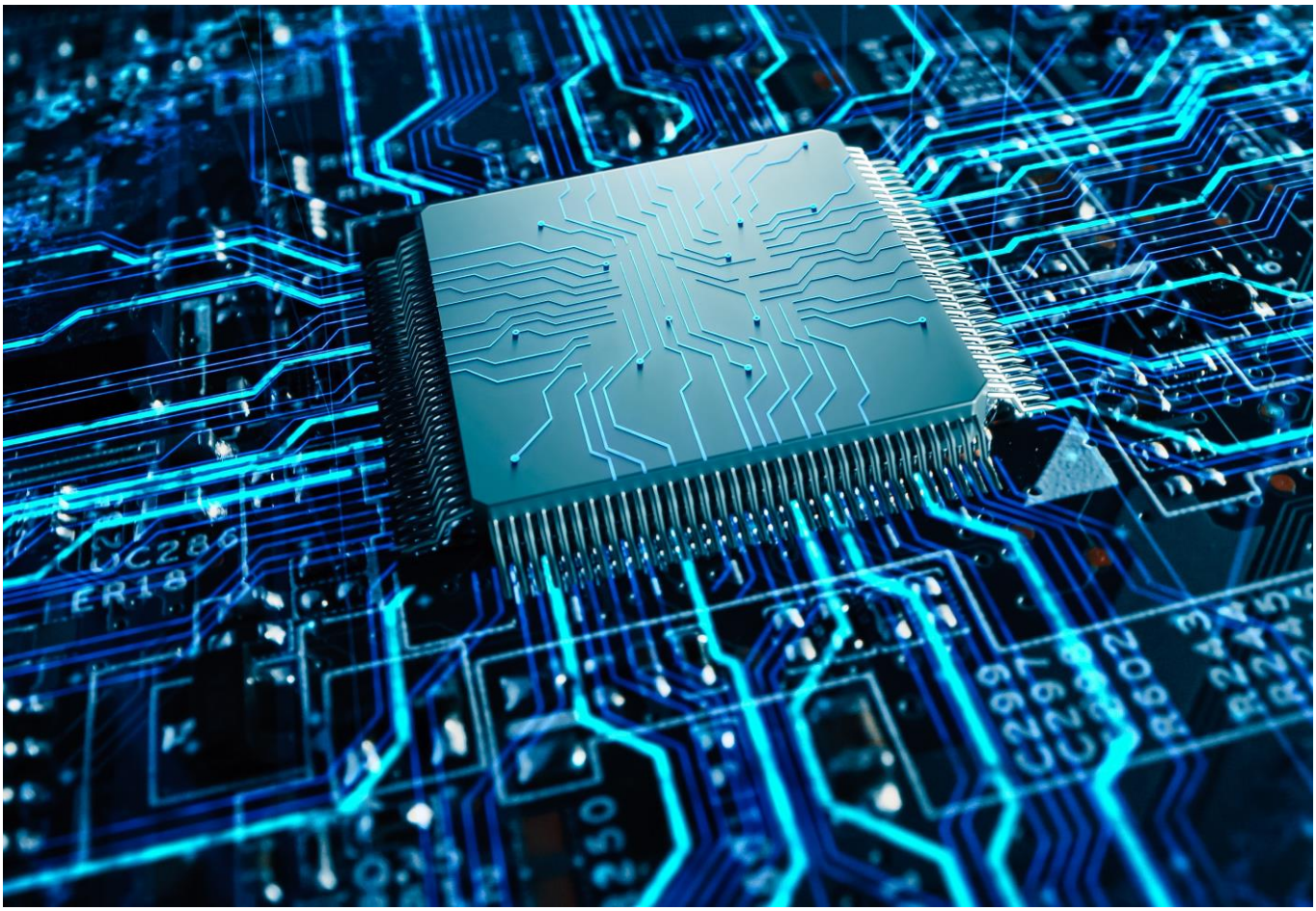
The financial services industry is a highly data-driven industry where speed, accuracy and management of risk

[2] Nielsen and Chuang. 2010. Quantum Computation and Quantum Information. p. 5. (https://doi.org/10.1017/CBO9780511976667).

are key to success. To support decision making, complex mathematical models are used. These models are limited by current classical approaches. Even with the very best high-performance computing hardware available, these models are computationally demanding and can take very long processing times.

However, quantum computers provide a fundamentally different way of solving these problems, which is not constrained by the same classical limitations. Quantum approaches, using superposition and entanglement, will support new approaches to complex mathematical models and may enable solutions to be found faster at potentially higher quality. It is projected that solving high-value financial problems with quantum computers may generate significant economic value for financial services.[3]

Global financial institutions are already exploring quantum computing use cases, often in collaboration with technology consulting firms and research partners. These experiments are focused on exploring how quantum approaches may eventually offer a benefit to the quality of the solutions, the speed in which they are found and the skills required to use this technology. The implementation maturity of quantum algorithms in financial institutions varies, with most applications at the exploratory or pilot stage.



[3] McKinsey & Company. 2026. *McKinsey Quantum Technology Monitor 2026: A commercial tipping point.* p. 24. (https://www.mckinsey.com/~/media/mckinsey/business%20functions/technology/our%20insights/mckinsey%20quantum%20technology%20monitor%202026%20a%20commercial%20tipping%20point/quantum-technology-monitor-2026.pdf?shouldIndex=false).

Portfolio and Asset Optimisation

Portfolio and asset optimisation is a common problem in finance, which involves making the best use of assets to maximise returns. Optimisation techniques must consider expected returns of assets, financial risks, market conditions, physical considerations and many other factors.

Quantum Algorithm Areas

Optimisation and machine learning

Implementation

Asset optimisation using quantum computing can use qubits to represent specific asset-allocation decisions, such as whether an asset should be included in a portfolio. Optimisation techniques such as the Quantum Approximate Optimisation Algorithm (QAOA) can then consider factors including asset value, expected return, market conditions and risk levels. Based on these inputs, QAOA can generate a set of potentially favourable asset-allocation options.

Quantum machine learning (QML) methods, such as quantum neural networks (QNNs), may also improve estimates of asset value and risk, thereby providing better inputs to optimisation models.

Case Studies

Citi Innovation Labs (Citi) conducted a study with Classiq in 2024 to test quantum computing for portfolio optimisation. Using historical data for six stocks, they encoded a risk-return optimisation for QAOA and enforced the budget constraint via a tuneable “penalty factor”, then varied that penalty across simulator runs. Results proved highly sensitive to penalty calibration, and smaller penalties yielded the best-quality solutions. The study claims no quantum advantage over classical methods, but establishes the tuning discipline needed to realise one as hardware matures. [4]

Huaxia Bank, jointly with SpinQ, developed a QNN for the optimisation of ATM placement and withdrawal of underused machines across China. The team extracted key data points including failure rates, usage trends and replenishment timings from 2,243 ATMs. The data was then converted using a technique called variational quantum embedding, which encodes data into a format suitable for the QNN. The QNN was executed on SpinQ's proprietary nuclear magnetic quantum computer to provide experimental results. The approach showed improved accuracy, higher precision and shorter computing time compared to the current classical algorithm. [5]

[4] AWS Quantum Technologies Blog. 2024. *Citi and Classiq advance quantum solutions for portfolio optimization using Amazon Braket*. (https://aws.amazon.com/blogs/quantum-computing/citi-and-classiq-advance-quantum-solutions-for-portfolio-optimization/).

[5] SpinQ. 2025. *Huaxia Bank Partners with SpinQ to Develop Quantum AI Models for Smarter Commercial Banking Decisions.* (https://www.spinquanta.com/news-detail/huaxia-bank-partners-with-spinq-to-develop-quantum-ai-models20250109075044).

Fraud Detection

Fraud detection seeks to identify potentially illegitimate transactions by recognising patterns in data. Once such transactions are identified, financial institutions can take steps to reverse, prevent or mitigate their impact.

Quantum Algorithm Areas

Machine learning

Implementation

QML methods may allow for a larger number of features and more complex relationships within financial transaction data to be evaluated to detect patterns of fraud.

Case Studies

Ping An Insurance collaborated with Origin Quantum to develop QML algorithms that could be used to identify financial fraud. The team developed a QNN to detect complex patterns of transactions indicative of money laundering. These quantum algorithms are intended to support improvements in the response speed of financial services in Ping An.[6]

Sales Optimisation

Accurately pricing assets in complex markets is a challenging task. Faster or more precise insights into an asset's future price can support financial decision-making across areas such as trading strategy optimisation, arbitrage and hedging.

Quantum Algorithm Areas

Machine learning and simulation

Implementation

QML can be employed to help make predictions about the future state of the market. Quantum simulation techniques can also be used to replicate the market's complex interactions using a quantum state to project an expected asset price.

Case Studies

HSBC worked alongside IBM to deliver experimental results showing a 34% improvement in predicting the probability of winning customer inquiries in the European corporate bond market. HSBC used quantum data embedding to train a classical machine learning model. This classical machine learning model then calculated the likelihood of winning each customer inquiry, informing a larger classical trading algorithm.[7]

[6] Hong Kong Institute of Bankers. 2025. *The Quantum Tectonic Shift: Digitally Rewiring the Banking Model*. Banking Today. p. 5–6. (https://www.hkib.org/storage/files/243/BT145%20Cover%20Story.pdf).

[7] HSBC. 2025. *HSBC Demonstrates World's First-known Quantum-enabled Algorithmic Trading with IBM.* (https://www.hsbc.com/news-and-views/news/media-releases/2025/hsbc-demonstrates-worlds-first-known-quantum-enabled-algorithmic-trading-with-ibm).

Risk Management

Risk management is critical to the effective operation of financial services. In transaction clearing, risk may arise when traders are able to use funds before their transactions have been fully cleared. Financial services organisations must also match and process tens of thousands of trades, often through queue-like systems. To reduce this risk, it is important that trades are verified and cleared within a short timeframe.

Quantum Algorithm Areas

Optimisation, simulation and machine learning

Implementation

To reduce the risk in trade scheduling, a variational quantum optimisation technique such as QAOA, can be used to quickly find the best pairs of trades. Simulation methods can be used to identify risk in a complex market, while machine learning techniques can be used to predict trade settlement failures.

Case Studies

Barclays demonstrated a proof-of-concept (PoC) for a quantum clearing algorithm designed to ensure the integrity of trades in securities. The goal of the PoC was to identify whether quantum algorithms could provide a speed-up over current classical methods for matching thousands of trades. When incorporating legal constraints and optionality restrictions, non-exact classical methods, known as heuristic methods, might provide a good result, but not the best result. A future large-scale quantum computer may be able to provide faster solutions than current-day heuristics.[8]

[8] IEEE. 2021. *Quantum Algorithms for Mixed Binary Optimization Applied to Transaction Settlement.* (https://ieeexplore.ieee.org/document/9369145).

1.3 Current State of Quantum Computing

Quantum computing is moving towards early-stage commercialisation, with many companies now providing access to quantum computers. Compared with existing classical high-performance computers, current quantum computers are prone to hardware errors and require significant expertise to use. Unlike classical computers, which are generally built on similar silicon-based foundational architectures, quantum computers vary considerably in their implementation.

Common quantum computing approaches include superconducting chips, ion traps, photonic chips, silicon quantum dots and neutral atom arrays. Each approach has strengths and limitations that may affect its suitability for certain tasks, meaning there is currently no single "best" approach. As the technology develops, and as engineering and materials challenges are overcome at different rates, some quantum computing approaches may mature into large-scale implementation faster than others. As a result, the most advanced quantum computing technologies today may not remain the most advanced in the future.

Across the quantum computing landscape, companies can vary from small startups, solely focused on their approach to quantum computation, to multi-national technology companies with large computing research and commercialisation groups.

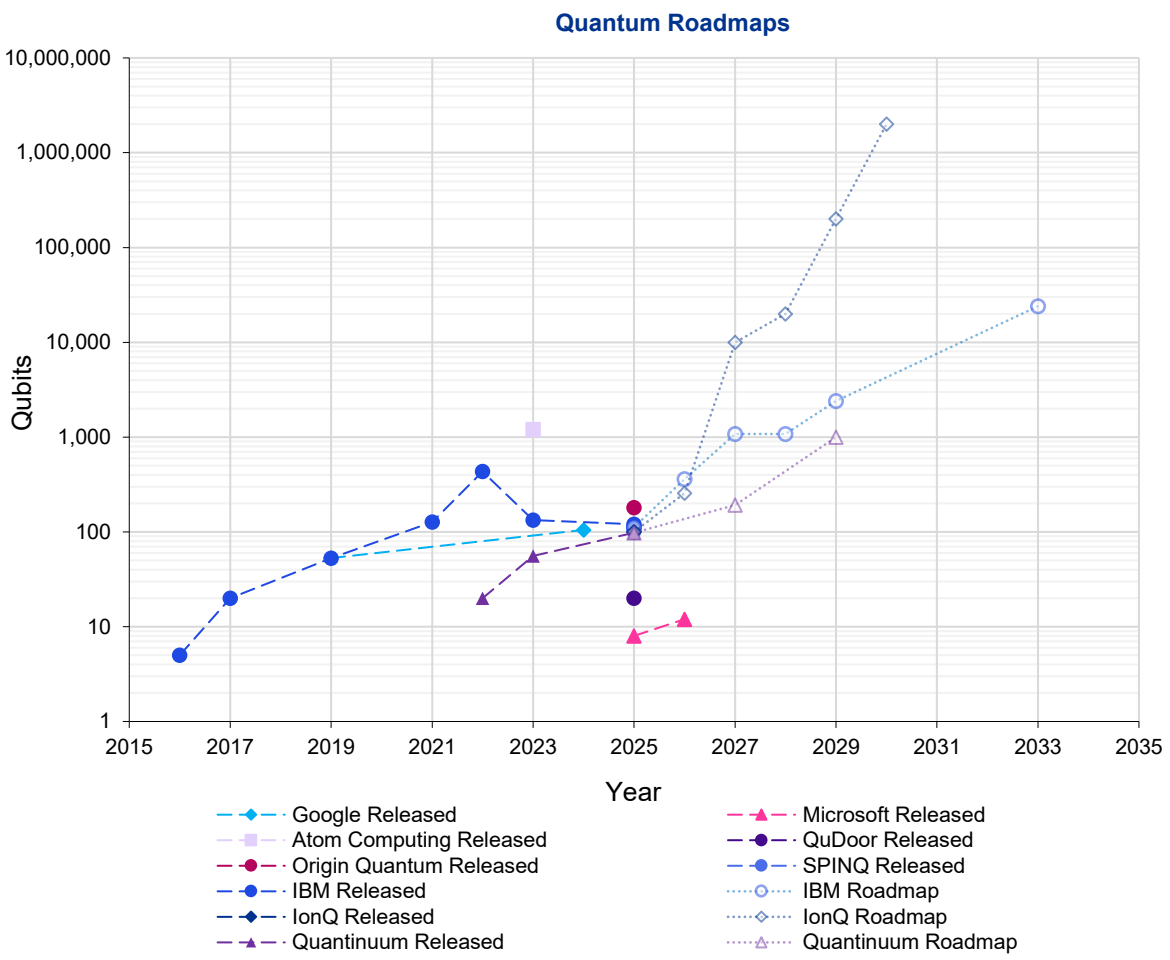
Table 1 shows a short comparison of some major quantum companies in 2026 and their latest devices.

Table 1: Summary of Quantum Companies

Company	Primary Device Types	Primary Operating Location(s)	Latest Device Name	Access Methods
IBM	Superconducting	United States	Nighthawk r1	Cloud Access
Google	Superconducting	United States	Willow	Restricted to Researchers Only
SpinQ	Superconducting	China	S Series	Cloud Access
Origin Quantum	Superconducting	China	WuKong 180	Cloud Access
IonQ	Trapped Ions	United States	IonQ Tempo	Cloud Access
QuDoor	Trapped Ions	China	AbaQ 1	Cloud Access
Quantinuum	Trapped Ions	United States United Kingdom	Helios	Cloud Access
Atom Computing	Neutral Atoms	United States	AC1000	Cloud Access
Pasqal	Neutral Atoms	France	Orion	Cloud Access
PsiQuantum	Photonics	United States Australia	N/A	No Access Available
Microsoft	Majorana Quasiparticles	United States	Majorana 2	No Access Available

Source: KPMG analysis; adapted from listed Quantum companies.

Figure 1: Quantum Roadmaps



Source: KPMG analysis; adapted from listed Quantum companies.

1.3.1 Scaling of Quantum Computing Systems

The scale of computations that a quantum device can carry out is determined by the number of qubits, the speed of operations and the error rates of those operations. Scaling the number of qubits increases the size of calculations that can be performed and improving the speed of operations means calculations are performed faster. The accuracy and reliability of outputs can be improved by reducing errors through physical improvement of the device and with error-correction techniques.

Many companies have published roadmaps outlining the expected development of their technologies, including projected qubit counts and milestones related to error correction. Figure 1 plots the number of physical qubits of released quantum computers and those projected in company roadmaps. This is based on public information from different providers, including extrapolation of physical qubits for IBM in the years 2029 and 2033, assuming implementation of their published error correction methods.[9]

This shows a steady increase in qubit numbers over the last decade, with hundreds of thousands of qubits projected within the next 10 years. These indicators are used to demonstrate progress in overcoming significant technical challenges and may also provide an indication of when quantum systems could become practically useful.

[9] IBM. 2024. *High-threshold and low-overhead fault-tolerant quantum memory*. (https://www.nature.com/articles/s41586-024-07107-7).

02 Post-Quantum Cryptography

2.1 Introduction to Cryptography

Cryptography is central to the secure operation of financial services, where the goal of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of data.[10] These security principles are fundamental to the secure operation and trust in financial systems.

- **Confidentiality** prevents potentially sensitive information from being exposed to unauthorised recipients. This is crucial for protecting payment information from being exposed when in transit, or for protecting customer records stored in a database.[11]
- **Integrity** helps to ensure that data has not been maliciously altered. This is used for ensuring that the contents of a transaction have not been changed,[12] or that malware has not been injected into software updates.[13]
- **Authentication** is used for identity verification, which is critical for identity and access management for mobile banking, payment authorisation and even fraud prevention.[14]
- **Non-repudiation** is used to provide proof that an entity has performed an action. This helps to ensure that an individual cannot deny having sent an order to a stockbroker or an order to a bank to transfer funds from one account to another.[15]

To achieve these security principles, cryptography uses a combination of three main types of algorithms: symmetric algorithms, asymmetric algorithms and hash functions.[16] Asymmetric algorithms can be used to establish a secure connection for sharing information, while information shared over that secured connection is kept confidential with a symmetric algorithm.

For the authentication of a sender's identity, digital signatures are used, which also use asymmetric algorithms. Then, to verify the integrity of communications, hash functions can be used to confirm that the contents of a message have not been altered in transit.

The security of some of these algorithms relies on mathematical problems that are considered computationally impractical to solve within a meaningful timeframe, using today's most powerful classical computers. However, this is projected to be at risk when large-scale quantum computers are available.

[10] Australian Cyber Security Centre (ACSC). 2026. *Guidelines for cryptography*. (https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism/cyber-security-guidelines/guidelines-for-cryptography).

[11] FS-ISAC. 2024. *Protecting Financial Data With Encryption Controls.* (https://www.fsisac.com/hubfs/Knowledge/ProtectingFinancialDataWithEncryptionControls.pdf).

[12] Fortinet. *What is cryptography?* (https://www.fortinet.com/resources/cyberglossary/what-is-cryptography). Accessed: June 23, 2026.

[13] National Institute of Standards and Technology. 2018. *Security Considerations for Code Signing.* (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01262018.pdf).

[14] PCI Security Standards Council. 2010. *PCI DSS Applicability in an EMV Environment: a guidance document.* (https://listings.pcisecuritystandards.org/documents/pci_dss_emv.pdf).

[15] IBM. *Non-Repudiation.* (https://www.ibm.com/docs/en/ibm-mq/10.0.x?topic=overview-non-repudiation). Accessed: June 23, 2026.

[16] Justin Moore. 2024. *Cryptography: Encryption and Hashing.* Colorado State University System. (https://it.csusystem.edu/cryptography-encryption-and-hashing/).

2.1.1 The Quantum Cyber Threat

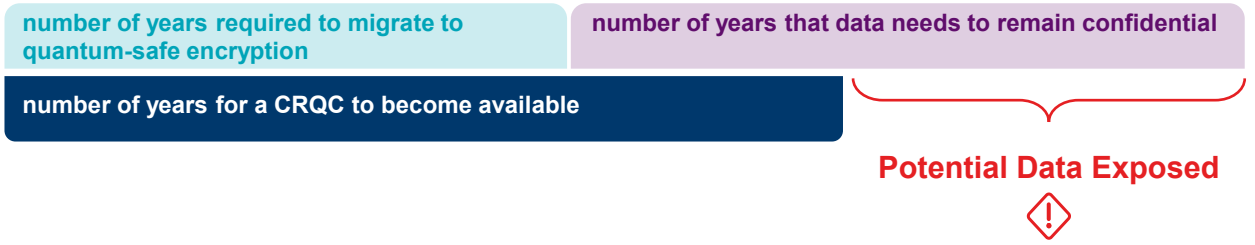
A CRQC could pose a significant threat to financial systems that rely on traditional asymmetric cryptography. This is because a quantum algorithm, namely Shor's algorithm, could break commonly used asymmetric encryption, such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC), within a meaningful time frame.[17]

In addition, symmetric encryption may also be weakened by Grover's algorithm. However, the speed-up provided by this algorithm is much smaller than that of Shor's, such that the current guidance released by the National Institute of Standards and Technology (NIST) of the United States suggests that current symmetric algorithms of sufficient key length will remain secure.[18]

Although a CRQC may not be available today, there is already a present threat to the confidentiality of certain information due to HNDL attacks. In such an attack, adversaries intercept and store encrypted information today, with the intention of decrypting it in the future, once a CRQC becomes available. This risk is particularly relevant for information that has a long-term sensitivity and needs to remain confidential for extended periods.

The applicability of this risk can be assessed by considering the confidentiality lifetime of the data, together with the number of years required to migrate to quantum-safe encryption. If the combined period is longer than the estimated time before a CRQC becomes available, then sensitive data may be exposed, before the end of its required confidentiality period. This concept is also known as Mosca's Theorem.

Figure 2: Mosca's Theorem



Source: KPMG analysis; adapted from Dr. Michele Mosca (2015).

The impact of quantum-enabled data breaches could be substantial, with estimates suggesting that the total value of data that could be exposed due to a quantum attack is in the range of trillions of dollars.[19]

In addition to data breaches, the threat to cryptography may also lead to major operational disruptions. For example, an attacker who could forge digital signatures using a quantum computer would be able to push malicious code updates, gain access to critical systems and impersonate trusted entities.

Financial systems such as secure payment networks and Distributed Ledger Technology (DLT) applications rely on cryptography for core functionalities. If the relevant cryptographic protections were compromised, these systems could face severe operational disruptions.

It is recognised that large-scale cyberattacks on financial institutions in recent years have resulted in disruption to trading and settlement processes, forcing firms to resort to manual workarounds and causing delays in regulatory reporting and market operations.[20] Although these were

[17] P W Shor. 1997. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* SIAM Journal on Computing. (https://doi.org/10.1137/S0097539795293172).

[18] National Institute of Standards and Technology. 2024. *Transition to Post-Quantum Cryptography Standards.* (https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf).

[19] Citi Institute. 2026. *Quantum Threat: The Trillion-Dollar Security Race Is On.* (https://www.citigroup.com/rcs/citigpa/storage/public/Citi_Institute_Quantum_Threat.pdf).

[20] Reuters. 2023. *ION brings clients back online after ransomware attack – source.* (https://www.reuters.com/technology/ion-starts-bring-clients-back-online-after-ransomware-attack-source-2023-02-07/) and Illumio. 2024. *Two Breaches, One Bank: Lessons from The ICBC Cyber Crisis.* (https://www.illumio.com/blog/two-breaches-one-bank-lessons-from-the-icbc-cyber-crisis).

not cryptographic attacks, they demonstrate the type of operational disruption that could occur if security systems are compromised.

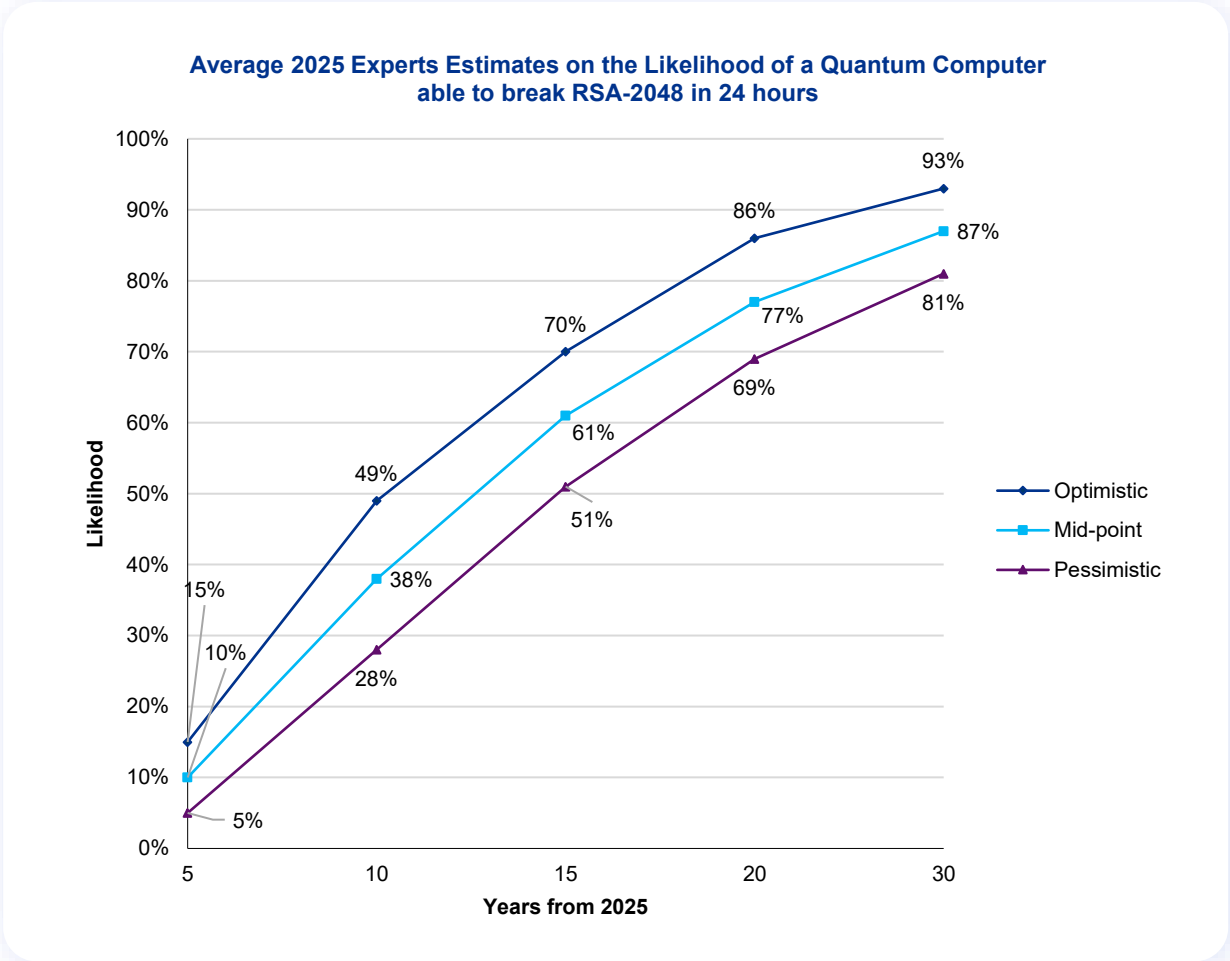
In a study conducted by the Hudson Institute in 2023, it was estimated that a single-day quantum attack on one of the five largest US financial institutions could cost the US economy between US$2.0 - $3.3 trillion (HK$15.6 - $25.9 trillion).[21]

2.1.2 Cryptographically Relevant Quantum Computer (CRQC) Timeline Estimates

Although quantum computing investment is high and companies are focused on increasing the operational scale of their systems, predicting when a CRQC may become operational is inherently difficult. While current quantum computers have qubit counts in the range of 100s to 1000s, the engineering challenges associated with large-scale quantum computing, and the means of overcoming them, remain an active area of research and development. Estimates of when a CRQC may become operational are therefore based on expert views, forward projections of current quantum technologies, company roadmaps and theoretical research.

In 2026, the Quantum Threat Timeline Report 2025 was published by the Global Risk Institute. This report details survey responses from experts in quantum computing, aimed at understanding when a CRQC may be operational. As presented in Figure 3, the respondents said that it is quite possible (28-49% likelihood) that this will happen in the next 10 years, and likely (51-70% likelihood) in the next 15 years.[22]

Figure 3: Expert Estimates on a CRQC Timeline[23]



Source: KPMG analysis; adapted from Global Risk Institute "Quantum Threat Timeline Report 2025" (2026).

[21] Arthur Herman and Alexander W Butler. 2023. *Prosperity at Risk: The Quantum Computer Threat to the US Financial System.* Hudson Institute. (https://www.hudson.org/technology/prosperity-risk-quantum-computer-threat-us-financial-system).

[22] Global Risk Institute. 2026. *Quantum Threat Timeline Report 2025.* (https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/).

[23] Global Risk Institute. 2026. *Quantum Threat Timeline Report 2025.* Figure 17. (https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/).

At some point, the number of qubits and the efficiency of quantum systems may be sufficient to break encryption within a practical timeframe. As efforts to scale quantum systems and improve their efficiency continue, significant theoretical reductions have been made in the number of qubits estimated to be required for a CRQC. These developments suggest that the timeline for a CRQC could potentially be earlier than previously expected.

For example, non-peer reviewed scientific papers show that, under certain theoretical assumptions, this number could be reduced to as low as 10,000 qubits, with the trade-off that it would take hundreds to thousands of days to complete the cryptographically relevant calculation,[24] while with more qubits this task may be completed faster.

Figure 4 illustrates how the theoretical requirements for a CRQC have changed over time, alongside trends in the scale of available quantum devices and future quantum roadmaps. The 2025 and 2026 data points have been published but are not yet peer reviewed. Other novel approaches that are not broadly applicable to most quantum computing types have not been included in Figure 4.

Importantly, the above quantum computer information and roadmaps are public information only and it is likely that quantum computers under development may not be presented in public disclosures. It is also possible that access to a CRQC, if achieved, may not be publicly disclosed immediately, meaning that an earlier timeline

Figure 4: Theoretical qubit limits for a CRQC, current quantum devices and future roadmaps[25 26 27 28]

Source: KPMG analysis; adapted from Cain et al. (2026), O'Gorman et al. (2017), Jones et al. (2012), and Gidney et al. (2021).

[24] Cain et al. 2026. *Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits.* Figure 3. (https://arxiv.org/abs/2603.28627).

[25] O'Gorman et al. 2017. *Quantum computation with realistic magic-state factories.* Table 1. (https://journals.aps.org/pra/abstract/10.1103/PhysRevA.95.032338).

[26] Jones et al. 2012. *Layered Architecture for Quantum Computing.* (https://journals.aps.org/prx/abstract/10.1103/PhysRevX.2.031007).

[27] Gidney et al. 2021. *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.* Table 2. (https://quantum-journal.org/papers/q-2021-04-15-433/pdf/).

[28] Gidney. 2025. *How to factor 2048 bit RSA integers with less than a million noisy qubits.* (https://arxiv.org/abs/2505.15917).

should be considered when determining the timeline of a CRQC. In the Global Risk Institute's publication, 32% of experts stated that "under the radar" research could bring forward the impact by 2 to 3 years, while 27% of experts stated that this research could bring it forward by more than 3 years.[29]

While Figure 4 focuses on the technical challenge of increasing the scale and efficiency of quantum computers to affect cryptography, regulatory timelines, updated procurement requirements and interoperability considerations will also drive mitigation efforts. These factors will require organisations to take action to manage quantum cyber risk and maintain normal business operations, irrespective of the availability of a CRQC. Further details are covered in Section 2.3.

2.2 Potential Solutions

2.2.1 Post-Quantum Cryptography

In response to quantum cyber risk, PQC has been developed as an alternative to widely used encryption schemes, such as RSA and ECC, that are vulnerable to quantum attacks.

These PQC algorithms use different mathematical problems where there is no known quantum or classical algorithm that could solve them in a meaningful time frame.[30] Fortunately, PQC can be implemented on classical hardware and is not an application of quantum technology but part of the solution to address quantum cyber risk.[31]

There are different types of PQC algorithms based on different mathematical concepts, including lattice-based, hash-based and code-based schemes, as well as approaches based on isogenies and multivariate polynomials. The algorithms that organisations choose to implement will depend on the specific use case and may be influenced by factors such as computational requirements, interoperability considerations, standards and regulatory guidance.

Practical issues such as processing times and memory requirements will be important considerations for PQC implementation as computational requirements vary between different types of cryptographic algorithms. This may impact some legacy hardware and Internet of Things (IoT) devices that may be unable to support the larger key sizes required by post-quantum algorithms.

2.2.2 Cryptography Management

To manage this issue, the adoption of PQC will require organisations to make changes to the way that encryption is governed throughout their IT estate. Considerations include the impact of post-quantum algorithms on system performance, managing downtime during cryptographic upgrades and ensuring interoperability between systems. A key consideration in the evolution of encryption management is the need for and development of cryptographic agility.

Cryptographic agility (crypto agility) refers to the ability of a system to replace cryptographic algorithms, keys and protocols without major operational disruption.[32] NIST further describes crypto agility as a "key practice that should be adopted at all levels, from algorithms to enterprise architectures".[33]

Crypto agility is important to consider during this cryptographic transition, because there is the possibility of a mathematical breakthrough occurring that reveals a vulnerability that could be exploited by a quantum or classical computer in any algorithm.

For example, Supersingular Isogeny Key Exchange (SIKE) is a key exchange algorithm that made it through three rounds of evaluation in the NIST selection process and looked to be a promising candidate for standardisation before being broken in 2022, in just one hour, with a single core, standard commercial server built in 2013. [34]

[29] Global Risk Institute. 2026. *Quantum Threat Timeline Report 2025.* (https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/).

[30] UQ Cyber Research Centre. *Post-Quantum Cryptography*. University of Queensland. (https://www.cyber.uq.edu.au/research-topics/post-quantum-cryptography). Accessed: June 23, 2026.

[31] National Institute of Standards and Technology (NIST). *What Is Post-Quantum Cryptography?* (https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography#how-does-post-quantum-cryptography-differ-from-quantum-cryptogra). Accessed: June 23, 2026.

[32] Palo Alto Networks. *What Is Cryptographic Agility?* (https://www.paloaltonetworks.com.au/cyberpedia/what-is-cryptographic-agility). Accessed: June 24, 2026.

[33] National Institute of Standards and Technology (NIST). 2025. *Considerations for Achieving Crypto Agility: Strategies and Practices.* (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39-upd1.pdf).

[34] Castryck, W. and Decru, T. 2022. *An efficient key recovery attack on SIDH.* (https://eprint.iacr.org/2022/975).

If a similar exploit is discovered in future for an algorithm that has been widely adopted, crypto agility would be a critical requirement for organisations to swiftly protect themselves against an attack.

It should be noted that PQC algorithms are recent developments, that have not been tested in production to the same extent as traditional algorithms. In a transition of this scale, there remains a possibility of unforeseen operational impacts or integration challenges arising due to the larger key sizes and computational overheads associated with PQC.

In some cases, organisations may choose to use hybrid encryption where both traditional and quantum-resistant algorithms are used at the same time to protect communications. This approach may enable organisations to manage a more gradual transition to PQC, whilst minimising the risk of operational disruptions.[35]

However, this comes with the additional consideration that, while two different algorithms are being used at the same time, hybrid encryption has additional overheads compared to pure PQC adoption.[36] Consequently, a hybrid approach may also require additional migration effort if a "second migration" is required to move from hybrid to pure PQC as traditional cryptography is phased out.

2.2.3 Quantum Key Distribution

In addressing quantum cyber risk, PQC is one path of mitigation, while another potential mitigation is Quantum Key Distribution (QKD). QKD technology utilises protocols based on quantum mechanics to transmit information and deals with one aspect of cybersecurity, the distribution of the cryptographic key. This means that QKD must be accompanied by quantum-resistant algorithms for the purpose of authentication.[37]

The security of QKD depends on physical quantum mechanical properties such that an adversary cannot intercept data sent across a QKD link undetected.[38] This contrasts with security achieved by a mathematical cryptographic function. These mathematical algorithms are considered computationally secure as long as there are no known attacks that could be carried out using available technology.[39]

Currently, there are many examples where QKD has been explored, mostly for PoC, demonstration and evaluation. For example, the Hong Kong Polytechnic University (PolyU) successfully completed Hong Kong's first chip-based quantum network test in 2025[40] and China has invested heavily over many years in QKD, with large-scale national quantum communication networks,[41] including a Beijing-Shanghai QKD link. In Japan, the Tokyo QKD Network has been used for various demonstrations including the transmission of biometric authentication and financial data.[42]

European jurisdictions are also actively researching QKD. For example, the Madrid Quantum Communications Infrastructure (MadQCI) in Spain is one of Europe's largest quantum communication networks and has been integrated with industrial networks in a step towards commercialisation.[43]

In the financial services sector, HSBC in the UK has joined BT and Toshiba's quantum-secured metro network and will trial the secure transmission of data including financial transactions and secure video communications. QKD may one day play a key role in protecting financial transactions, client data and proprietary information across the financial sector.[44]

However, this approach is still developing, and some government organisations do not endorse QKD because it

[35] Palo Alto Networks. *What Is Hybrid Cryptography?* (https://www.paloaltonetworks.com/cyberpedia/what-is-hybrid-cryptography#how-does-hybrid-cryptography-actually-work). Accessed: June 24, 2026.

[36] Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson and David Cooper. 2024. *Transition to Post-Quantum Cryptography Standards (NIST IR 8547, Initial Public Draft).* National Institute of Standards and Technology (NIST). (https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf).

[37] Australian Cyber Security Centre (ACSC). 2026. *Quantum technology primer: Communications.* (https://www.cyber.gov.au/business-government/secure-design/quantum/quantum-technology-primer-communications).

[38] Henning Soller and Martina Gschwendtner. 2026. *Quantum communication and computing: Elevating the banking sector.* McKinsey & Company. (https://www.mckinsey.com/industries/financial-services/our-insights/quantum-communication-and-computing-elevating-the-banking-sector).

[39] Ada Computer Science. *Computational security.* (https://adacomputerscience.org/concepts/encrypt_computational_security). Accessed: July 10, 2026.

[40] The Hong Kong Polytechnic University. 2025. *PolyU Successfully Completes Hong Kong's First Chip-Based Quantum Network and Test.* (https://www.polyu.edu.hk/media/media-releases/2025/1112_polyu-successfully-completes-hong-kongs-first-chip-based-quantum-network-and-test/).

[41] Dongyoun Cho. 2026. *QKD governance gap: certification, fragmentation and the cost of delay.* The International Institute for Strategic Studies (IISS). (https://www.iiss.org/online-analysis/online-analysis/2026/04/qkd-governance-gap-certification-fragmentation-and-the-cost-of-delay/).

[42] Q-STAR (Quantum STrategic industry Alliance for Revolution). 2024. *Current Status of Quantum Cryptography and Toward Its Practical Implementation.* (https://qstar.jp/archives/quantum/current-status-of-quantum-cryptography-and-toward-its-practical-implementation).

[43] Vincent Martin et al. 2023. *MadQCI: A Heterogeneous and Scalable SDN QKD Network Deployed in Production Facilities.* (https://arxiv.org/abs/2311.12791).

[44] HSBC. 2023. *HSBC Becomes First Bank To Join The UK's Pioneering Commercial Quantum Secure Metro Network.* (https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-becomes-first-bank-to-join-the-uks-pioneering-commercial-quantum-secure-metro-network).

is highly implementation-dependent, expensive and requires specialised infrastructure. For example, the National Security Agency (NSA) has stated that it does not recommend QKD for securing national security systems[45] due to infrastructure cost, increased insider threat and denial of service risks and challenges around validating the security of QKD schemes. These challenges may be overcome in future, enabling QKD to be deployed as a secure and reliable method of communication resistant to quantum cyber risk.

2.3 PQC Landscape

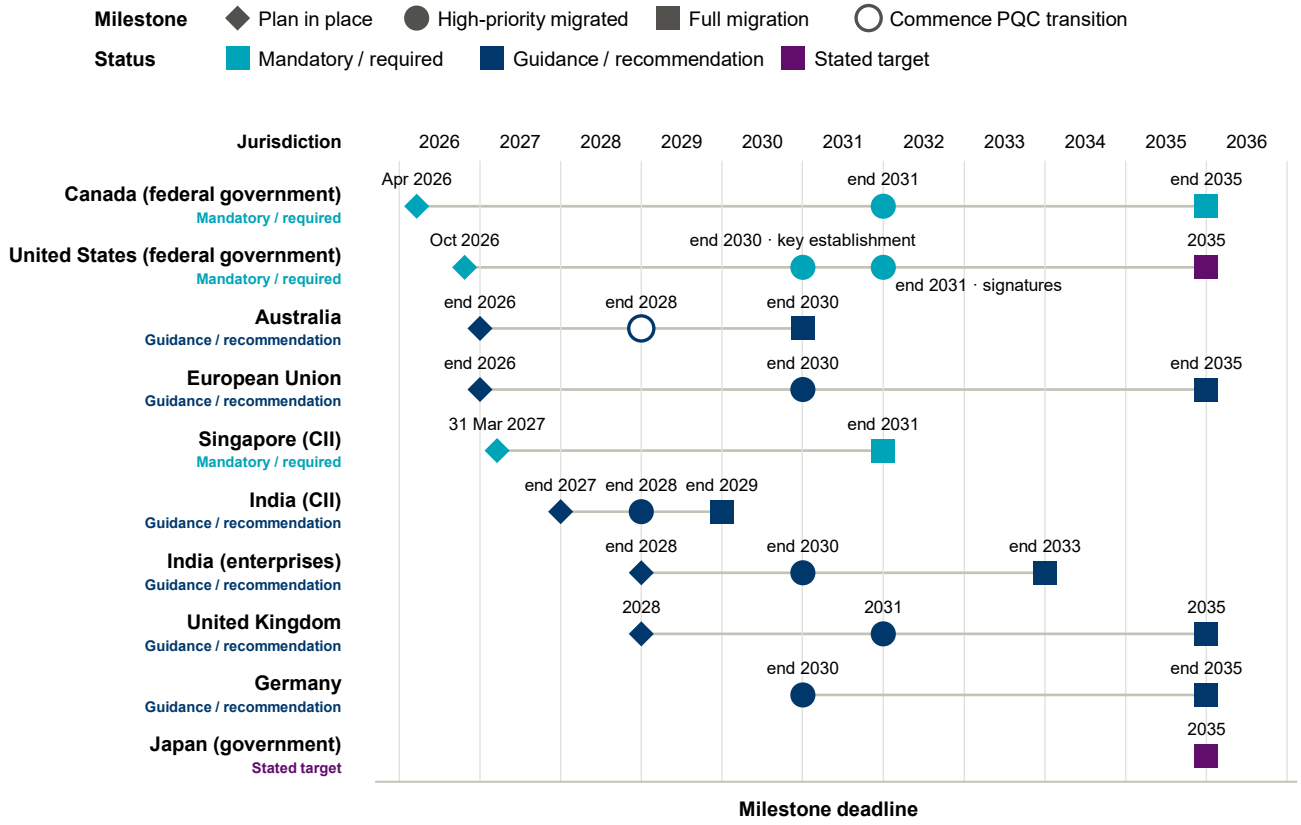
Globally, new standards, regulations and remediation timelines have been introduced in response to quantum cyber risk. These developments are intended to inform, guide, encourage and, in some cases, mandate action to address quantum-related threats. Governments, working groups, regulators and technology providers all emphasise that migration is a multi-year activity, and many have published roadmaps for transition to PQC.

While the definitions of individual milestones may vary, many of the published timelines indicate that PQC transition should be completed in the period between 2030 and 2035. Consequently, organisations that operate on a global scale should identify the impact of these changes based on the jurisdictions in which they operate or interact.

However, these PQC transition timelines are constantly being revised due to new scientific and technological breakthroughs. As a result, AIs should continue to monitor these breakthroughs and adjust their timelines accordingly.

For example, in March 2026, Google announced 2029 as the timeline for its PQC migration,[46] and in June 2026 the

Figure 5: Government PQC Migration Deadlines



Note: Milestone definitions vary by jurisdiction and are not directly comparable.

Source: KPMG analysis

[45] National Security Agency. *Quantum Key Distribution (QKD) And Quantum Cryptography (QC).* (https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/). Accessed: June 24, 2026.

[46] Heather Adkins & Sophie Schmieg. 2026. *Quantum frontiers may be closer than they appear.* Google Blog Safety & Security. (https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/).

President of the United States of America issued an executive order[47] to transition all high value assets to use PQC for key establishment by December 31, 2030, and digital signatures by December 31, 2031.

In view of the long-term risks posed by quantum computing, government regulatory bodies and standard-setting authorities worldwide are also strengthening expectations and guidance for organisations to assess and mitigate these risks.

The Asia-Pacific (APAC) region presents a diverse PQC landscape with variations in standardisation efforts, guiding policies and strategic priorities. China launched a programme for the development of PQC algorithms, seeking to pursue a sovereign cryptographic ecosystem. It is now performing evaluations of these algorithms in 2026 to be selected for standardisation. In June 2026, the Institute of Commercial Cryptography Standards (ICCS) in China released guidelines to self-assess performance of Key Encapsulation Mechanisms (KEMs), digital signature schemes, key exchange protocols and cryptographic hash algorithms in various architectures.[48]

Japan is focusing on cryptographic standards for government agencies and has released cipher lists for procurement of e-government systems ensuring alignment with international standards.[49] Similarly, South Korea is actively investing in PQC research and has passed an amendment bill in the cabinet which includes requirements for public institutions, central and local governments to develop and plan their transition.[50] There is further development in the APAC region with regulatory bodies in India,[51] Singapore,[52] Australia,[53] and New Zealand[54] issuing guidance and phased migration roadmaps for PQC adoption.

The United States has adopted a centrally coordinated approach to PQC with NIST acting as the primary standard-setting authority. NIST published three PQC standards in August 2024 for key exchange and digital signatures. NIST is currently evaluating additional PQC algorithms to provide cryptographic diversity. These new standards are expected to be released in 2027.[55] As mentioned previously, the US has also released mandates for the adoption of quantum-resistant algorithms for national security systems and federal agencies. In Canada, the PQC Migration Roadmap published by the Canadian Centre for Cyber Security aligns with the NIST standardised PQC algorithms to ensure interoperability with US systems.[56]

In Europe, agencies have aligned with the NIST standards as outlined in the European Commission's Coordinated Implementation Roadmap for PQC published in 2023.[57] The national authorities in Europe also encourage algorithm diversity beyond NIST selections, with Guidance from Germany (BSI),[58] France (ANSSI)[59] and the Netherlands (NCSC-NL)[60] recommending that organisations assess the use of alternative algorithms alongside NIST finalised algorithms.

[47] The White House. 2026. *Securing the Nation Against Advanced Cryptographic Attacks.* (https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/).

[48] Institute of Commercial Cryptography Standards. 2026. *Announcement on Releasing Guidelines for Performance Self-Assessment of Cryptographic Algorithms.* NGCC. (https://www.niccs.org.cn/niccs/Notice/pc/content/content_2066798866453762048.html).

[49] Cryptography Research and Evaluation Committees. 2026. *CRYPTREC Ciphers List.* CRYPTREC Japan. (https://www.cryptrec.go.jp/en/list.html).

[50] Ministry of Science and ICT. 2026. *Korea Strengthens Legal Framework to Become a Global Quantum Leader.* MSIT South Korea. (https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=1263&searchOpt=ALL&searchTxt=).

[51] Department of Science and Technology. 2026. *Implementation of Quantum Safe Ecosystem in India.* DST Task Force. (https://dst.gov.in/sites/default/files/Report_TaskForce_PQMigration_4Feb26%20%28v1%29.pdf).

[52] Monetary Authority of Singapore. 2024. *Advisory on addressing the Cybersecurity Risks associated with Quantum.* MAS Circular. (https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf).

[53] Australian Signals Directorate. 2025. *Stay ahead of the quantum threat with post-quantum cryptography.* ASD Guideline. (https://www.cyber.gov.au/about-us/view-all-content/news/stay-ahead-of-the-quantum-threat-with-post-quantum-cryptography).

[54] National Cyber Security Centre. 2020. *Preparing for Quantum-Safe Cryptography.* (https://www.ncsc.gov.uk/paper/preparing-for-quantum-safe-cryptography).

[55] Chad Boutin. 2025. *NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption.* NIST. (https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption).

[56] Head of Canadian Centre for Cyber Security. 2026. *Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information - ITSP.40.111.* Government of Canada. (https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111).

[57] European Commission. 2025. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, EU Policy and Legislation.* (https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography).

[58] Federal Office for Information Security. 2026. *Technical Guidance on Cryptographic Mechanisms.* BSI Germany. (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=9,%20BSI%20-%20Bundesamt%20f%C3%BCr%20Sicherheit%20in%20der%20Informationstechnik%20-%20BSI%20TR-02102-1%20%22Cryptographic%20Mechanisms:%20Recommendations%20and%20Key%20Lengths%22%20Version:%202025-1).

[59] Mes Services Cyber. 2026. *ANSSI views on crypto agility for developers and system architects.* ANSSI. (https://messervices.cyber.gouv.fr/documents-guides/ANSSI-views-on-crypto-agility.pdf).

[60] General Intelligence and Security Service. 2024. *PQC Migration Handbook.* AIVD Netherlands. (https://english.aivd.nl/documents/2024/12/3/the-pqc-migration-handbook).

The United Kingdom through the National Cyber Security Centre (NCSC) has also defined a structured and time-bound PQC transition that is aligned with NIST recommendations.[61] In this guidance, NCSC recommends completing planning and discovery activities by 2028, undertaking early and priority migration between 2028 and 2031, and completing full migration to PQC by 2035.

Financial organisations operating internationally also need to consider sector-specific PQC guidelines to maintain interoperability and continuation of operations. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC)[62] has issued guidance that identifies payment infrastructure as a critical early target for post-quantum readiness. The Payment Card Industry Data Security Standard (PCI-DSS) version 4.0,[63] effective in March 2025, has included a requirement for organisations to maintain a complete cryptographic inventory, manage cryptography throughout its lifecycle and implement risk-based controls to address cryptographic vulnerabilities.

Banks and other financial institutions have already begun testing the implementation of PQC. HSBC's quantum pilot used PQC to safely move gold tokens across distributed ledgers.[64] In Europe, the Bank of France and Deutsche Bundesbank used quantum-safe Virtual Private Networks (VPNs) to secure payment transactions.[65] Daiwa Securities Group in Japan has tested securing online financial services with PQC.[66] A key finding across these pilots is that PQC is feasible but organisations must consider crypto agility capabilities and ensure infrastructure preparedness before large-scale algorithm replacement.

[61] National Cyber Security Centre. 2024. *Next steps in preparing for post-quantum cryptography.* NCSC UK. (https://www.ncsc.gov.uk/paper/next-steps-in-preparing-for-post-quantum-cryptography).

[62] Financial Services Information Sharing and Analysis Center. 2026. *Post Quantum Cryptography Resources.* FS-ISAC Guidance. (https://www.fsisac.com/knowledge/pqc).

[63] PCI Standards Security Council. 2024. *PCI DSS v4.0.1.* PCI SSC Blog. (https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1).

[64] HSBC London. 2024. *HSBC pilots quantum-safe technology for tokenised gold.* HSBC News. (https://www.hsbc.com/news-and-views/news/media-releases/2024/hsbc-pilots-quantum-safe-technology-for-tokenised-gold).

[65] BIS Innovation Hub. 2025. *Project Leap phase 2: quantum-proofing payment systems.* BIS Publication. (https://www.bis.org/publ/othp107.htm).

[66] Daiwa Institute of Research. 2026. *Post-Quantum Cryptography (PQC): Proof-of-Concept Results and a Cryptographic Migration Approach in the Daiwa Securities Group.* Daiwa Securities Group. (https://www.dir.co.jp/report/technology/security/20260331_025651.pdf).

03 Current Hong Kong Landscape

The section is organised into two parts. Section 3.1 examines the sector's awareness of and engagement with quantum computing as an emerging technology. Section 3.2 then examines the sector's preparedness for the cryptographic transition that quantum computing will necessitate, drawing on a structured assessment of PQC readiness across four dimensions. Unless otherwise stated, percentages presented in this section represent the proportion of survey respondents, rather than the entire banking sector. Percentages may not add up to 100% due to rounding or because some questions allowed multiple responses.

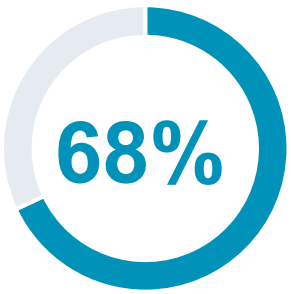
3.1 Hong Kong Banking Sector's Quantum Computing Readiness

This section examines how Hong Kong's banking sector understands and anticipates quantum computing as an emerging technology. It covers the sector's familiarity with quantum computing, current adoption status, anticipated use cases, investment intentions and timelines, and the barriers AIs face as they prepare for the post-quantum era.

3.1.1 Awareness and Familiarity with Quantum Computing

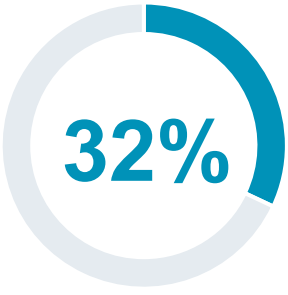
Awareness represents the first stage of adoption, and the findings indicate that most survey respondents have at least some awareness of quantum computing, even though more advanced familiarity remains limited to a smaller group of AIs. The majority of survey respondents reported at least a basic awareness of the technology, with 68% indicating basic awareness or a more advanced level of engagement. Familiarity within this group nonetheless varied considerably. 37% of survey respondents reported only basic awareness, while a smaller 22% were actively exploring quantum computing and 9% had established a dedicated specialist team. A further 32% reported no consideration or discussions about quantum computing in planning. This distribution reflects quantum computing's nascent position within the banking industry where it is broadly recognised, but not yet supported by deep institutional capability across most AIs.

Figure 6: Quantum Computing Engagement Across the Sector



of AIs have at least a basic awareness of quantum computing

of AIs have discussed quantum computing at the board-level



of AIs have undertaken quantum computing-related initiatives

Source: HKMA survey, KPMG analysis

Internal discussion follows a similar pattern. Around half of survey respondents reported that quantum computing had been discussed at the board-level, whether in formal or informal terms. Of these, 20% described the discussion as formal, encompassing broader technology strategy, specific quantum computing agenda items, and related risk assessment, while 30% characterised it as informal. These findings suggest that quantum computing is beginning to receive attention at a strategic level within parts of the sector, although engagement remains at an early stage for most AIs.

3.1.2 Current Adoption Status

Adoption levels remain considerably lower than overall awareness. 68% of survey respondents reported having no quantum-related initiatives in place, indicating that adoption across the sector remains low.

A smaller cohort has nonetheless begun to engage with the technology. 32% of survey respondents indicated that they have started exploring or piloting quantum computing applications, with activity largely confined to these early phases rather than operational deployment. Among the AIs that reported some level of activity, the areas most frequently being explored were PQC, fraud detection and cybersecurity, and portfolio optimisation.

The examples below are drawn from the free-text responses of the small number of AIs that reported activity in each area. They are illustrative of the types of initiative being explored and are not indicative of the prevalence of such activity across the wider population of AIs.

Risk Modelling

Enabling Technology Examples: Quantum Random Number Generator (QRNG)

Use Cases: Some AIs have begun exploring the use of quantum algorithms to enhance risk assessment accuracy, allowing for more precise and efficient risk management. Preliminary investigation has also been undertaken into the application prospects of quantum Monte Carlo simulation in credit risk calculations. A further area of activity is the use of QRNG to enhance stochastic modelling in Monte Carlo simulations for forecasting and risk assessment, improving the quality of randomness in simulation and leading to more accurate financial projections.

Portfolio Optimisation

Enabling Technology Examples: QAOA

Use Cases: Some AIs are actively exploring the potential of quantum optimisation algorithms in refining their asset allocation and portfolio construction strategies. Current efforts are concentrated on literature review and technical tracking, with collaborations involving external vendors. Some AIs have also indicated an interest in exploring PoCs targeting complex risk-return trade-offs and constraints that are challenging for classical approaches. These efforts underline a substantive investigative endeavour to integrate quantum techniques alongside existing optimisation methods.

Fraud Detection and Cybersecurity

Enabling Technology Examples: QML

Use Cases: Some AIs are investigating the potential of QML models to enhance the accuracy and efficiency of fraud detection systems. These explorations also extend to specific sectors such as insurance, with an emphasis on hybrid quantum-classical models for high-volume transaction environments.

Pricing and Derivatives Modelling

Enabling Technology Examples: Quantum Monte Carlo, Low-Depth Algorithms for Quantum Amplitude Estimation

Use Cases: An AI's PoC tested a quantum Monte Carlo algorithm for derivatives pricing, with experiments on a simplified example conducted on quantum hardware. Quantum computing has separately been explored to optimise pricing models for financial derivatives, improving the speed and accuracy of complex financial calculations. Low-depth quantum amplitude estimation is a further reported application in derivatives pricing.

QKD

Enabling Technology Examples: QKD

Use Cases: QKD has been tested by several AIs to secure data transmission between data centres, and to secure cryptographic key exchange in high stakes financial transactions such as foreign exchange trading.

Cryptography/ PQC

Enabling Technology Examples: PQC

Use Cases: Some AIs are actively conducting PoCs to develop Cryptographic Bill of Materials (CBOM) tools and assess the interoperability of PQC solutions within the industry. Further internal analyses are underway to evaluate the potential impact of quantum technologies on existing cryptographic capabilities, which will critically inform future key-length and algorithm decisions. These efforts underscore the sector's proactive stance in anticipating and preparing for future challenges in quantum-resilient security.

3.1.3 Anticipated Use Cases and Investment

Beyond current adoption activity, AIs were also asked to identify the applications they consider most relevant, the level of investment they anticipate committing, and their expected timelines for engagement. The most frequently cited use cases were fraud detection and cybersecurity, PQC, and risk modelling.

Investment intentions, however, remain measured. Around 39% of survey respondents indicated plans to allocate a portion of their innovation budget to quantum computing-related initiatives over the next three to five years. Among those planning to invest, the most commonly reported allocation level was below 5% of the innovation budget (28%), while a smaller proportion of 11% of survey respondents indicated allocations of 5% or above. The remaining 61% of survey respondents reported no planned budget allocation. For most AIs, dedicated investment remains limited or absent at this stage, reflecting the cautious posture observed across awareness and adoption findings.

3.1.4 Adoption Barriers in Quantum Computing

The cautious posture observed across awareness, adoption, and investment findings is closely linked to the barriers AIs currently face. For the substantial share of AIs reporting no current plans to adopt quantum computing, the most frequently cited reasons were that the technology is not yet sufficiently mature, that its business value remains unclear or unproven, and that AIs preferred to wait for broader industry adoption before committing.

AIs identified a range of challenges constraining their adoption of quantum computing. The barrier most frequently ranked among AIs' top three concerns was technology maturity and uncertainty, placed among the top three by 73% of survey respondents. This was followed by the difficulty of identifying commercially viable use cases, cited by 53%, and a shortage of internal expertise and quantum-related skills, cited by 47%. Concerns relating to technology maturity and the lack of clear business value were consistent with the reasons cited by AIs reporting no immediate plans to adopt, suggesting that these challenges are shared across the sector rather than confined to AIs yet to engage.

3.1.5 Implications and Potential Solutions

Looking ahead, AIs were also asked how they expect the role of quantum computing in the financial services industry to evolve over the coming decade. AIs broadly anticipated a dual role for the technology. The more immediate of the two relates to security: AIs pointed to the need to migrate toward PQC, driven by the HNDL threat as mentioned in Section 2, whereby data captured today could be decrypted once quantum capabilities mature. Accordingly, cryptography and quantum-resilient security were seen as the areas likely to feel the earliest impact. The second role, expected to develop later, is as a specialised tool for accelerated computation. Beyond its defensive applications, AIs anticipated target use cases in risk modelling, portfolio optimisation, derivative pricing, and fraud detection, with AIs generally expecting a hybrid approach in which quantum computing complements rather than replaces existing classical frameworks before becoming more widely established.

AIs viewed the timeline for this transition as gradual. The near term was associated with research and capability building, with pilots anticipated in the next three to five years, and broader, efficiency-driven use of the technology expected only once the underlying hardware has matured. These views are consistent with the medium to long-term adoption timelines reported earlier, suggesting that the sector continues to regard quantum

Figure 7: Most Frequently Cited Barriers to Quantum Computing Adoption

Note: Figures represent the share of AIs that ranked each barrier among their top three most significant concerns. Percentages are calculated over all AIs that responded to the question.

Source: HKMA survey, KPMG analysis

computing as a longer-term priority rather than an immediate operational focus, while recognising that preparation on the security front is already warranted.

When asked what would most help them advance, AIs identified several forms of support as particularly valuable. The support most frequently ranked among AIs' top three priorities was practical guidance and whitepapers on technology adoption, identified by 78% of survey respondents, followed by clear supervisory guidelines and expectations for quantum computing, cited by 74%, and industry forums for sharing best practices, cited by 49%.

These preferences suggest that guidance, supervisory clarity, and structured opportunities for industry knowledge sharing may play an important role in supporting future readiness across the sector. The specific actions through which these could be delivered are considered further in Section 4.

Taken together, the survey findings indicate that Hong Kong's banking sector remains at an early stage of quantum computing readiness: broadly aware of the technology's potential, with a number of AIs beginning to explore its applications, but with wider adoption still constrained by operational, technological, and capability-related challenges. With coordinated support to address these constraints, the sector is better placed to build on this early awareness as the technology matures.

3.2 Hong Kong Banking Sector's PQC Readiness

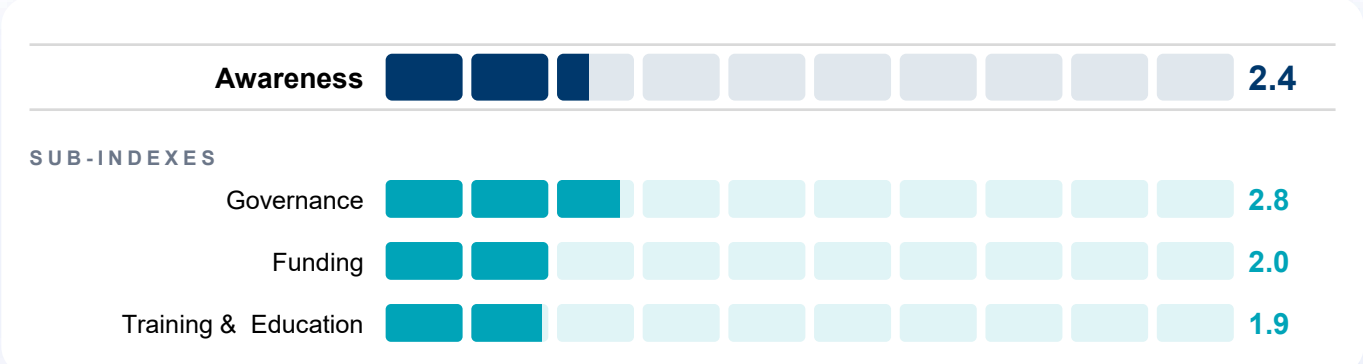
While the preceding section examined Hong Kong AIs' awareness of and engagement with quantum computing, the implications of the technology extend beyond its potential applications. As quantum computing capabilities continue to advance, AIs will also need to prepare for the impact on existing cryptographic systems that support payments, data protection, authentication, and secure communications.

This section examines the sector's readiness for PQC, drawing on findings from the same survey. The assessment considers readiness across four dimensions: Awareness, Planning, Pilots, and Practical Preparedness. Each dimension comprises a set of sub-indices, and scores are reported on a scale of 0 to 10. Together, these dimensions provide an indication of the sector's overall readiness for the transition to quantum-resistant cryptographic standards. Unless otherwise stated, findings are reported in aggregate across all responding institutions. The overall PQC readiness score across the sector was 2.3/10. By institution type, the average PQC readiness score was 2.6/10 among retail banks and 2.2/10 among non-retail banks.

3.2.1 Awareness of Quantum Risk and PQC

This subsection examines the extent to which AIs have established the institutional foundations needed to support a PQC transition. It considers how AIs govern and oversee quantum-related risk at the leadership level, allocate funding to the transition, and develop workforce capability through training and education. These are assessed across three sub-indices: Governance, Funding, and Training and Education. The overall Awareness index score across the sector was 2.4/10. By institution type, the average Awareness index score was 2.7/10 among retail banks and 2.4/10 among non-retail banks.

Figure 8: Awareness – Index & Sub-index Scores



Source: HKMA survey, KPMG analysis

Governance

The Governance sub-index assesses the degree to which quantum risk visibility has reached executive leadership and is reflected in governance and decision-making processes.

When asked about executive oversight of quantum-related risk, 39% of survey respondents reported having no formal governance in place, while a further 42% indicated that quantum risks are managed informally through existing cybersecurity or risk governance forums without dedicated focus. Around 18% of survey respondents reported having established a formal quantum readiness steering committee or working group with defined reporting cycles and responsibilities, while a small number reported that quantum risk oversight is embedded at the executive level with strategic alignment and formal reporting. Dedicated governance arrangements for quantum-related risk remain uncommon. Nevertheless, a majority of survey respondents reported that quantum-related issues are considered either through existing governance forums or through more formal oversight mechanisms.

Regarding executive leadership engagement with the broader PQC transition, 50% of survey respondents reported that executive leadership acknowledges the importance of PQC readiness and provides guidance and support. However, governance structures remain limited and prioritisation is typically focused on specific high-risk areas. A further 12% reported a more structured approach, with executive leadership actively sponsoring PQC readiness through formal governance arrangements, funding commitments, and support for migration activities, including a small number that have integrated PQC readiness into their broader strategic vision. By contrast, 38% reported minimal or no executive sponsorship, with leadership engagement occurring on an ad-hoc basis or not at all. Executive engagement with PQC readiness was reported by a majority of AIs, although formal sponsorship and strategic integration remain limited to a smaller group.

The findings on ownership and accountability present a mixed picture. While 39% of survey respondents reported no formal assignment of ownership for cryptographic assets and a further 33% indicated that ownership is informally assigned or managed by individual teams, around 28% reported having formally defined ownership roles or governance processes with documented responsibilities. Formal ownership and accountability arrangements have therefore been established at a number of AIs, although such practices are not yet widespread across the sector.

Funding

The Funding sub-index examines how AIs allocate financial resources to support their PQC transition.

Just over half of the survey respondents reported having no dedicated funding allocated to PQC transition efforts. A further 42% indicated that funding is allocated on a project-by-project basis rather than through a standing budget commitment. Around 7% reported having a more structured approach, either through annual budgets with defined allocations for quantum security or through comprehensive multi-year investment programmes. While dedicated funding arrangements remain limited, the prevalence of project-based funding suggests that some institutions have begun to allocate resources to PQC-related activities.

Training and Education

The Training and Education sub-index examines whether AIs have built the workforce capabilities needed to support the PQC transition.

On executive education, half of the survey respondents reported that no awareness or education programme exists for executive leadership, with any understanding of quantum-related risks remaining informal and unstructured. However, 43% indicated that leadership receives periodic briefings on quantum computing developments, with content tailored to their roles and strategic responsibilities. A smaller group of around 7% reported having structured programmes in place, including dashboards, targeted insights, and scenario updates designed to guide quantum security strategy.

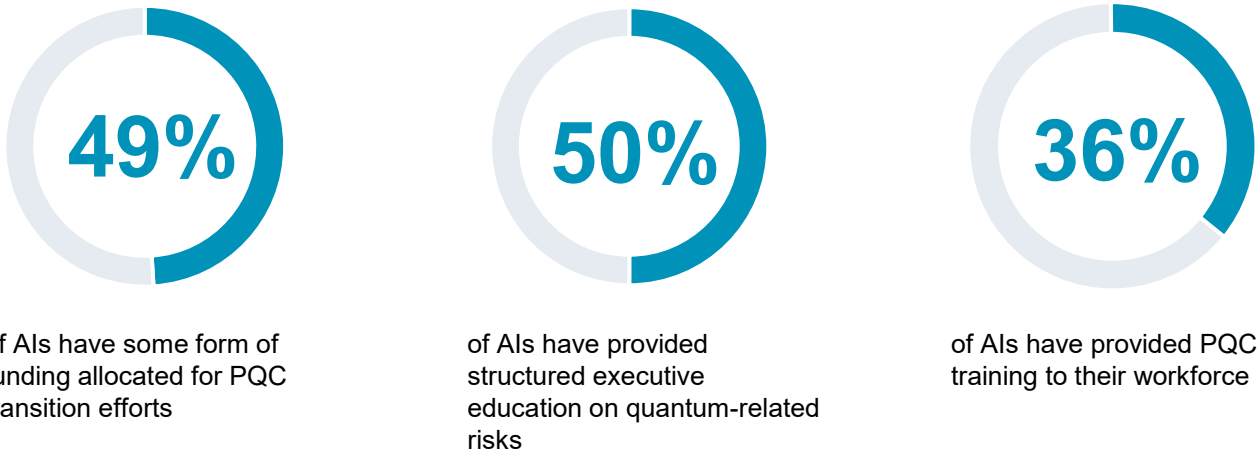
Beyond executive-level awareness, AIs were also asked whether they have provided training on quantum threats and PQC to their broader workforce. Around 64% of survey respondents reported that no such training has been provided. Among the AIs that have delivered training, approaches varied in format, content, and audience.

Training was delivered through a combination of internal and external channels, including awareness sessions, e-learning programmes, workshops, vendor briefings, industry events, webinars, and specialist training provided by third parties. The content covered both foundational

and applied topics, ranging from basics of quantum computing and PQC to migration planning, cryptographic agility, emerging standards, regulatory developments, and the potential implications of quantum threats for existing cryptographic systems.

Training activities were directed primarily at IT personnel, with some AIs extending coverage to risk, compliance, cybersecurity, and legal functions. This concentration of training among technical teams is consistent with the broader findings of this subsection and suggests that workforce capability development remains focused on specialist functions at most AIs.

Figure 9: Funding, Executive Education, and Workforce Training for PQC Readiness

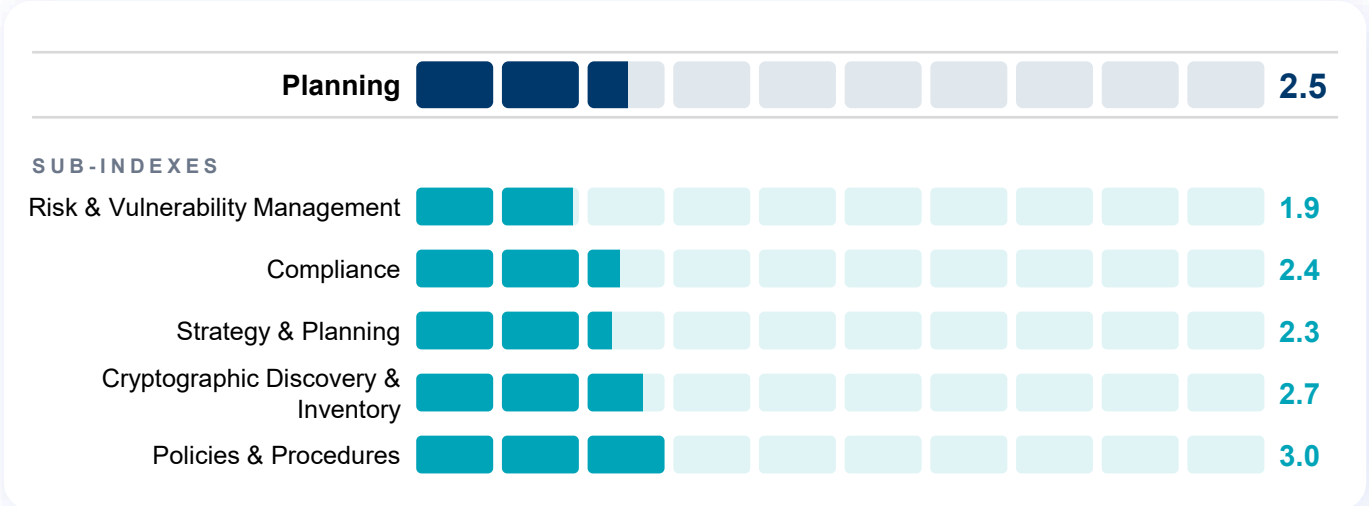


Source: HKMA survey, KPMG analysis

3.2.2 PQC Transition Planning

This subsection examines the extent to which AIs have moved from awareness to structured action in preparing for the post-quantum transition. It considers how AIs assess and manage quantum-related risks, align their cryptographic practices with recognised standards, design and implement transition strategies, build visibility into their cryptographic assets, and develop the policies needed to govern the transition. These areas are assessed across five sub-indices: Risk and Vulnerability Management, Compliance, Strategy and Planning, Cryptographic Discovery and Inventory, and Policies and Procedures. The overall Planning index score across the sector was 2.5/10. By institution type, the average Planning index score was 2.8/10 among retail banks and 2.4/10 among non-retail banks.

Figure 10: Planning – Index & Sub-index Scores



Source: HKMA survey, KPMG analysis

Risk and Vulnerability Management

The Risk and Vulnerability Management sub-index examines how institutions identify, monitor, and assess quantum-related exposure across their own assets, third-party relationships and ongoing operations.

When asked to characterise their overall level of quantum-related exposure, 66% of survey respondents indicated that they had not yet assessed their exposure. Among the remainder, 15% assessed their exposure as low and 13% as medium, while only 5% considered it to be high. These findings suggest that most AIs have not yet established a formal view of their quantum-related exposure. Among those that have undertaken an assessment, exposure was commonly assessed as low or medium rather than high.

The findings relating to risk quantification present a similar picture. Just over half of the survey respondents reported having no formal process to quantify, classify or validate quantum-related risks. A further group of 35% indicated that they identify such risks only informally, relying on ad-hoc assessments without consistent scoring or prioritisation, while a smaller proportion of 13% reported having a formal framework or automated system in place to quantify their exposure. These findings suggest that structured quantification of quantum-related risk is not yet widespread across the sector. While some institutions have begun to establish more formal assessment capabilities, many continue either to assess such risks informally or not at all. As a result, the integration of quantum-related risk into existing risk management processes remains limited.

The assessment of quantum-related vulnerabilities across both internal cryptographic assets and third-party relationships follows a comparable pattern, although third-party assessment appears to be less developed. For internal assets, 45% of survey respondents reported having no process for identifying or assessing vulnerabilities, while around 13% reported having a documented methodology or an approach embedded within enterprise risk processes. For third-party readiness, the proportion with no assessment process was higher at 60%, with only 8% reporting a structured evaluation framework for vendors' quantum readiness and cryptographic agility. In both areas, AIs that had undertaken some form of assessment most commonly reported informal or limited approaches rather than structured, enterprise-wide processes.

The integration of quantum-related risk into ongoing planning and decision-making remains limited across much of the sector. Half of the survey respondents reported that strategic planning, risk reporting and decision-making processes do not currently consider developments relating to quantum threats. A further 29% indicated that plans are updated only occasionally in response to major announcements, standards developments, or other external triggers, without regular monitoring processes in place. Around 17% reported that quantum-related developments are regularly monitored and incorporated into cryptographic transition planning, with migration timeline, policies, and vendor coordination updated in response to emerging developments. A smaller group of 5% indicated that quantum risk monitoring is embedded within ongoing risk reporting and decision-making processes, supported by activities such as impact modelling, vendor readiness tracking, and alignment with broader business risk and data protection objectives. Taken together, these findings suggest that the integration of quantum-related risk into institutional planning remains at an early stage, with only a small proportion of AIs reporting structured and ongoing monitoring practices.

Compliance

The Compliance sub-index examines whether institutions have begun to align their cryptographic practices with recognised post-quantum standards and authoritative guidance.

This is reflected in the findings on PQC algorithm selection where just over half of the survey respondents (53%) reported that no recognised standards or compliance requirements are considered in their PQC algorithm selection or validation. A further 24% indicated that basic validation of PQC algorithms is performed but without formal mapping to recognised standards or authoritative guidance. Around 23% of survey respondents reported having a formal process or automated system that ensures algorithm selection is explicitly aligned with applicable standards. These findings suggest that alignment with recognised standards remains limited across much of the sector, although a few AIs have begun to establish structured processes in this area.

The findings for the upkeep of cryptographic libraries and tooling present a more developed picture. While 46% of survey respondents reported that they have not established formal processes to update cryptographic implementation tools, libraries, or patterns, over a third indicated that they have processes in place to regularly

update cryptographic libraries, Application Programming Interfaces (APIs), coding guidance, and implementation templates. A further 18% reported that their cryptographic implementation tools are continuously monitored, tested, and updated through lifecycle-integrated processes. These findings suggest that processes for maintaining cryptographic libraries and implementation tools have been established at a few AIs, although formalised practices are not yet widespread across the sector.

Strategy and Planning

The Strategy and Planning sub-index covers the design and implementation of remediation strategies, migration timelines, resource allocation, and cryptographic upgrade frameworks.

A PQC remediation strategy, setting out how an AI will identify, prioritise, and replace vulnerable cryptographic systems with quantum-resistant alternatives, is a foundational element of any structured transition programme. Half of the survey respondents reported that no such strategy exists or has been initiated. A further 39% indicated that the need for a remediation strategy has been recognised and that a draft or partially developed strategy is in progress, although it has not yet been formally approved. Around 12% reported having a documented and approved remediation strategy in place, including a small proportion with detailed implementation plans, timelines, and assigned resources. These findings indicate that formal remediation planning remains at an early stage across much of the sector. However, a substantial proportion of AIs reported that strategy development activities are already underway.

Beyond the existence of a remediation strategy, the survey examined how AIs define and structure the practical plans needed to execute cryptographic upgrades. Half of the survey respondents reported having no structured plan in place, with actions described as sporadic and lacking systematic coordination. A further 30% indicated that cryptographic upgrades occur in an informal and reactive manner, typically during system transitions or in response to known issues. Around 20% of survey respondents reported having a structured planning process that accounts for technical dependencies, interoperability constraints, and critical path systems, including a small number that used advanced modelling tools and dependency mapping to coordinate across internal and external stakeholders. These findings indicate that structured planning for cryptographic upgrades has been established at a number of AIs, although most continue to rely on informal processes or have yet to develop coordinated upgrade plans.

Alongside the structure of these plans, AIs were asked how long they expect their PQC migration to take once initiated. Around 32% of survey respondents indicated that they have no migration plan or do not currently see a need for migration. Among those that provided an estimate, the most common expectation was 1 to 5 years, cited by 36% of survey respondents, followed by 5 to 10 years by 26% of AIs, while a smaller proportion of 5% anticipated a timeline of more than 10 years. The responses indicate a broad range of expectations across the sector, likely correlated to the size and organisational complexity of the institution.

The allocation of resources to support these plans and timelines remains limited and uneven across AIs. Around two thirds of survey respondents reported having no dedicated staff or tools allocated for PQC implementation or cryptographic transition work. A further 22% indicated

Figure 11: Expected Duration of PQC Migration Once Initiated

Note: Share of AIs reporting their expected duration of PQC migration once initiated. Percentages are calculated based on all AIs that responded to the question.

Source: HKMA survey, KPMG analysis

that resource needs have been documented but remain subject to reallocation due to competing priorities. Around 11% reported having dedicated teams and infrastructure specifically allocated and protected for cryptographic transition projects. The findings indicate that a small portion of survey respondents have started to allocate personnel and infrastructure to support PQC transition activities.

AIs were also asked about the extent to which PQC planning has extended beyond internal readiness activities to customer-facing considerations, specifically whether they have assessed customer reliance on cryptographic services and identified which customer segments or products may require PQC-related preparation or support. Over half of the surveyed AIs (59%) reported having no formal assessment of customer reliance, while a further 32% indicated that basic assessments are conducted but tend to focus on immediate needs without a thorough analysis of PQC-related implications. Around 9% reported having a structured assessment framework that evaluates customer reliance on cryptographic services, incorporating factors such as product dependencies and potential quantum-related risks. Formal assessment of customer reliance on cryptographic services remains limited across the sector. While a small number of AIs reported having structured assessment frameworks in place, most have yet to incorporate customer-facing considerations into their PQC planning activities.

Cryptographic Discovery and Inventory

The Cryptographic Discovery and Inventory sub-index assesses whether AIs have established foundational visibility into their cryptographic assets that effective planning requires. A comprehensive cryptographic inventory, sometimes referred to as a CBOM, provides the foundation for assessing exposure, prioritising remediation activities, and tracking transition progress.

The first step in building a cryptographic inventory is the identification and discovery of cryptographic assets across the AI's technology estate. Over a third of surveyed AIs (36%) reported having no formal process in place for identifying cryptographic assets, while 40% indicated that discovery is limited to manual inventories covering only known high-value systems without full coverage across all environments. Around 24% of survey respondents reported using automated discovery tools, though in most cases these are not yet universally applied across all environments. These findings suggest that while a majority of AIs have undertaken some form of cryptographic asset identification activity, the depth and breadth of coverage remain limited at most AIs.

The documentation and ongoing management of cryptographic inventories remains an area of limited maturity. Close to half of the surveyed AIs (45%) reported having no formal CBOM in place, with a further 29% relying on informal inventory tools such as spreadsheets, with limited attributes and manual update processes. The governance and maintenance of these inventories is similarly underdeveloped, with around 36% of survey respondents reporting no formal procedures for maintaining or updating their CBOM and a further 37% describing procedures that are informally or inconsistently applied. Nonetheless, around a quarter of survey respondents reported having documented procedures with defined roles and review cycles for CBOM governance, and a comparable proportion reported structured processes for updating inventories in response to system or dependency changes.

Policies and Procedures

The Policies and Procedures sub-index examines whether AIs have developed the operational governance frameworks needed to guide their PQC transition.

At the foundational level, 45% of survey respondents reported having no policies that mention or address cryptographic and quantum risks, while a further 41% indicated that these risks are briefly acknowledged within existing cybersecurity or risk management policies but without dedicated guidance or implementation detail. Around 14% of survey respondents reported having dedicated policy documents or a comprehensive policy framework covering risk recognition, impact assessment, and transition planning guidelines. These findings suggest that dedicated policies relating to quantum-related risk remain limited across much of the sector.

The review and maintenance of policies remain less developed. Just over half of the survey respondents, reported having no process for reviewing or updating quantum-related policies, while a further 34% indicated that manual reviews are conducted annually but with limited scope or documentation. Around 12% of AIs have structured review processes or automated policy maintenance integrated with threat intelligence. These findings suggest that policy maintenance practices remain at an early stage across much of the sector.

The management of cryptographic requirements across third-party relationships presents a more developed picture. Around 39% of survey respondents reported having well-defined cryptographic requirements for third-party components, services and communication channels, enforced through contracts, technical assessments, and integration standards. A further 5% reported implementing a comprehensive framework with continuous monitoring, periodic audits, and service-level governance. By contrast, around 28% reported no visibility into third-party cryptographic protections, and 28% indicated reliance on third-party assurances or default encryption settings. These findings suggest that a substantial proportion of AIs have begun to formalise their management of third-party cryptographic requirements, although practices remain uneven across the sector.

3.2.3 Pilots and Proof-of-Concept (PoC) Testing

This subsection examines the extent to which AIs have moved beyond planning into active experimentation with PQC solutions. It is assessed through a single sub-index, Cryptography Migration Testing, which covers how AIs design, execute, and validate PQC pilots and PoC exercises. The overall Pilot index and its sub-index score across the sector was 1.8/10. By institution type, the average Pilot index and its sub-index score was 2.0/10 among retail banks and 1.8/10 among non-retail banks.

Cryptography Migration Testing

The most direct indicator of where the sector stands on PQC experimentation is whether AIs have conducted or planned any PoC or live testing of PQC algorithms or cryptographic agility solutions. Of all survey respondents, 71% reported that they had neither conducted nor planned any such testing activity, while 29% indicated that they had. Among those that reported activity, around 39% described completed PoC exercises, with the remainder at various stages of planning or execution.

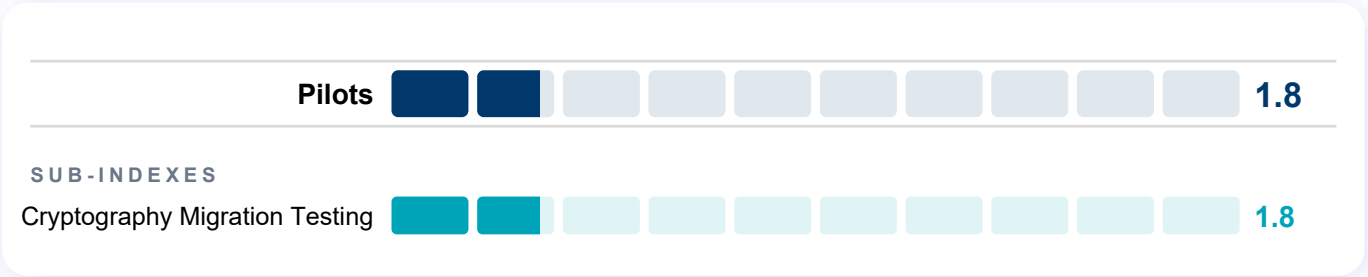
The following are examples of completed PoCs:

- **Websites, APIs, and Legal Document Signatures:** One AI completed a PoC to assess how post-quantum protections could be applied to selected websites, APIs and digital signing processes. The exercise confirmed that quantum-safe protections could be introduced for internet-facing services and that the approach could be scaled across relevant assets. The AI also explored how long-term legal document signatures could be strengthened using post-quantum techniques, while preserving the existing signing process as far as possible. In addition, the PoC compared post-quantum options with current cryptographic approaches to understand the potential impact on performance, processing time and storage requirements.

- **Cloud Key Management:** One AI completed a PoC to assess how cloud-based key management could support a future transition to PQC. The exercise reviewed whether existing key management services could accommodate future quantum-safe approaches, including changes to key types, rotation processes and integration with related systems. The PoC found that current cloud key management capabilities provide a useful foundation for crypto-agile operations, although full PQC support remains dependent on vendor roadmaps. The AI also identified practical integration patterns for future PQC-enabled keys without requiring major redesign of existing applications.

- **Internet-Facing System Using Content Delivery Network (CDN):** One AI completed a PoC to assess how post-quantum protections could be applied to a customer-facing internet system delivered through a content delivery network. The exercise tested whether

Figure 12: Pilots – Index & Sub-index Scores



Source: HKMA survey, KPMG analysis

secure connections between user devices and the CDN platform could support quantum-safe protections over public internet channels. The PoC confirmed that the CDN platform could support post-quantum connectivity for the tested scenario, while also highlighting that related back-end systems would need to meet modern connection requirements to achieve end-to-end protection. The findings provide a useful basis for planning future PQC adoption across customer-facing digital channels.

- **PQC Testing for Distributed Ledger Connectivity:** One AI completed a PoC to assess how PQC could be applied across distributed ledger connectivity, secure communication channels and cryptographic inventory activities. The exercise tested whether PQC could be introduced without materially affecting network performance. It also explored how different security approaches could be combined to strengthen secure communications.

- **Cryptographic Inventory:** One AI completed a PoC to deploy a tool across selected test environments to identify cryptographic assets and support the development of a cryptographic inventory. The PoC found that such tools can help improve visibility over cryptographic assets, although a complete inventory is likely to require a combination of automated tooling, manual review and vendor input.

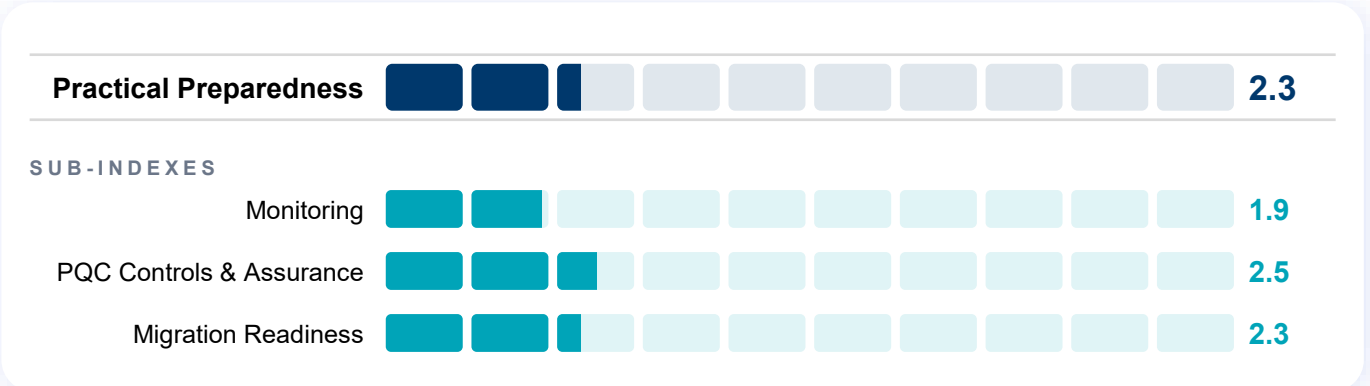
Beyond whether AIs have initiated pilot activity, the findings also examined how cryptographic and post-quantum solutions are tested and validated across their lifecycle. 26% of survey respondents indicated that testing is performed informally or only during deployment, with limited validation of functionality and minimal real-world workload simulation. Around 23% of AIs reported having a defined or fully integrated testing process, including structured validation within planned test cases and, in a small number of cases, continuous verification of performance, correctness, and resilience. These findings indicate that structured testing practices for PQC solutions have been established at a number of AIs, although such practices remain limited across much of the sector.

The rigour with which AIs validate their migration plans, fallback mechanisms, and recovery behaviour presents a less developed picture. Nearly three quarters of survey respondents reported performing no validation of PQC migration plans, fallback mechanisms, or cryptographic recovery behaviour. A further 16% indicated that basic test cases are created but do not represent real-world failure scenarios or meaningful system stress conditions. Around 11% reported structured testing that includes rollback paths, fallback scenarios, and resilience checks under defined cryptographic failure conditions. These findings suggest that validation of migration plans and recovery arrangements remains at an early stage across much of the sector.

3.2.4 Practical Preparedness

This subsection examines whether AIs have the technical infrastructure, controls, and operational capabilities needed to execute and sustain a PQC transition. It considers how AIs track transition progress, validate their cryptographic controls, and assess the readiness of their systems and architectures for post-quantum requirements. These areas are assessed across three sub-indices: Monitoring, PQC Controls & Assurance, and Migration Readiness. The overall Preparedness index score across the sector was 2.3/10. By institution type, the average Preparedness index score was 3.0/10 among retail banks and 2.1/10 among non-retail banks.

Figure 13: Practical Preparedness – Index & Sub-index Scores



Source: HKMA survey, KPMG analysis

Monitoring

The Monitoring sub-index covers how AIs track and report on transition progress and programme performance.

Over half of the surveyed AIs (58%) reported that progress on quantum readiness or cryptographic transition activities is not tracked, with no reporting mechanisms, metrics, or dashboards in place. A further 29% indicated that progress is monitored informally or through manual updates, with reporting limited to high-level summaries or project updates provided on request. Around 13% of survey respondents reported having defined metrics, milestones, and reporting processes, with regular updates provided to governance groups and progress monitored against migration plans and risk timelines. These findings suggest that structured monitoring and reporting of PQC transition activities remain limited across much of the sector.

AIs can consider establishing a set of metrics to track PQC transition progress and report it to management. Useful indicators fall into four areas:

- **Discovery coverage:** the percentage of applications, endpoints and third-party interfaces with a completed cryptographic inventory or CBOM, and the proportion of certificates and keys with a named owner.
- **Risk exposure:** the share of systems holding long-lived sensitive data that still rely solely on classical asymmetric algorithms, and remaining use of deprecated key sizes.
- **Migration progress:** the percentage of external TLS endpoints supporting hybrid key exchange, the proportion of PKI and code-signing infrastructure remediated, and the number of critical vendors with a published PQC roadmap.
- **Crypto agility:** the average time to rotate or replace an algorithm, the number of systems with hardcoded cryptographic implementations, and the proportion of systems where algorithms can be changed through configuration rather than code changes.

Reporting these metrics against an agreed target state, through existing technology risk and audit committee channels, gives AIs a clear view of progress, highlights concentration risk in third-party dependencies, and supports decisions on sequencing and investment.

PQC Controls and Assurance

The PQC Controls and Assurance sub-index examines whether deployed cryptographic controls are correctly implemented, validated, and resilient.

The design of data protection controls across different environments provides one indication of how AIs are preparing their control frameworks for post-quantum algorithms. Over a third of survey respondents (36%) reported having no defined strategy for protecting data across environments, with post-quantum considerations absent from the design of data protection controls. However, a larger group of 51% indicated that standard data protection controls are applied but do not incorporate quantum-related risks or consider future post-quantum algorithm requirements. Around 13% reported having a formal strategy that incorporates data classification rules and considerations for PQC migration.

A similar pattern was observed for the design of cryptographic controls for communication protocols. Close to half of the survey respondents (43%) reported that communication protocols are configured using default or legacy cryptographic settings with no consideration for PQC requirements, hybrid support, or future algorithm migration. A further 47% indicated that protocols use modern classical cryptography and that some PQC options may be explored, but without a structured design approach for agility or controlled algorithm transition. Around 9% reported that communication protocols are designed with defined agility requirements, supporting configurable algorithms, hybrid key exchange options, and controlled upgrade paths.

A comparable picture emerges in the validation of deployed cryptographic controls. Close to half of the survey respondents (45%) reported that informal and inconsistent validation or testing is performed on deployed cryptographic implementations. A further 35% indicated that manual configuration checks are performed on a limited number of systems. Around 21% of survey respondents reported having formal validation processes or automated continuous monitoring that reviews deployed controls for correctness, including algorithm selection, key sizes, protocol versions, and configuration settings. The findings indicate that formal validation of deployed cryptographic controls remains limited across much of the sector.

Fallback behaviour and supply chain vulnerabilities present a comparable picture. Close to half of the survey respondents reported performing no evaluation of fallback behaviour, downgrade risks, or supply chain-related cryptographic vulnerabilities. A further 29% indicated that fallback or downgrade risks are informally noted during vendor or system security reviews but without structured assessment or documentation. Around 26% of survey respondents reported having formal assessment processes or automated approaches integrated into vendor assurance and supply chain monitoring. These findings suggest that a number of AIs have established structured processes to assess fallback behaviour and supply chain-related cryptographic risks, although such practices are not yet widespread across the sector.

Migration Readiness

The Migration Readiness sub-index assesses whether AIs' systems and architectures are structurally prepared for post-quantum requirements.

The starting point for migration readiness is whether AIs have assessed their technical infrastructure for post-quantum security requirements. Around half of the survey respondents reported having conducted some form of assessment, with 40% indicating that high-level assessments are conducted for selected systems, focusing mainly on known cryptographic components, but with readiness for PQC reviewed informally or inconsistently tracked. Around 9% reported having a formal assessment framework or systematic approach that evaluates system and platform readiness, including factors such as cryptographic agility, hardware support, protocol compatibility, and upgrade constraints.

A closely related consideration is whether AIs have embedded cryptographic agility into their system architectures, specifically whether their systems are designed to allow cryptographic algorithms to be updated or replaced without requiring extensive changes to the underlying systems. Close to half of the survey respondents (46%) reported that no cryptographic agility requirements exist, while a further 39% indicated that some preliminary planning exists for a subset of critical systems, but that agility has not been formally defined or consistently integrated. Around 14% of survey respondents reported having formally defined and documented cryptographic agility requirements integrated into their architecture and software design processes.

The application of these requirements across operational delivery processes and key management practices reflects a comparable level of maturity. Close to half of the survey respondents (46%) reported no planning or requirements to support cryptographic upgrades or agility, while a further 42% described preliminary planning for a small number of critical systems without formal definition, timelines, or institution-wide applicability. Around 12% reported having formally defined agility procedures integrated into delivery processes, including, in a small number of cases, automation tools that validate cryptographic configurations and support seamless algorithm upgrades.

Across all four dimensions of the assessment, the findings present a consistent picture of a sector in which PQC readiness remains at an early stage for the majority of the survey respondents. Awareness-related foundations such as governance, funding, and workforce training have seen some initial activity, though dedicated structures remain the exception rather than the norm. Planning capabilities, including risk assessment, remediation strategy development, cryptographic inventory, and policy frameworks, are similarly nascent, with most survey respondents yet to move beyond informal or preliminary approaches. Pilot activity is concentrated among a minority of the sector, with around a quarter of survey respondents having conducted or planned some form of PoC testing. Practical preparedness, spanning progress monitoring, validation of deployed controls, and infrastructure assessment, also remains at an early stage across most of the sector.

At the same time, the findings consistently identify a small but recognisable cohort of AIs that have progressed further across multiple dimensions, having established formal governance arrangements, structured planning processes, active pilot programmes, and more mature operational practices. The gap between this group and the broader sector is significant, and closing it will require coordinated effort across institutions, industry stakeholders, and the HKMA. The following subsections examine the specific barriers that constrain this progress and the forms of support that AIs consider most valuable in addressing them.

3.2.5 Adoption Barriers in PQC

AIs were asked about the specific obstacles they face or anticipate across four domains, spanning risk assessment,

cryptographic inventory, roadmap development, and vendor and industry engagement. Unless otherwise stated, the figures reported below represent the share of AIs that ranked a given challenge among their top three most significant concerns.

Barriers to Risk Assessment

The challenge most frequently ranked among AIs' top three concerns in assessing quantum-related risks was the lack of established models, tools, or industry-standard frameworks to systematically quantify and evaluate quantum-related risks, cited by 73% of survey respondents. This was followed by dependencies on external stakeholders, with around 52% noting that risk assessments can only be completed with input from other parties, such as updates from vendors on their quantum preparations. The rapid evolution of the quantum computing landscape was cited by 47%, with AIs noting the difficulty of completing a comprehensive and sustainable risk assessment against a threat whose timeline and technical characteristics continue to develop. These findings are consistent with the limited risk quantification capabilities observed in Section 3.2.2 and indicate that AIs continue to face challenges in systematically assessing and evaluating quantum-related risks.

The challenge in risk assessment is exacerbated by the fact that AIs often lack system-level visibility over where asymmetric cryptography is used. Because legacy public-key algorithms are deeply embedded across internal, vendor and third-party systems, compliance and IT teams cannot reliably map the institution's true cryptographic footprint.

Barriers to Cryptographic Inventory

Creating a complete inventory of cryptographic assets emerges as a significant challenge for many AIs. The challenge most frequently ranked among AIs' top three was technical complexity, with 79% of survey respondents citing the difficulty of identifying and mapping cryptographic assets across complex IT environments and legacy infrastructure. This was followed by scale and volume, cited by 71% noting that the number of applications and systems involved makes a manual or tool-assisted inventory difficult to manage at an enterprise level. External dependencies were cited by around 60%, reflecting limited visibility into cryptographic assets

Figure 14: Adoption Challenges

Areas	Challenges	Survey Findings
Risk Assessment	Lack of methodology and frameworks	73%
	Dependencies on external stakeholders	52%
	Dynamic threat landscape	47%
Cryptographic Inventory	Technical complexity of IT environments	79%
	Scale and volume of application systems	71%
	External dependencies	60%
Roadmap Development	Legacy systems and technical debt	71%
	Strategic uncertainty	67%
	Enterprise architecture alignment	49%
Vendor & Industry Engagement	Dependencies on critical third parties	87%
	Vendor readiness and roadmaps	85%
	Unclear ecosystem for engagement	60%

Note: Figures represent the share of AIs that ranked each challenge among their top three most significant concerns. Percentages are calculated over all AIs that responded to the respective question.

Source: HKMA survey, KPMG analysis

embedded in third-party and commercial off-the-shelf software, where vendor-controlled information and black-box implementations restrict the completeness of any inventory exercise.

Barriers to Roadmap Development

Developing and implementing a formal PQC transition roadmap presents a distinct set of challenges. The barrier most frequently ranked among AIs' top three was legacy systems and technical debt, with 71% of survey respondents citing the difficulty of defining a realistic transition path for IT systems and infrastructure that cannot support PQC or cryptographic agility. This was closely followed by strategic uncertainty, cited by 67%, reflecting the difficulty of formulating and maintaining a roadmap with actionable milestones given the pace of change in PQC standards, marketplace offerings, and international frameworks. Enterprise architecture alignment was cited by 49%, with AIs noting the challenge of embedding evolving PQC standards and cryptographic agility requirements into existing IT governance, system development, and change management processes. The prominence of legacy systems as the leading barrier is consistent with the cryptographic inventory findings discussed above, where technical complexity and the difficulty of mapping assets across legacy environments were similarly identified as primary constraints.

The development of a PQC transition roadmap also depends on the external readiness of vendors, cloud providers, FMIs and common utility providers. In practice, AIs cannot develop credible migration plans in isolation, as many critical systems rely on third-party software, hosted platforms, managed services, shared infrastructure and externally operated connectivity arrangements. Without clear information on external parties' PQC timelines and supported algorithms, AIs may find it difficult to sequence their own remediation activities, assess implementation dependencies or determine whether interim risk mitigation measures are required.

Barriers to Vendor and Industry Engagement

The barriers relating to vendor and industry engagement attracted consistently high rankings across AIs, highlighting the importance of external coordination in supporting PQC transition efforts. The challenge most frequently ranked among AIs' top three was dependencies on critical third parties, cited by 87% of survey respondents, who noted the lack of a clear pathway or platform to discuss, plan, test, and implement PQC transition activities with common utility providers. This was closely followed by vendor readiness and roadmaps, cited by 85%, reflecting concerns that key technology providers lack clear PQC timelines or solutions, limiting the extent to which vendor engagements can yield actionable transition plans. Around 60% cited an unclear ecosystem for engagement, noting limited knowledge of which external groups or initiatives are most critical to engage with and how such engagements would support the PQC transition.

These dependencies are particularly significant because many cryptographic services used by AIs are embedded in infrastructure that sits outside their direct control. PQC readiness may depend on the capabilities and migration timelines of third-party platforms, network appliances, certificate authorities and certificate management providers, cloud services, hardware security modules (HSMs), payment infrastructure, and other shared utilities. If these external components do not support appropriate post-quantum algorithms, larger keys and certificates, hybrid modes, interoperability testing or coordinated cut-over arrangements, individual AIs may be unable to complete migration safely even where their internal systems are ready. Ecosystem coordination is therefore essential to align roadmaps and clarify dependencies across interconnected financial services infrastructure.

Overall, the findings across these barriers indicate that AIs face challenges across every stage of the PQC readiness journey. Methodological gaps and the absence of established frameworks constrain risk assessment. Technical complexity, scale, and limited third-party visibility impede cryptographic inventory efforts. Legacy infrastructure and strategic uncertainty complicate roadmap development. The maturity of the vendor landscape and the lack of structured coordination mechanisms further affect AIs' ability to plan and execute their transition activities. The consistency with which these challenges were identified across AIs suggests that many of the barriers are shared across the sector rather than confined to a small number of AIs.

3.2.6 Industry Support Needs

AIs were also asked about the forms of external support they consider most valuable in advancing their transition, and the degree to which they would engage with HKMA-facilitated initiatives. Unless otherwise stated, the figures reported below represent the share of AIs that ranked a given form of support among their top three priorities.

Forms of Support

The form of support most frequently ranked among AIs' top three priorities was clear supervisory expectations and timelines for PQC transition, cited by 87% of survey respondents. This was followed by practical guidance and whitepapers on how to approach the PQC transition, cited by around 77%, and industry forums and best-practice sharing, cited by around 48%.

The strong demand for supervisory clarity is consistent with the finding in Section 3.2.5 that strategic uncertainty is a leading barrier to roadmap development. In free-response elaborations, AIs described how clear supervisory expectations and timelines would support planning and vendor engagement, promote consistent readiness approaches across the Hong Kong banking sector, and facilitate implementation planning across multiple stakeholders. Several AIs noted that defined timelines would support internal planning, budgeting, and prioritisation, helping to align resource allocation and governance activities with PQC transition objectives. AIs also highlighted the role that regulatory signalling can play in supporting executive alignment and board-level buy-in, particularly where PQC initiatives compete with other strategic priorities for attention and resources.

On practical guidance, AIs emphasised the value of published materials that could help address gaps in methodology and risk planning. Specific areas identified included the application of PQC standards to cryptographic inventory development and roadmap preparation, as well as guidance to support risk assessment and migration planning activities. AIs also noted that authoritative guidance could encourage external vendors to develop and communicate their own PQC strategies, contributing to broader ecosystem readiness.

On industry forums, AIs described these as an important channel for supporting the sector's transition efforts. AIs highlighted the value of shared platforms that enable participants to exchange experiences, avoid common pitfalls, and converge on interoperable approaches. AIs also noted that such forums could help reduce the risk of fragmented implementation across institutions and vendors.

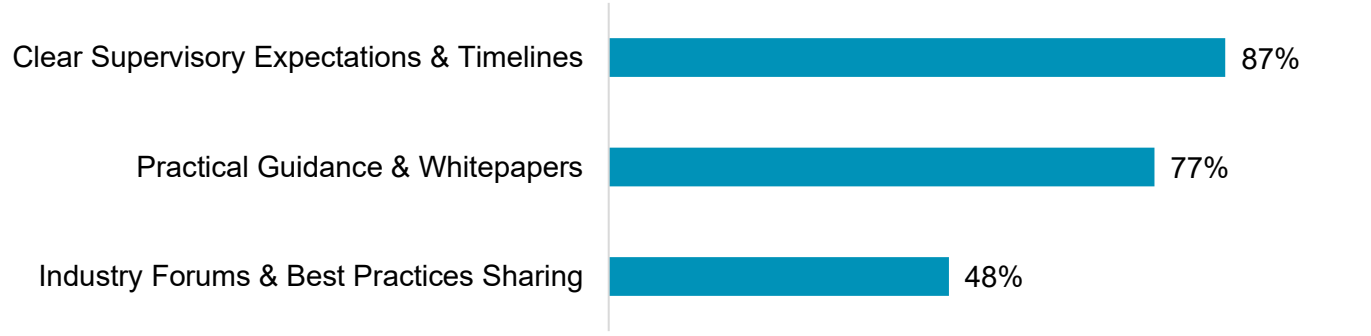
3.3 Conclusion

Sections 3.1 and 3.2 provide a comprehensive view of the current state of quantum computing and PQC readiness across Hong Kong's banking sector.

On quantum computing, the findings indicate that the sector has established broad awareness of the technology, although deeper institutional capability remains limited to a relatively small number of AIs. While some AIs have begun exploring quantum computing applications, active adoption remains constrained by technology maturity, uncertainty regarding commercial value, and a shortage of internal expertise. Overall, quantum computing continues to be regarded as a longer-term strategic consideration, with most AIs remaining in the early stages of exploration and capability building.

On PQC readiness, the assessment indicates that the sector remains at an early stage of preparing for the cryptographic transition expected to accompany advances in quantum computing. Across the four dimensions of the

Figure 15: Forms of Support Ranked as Most Valuable for PQC Transition



Note: Figures represent the share of AIs that ranked each form of support among their top three priorities. Percentages are calculated over all AIs that responded to the question.

Source: HKMA survey, KPMG analysis

assessment – Awareness, Planning, Pilots, and Practical Preparedness – the majority of AIs have yet to establish the formal structures, processes, and capabilities needed to support a sustained transition programme. At the same time, a small but identifiable cohort of AIs has established more developed capabilities across multiple dimensions, indicating that progress is already underway within parts of the sector.

The findings across both sections exhibit several common themes. Uncertainty surrounding quantum computing timelines, PQC standards, and regulatory expectations continues to constrain planning across the sector and influences AIs' investment decisions. Resource constraints, including limited funding and gaps in internal expertise, further affect AIs' ability to progress their transition efforts. AIs also identified the limited maturity of the vendor and industry ecosystem as a significant challenge, highlighting the importance of external coordination in supporting sector-wide readiness.

The support priorities identified by AIs align closely with these findings. Practical guidance, clear supervisory expectations, and structured industry forums were consistently identified as the forms of support regarded as most valuable. Together, these findings provide further context on the areas in which AIs consider external support to be most beneficial as they progress their quantum computing and PQC readiness efforts. The implications of these findings, together with the recommendations to support the sector's transition, are discussed in Section 4.

04 Way Forward

4.1 The Imperative of Acting Now

The transition to PQC will be unavoidable, complex and multi-year. For financial institutions, the question is therefore not whether to prepare, but how early and how orderly that preparation should begin. The scale of this transition reflects the deep and widespread use of cryptography across banking operations, including payments, customer channels, authentication, data protection, internal systems, and third-party connections. For large and complex organisations, the time required to identify vulnerable cryptography, assess dependencies, engage vendors, test replacement options and execute migration at scale is substantial.

Early preparation matters because the risk does not begin only when a CRQC becomes available. Sensitive information that is captured today may remain vulnerable to HNDL attacks if it needs to remain confidential for many years and is not protected by quantum-resistant cryptography in time. Delay may therefore increase both cyber risk exposure and the scale of the eventual remediation effort. It may also raise the risk of operational disruption if migration has to be carried out under tighter time constraints, or if critical systems, customer-facing services and external connections are not ready to transition in a coordinated manner.

The case for acting now is also being reinforced by developments in standards, procurement practices and regulation. International standards bodies and government authorities have already begun publishing PQC standards, migration guidance and implementation expectations. Over time, these developments are likely to influence product design, vendor roadmaps, and procurement considerations. In practice, this means that institutions may increasingly need to procure PQC-capable products, assess vendor readiness, and align with evolving external requirements in order to maintain interoperability, resilience and sound risk management.

Delaying action may also reduce flexibility and increase cost. As more organisations begin their transition, demand for specialist skills, testing capacity and implementation support is likely to rise. Institutions that defer planning may therefore face greater competition for scarce expertise, less time to address legacy technology constraints, and more compressed implementation timelines. By contrast, institutions that begin early are more likely to be able to assess their exposure in an orderly manner, prioritise the most critical areas, and build the capabilities needed to support a controlled transition over time.

Taken together, these considerations point to a clear conclusion: PQC readiness should be treated as a present-day strategic and operational priority. While the timing and form of the quantum threat remain uncertain, the lead time required for migration, the persistence of long-lived data risks, and the growing momentum of international standards and supervisory expectations all argue for early and deliberate preparation.

4.2 Transition Approach

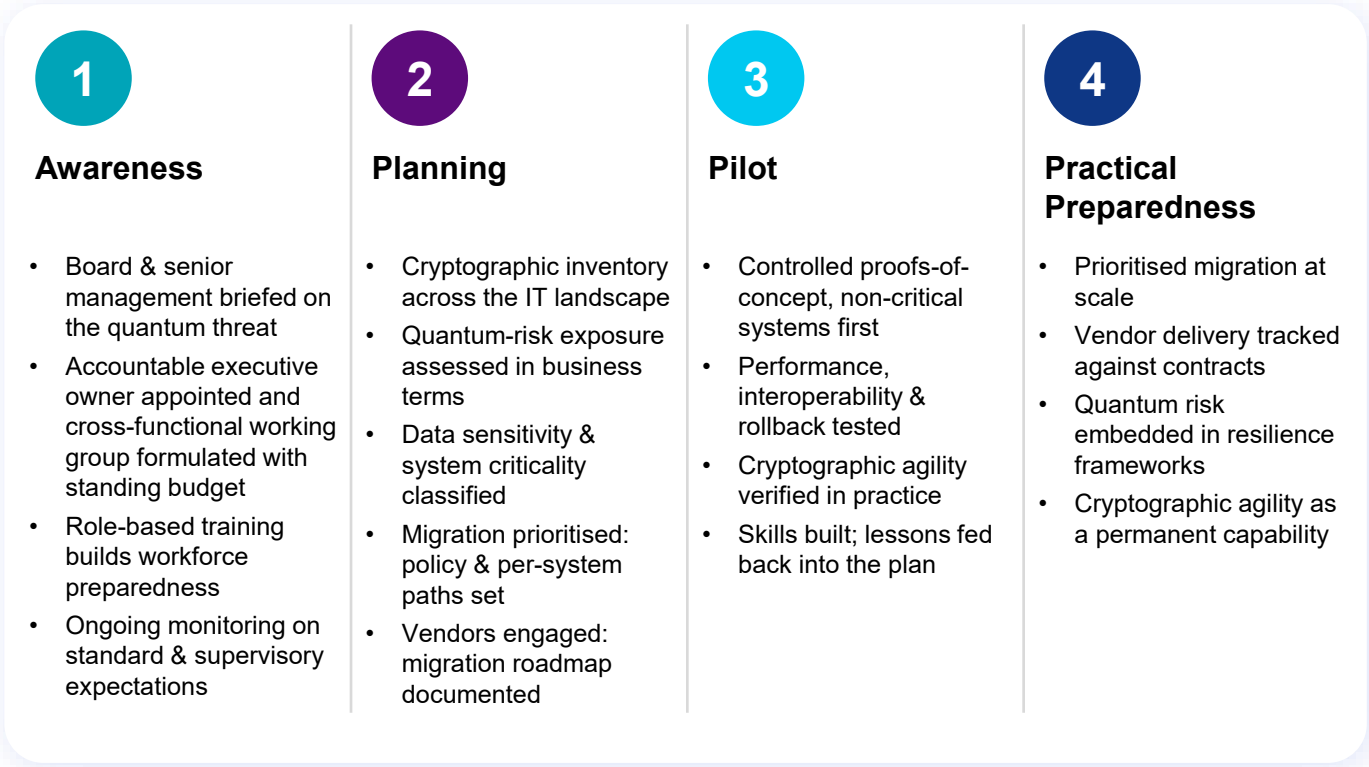
This section sets out a practical transition approach for AIs to prepare for the quantum era. The objective is not to prescribe a single implementation model, but to provide a structured approach, with practical options for implementation, that institutions can apply in a manner proportionate to their size, complexity and risk profile.

Two considerations should guide this work. First, PQC readiness is not a standalone technology exercise. It is a multi-year programme that cuts across governance, architecture, procurement, operations, legal arrangements and third-party dependencies. Secondly, the transition should not be treated as a one-off migration.

A growing body of international guidance[67,68,69,70,71] describes how large organisations should approach the transition to PQC. These frameworks converge on the same underlying journey: establish governance, discover what cryptography is in use, assess and prioritise, plan, implement, and monitor. The underlying objective is to build cryptographic agility, that is the ability to replace or update cryptographic algorithms, protocols and keys in an orderly manner as standards, threats and technologies evolve.

The transition approach is organised across four stages: from Awareness, Planning, Pilot, to Practical Preparedness. These stages should not be viewed as strictly linear. In practice, institutions are likely to move through them in overlapping and iterative waves, with lessons from early work informing subsequent activities.

Figure 16: PQC Migration Action Plan



Source: KPMG analysis

Stage 1: Awareness

Quantum readiness begins at the senior leadership level. The first stage is to establish ownership, understanding and institutional direction. Quantum-related risk should be recognised as a strategic issue requiring senior management attention, rather than being treated solely as a technical matter.

Key actions for AIs:

- **Engage the board and senior management:** Ensure that senior leadership understands the relevance of PQC to the institution's business, operations and risk profile, including the implications for long-lived sensitive data, critical systems and customer-facing services.

[67] Bank for International Settlements. 2025. *Quantum-readiness for the financial system: a roadmap*. (https://www.bis.org/publ/bppdf/bispap158.pdf).

[68] Post Quantum Cryptography Coalition. 2025. *Post-Quantum Cryptography (PQC) Migration Roadmap*. (https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf).

[69] NIST. 2024. *Transition to Post-Quantum Cryptography Standards*. (https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf).

[70] National Cyber Security Centre. 2025. *Timelines for migration to post-quantum cryptography*. (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines).

[71] Australian Signals Directorate. 2025. *Planning for post-quantum cryptography*. (https://www.cyber.gov.au/sites/default/files/2025-09/Planning%20for%20post-quantum%20cryptography%20%28September%202025%29.pdf).

- **Establish ownership and governance:** Identify an accountable executive sponsor and a cross-functional governance structure covering technology, cybersecurity, risk, legal, procurement, operations and relevant business units.
- **Build workforce capability:** Develop role-based training and awareness programmes so that relevant functions understand their part in the transition, including first, second- and third-line responsibilities.
- **Maintain horizon scanning:** Put in place a standing process to monitor developments in PQC standards, migration guidance, supervisory expectations, vendor roadmaps and international timelines. Awareness must be made continuous.

Stage 2: Planning

The second stage is to translate awareness into a structured transition plan. AIs will need sufficient visibility over their cryptographic landscape, dependencies and risk exposures before they can prioritise migration activity effectively.

Key actions for AIs:

- **Develop a cryptographic inventory (CBOM):** Build and maintain a reliable inventory of the cryptographic assets including algorithms, libraries, protocols, certificates, keys, third-party components and dependencies. This should be treated as a living record with a named owner rather than a one-off exercise.
- **Assess quantum-related exposure:** Identify where quantum-vulnerable cryptography is used across critical systems, customer channels, payment and settlement flows, interbank connections, and systems supporting regulatory, legal or contractual obligations.
- **Assess data sensitivity and system criticality:** Prioritise areas where confidentiality needs to endure for many years, and where operational disruption would be difficult to tolerate.
- **Set migration priorities:** Use the above assessments to establish a risk-based sequence for migration, focusing first on the areas with the greatest combination of exposure, long-lived sensitivity and operational importance.
- **Define policy and architectural principles:** Determine target standards, approach to hybrid cryptography where relevant, and requirements for cryptographic agility in future architecture and procurement decisions.
- **Decide the migration approach for each system:** Determine whether each relevant system should be upgraded, replaced, isolated, retired, or subject to time-bound risk acceptance, taking into account dependencies, sequencing constraints and funding implications.
- **Engage vendors and third parties early:** Request PQC roadmaps from critical providers, assess external dependencies, and incorporate quantum-readiness expectations into procurement and contract renewal processes.
- **Develop a multi-year migration roadmap:** Consolidate the AI's priorities, migration paths, dependencies, resource requirements and vendor commitments into a documented roadmap with milestones, responsibilities and governance reporting.

Stage 3: Pilot

The third stage is to move from planning to controlled experimentation. Pilots and PoC exercises help institutions test assumptions, build practical capability and identify interoperability or performance issues before broader implementation begins.

Key actions for AIs:

- **Select pilot use cases deliberately:** Start with lower-risk environments, but include representative systems and at least some externally connected use cases where interoperability can be tested.
- **Define clear testing objectives:** Pilots should address specific implementation questions, such as compatibility, latency, certificate handling, key management, rollback, vendor support and operational resilience. Pilots should confirm that systems can switch algorithms and roll back safely under realistic conditions.
- **Test in controlled environments:** Conduct trials in test or limited-production settings to assess the operational implications of PQC and hybrid implementations before wider rollout.

- **Capture lessons and standardise playbooks:** Document pilot outcomes, integration patterns, fallback procedures and testing approaches so that lessons can be reused across future migration waves.

Stage 4: Practical Preparedness

The final stage is to establish the operational foundation for migration at scale. This includes the controls, processes and programme discipline needed to execute the transition over time and sustain readiness as part of BAU operations.

Key actions for AIs:

- **Run the migration as a structured programme:** Track delivery against priorities, milestones and dependencies, with regular reporting to governance forums.
- **Strengthen trust infrastructure:** Prepare the AI's broader cryptographic trust architecture, including certificate and key lifecycle, to support future migration activity at scale.
- **Hold vendors to schedule:** The AI should manage material providers against their commitments. This may include tracking delivery against contractual milestones, maintaining readiness scorecards, and escalating where a supplier's delay threatens the AI's own readiness, including exercising exit options where needed.
- **Coordinate externally:** Work with counterparties, FMIs and other connected parties to support interoperability, sequencing and cut-over planning.
- **Maintain assurance over migrated systems:** Validate implementations, detect fallback to legacy cryptography, test rollback arrangements and maintain oversight of residual risks.
- **Monitor systems subject to time-bound risk acceptance:** For systems that are not yet migrated and are subject to time-bound risk acceptance, periodically reassess the residual risk, review the continued effectiveness of mitigating measures, and confirm that the rationale for deferred migration remains valid.
- **Embed PQC readiness into BAU processes:** Integrate quantum-related considerations into existing frameworks such as technology risk management, operational resilience, third-party risk management, internal audit and compliance monitoring.

4.3 Strategic Recommendations

While Section 4.2 sets out a practical, stage-based approach for AIs to prepare for the transition to PQC, this section highlights a set of cross-cutting recommendations to support implementation across the institution. These recommendations are intended to help AIs carry out the transition in a way that is sustainable, risk-based and aligned with existing governance and control frameworks.

The key message is that PQC readiness should not be treated as a narrow technology upgrade. It is an enterprise-wide transition that will require sustained coordination across governance, technology, cybersecurity, procurement, business functions, and risk and compliance. The recommendations below therefore focus on the institutional disciplines that will matter most over the course of a multi-year migration.

Table 2: PQC Migration Strategic Recommendations

Recommendation	Lead Function	Key actions
Govern quantum risk as an enterprise risk	Board & senior management	• Treat quantum-related risk as an enterprise risk and consider it within existing risk appetite and governance frameworks • Secure multi-year funding spanning budget cycles and leadership tenures • Require readiness reporting on inventory completeness, migration paths, vendor readiness
Build for cryptographic agility	Technology leadership	• Embed cryptographic agility in architecture standards, and prohibit hard-coded cryptography • Modernise foundational capabilities, including transport security, key management and certificate lifecycle management • Plan for the possibility of accelerated transition timelines, including by identifying interim safeguards, priority systems, and decision triggers for escalation
Identify and prioritise the cryptographic exposure	Security function	• Own the cryptographic inventory (CBOM) and the risk-based prioritisation • Build HNDL into threat models • Use certified, standards-compliant implementations and avoid bespoke cryptography • Own assurance including interoperability, rollback and fallback-detection testing
Hold the vendor base accountable	Technology & procurement	• Require post-quantum roadmaps from critical providers • Make quantum-readiness clauses standard in technology procurement • Treat cryptographic transparency as a selection criterion
Prepare the business, customers and counterparties	Business lines	• Assess affected products, services and obligations and how failures could affect customers • Prepare the customer-facing infrastructure, including channels, payment and settlement systems, and client authentication mechanisms • Coordinate cut-over with counterparties • Consider how the AI's transition approach should be communicated to relevant external stakeholders
Use and strengthen existing frameworks	Risk & compliance	• Extend existing frameworks, such as resilience, third-party risk, change governance to include quantum risks • Maintain a regulatory horizon scan across all jurisdictions of operation • Plan to the most demanding applicable timeline for group-wide programmes • Keep the migration auditable, including documenting prioritisation, residual risk, vendor reliance

Source: KPMG analysis

Govern quantum risk as an enterprise risk

Quantum-related risk should be treated as an enterprise risk, rather than a stand-alone information technology issue. Boards and senior management should ensure that the institution has clear ownership, appropriate governance, and a risk-based approach to decision-making. In practice, this means understanding where the institution's most material exposures lie, how they could affect business operations and customer outcomes, and what level of risk the institution is prepared to tolerate during the transition period.

Because the transition is likely to span multiple budget cycles and leadership tenures, governance arrangements should be durable rather than project-based. Senior management should require regular reporting on progress, grounded in a small number of practical indicators, such as the completeness of the cryptographic inventory, the proportion of critical systems with an agreed migration approach, and the readiness of material third parties.

Start today

Identify an accountable executive owner and establish quantum risk as a standing item within relevant governance forums.

Pitfall to avoid

Treating timeline uncertainty as a reason to defer action, or allowing accountability to remain unclear across functions.

Build for cryptographic agility

The strategic objective of the transition should not be limited to replacing one set of algorithms with another. AIs should use the transition to strengthen their ability to update cryptographic algorithms, protocols and keys in an orderly and repeatable manner over time. This is the essence of cryptographic agility.

Technology leadership should therefore ensure that cryptographic agility is built into architecture standards, system design principles, and procurement expectations. Institutions should avoid hard-coded cryptographic dependencies in internally developed systems and should modernise foundational capabilities such as certificate lifecycle management, key management and cryptographic configuration management. These investments support not only PQC readiness, but also broader technology resilience and maintainability.

Start today

Review architecture and engineering standards to identify where cryptographic agility should be made an explicit requirement.

Pitfall to avoid

Treating PQC migration as a simple drop-in algorithm replacement, without addressing architectural constraints, legacy design choices or operational dependencies.

Identify and prioritise the cryptographic exposure

Not all systems and data will need to be addressed at the same pace. AIs should prioritise their transition based on a combination of factors, including where quantum-vulnerable cryptography is used, how sensitive the protected data is, how long confidentiality needs to endure, and how critical the relevant systems are to operations, customer services and regulatory obligations. This requires a sufficiently robust cryptographic inventory and a practical understanding of where the institution's most important exposures lie. The security function should play a central role in establishing this visibility and translating it into a prioritised migration view.

In practice, this prioritisation should take account of factors such as the sensitivity and confidentiality lifetime of the data involved, the criticality of the relevant systems, the potential impact on customers or market operations, dependencies on third parties and connected infrastructures, vendor readiness, and the complexity of remediation. HNDL should be incorporated into the AI's threat modelling and data protection considerations, especially for information that may remain sensitive for many years.

Implementation should rest on certified, standards-compliant cryptographic modules and established libraries wherever possible. The security function should not accept developing or customising cryptographic implementations in-house. As the transition progresses, institutions should also ensure that assurance activities cover interoperability, rollback arrangements and detection of fallback to legacy cryptography.

Start today

Begin by identifying the data and systems for which long-term confidentiality or continued cryptographic integrity is most important.

Pitfall to avoid

Relying solely on automated discovery tools or assuming that all exposures are equally urgent.

Hold the vendor base accountable

For many AIs, a significant share of the technology landscape is vendor-provided or externally dependent. This means that an institution's effective readiness will depend not only on its own planning, but also on the readiness of key suppliers, cloud providers, software vendors, HSM providers, certificate-related services, FMIs and common utilities.

Technology and procurement functions should therefore engage critical third parties early and systematically. Institutions should request PQC roadmaps from material providers, assess external dependencies as part of transition planning, and incorporate quantum-readiness expectations into procurement processes, contract renewals and ongoing vendor oversight. Cryptographic transparency should increasingly be treated as a relevant factor in supplier selection and supplier risk assessment.

Start today

Add quantum-readiness questions and roadmap expectations into discussions with critical vendors and, where appropriate, into new procurement and renewal processes.

Pitfall to avoid

Assuming that vendor readiness will emerge in time without structured engagement, or treating third-party dependence as a later-stage issue.

Prepare the business, customers and counterparties

PQC readiness is not only a technical matter. It also has implications for products, services, customer channels, contractual commitments and external connectivity. Business lines should therefore understand which customer-facing services and business processes depend on vulnerable cryptography, and where failure, delay or incompatibility could affect customers, counterparties or market participation.

This is particularly relevant for services that depend on secure digital channels, client authentication, digital signatures, payment and settlement processes, and connectivity with external parties. The transition will need to be planned in a way that supports continuity of service and minimises customer and market disruption. Where relevant, institutions should also consider how their transition approach will be communicated to customers, counterparties and other stakeholders.

Start today

Identify business services and customer journeys that depend most heavily on cryptographic trust, external interoperability or long-lived digital assurance.

Pitfall to avoid

Treating the transition as an internal infrastructure exercise only, without considering customer impact, contractual implications or external coordination needs.

Use and strengthen existing frameworks

AIs should, where possible, carry the transition through existing governance, risk and control frameworks rather than creating entirely separate structures. Quantum-related considerations can often be integrated into existing arrangements for technology risk management, cyber resilience, third-party risk management, change governance, operational resilience, internal audit and compliance monitoring.

For AIs in Hong Kong, this means that the transition should be considered alongside existing supervisory guidance and expectations such as technology risk management under the HKMA's Supervisory Policy Manual (TM-G-1), the Cyber Resilience Assessment Framework (C-RAF), and operational resilience planning under OR-2, rather than being treated as a disconnected workstream. Compliance functions should also maintain a horizon scan of relevant developments across jurisdictions, recognising that standards, regulatory

expectations and migration timelines are evolving at different speeds. Institutions operating across multiple jurisdictions may need to plan with reference to the most demanding applicable expectations.

The transition should also be auditable. Decisions relating to prioritisation, residual risk, vendor dependence and implementation choices should be documented clearly enough to support later internal review, assurance and supervisory engagement.

Start today

Add quantum-related considerations to existing risk reviews, third-party risk assessments, resilience planning exercises or compliance horizon scanning activities.

Pitfall to avoid

Building duplicative governance and control processes when the transition can be integrated into existing frameworks more efficiently.

Taken together, these recommendations point to a clear strategic approach. AIs should govern quantum-related risk at the enterprise level, build cryptographic agility into future architecture, prioritise based on exposure and long-term sensitivity, engage vendors and external dependencies early, prepare business-facing services alongside technology components, and embed the transition within existing governance and control frameworks.

These are not one-off measures. They are the institutional disciplines that will determine whether the transition can be carried out in an orderly, risk-based and sustainable way over the years ahead.

4.4 Support from the HKMA

The HKMA recognises the importance of advancing quantum computing and strengthening PQC readiness across Hong Kong's banking sector. It also acknowledges the practical barriers faced by AIs and will continue to support the sector in addressing these challenges in an orderly and coordinated manner.

The HKMA will continue to support the banking sector's transition to PQC, with the aim of achieving full sectoral readiness by 2030 through practical guidance, training and workshops, industry engagement, and collaboration with academic and industry partners. These efforts are intended to provide clarity, translate guidance into actionable tools, create practical channels for industry coordination, and help AIs turn awareness into practical action. Given the interconnected nature of the banking sector, coordinated readiness and industry-wide collaboration will be important to maintaining the resilience and trust on which the banking system as a whole depends.

PQC toolkit

As discussed earlier in this paper, AIs face practical challenges in translating PQC readiness from a strategic objective into an executable transition plan. These challenges include establishing a reliable view of cryptographic assets, assessing quantum-related risks in the absence of mature methodologies, prioritising systems for migration, and embedding cryptographic agility into future architecture. The transition approach above sets out the steps AIs can take to address these issues, but a common practical reference point would help promote consistency and reduce duplicated effort across the sector.

To support the industry, the HKMA will work with academic and industry partners to co-develop a PQC toolkit, with the aim of helping AIs identify priorities for transition planning and providing reference architecture to support greater cryptographic agility.

Training and workshops

The barriers to PQC transition are not limited to the availability of standards or technology solutions. AIs also face practical capability gaps in understanding quantum-related risks, developing cryptographic inventories, prioritising migration activities, embedding cryptographic agility, and engaging vendors and external stakeholders. Apart from a common reference point in the PQC toolkit, effective implementation will also require AIs to build the necessary knowledge, confidence and practical capabilities across the organisation.

To support this capability-building effort, the HKMA will organise training and workshops for AIs on quantum computing and PQC readiness. These sessions will provide a structured platform for AIs to deepen their understanding of the quantum threat, exchange practical experience, and build a more consistent approach to PQC transition across the banking sector.

The HKMA has already conducted training sessions and workshops on quantum computing and PQC readiness, and will continue to expand these efforts to support AIs. These activities are intended to address both strategic and implementation needs. At the senior level, they may cover the implications of quantum computing for banking, the urgency of early preparation, and governance expectations. At the working level, the sessions may focus on practical topics such as cryptographic inventory development, quantum risk assessment, cryptographic agility, vendor engagement and migration assurance. They may also include scenario-based discussions and peer-sharing sessions to help AIs learn from emerging practices and align on interoperable approaches. Through these activities, the HKMA aims to strengthen sector-wide capability, reduce fragmentation in implementation, and support AIs in adopting the action plan and strategic recommendations mentioned earlier.

Industry collaboration and engagement

Many AIs also recognise that PQC transition depends on effective coordination with vendors, FMIs, common utility providers, counterparties and other external stakeholders. These dependencies create practical barriers: AIs often need vendor input to assess quantum-related risks, have limited visibility into cryptography embedded in third-party and commercial off-the-shelf software, and cannot finalise migration sequencing or interoperability testing without clearer vendor roadmaps and alignment with connected parties.

To help address these challenges, the HKMA will support the industry by hosting and facilitating industry engagement events and forums that bring together AIs, technology vendors, FMIs, academic partners and other relevant stakeholders. These platforms will provide opportunities for participants to exchange practical experience, discuss common implementation challenges, foster partnerships, and expand professional networks across the quantum computing and PQC ecosystem. They will also help promote greater alignment on sequencing, interoperability considerations and emerging good practices, thereby supporting a more coordinated and consistent sector-wide transition.

These engagement opportunities may be delivered through existing and future HKMA-led platforms and industry events, including FiNETech events, technical sharing sessions and other focused forums. Through these channels, the HKMA aims to encourage dialogue between demand-side institutions and solution providers, support collaboration on pilot initiatives, and help the banking sector build the partnerships needed to progress PQC readiness collectively.

4.5 Conclusion

Quantum computing has the potential to unlock significant advances for the financial services industry. At the same time, it poses a potentially significant risk to the cryptographic foundations that protect customer data, digital transactions, payment systems and FMI. Addressing this risk through PQC will be a multi-year undertaking. AIs should therefore begin preparing now, while there is still time to build the necessary visibility, capability and cryptographic agility to manage the transition in a controlled and risk-based manner.

Figure 17: Practical Steps to Advance AIs' PQC Readiness

Source: KPMG analysis

Against this backdrop, the immediate actions outlined below warrant early attention. They are practical steps that AIs of different sizes can begin now, generally without significant expenditure, and can help reduce the lead time required to achieve PQC readiness.

Quantum readiness also has a collective dimension. The resilience of the financial system will depend not only on the preparedness of individual institutions, but also on the migration of interconnected infrastructure, such as payment systems, settlement platforms and correspondent networks. This will require coordination of timelines, technical choices and interoperability arrangements across the wider ecosystem.

The HKMA will continue to monitor international standards and supervisory developments, engage with the industry on quantum readiness, and consider further guidance as the landscape evolves. The transition to PQC will span a number of years and require sustained collaboration between regulators, financial institutions, and technology providers. By acting early and in an orderly manner, building awareness, strengthening planning, testing in a controlled way, and embedding readiness into BAU processes, AIs in Hong Kong will be better placed to safeguard resilience, customer trust and long-term security in the quantum era.

05 Appendix

5.1 Technical Appendix

Quantum Superposition and Entanglement

Superposition is a quantum mechanical effect that lets something exist in two (or more) states at the same time. A common analogy is a spinning coin: while not yet observed as heads or tails it could be considered to be in both states at the same time. This is an analogy, which helps to convey the idea that a quantum system can represent multiple possible states simultaneously. This means a quantum computer is capable of doing calculations on multiple outcomes at the same time. This property allows quantum computers to potentially speed up tasks where one would need to search many billions of answers to find the right one.

Entanglement is a quantum mechanical effect in which two or more quantum systems become correlated in a way that cannot be described independently. Using the coin analogy, entanglement may be thought of as the outcome of one coin flip determining the other. For example, the coins may be connected in such a way that if one of the coins lands on heads then the other coin must land on tails. This is a simplified illustration, but it conveys the concept that entangled systems can exhibit connections across a system, that are stronger than those seen in classical systems.

Superposition and entanglement are among the key properties that allow quantum algorithms to behave differently from classical algorithms. Quantum operations performed on qubits in superposition can be thought of as being performed on many distinct states, at once. Entanglement allows quantum operations to manipulate all possible outcomes to make a specific desired outcome probabilistically more likely. Quantum computers may perform certain mathematical operations faster or more accurately than classical computation, although this advantage is problem-specific rather than for every case.

Additional Financial Use Cases

There are many quantum computing use cases in the financial sector, which can be broadly categorised into three problem domains: optimisation, simulation and machine learning. Different quantum approaches can be used to solve problems within these use cases in a variety of ways. Use cases with several approaches will appear in multiple domains in the figure below.[72]

Figure 18.1: Potential Financial Use Cases

Optimisation	Simulation	Machine Learning
Portfolio Optimisation	Asset and Derivative Pricing	Asset and Derivative Pricing
Hedging	Risk Analysis	Fraud Detection
Swap Netting	Netting Requirements	Predicting Market Volatility
Arbitrage	CDOs Management	Risk Clustering
Credit Scoring	Economic Capital Requirements	Credit Scoring
Crises Prediction	Crises Prediction	Crises Prediction
Settlement Optimisation	Stress Testing for Banks and Markets	Natural Language Processing

Source: KPMG analysis

[72] Manqoba Q. Hlatshwayo, Manav Babel, Dalila Islas-Sanchez, et al. 2026. *A Technical Review of Quantum Computing Use Cases for Finance and Economics.* Quantum Reports (MDPI). (https://www.mdpi.com/2624-960X/8/1/26).

Figure 18.2: Potential Financial Use Cases (Cont.)

Optimisation	Simulation	Machine Learning
Portfolio Diversification	Stochastic Differential Equation Solving for Financial Markets	Time Series Analysis
Nash Equilibrium	Macroeconomics	Generative Models

Source: KPMG analysis

Quantum Computer Properties

In simple terms, three key properties are often compared across quantum computing platforms: number of qubits, two-qubit gate error rates and two-qubit gate operation speed.

- **Number of Qubits:** Qubits are the fundamental way to represent information on a quantum computer. The number of qubits defines the scale of the problem that can be processed on the quantum computer. Without enough qubits, large-scale calculations cannot be run on the device.
- **Two-Qubit Gate Error Rates:** Gates are the operations used to manipulate information in the quantum computer. Each operation introduces some probability of error. Lower error rates make it possible to run longer and more complex algorithms. If error rates are too high, the results of large computations become unreliable.
- **Two-Qubit Gate Operation Speed:** Gate speed measures how quickly operations can be performed. Faster gate operations can shorten the runtime of quantum algorithms, so that large-scale calculations may be completed within a practical timeframe.

One-qubit error rates and gate speeds are also important, but they are generally less constraining than the two-qubit equivalents. As a result, two-qubit gates are often treated as a more significant bottleneck for large-scale quantum computation.

Key Quantum Algorithms

Quantum computers do not use the same algorithms as standard computers. As a completely new type of computation, new algorithms have been created to specifically leverage the capabilities of quantum computers. While the list of quantum algorithms is continuing to grow, a short list of important algorithms can be seen below.

Table 3: Example of Quantum Algorithms

Algorithm	Release Year	Description
Universal Quantum Simulation[73]	1996	This quantum algorithm simulates quantum mechanical processes far more efficiently than classical computers. Applications in simulating complex financial markets including pricing multi-asset derivatives.
Shor's Algorithm[74]	1997	This quantum algorithm could be used to break widely used encryption methods. Applications in breaking RSA and elliptic curve cryptography.
Harrow-Hassidim-Lloyd (HHL) Algorithm[75]	2009	This quantum algorithm can offer asymptotic advantages for certain structured linear systems under specific assumptions. Applications in understanding the price evolution of derivatives and market pattern recognition.
QAOA[76]	2014	This quantum algorithm was found to be better than known classical optimisation algorithms at the time for certain hard optimisation tasks. Applications in financial asset pricing and risk management.

Source: KPMG analysis

[73] Lloyd. 1996. *Universal Quantum Simulators*. (https://www.science.org/doi/10.1126/science.273.5278.1073).
[74] P W Shor. 1997. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing. (https://doi.org/10.1137/S0097539795293172).
[75] Harrow et al. 2009. *Quantum algorithm for solving linear systems of equations*. (https://arxiv.org/abs/0811.3171).
[76] Farhi et al. 2014. *A Quantum Approximate Optimization Algorithm*. (https://arxiv.org/abs/1411.4028).

Even at the current scale, quantum computers have demonstrated performance advantages over classical supercomputers on certain narrowly defined tasks. In 2019, Google published a paper claiming that a specific quantum computation would take an infeasibly long time on then-available classical supercomputing approaches.[77] In 2026, Q-CTRL and IBM also released a pre-print reporting a significant performance advantage in a particular quantum simulation task.[78]

Cryptographic Algorithms

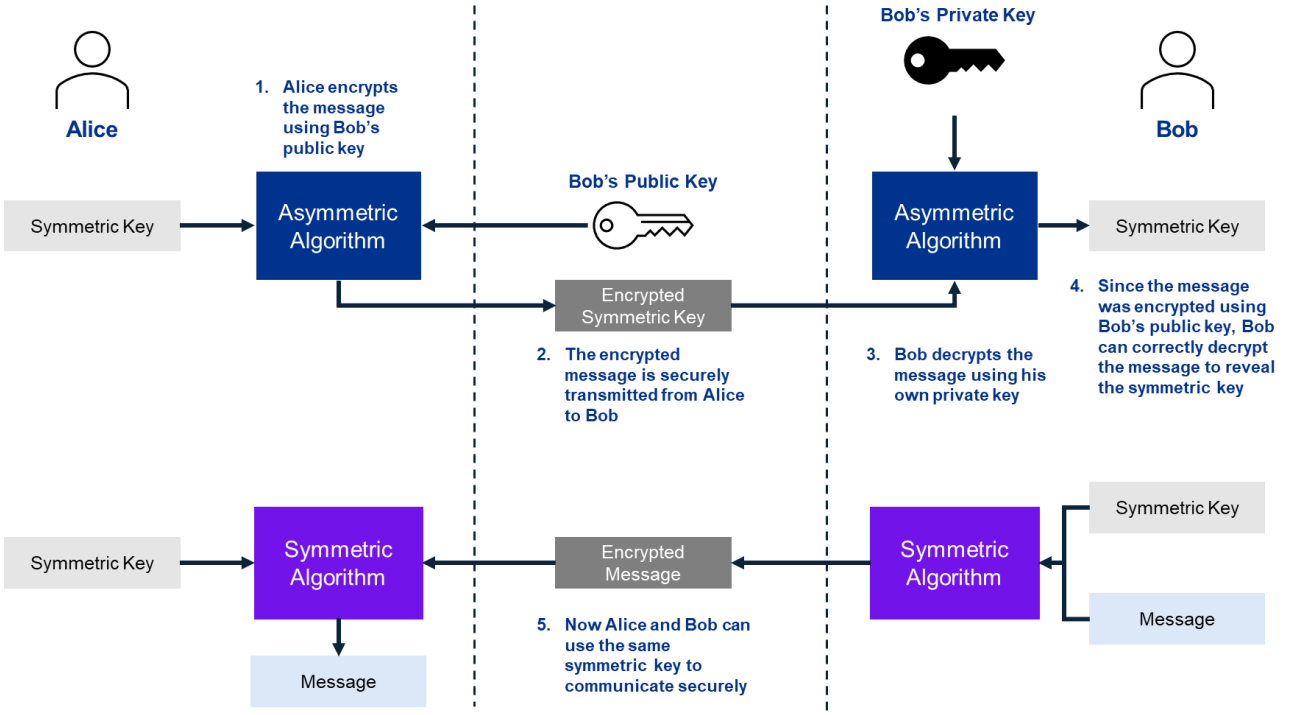
Asymmetric algorithms are generally more computationally intensive than symmetric algorithms. However, symmetric algorithms alone do not solve the problem of how two parties can securely establish a shared secret in the first place. Asymmetric cryptography is therefore often used to establish or encapsulate a shared key, which can then be used for faster symmetric encryption of subsequent communication.[79] KEMs are a class of asymmetric algorithms designed for this purpose. In simplified terms, they allow two parties to derive or exchange a shared secret over an insecure channel.

Digital signature algorithms are another type of asymmetric cryptographic primitive. The sender uses a private key to generate a signature over a message, and the recipient uses the corresponding public key to verify the signature. Digital signatures are commonly used together with hash functions to support authentication and integrity.[81]

A hash function provides an output of a fixed length, irrespective of the input. A hash will always provide the same output for the same input and is not reversible. In operation, a hash is generated for the message being sent, which is then encrypted using the sender's private key. Any intentional or unintentional changes to the message will result in the hash being changed. The recipient then generates their own hash of the message or digital document and decrypts the sender's hash using the sender's public key. If the two hash values match, then the sender is authenticated and the recipient can be sure that the message has not been modified.

Figure 20 shows how digital signatures and hash functions work together with asymmetric algorithms to provide security.

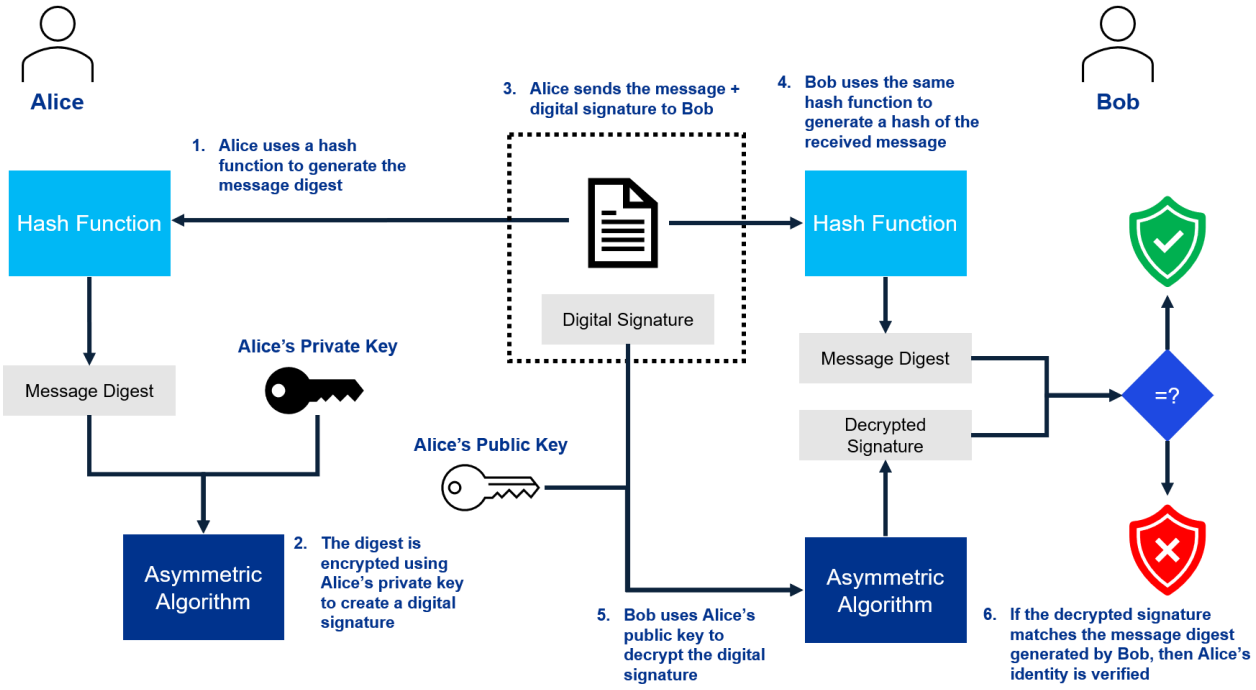
Figure 19: Asymmetric Key Encryption[80]



Source: KPMG analysis

[77] Google. 2019. *Quantum supremacy using a programmable superconducting processor*. (https://www.nature.com/articles/s41586-019-1666-5).
[78] Q-CTRL. 2026. *Fast, accurate, high-resolution simulation of large-scale Fermi-Hubbard models on a digital quantum processor*. (https://arxiv.org/abs/2605.04025).
[79] The Open University. 2016. *An introduction to encryption and cryptography*. OpenLearn. (https://www.open.edu/openlearn/digital-computing/network-security/content-section-4.1).
[80] IBM Quantum Learning. 2026. *Asymmetric key cryptography*. (https://quantum.cloud.ibm.com/learning/en/courses/quantum-safe-cryptography/asymmetric-key-cryptography).
[81] Cybersecurity and Infrastructure Security Agency (CISA). 2026. *Understanding Digital Signatures*. (https://www.cisa.gov/news-events/news/understanding-digital-signatures).

Figure 20: Digital Signatures[82]



Source: KPMG analysis

Asymmetric algorithms rely on computationally hard problems such as integer factorisation and the (elliptic curve) discrete logarithm problem. The security of symmetric algorithms and hash functions is often described in terms of the computational complexity to carry out an unstructured search. In other words, how long it would take to search through all the possible options to find the correct key.

Until the 1990s, the best-known methods for solving these problems were classical algorithms, under which the relevant security assumptions remained acceptable at practical key sizes. Even with advances in classical computing, including High Performance Computing, cryptographically relevant instances of the integer factorisation and discrete logarithm problem remain computationally infeasible to solve within a meaningful timeframe using the best-known classical approaches.

However, in 1997, Peter Shor[83] published a quantum algorithm that provides an exponential speed-up for integer factorisation and discrete logarithm-type problems. In principle, this means that widely used forms of asymmetric encryption could be broken much more efficiently by a quantum computer of sufficient scale than any known classical computer.[84]

Then, in 1996, Lov Grover[85] published a quantum algorithm that, in theory, reduces the effective security margin of brute-force search against symmetric algorithm. In simplified terms, this is often described as halving the number of bits of security. For example, AES-256 is often said to offer an effective security level closer to AES-128 against an idealised Grover-style quantum search.

Guidance from NIST suggests that AES-128 is still deemed secure due to the challenges around the physical implementation of Grover's algorithm.[86] AES-256 is still recommended by various international bodies for higher sensitivity data, regardless of the quantum threat. For example, CNSA 2.0 specifies AES-256 for all symmetric encryption for National Security Systems.[87]

[82] IBM Quantum Learning. 2026. *Asymmetric key cryptography*. (https://quantum.cloud.ibm.com/learning/en/courses/quantum-safe-cryptography/asymmetric-key-cryptography). Accessed: July 17, 2026.
[83] P W Shor. 1997. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. SIAM Journal on Computing. (https://doi.org/10.1137/S0097539795293172).
[84] National Institute of Standards and Technology (NIST). 2026. *What is post-quantum cryptography?*. (https://www.nist.gov/cybersecurity-and-privacy/what-post-quantum-cryptography#how-does-current-cryptography-work-and-how-would-a-quantum-compu). Accessed: July 17, 2026.
[85] Lov K. Grover. 1996. *A fast quantum mechanical algorithm for database search*. (https://arxiv.org/abs/quant-ph/9605043).
[86] National Institute of Standards and Technology (NIST). 2024. *Transition to Post-Quantum Cryptography Standards*. (https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf).
[87] National Security Agency. 2022. *Announcing the Commercial National Security Algorithm Suite 2.0*. (https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF).

5.2 List of Abbreviations

- **AES:** Advanced Encryption Standard
- **AI:** Authorized Institution
- **ANSSI:** Agence nationale de la sécurité des systèmes d'information
- **APAC:** Asia-Pacific
- **API:** Application Programming Interface
- **ASD:** Australian Signals Directorate
- **BAU:** Business as Usual
- **BSI:** Federal Office for Information Security, Germany
- **CBOM:** Cryptographic Bill of Materials
- **CDN:** Content Delivery Network
- **C-RAF:** Cyber Resilience Assessment Framework
- **CISA:** Cybersecurity and Infrastructure Security Agency
- **CNSA:** Commercial National Security Algorithm Suite
- **CRQC:** Cryptographically Relevant Quantum Computer
- **CSA:** Cyber Security Agency of Singapore
- **DES:** Data Encryption Standard
- **DLT:** Distributed Ledger Technology
- **ECDH:** Elliptic Curve Diffie-Hellman
- **ECC:** Elliptic Curve Cryptography
- **ENISA:** European Union Agency for Cybersecurity
- **FMI:** Financial Market Infrastructure
- **FS-ISAC:** Financial Services Information Sharing and Analysis Center
- **HBS:** Hash-Based Signatures
- **HHL:** Harrow-Hassidim-Lloyd Algorithm
- **HKMA:** Hong Kong Monetary Authority
- **HNDL:** Harvest Now, Decrypt Later
- **HQC:** Hamming Quasi-Cyclic
- **HSM:** Hardware Security Module
- **ICCS:** Institute of Commercial Cryptography Standards
- **IETF:** Internet Engineering Task Force
- **IoT:** Internet of Things
- **ISO:** International Organisation for Standardisation
- **KEM:** Key Encapsulation Mechanism
- **LMS:** Leighton-Micali Signature
- **LWE:** Learning With Errors
- **MAS:** Monetary Authority of Singapore
- **MDPI:** Multidisciplinary Digital Publishing Institute
- **ML-DSA:** Module-Lattice-Based Digital Signature Algorithm
- **ML-KEM:** Module-Lattice-Based Key Encapsulation Mechanism
- **NCSC:** National Cyber Security Centre
- **NGCC:** Next-Generation Commercial Cryptographic Algorithms Program
- **NIS2:** Network and Information Security Directive 2
- **NIST:** National Institute of Standards and Technology
- **NSA:** National Security Agency
- **NSS:** National Security Systems
- **PCI-DSS:** Payment Card Industry Data Security Standard
- **PKI:** Public Key Infrastructure
- **PoC:** Proof of Concept
- **PQC:** Post-Quantum Cryptography
- **QAOA:** Quantum Approximate Optimisation Algorithm
- **QKD:** Quantum Key Distribution
- **QML:** Quantum Machine Learning
- **RFC:** Request for Comments
- **RSA:** Rivest-Shamir-Adleman
- **SIKE:** Supersingular Isogeny Key Exchange
- **SLH-DSA:** Stateless Hash-Based Digital Signature Algorithm
- **TLS:** Transport Layer Security
- **TM-G-1:** Technology Risk Management module of the HKMA Supervisory Policy Manual
- **VPN:** Virtual Private Network
- **XMSS:** eXtended Merkle Signature Scheme

5.3 Glossary of Key Terms

- **Asymmetric cryptography:** Cryptography that uses a public key and a private key to support secure key exchange, authentication and digital signatures.
- **Classical computer:** A conventional computer that processes information using bits, where each bit represents either 0 or 1.
- **Code-based cryptography:** A class of post-quantum cryptography based on the difficulty of decoding certain error-correcting codes.
- **Cryptographic agility:** The ability of systems to replace cryptographic algorithms, keys and protocols without major operational disruption.
- **Cryptographic Bill of Materials:** A structured inventory of cryptographic assets, algorithms, certificates, libraries, protocols and dependencies across an organisation's technology estate.
- **Cryptographic inventory:** A structured record of cryptographic algorithms, keys, certificates, libraries, protocols and dependencies used across an organisation's technology estate.
- **Cryptographically relevant quantum computer:** A quantum computer capable of breaking widely used public-key cryptographic schemes within a practical timeframe.
- **Data secrecy lifetime:** The period for which information must remain confidential to avoid harm, regulatory impact or business disruption.
- **Digital signature:** A cryptographic mechanism used to verify the identity of a sender and confirm that a message or document has not been altered.
- **Distributed ledger technology:** A technology architecture in which records are maintained across multiple nodes or participants rather than a single central database.
- **Downgrade risk:** The risk that a system falls back to weaker or legacy cryptography during negotiation, migration or failure handling.
- **Entanglement:** A quantum property in which two or more quantum systems become linked so that their states are correlated, even when separated.
- **Fallback mechanism:** A defined process that allows systems to recover or revert safely if a cryptographic migration or upgraded configuration fails.
- **Hash function:** A mathematical function that converts data into a fixed-size value used to support integrity checks and digital signatures.
- **Harvest now, decrypt later:** An attack scenario in which encrypted data is collected today and stored for decryption once sufficiently capable quantum computers become available.
- **Hybrid cryptography:** An approach that combines traditional cryptographic algorithms with post-quantum algorithms during a transition period to support interoperability and reduce migration risk.
- **Key encapsulation mechanism:** A public-key technique used to establish a shared secret key between parties for secure communication.
- **Lattice-based cryptography:** A class of post-quantum cryptography based on hard mathematical problems involving high-dimensional lattices.
- **Legacy cryptography:** Older cryptographic algorithms, protocols or implementations that may no longer meet current security expectations or future quantum-resilience needs.
- **Migration roadmap:** A documented plan that defines priorities, milestones, owners, dependencies and timelines for moving systems to quantum-resistant cryptography.
- **Mosca's Theorem:** A framing that compares data secrecy lifetime, migration time and the time until a quantum threat materialises to determine whether action is already required.
- **Post-quantum cryptography:** Cryptographic algorithms designed to remain secure against attacks by both classical and quantum computers, while running on conventional computing infrastructure.
- **Quantum algorithm:** An algorithm designed to use quantum computing properties to solve specific types of problems differently from classical algorithms.
- **Quantum computing:** A computing model that uses quantum mechanical properties such as superposition and entanglement to perform certain calculations differently from classical computers.
- **Quantum key distribution:** A method for distributing cryptographic keys using quantum communication techniques, with the aim of detecting interception attempts.
- **Quantum machine learning:** The use of quantum computing techniques to support machine learning tasks, often in hybrid quantum-classical models.
- **Quantum readiness:** An organisation's capability to understand, govern, plan, test and implement changes needed to manage quantum-related opportunities and risks.

- **Qubit:** The basic unit of information in a quantum computer, analogous to a bit in a classical computer but capable of representing quantum states.
- **Shor's algorithm:** A quantum algorithm that can theoretically break widely used public-key cryptography by efficiently solving integer factorisation and discrete logarithm problems.
- **Superposition:** A quantum property that allows a qubit to exist in a combination of states until measured.
- **Symmetric cryptography:** Cryptography that uses the same secret key for encryption and decryption, commonly used for efficient data protection once a key has been securely shared.
- **Transport Layer Security:** A widely used protocol for securing communications over networks, including web and application traffic.
- **Trust infrastructure:** The certificates, keys, roots of trust, identity mechanisms and related processes that allow systems and parties to authenticate one another securely.