

The Post-Quantum Shift

Understanding the Quantum Threat and Preparing FinTechs for the Next Era of Digital Trust

SFA

SINGAPORE FINTECH ASSOCIATION

Foreword

Cryptography underpins trust in our digital world. It protects our transactions, identities and sensitive information, helping to keep essential services secure and reliable. Advances in quantum computing could undermine the cryptography we use today, putting that trust at risk.

There is no definitive timeline for when the quantum threat will arrive, but the risks are already present. Data that needs to remain confidential for years can be intercepted today and stored for decryption in the future, a threat known as “Harvest Now, Decrypt Later”.

Preparing for this future will take time. Organisations should start now, while there is still time to migrate in an orderly manner.

The financial sector has reason to act early. It relies on cryptography at scale to protect customer information, authenticate identities and secure high-value transactions. From making everyday payments to managing savings and accessing essential financial services, any disruption will have a direct impact on the lives and livelihood of Singapore. Disruptions to financial services could also cascade across businesses and essential services that depend on them. Given that the sector is deeply interconnected, its resilience will depend on the readiness of the wider financial ecosystem.

The financial sector is also well-placed to lead in building quantum-safe resilience. Financial institutions have mature risk-management practices and experience in managing complex technology transitions across their supply chains. By acting early and collectively, they can also accelerate vendor readiness and develop best practices that could benefit other sectors.

Quantum-safe migration is ultimately a national undertaking that requires coordinated action. To achieve this, CSA has set clear timelines to guide migration efforts, and is building enablers for organisations to act. Critical Information Infrastructure (CII) Owners will need to submit their migration plans by March 2027 and complete migration by 2031, while other organisations exposed to quantum risk should migrate by 2035. Our Quantum-Safe Migration Handbook and the Quantum Readiness Index help organisations assess their readiness and plan for migration. The new Quantum-Safe Kickstarter Grant also supports early pilots to build practical experience and surface implementation challenges.

Government cannot drive this transition alone. While CSA provides national guidance and works with sectoral regulators like MAS to translate national direction into sector-relevant expectations, industry plays a critical role in this transition as well. Notably, industry associations such as the Singapore FinTech Association (SFA) bring organisations together to share practical lessons and drive collective action. I therefore welcome this report by SFA. which translates quantum-safe migration into practical steps for financial institutions and FinTech firms.

Our message is simple: prioritise what matters, understand your risks and dependencies, establish ownership, and start preparing now. Importantly, migration plans should remain adaptable as technologies and solutions evolve.

By acting early and through close partnership, we can safeguard the trust and resilience of Singapore’s digital economy.

Gwenda Fong
Commissioner of Cybersecurity and Chief Executive,
Cyber Security Agency of Singapore

Foreword

Every FinTech in Singapore runs on cryptography it did not write and, in most cases, cannot see: the TLS handshake on a payment API, signature on a mobile token, certificate chain behind a cloud login. It works so quietly that most of us stopped thinking about it years ago. Quantum computing asks us to start again.

No one can confidently predict when a cryptographically relevant quantum computer will arrive. What we can say is that the public-key algorithms protecting today's financial systems have a known expiry, their replacements have been standardised and MAS as well as CSA have put dates on paper. Their guidance sets the destination. This report is the industry's own map for getting there. For a FinTech, the question is now where the requirements will arrive from: A supervisory expectation, a bank's vendor questionnaire, or a procurement clause.

I chair this subcommittee as a practitioner who sells to banks and sits in other firms' supply chains, so I have seen both sides of the vendor questions in *Chapter 4*. From that seat, most of the early work looks ordinary: Know which algorithms you depend on, who owns them, how long the data they protect must stay secret and what your suppliers plan to do about it. The firms that find this hard are usually the ones that have never looked.

So, we wrote a practical guide for our ecosystem. Singapore's FinTech community has a habit of moving early and moving together. On this subject, both will matter.

Pramodh Rai
Chair, Cyber Security & Quantum Computing Subcommittee, Singapore FinTech Association
Co-founder and CEO, Cyber Sierra

In financial services, we spend considerable time protecting the systems we rely on today. Some of the most important security challenges we face tomorrow will come from the technology decisions we are making right now.

Working across cybersecurity, digital identity and financial technology in this region, I have seen how deeply cryptography is embedded in our digital ecosystem, and how little visibility most organisations have into those dependencies. As quantum computing advances, the real concern is not when the threat will emerge, but whether we will be ready when it does.

That is the question this report sets out to answer. As Report Lead, I wanted us to move past the technical complexity and ask what readiness actually means for a FinTech. For most, the challenge is not a lack of awareness but knowing where to begin while balancing business priorities, regulatory expectations and limited resources. We have tried to make the answer accessible, relevant and, above all, actionable.

Bringing this report together reinforced something I see regularly in cybersecurity: technology alone is never the complete answer. Resilience takes collaboration, clear ownership and the willingness to act before risks become crises. Singapore's regulators, agencies, research institutions and industry have laid a strong foundation. What matters now is how we build on it.

I am grateful to my fellow subcommittee members and the industry experts who shared their perspectives. We cannot control when the quantum era will arrive. But we can control how prepared we are to face it.

Sanjeev Velayuthan
Member & Report Lead, Cyber Security & Quantum Computing Subcommittee,
Singapore FinTech Association,
Senior Regional Lead – ASEAN, Wultra

Table of Contents

Foreword 2

Opening Perspective: The Next Challenge for Digital Trust 6

01 Understanding the Post-Quantum Shift **7**

The Security Issue Is Digital Trust 9
Preparation Before Q-Day: Why Timing Matters 10
From Classical to Post-Quantum Cryptography 11
Crypto-Agility, Inventory and Hybrid Readiness 12

02 Singapore's Post-Quantum Readiness Landscape **13**

MAS: Financial-Sector Guidance and Developments 14
CSA: National Guidance and Migration Milestones 17
Singapore's Quantum-Safe Infrastructure and Industry Trials 21
National Initiatives and Support for Quantum Readiness 23
What Singapore's Quantum-Safe Direction Means for FinTechs 25

03 Perspectives from Quantum Resilience Leaders **28**

Professor Yehuda Lindell - Head of Cryptography, Coinbase 30
Dr. Tan Teik Guan - Co-Founder and Chief Executive Officer, pQCee 31
Petr Dvorak - Founder and Chief Executive Officer, Wultra 32
Winston Chir - Independent Technology Advisor 33

04 Vendor and Third-Party Readiness Checklist **35**

The Vendor Dependency Problem 36
Mapping the FinTech Technology Supply Chain 37
What Vendors Need to Demonstrate 37
Domain-Specific Vendor Considerations 38
Assessing and Managing Vendor Readiness 39
Procurement, Contracts and Third-Party Risk 39
Continuous Monitoring and Migration Testing 40
Practical Vendor PQC Readiness Checklist 40

05 Ignition Guide: Practical First Steps and Readiness Roadmap 41

From Awareness to Readiness: A 12-Month Action Plan 42
Readiness Roadmap Summary 44
What Fintechs Should Avoid in the First Year 44
Practical Deliverables 45

Quick Reference: What FinTechs Should Take Away 46
Closing Perspective 47
Sources / References 48
About Singapore FinTech Association (SFA) 50
Acknowledgements 51

Opening Perspective: The Next Challenge for Digital Trust

Every day, FinTechs rely on cryptography to keep financial transactions secure, protect customer information and establish trust across digital services. Much of this happens behind the scenes, from mobile banking applications and payment platforms to APIs, cloud services and connections with technology providers.

Quantum computing could eventually change how we protect these systems. Today's quantum computers are not capable of breaking the public-key cryptography widely used in financial services. However, future quantum computers with sufficient capability could compromise algorithms such as RSA and elliptic-curve cryptography, which underpin secure communications, authentication and digital signatures.

For Singapore's FinTech community, this is more than a technical concern. It has implications for business continuity, customer confidence and the long-term security of digital financial services.

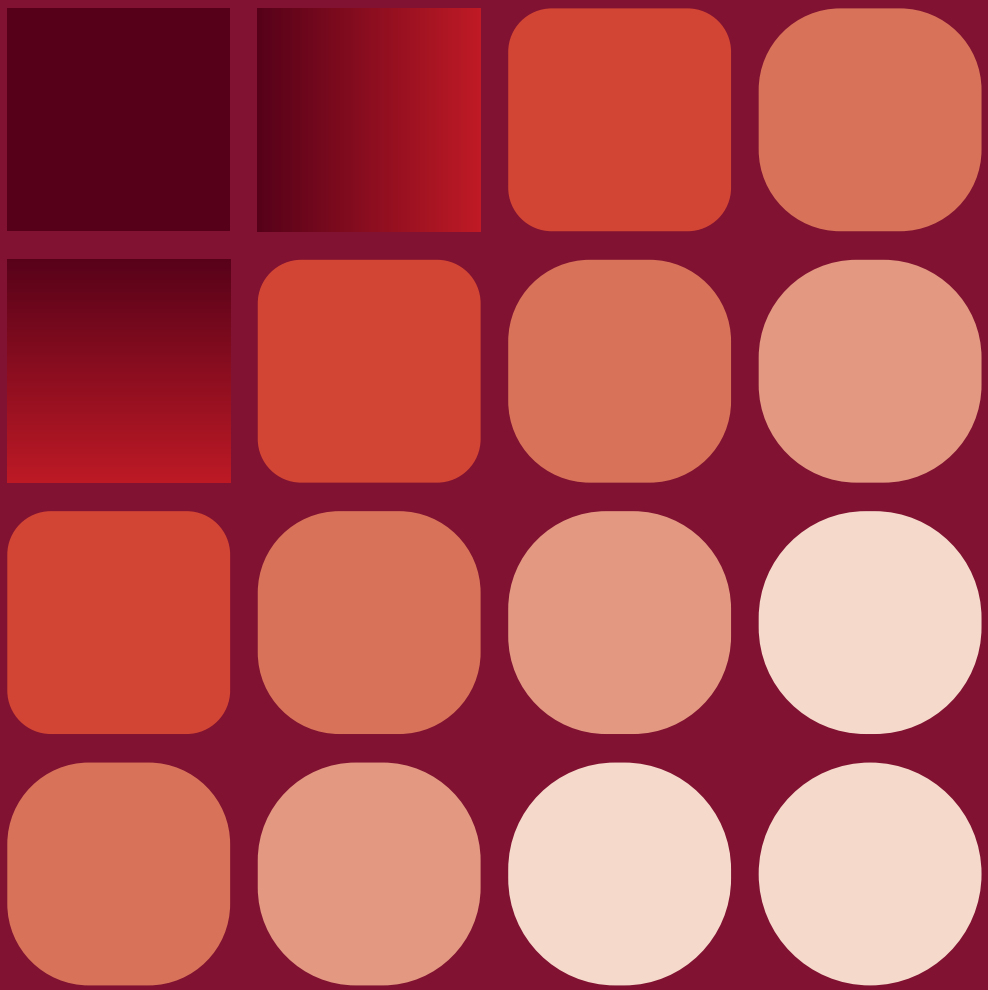
The challenge is that cryptography is deeply embedded in the systems FinTechs use every day, often through technologies and services provided by third parties. Knowing which algorithms are being used, where they are used and who is responsible for updating them is not always straightforward. This becomes particularly important when dealing with sensitive information that needs to remain protected for many years.

The good news is that FinTechs do not need to change everything overnight. There is still time to prepare, and much of that preparation can begin with practical steps: understanding existing cryptographic dependencies, speaking with technology providers, identifying areas of greater risk and ensuring systems can support new cryptographic standards when the time comes.

This report has been developed by the SFA Cybersecurity & Quantum Computing Subcommittee to help Singapore's FinTech community make sense of these developments. It brings together the technical background, Singapore's evolving quantum-safe landscape, industry perspectives and practical guidance to help FinTechs understand what is changing, where they may be exposed and what they can start doing today.

01

Understanding the Post-Quantum Shift



01

Understanding the Post-Quantum Shift

Quantum computing uses principles of quantum mechanics to process information differently from classical computers. Rather than being a faster version of conventional computing, it is a specialised technology designed to solve certain types of problems.

Classical computers use bits that represent either 0 or 1. Quantum computers use qubits, which can exist in a combination of quantum states before measurement. Through properties such as superposition, entanglement and interference, quantum algorithms can solve certain problems more efficiently than known classical approaches. However, this advantage is problem-specific and does not mean quantum computers are automatically faster or can solve every problem.

Building reliable quantum computers remains challenging. Qubits are sensitive to noise and errors, requiring quantum error correction to create stable logical qubits from multiple physical qubits. This distinction is important when assessing claims about progress, as higher physical qubit counts do not necessarily translate into greater practical capability.

Quantum computing is not expected to replace conventional computing infrastructure such as payment systems, databases or mobile applications. Its more significant cybersecurity implication is the potential for sufficiently capable quantum computers to break widely used public-key cryptography, affecting secure communications, digital signatures, authentication, identity systems and the protection of sensitive information.

Several landmark developments shaped modern quantum computing, including Richard Feynman's work on quantum simulation and David Deutsch's model of a universal quantum computer. Later, Peter Shor's and Lov Grover's algorithms demonstrated why quantum computing also matters for cybersecurity: Shor's algorithm showed how sufficiently capable quantum computers could undermine widely used public-key cryptography, while Grover's algorithm demonstrated a quantum speed-up with implications for symmetric encryption and hashing.

It has potential applications in areas such as simulation, optimisation and machine learning, but its most significant cybersecurity implication is its potential impact on cryptography. Shor's algorithm could enable a sufficiently capable quantum computer to break widely used public-key cryptography, including RSA, Diffie-Hellman and elliptic-curve cryptography. Grover's algorithm presents a more limited threat to symmetric encryption and hashing, which can generally be addressed through stronger security parameters.

Quantum computing continues to advance, particularly in error correction, logical qubits and scalable architectures. However, as of 2026, no publicly known quantum computer is capable of breaking the public-key cryptography protecting today's financial systems. Industry roadmaps nevertheless indicate continued progress. IBM, for example, is targeting its Starling fault-tolerant quantum computer for 2029, although this remains a development target rather than a confirmed timeline for a cryptographically relevant quantum computer.

The immediate priority, given the continued progress in quantum computing, is to understand where vulnerable public-key cryptography is used and prepare for its eventual replacement. For financial services, this includes secure communications, authentication, digital signatures and transaction systems. Because migration across interconnected systems and technology providers may take years, preparation needs to begin well before the threat becomes operational.

The Security Issue Is Digital Trust

Modern financial services depend on cryptography to do much more than keep information secret. Public-key cryptography supports secure communications, digital signatures, certificates, authentication, software integrity and transaction authorisation. It is woven through mobile applications, payment platforms, APIs, cloud services, identity systems and connections to technology providers.

The main quantum concern is public-key cryptography. RSA relies on integer factorisation, while Diffie-Hellman and elliptic-curve cryptography depend on discrete-logarithm problems that are impractical for classical computers to solve at appropriate key sizes. A sufficiently capable fault-tolerant quantum computer running Shor's algorithm could overcome those protections. Grover's algorithm has implications for symmetric encryption and hashing, but the impact is more limited and can generally be managed through stronger security parameters.

This makes the issue one of digital trust, not simply encryption. A future weakness could affect whether an organisation can still trust that a transaction was authorised by the right party, a certificate represents the right system, a software update is genuine or a digitally signed action remains authentic. For financial services, confidentiality, authenticity and integrity therefore need to be considered together.

"Dr. Tan Teik Guan cautions against viewing quantum risk only through the lens of encrypted data. In financial services, the authenticity of transactions, identities and digitally signed actions can be just as important. Future cryptographic weaknesses could therefore affect not only what remains confidential, but also what can still be trusted as genuine."

Dr. Tan Teik Guan
Co-Founder & CEO, pQCee

Preparation Before Q-Day: Why Timing Matters

The date on which a quantum computer becomes capable of threatening widely deployed public-key cryptography is often referred to as "Q-Day". Nobody can predict that date with confidence. Significant engineering challenges remain, and estimates continue to vary.

The more practical issue is that migration itself can take years. Cryptography is embedded across applications, certificates, APIs, cloud services, HSMs, SDKs, identity platforms and third-party systems. Some components can be updated through configuration or software releases; others may depend on hardware replacement, vendor support, partner interoperability or changes to customer journeys. Waiting until the threat is immediate could leave organisations trying to make complex changes under time pressure.

Harvest now, decrypt later (HNDL) brings the timeline forward further. An attacker can capture encrypted information today and retain it until future quantum capabilities make decryption possible.
The greatest concern is information that must remain confidential for many years, such as identity records, KYC information, financial histories and contractual data.
A useful prioritisation question is simple: would disclosure of this information years from now still cause material harm?

Classical forward secrecy does not remove this risk. Recorded key exchanges based on vulnerable public-key mechanisms could still be attacked in the future. Reducing HNDL exposure, therefore, requires attention to the cryptography used to establish session keys, as well as to data retention, minimisation, and secure disposal.

"Professor Yehuda Lindell cautions against allowing uncertainty over timing to become a reason for delay. His view is that organisations should focus less on predicting an exact Q-Day and more on whether migration can be completed safely within their planning horizon.
He also notes that HNDL risk should be prioritised rather than treated uniformly: long-lived, high-value information and situations where a single key protects large volumes deserve greater attention."

Professor Yehuda Lindell
Head of Cryptography, Coinbase

"Petr Dvorak highlights that HNDL is only part of the picture. He also describes 'trust now, forge later', where future cryptographic weaknesses could undermine signatures and evidence of authenticity, and 'buy now, waste later', where technology purchased today may have a shortened useful life if it cannot adapt to new cryptographic requirements."

Petr Dvorak
Founder & CEO, Wultra

From Classical to Post-Quantum Cryptography

Post-quantum cryptography (PQC) uses algorithms designed to resist attacks from both classical and quantum computers. Unlike quantum key distribution (QKD), PQC runs on conventional computing infrastructure and can be integrated into existing applications, networks and financial systems. For most organisations, this makes PQC the principal technical path for replacing quantum-vulnerable public-key cryptography.

A major milestone came in August 2024, when the US National Institute of Standards and Technology (NIST) finalised its first three PQC standards: FIPS 203 for ML-KEM key establishment, and FIPS 204 and FIPS 205 for the ML-DSA and SLH-DSA digital signature schemes. Further algorithms remain under development and evaluation, including FN-DSA and HQC. These standards give organisations a recognised foundation for testing and migration rather than requiring them to wait for an entirely new generation of cryptographic algorithms.

Migration is not, however, a simple one-for-one replacement. PQC keys, signatures and messages can be larger and may behave differently across existing protocols and infrastructure. This can affect certificates, TLS handshakes, HSMs, APIs, databases, network devices, third-party integrations and customer-facing applications. End-to-end testing therefore matters as much as selecting the algorithm itself.

Symmetric encryption is affected differently. Algorithms such as AES can remain suitable with appropriate key sizes, which is why the more immediate migration priority is the public-key cryptography used for key establishment, authentication and digital signatures.

> QKD takes a different approach by using quantum properties to distribute cryptographic keys and requires specialised network infrastructure. It can provide an additional layer of protection for selected high-value communications, but it is not a substitute for PQC. This distinction is particularly relevant to Singapore, where post-quantum cryptography and quantum-safe network infrastructure are being explored in parallel as part of the broader national readiness effort.

Crypto-Agility, Inventory and Hybrid Readiness

Post-quantum migration will not happen everywhere at once. Standards will continue to evolve, vendors will move at different speeds, and organisations may need to operate existing and new cryptography side by side. The ability to make these changes without major disruption is known as crypto-agility.

> Crypto-agility means being able to update algorithms, keys, certificates and protocols as requirements evolve. It depends on configurable cryptography, clear ownership, tested change and rollback processes, and visibility into dependencies controlled by external providers. Hardcoded algorithms, legacy infrastructure and vendor restrictions can make migration slower, more complex and more costly.

That visibility starts with a cryptographic inventory. Organisations need to understand where vulnerable cryptography is used across applications, certificates, APIs, cloud services, HSMs, SDKs and third-party platforms. For critical systems, the inventory should capture the algorithms and protocols in use, key or certificate dependencies, system owner, vendor, business criticality, upgrade requirements and the sensitivity and lifetime of the data being protected. Payments, authentication, digital signatures and systems handling long-lived sensitive information are sensible places to begin.

> "Winston Chir notes that one of the most underestimated challenges is identifying where vulnerable cryptography is embedded. The difficult part is often not selecting a replacement algorithm, but finding RSA, ECC and related dependencies across applications, PKI, identity systems and infrastructure, and then changing them without disrupting live services."
>
> **Winston Chir**
> Independent Technology Advisor

Hybrid approaches can support the transition. For key establishment, classical mechanisms can be combined with post-quantum algorithms such as ML-KEM, allowing organisations to introduce quantum-resistant protection while maintaining compatibility during migration. RFC 10024, for example, specifies hybrid key-exchange groups including X25519MLKEM768 for TLS 1.3. Hybrid key exchange does not, however, make an entire application quantum-safe. Authentication, certificates, digital signatures and other cryptographic components may still require separate migration and testing.

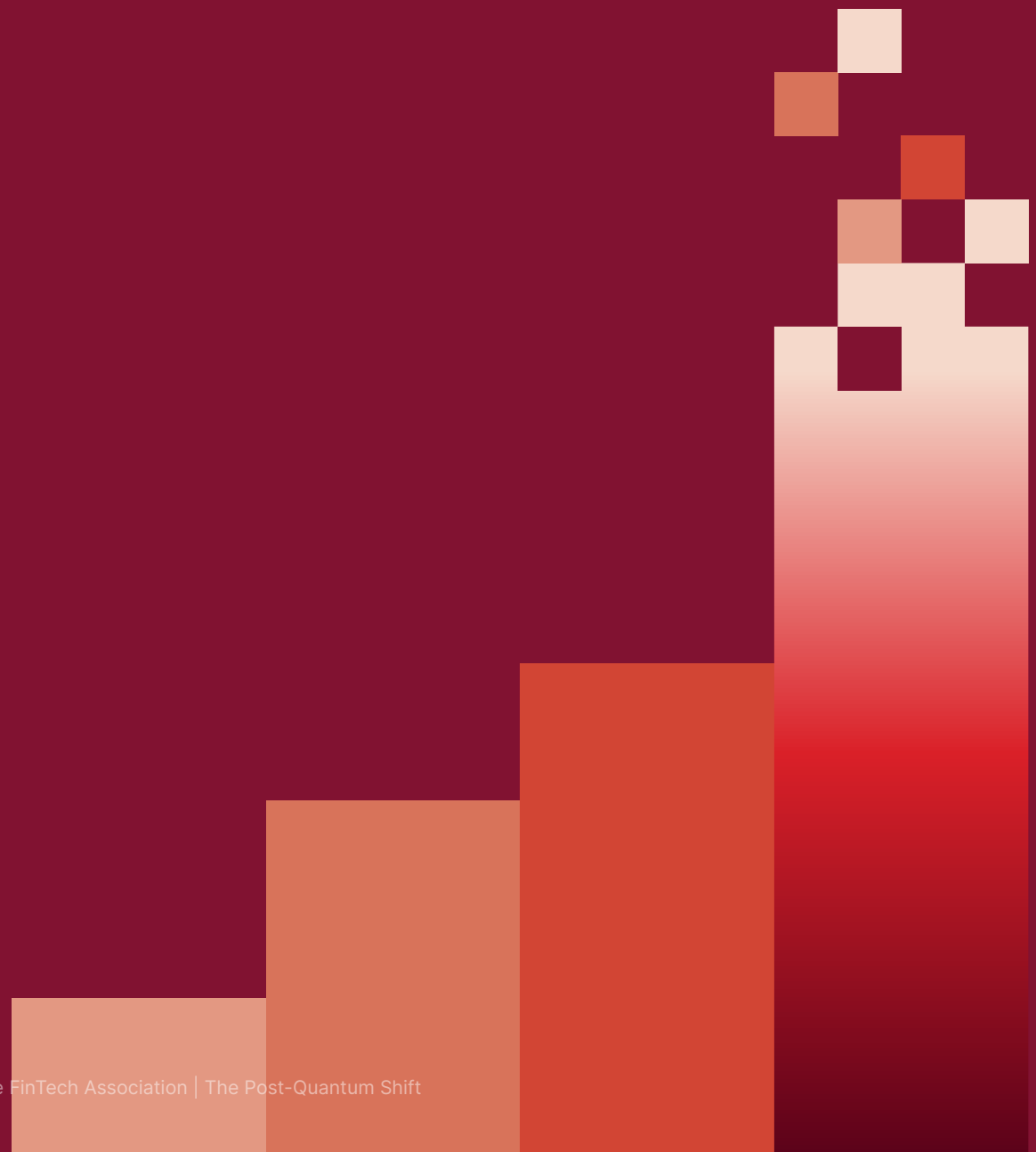
Vendor readiness is equally important. Cloud platforms, payment providers, identity services, certificate infrastructure, HSM vendors and software libraries may control cryptographic components that an organisation cannot change independently. Organisations therefore need to understand what they control directly, what depends on suppliers, what those suppliers plan to support and how changes will be tested across real systems and customer journeys.

Taken together, these concepts form the practical foundation of post-quantum readiness: protect digital trust, prioritise long-lived exposure, move towards standardised PQC, maintain crypto-agility, build visibility through cryptographic inventory and prepare for a phased transition.

Singapore's approach reflects many of these same principles. Financial-sector guidance, national cybersecurity initiatives, technical standards and infrastructure trials increasingly address cryptographic inventory, data sensitivity, crypto-agility, vendor engagement, PQC and quantum-safe communications. The next chapter examines how these concepts are being translated into Singapore's post-quantum readiness landscape.

02

Singapore’s Post-Quantum Readiness Landscape



02

Singapore's Post-Quantum Readiness Landscape

Singapore's approach to post-quantum readiness now spans financial-sector guidance, national cybersecurity initiatives, technical standards and infrastructure trials. The Monetary Authority of Singapore (MAS) issued guidance to financial institutions in 2024 and announced plans for further supervisory expectations, including migration milestones and timelines. The Cyber Security Agency of Singapore (CSA) has introduced practical guidance, readiness assessment tools and national migration targets, supported by local quantum-safe network initiatives.

These developments have direct implications across the financial ecosystem. MAS-regulated institutions face evolving supervisory expectations, while technology providers may encounter corresponding requirements through customer contracts, procurement and third-party risk management.

MAS: Financial-Sector Guidance and Developments

The 2024 Quantum Risk Advisory

On 20 February 2024, the Monetary Authority of Singapore (MAS) issued Circular MAS/TCRS/2024/01, Advisory on Addressing the Cybersecurity Risks Associated with Quantum, to the Chief Executive Officers of financial institutions.

Addressing CEOs reinforces that quantum readiness is a governance responsibility, not solely a technical concern. The advisory complements MAS's existing Technology Risk Management and Cyber Hygiene requirements rather than establishing a separate regulatory regime.

Its central recommendation is crypto-agility: enabling financial institutions to transition from vulnerable cryptographic algorithms to post-quantum cryptography (PQC) without significant disruption. MAS also recognises other approaches, including quantum key distribution (QKD), as potential risk mitigation measures.

The Eleven Recommended Measures

The MAS advisory outlines eleven recommended measures across three areas, providing a practical reference for financial institutions and technology vendors preparing for post-quantum risks.

Keeping Abreast of Developments and Raising Awareness

Measure	
(a)	Monitor quantum computing developments for threats to financial services, and mitigation using solutions such as PQC and QKD.
(b)	Ensure senior management and relevant third-party vendors understand the potential threats and the importance of transitioning.
(c)	Work closely with third-party IT vendors on supply chain risks arising from quantum threats, and request that vendors provide quantum-resistant solutions when they become commercially available.
(d)	Connect with industry groups, research bodies or Information Sharing and Analysis Centres to exchange information and collectively mitigate systemic quantum risk.

Maintaining an Inventory of Cryptographic Assets

Measure	
(e)	Identify and maintain an inventory of cryptographic solutions, recording the algorithm and key length, the ownership and parties responsible for maintaining the asset, and the specific system or application where the algorithm is embedded.
(f)	Classify IT and data assets dependent on vulnerable cryptography, based on sensitivity, criticality, risk exposure, and the period for which they are deemed sensitive.
(g)	Assess whether existing system infrastructures can support crypto-agility, and consider upgrading them where limitations exist, such as processing power, infrastructure design or discontinued vendor support.

Developing Strategies and Building Capabilities

Measure	
(h)	Uplift the technical competencies of relevant staff.
(i)	Review policies, standards and procedures to ensure they remain relevant through the transition.
(j)	Develop risk mitigation strategies for assets that cannot be migrated to PQC, and plan for contingency scenarios where quantum risks materialise substantially ahead of the predicted timeline.
(k)	Where resources permit, consider proof-of-concept trials with quantum security solutions to understand operational impact and implementation challenges.

Three MAS measures are particularly relevant.

- ***Measure (c)** addresses quantum-related supply-chain risks and encourages financial institutions to engage technology vendors on quantum-resistant solutions.*
- ***Measure (e)** specifies that cryptographic inventories should record algorithms, key lengths, ownership and affected systems.*
- ***Measure (f)** requires consideration of data sensitivity and how long information must remain protected, reinforcing the importance of harvest now, decrypt later risks.*

On 10 June 2026, MAS published Consultation Paper P012-2026 proposing amendments to its Technology Risk Management notices requiring comprehensive IT asset inventories, explicitly including cryptographic assets, open-source software and third-party components. The consultation closed on 31 July 2026, with implementation proposed 12 months after finalisation. These remain proposed requirements until the amended notices are formally issued.

MAS Quantum-Safe Experiments

MAS has moved beyond guidance into practical experimentation. Measure (k) encourages proof-of-concept trials, and MAS has participated in two initiatives exploring quantum-safe communications.

In November 2024, MAS and Banque de France completed a joint post-quantum cryptography experiment to secure email communications at the application layer, providing confidentiality, authentication and integrity. The trial used Microsoft Outlook with CryptoNext's PQC email plugin and adopted a hybrid approach combining classical and post-quantum algorithms to maintain compatibility with existing systems. Testing had been underway since 2023.

The joint report demonstrated the feasibility of implementing PQC within existing infrastructure and reinforced the importance of crypto-agility. In his foreword to the joint Banque de France-MAS report, Damien Pang, MAS Executive Director (Data and Technology Architecture) and Deputy Chief FinTech Officer, emphasised the need for collective action, stating that "no entity is immune to quantum threats until the collective community elevates its defense."

The experiment provides a useful foundation for assessing how similar post-quantum approaches might be extended to other financial communications, including cross-border payment messaging. Such applications would require separate technical and operational validation.

A second initiative, a quantum key distribution sandbox involving four local and international banks, is covered later in this report.

MAS's Next Steps Towards Quantum Resilience

On 28 July 2026, MAS Managing Director Chia Der Jiun announced plans to issue supervisory expectations later in the year, setting out milestones and timelines to guide financial institutions towards quantum resilience. The key priorities include identifying cryptographic assets, prioritising the migration of vulnerable systems based on risk, and strengthening the technical capabilities and governance needed to support the transition.

"MAS also outlined its aim for financial institutions to achieve quantum resilience before the end of the decade."

This represents a clearer direction compared with its 2024 advisory, which encouraged early preparation but did not prescribe a migration deadline.

As of October 2026, the detailed supervisory expectations had not yet been publicly issued. The proposed milestones and timelines should therefore be understood as MAS's stated direction rather than requirements already in force.

CSA: National Guidance and Migration Milestones

MAS and CSA play complementary roles in supporting Singapore's post-quantum readiness. MAS provides financial-sector supervisory guidance, while CSA sets the broader direction for national quantum-safe migration, and develops cross-sector guidance and support initiatives. Their priorities are closely aligned, particularly around inventory, governance, technical preparedness and vendor engagement.

Mapping CSA's Five Readiness Domains to MAS Measures

CSA domain	CSA no-regret move	Corresponding MAS measures
Risk Assessment	Identify most critical systems; run cryptographic asset discovery on those first	(e) inventory (f) asset classification including sensitivity period
Governance	Identify who is accountable for migration decisions	(e) (ii) ownership per asset (i) policies and procedures (b) senior management understanding
Technology	Identify replacement algorithms for priority systems; understand trade-offs	(a) monitor developments (g) infrastructure crypto-agility (j) non-migratable assets and contingency (k) proof-of-concept trials
Training and Capability	Brief senior leadership now	(b) senior management awareness (h) staff competencies
External Engagements	Contact key vendors for post-quantum roadmaps	(c) vendor supply chain and requests (d) industry groups, research bodies, ISACs

The two frameworks can support a coordinated readiness programme. MAS-regulated institutions can use the advisory measures alongside CSA's Quantum Readiness Index to assess maturity and track progress. Technology vendors can also adopt this approach to prepare for customer assessments.

MAS provides more specific guidance on cryptographic inventory requirements, while CSA's framework offers a broader structure for governance and maturity assessment.

While CSA has set a common timeline for CII migration, MAS has indicated that the financial institutions should aim to achieve quantum resilience before the end of the decade, with further supervisory expectations to follow. Financial institutions should therefore consider both sets of guidance together.

The Quantum-Safe Migration Handbook and Readiness Index

On 16 July 2026, the Cyber Security Agency of Singapore (CSA) published two linked resources: the Quantum-Safe Migration Handbook and the Quantum Readiness Index. Both are freely available and represent important practical tools in Singapore's quantum-safe readiness efforts.

The Handbook was developed by CSA with GovTech and IMDA, in collaboration with industry partners including Accenture, AWS, Cisco, Deloitte, IBM, PQStation and the Association of Information Security Professionals, with additional feedback from other industry participants. The Quantum Readiness Index was developed by CSA in consultation with A*STAR, Accenture, Deloitte, evolutionQ, SGTech, SpeQtral and the World Economic Forum.

Both followed a public consultation that began in October 2025. CSA makes clear that these resources are informational, non-mandatory and not exhaustive, and will continue to evolve as the field develops.

> On 14 October 2026, at Singapore International Cyber Week (SICW) 2026, CSA issued its Advisory on Quantum-Safe Migration for Organisations, encouraging organisations exposed to quantum-related risks to develop migration plans by the end of 2027 and work towards completing migration by 2035. The advisory reinforces practical priorities, including identifying critical systems and long-lived sensitive data, establishing ownership, engaging vendors and maintaining crypto-agility. These broader recommendations should be distinguished from the separate milestones applicable to CII owners.

How CSA Frames the Timeline

In its preface, the Handbook cites expert estimates placing "Q-day" within five to ten years, while acknowledging more conservative estimates of ten to twenty years. It also warns that adversaries may already be harvesting encrypted data for future decryption. Despite uncertainty over the timeline, CSA emphasises that migration should begin well before quantum threats materialise.

The Handbook highlights two reasons for early action: migration can take years, and delays prolong exposure to harvest now, decrypt later risks.

CSA also identifies a significant challenge: cryptography is "deeply embedded across software libraries, hardware modules, and protocols," with dependencies often poorly documented or controlled by third-party providers. This reinforces the importance of understanding existing cryptographic dependencies before planning migration.

CSA's Five Readiness Domains and No-Regret Moves

The Handbook and Readiness Index share five domains. The Handbook provides guidance, while the Index assesses organisational readiness. Each domain identifies a "no-regret move" - an action worth taking regardless of how quantum technologies and standards evolve.

Domain	No-regret move
Risk Assessment	Identify your most critical systems and run cryptographic asset discovery on those first. Do not attempt to inventory everything at once.
Governance	Identify who is accountable for quantum-safe migration decisions - the person who owns the outcome and approves the plan.
Technology	For your priority systems, identify which quantum-safe algorithms can replace the vulnerable ones currently in use. Understand performance trade-offs before committing.
Training and Capability	Brief senior leadership on the quantum threat now, so they can approve resources and timelines.
External Engagements	Contact your key vendors now and ask for their post-quantum roadmaps.

Three measures require relatively little initial investment: assigning ownership, briefing leadership and engaging vendors. Risk assessment and technology evaluation demand more technical effort, but CSA recommends starting with priority systems rather than attempting organisation-wide migration immediately.

The Handbook identifies four stakeholder groups: senior management and the board, cybersecurity teams, IT and technology strategy teams, and business units responsible for continuity. It also provides a RACI model and outlines two governance approaches: integrating migration into existing structures or establishing a dedicated team. The appropriate approach depends on organisational complexity, resources and the need for sustained coordination.

Recommended Cryptographic Approaches

CSA identifies post-quantum cryptography (PQC) as the primary migration approach for most organisations, while stating that QKD should be considered for layered defence or niche use cases where its specific security properties are warranted. CSA also makes clear that QKD is not a replacement for PQC.

The Handbook provides the following algorithm recommendations:

Category	Deprecated	Recommended
Asymmetric cryptography	RSA, DH, ECC - all key sizes	ML-KEM, ML-DSA, SLH-DSA. For firmware signing only: LMS, XMSS
Symmetric cryptography	AES with key sizes below 128-bit	AES-256
Hash functions	SHA with output sizes below 256-bit, such as SHA-224	Hash functions >=256-bit

CSA also highlights operational considerations. PQC keys, signatures and related messages can be larger than their classical equivalents, potentially affecting bandwidth, storage, latency and interoperability. These impacts are particularly relevant to TLS handshakes, certificate chains, payment infrastructure and mobile applications.

An important distinction applies to symmetric encryption. While CSA recommends AES-256 for migration, NIST considers AES-128 secure against foreseeable quantum threats and does not require its immediate replacement. Organisations should therefore assess AES-256 adoption against their security requirements, risk exposure and applicable standards rather than treating AES-128 as inherently quantum-vulnerable.

Why Standards Are Still Evolving

CSA acknowledges that "no approach to quantum-safe technology can be considered settled." Although NIST finalised its first three post-quantum standards in August 2024, further algorithms remain under evaluation, including additional key-establishment and digital signature schemes.

In May 2026, NIST selected nine candidates for the third round of its additional digital-signature process. One of them, HAWK, was withdrawn by its submitters in July 2026 after an AI-assisted cryptanalytic attack was published. This illustrates why organisations should adopt established standards while retaining the flexibility to accommodate future changes.

These developments reinforce the importance of crypto-agility. Organisations should proceed with established standards rather than delay migration, while ensuring their systems can accommodate future changes to algorithms.

With further standards expected over the coming years, post-quantum migration should be treated as an evolving capability rather than a one-time technology replacement.

Using The Quantum Readiness Index

The Quantum Readiness Index is a self-assessment questionnaire covering CSA's five domains, with maturity levels and recommendations for improvement. It helps organisations assess their readiness, identify priorities and, importantly, facilitate discussions with senior management to secure support.

The recommended process: complete the assessment, identify gaps, use the Handbook to develop and implement action plans, and reassess periodically to measure progress.

The Index is not a certification but a tool for continuous improvement. Its practical value lies in providing management and boards with a measurable view of progress, showing whether quantum readiness is genuinely improving over time.

Migration Milestones for CII Owners

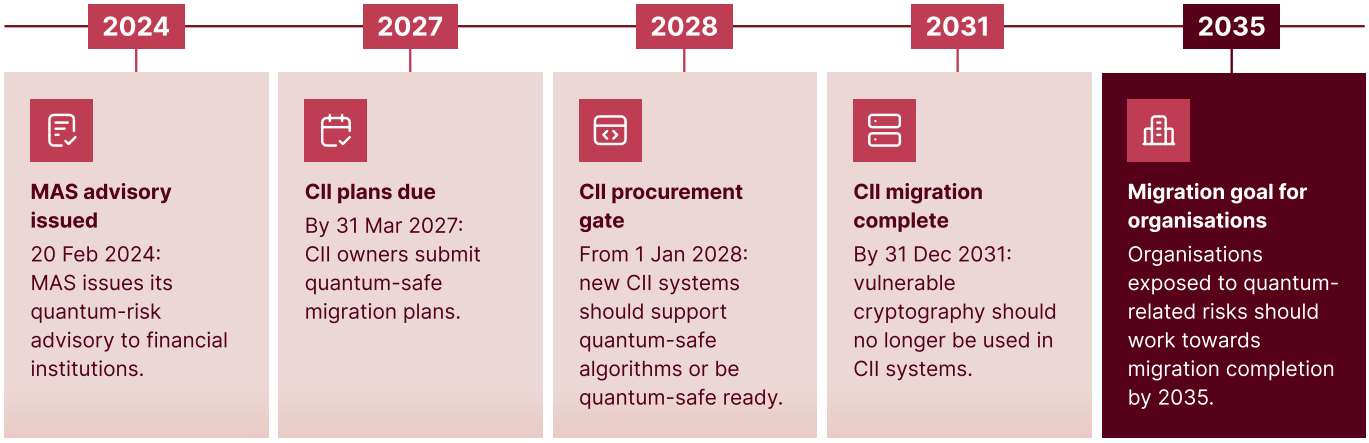
CSA has communicated specific quantum-safe migration milestones for Critical Information Infrastructure (CII) owners, covering migration planning, future procurement and completion of migration. The Quantum-Safe Migration Handbook is an informational resource and should not itself be treated as the legal instrument establishing these obligations. CII owners should refer to applicable CSA directions and guidance to determine their requirements.

Date	Requirement
By 31 March 2027	Submission of CII owner quantum-safe migration plan to CSA.
From 1 January 2028	Procurement and implementation of new CII computers and computer systems that have a digital component should either (a) support quantum-safe algorithms/technologies; and/or (b) be quantum-safe ready.
By 31 December 2031	Completion of quantum-safe migration across CII computers and computer systems, meaning vulnerable cryptography should no longer be used.

CSA, GovTech and IMDA are developing further guidance to support implementation. The 2028 procurement milestone is particularly relevant to technology suppliers. It may influence procurement specifications, RFPs and vendor assurance requirements for systems supplied to CII owners.

Banking and finance are one of Singapore's eleven CII sectors, although individual CII designations are not publicly disclosed. Technology providers should therefore assess customer requirements without assuming that particular institutions hold CII status.

Singapore's Quantum-Safe Migration Milestones



Singapore's Quantum-Safe Infrastructure and Industry Trials

Singapore has built and tested quantum-safe network infrastructure alongside publishing guidance. Two linked programmes are relevant.

The National Quantum-Safe Networks (NQSN)

Participants include the National University of Singapore and its Centre for Quantum Technologies, Nanyang Technological University, Singapore University of Technology and Design, GovTech, Horizon Quantum and SpeQtral. The testbed is supported by the National Quantum Office and the Quantum Engineering Programme.

The testbed uses a multi-layer architecture aligned with ITU-T Y.3800 and IMDA's quantum key distribution network standards. It comprises four layers: a quantum layer connecting QKD modules over fibre; a key management layer supporting interoperability between QKD systems; a network management layer for centralised monitoring and control; and an application layer supporting quantum-safe communications.

This architecture enables testing of interoperability, network management and integration with existing communications infrastructure.

National Quantum Safe Network Plus (NQSN+)

The National Quantum-Safe Network Plus (NQSN+) was announced by Deputy Prime Minister Heng Swee Keat on 6 June 2023 at ATxSummit, with the aim of establishing nationwide quantum-safe communications.

While NQSN serves as a research and industry testbed, NQSN+ extends the initiative towards nationwide deployment. IMDA subsequently appointed two operator groupings in November 2023: SPTel in partnership with SpeQtral, and Singtel, to develop interoperable quantum-safe networks accessible to businesses.

Financial Sector QKD Sandbox: Implementation and Findings

On 14 August 2024, MAS signed a Memorandum of Understanding with DBS, HSBC, OCBC, UOB, SPTel and SpeQtral to conduct a quantum key distribution (QKD) proof-of-concept sandbox for financial services. The September 2025 post-implementation report states that the solution, provided by SPTel and SpeQtral, operated on IMDA's NQSN+ infrastructure using trusted network nodes.

The sandbox ran in two phases: September-November 2024 with MAS, DBS and OCBC, followed by January-March 2025 with MAS, HSBC and UOB. Participants deployed QKD equipment and key management infrastructure in environments isolated from production networks to test the secure transmission of simulated financial data. The implementation followed relevant ETSI, ISO/IEC and ITU-T standards, including ETSI GS QKD 014, ETSI GS QKD 016, ETSI GS QKD 020, ISO/IEC 23837-1:2023 and ITU-T X.1713.

The published findings highlighted both potential applications and practical limitations:

- **Relevant use cases:** QKD could strengthen communications carrying sensitive financial information, particularly between data centres and within individual institutions.
- **Security assurance:** Trusted nodes require stronger assurance, including tamper resistance, auditability and layered security controls.
- **Interoperability:** Integration across different QKD providers and existing IT environments remains challenging. ETSI GS QKD 020, published in June 2026, provides a relevant interoperability specification.
- **Implementation and cost:** Participants identified gaps in deployment guidance, integration frameworks and cost-benefit justification. Specialised QKD hardware and infrastructure remain significant investment considerations.
- **Hybrid readiness:** The findings emphasised combining QKD with post-quantum cryptography (PQC) and maintaining crypto-agility as standards evolve.

The sandbox also found that QKD applications are more immediately practical within a single financial institution than across multiple institutions, given the point-to-point nature of QKD key distribution. Data-centre connectivity therefore represents a more immediate deployment opportunity than broad interbank integration.

Overall, the trial demonstrated QKD's potential for securing selected financial communications while identifying the technical, operational and economic challenges that must be addressed before wider adoption.

Perspectives from Participating Banks and Technology Providers

The banks and technology providers characterised the sandbox differently, reflecting their respective priorities. The following remarks are drawn from Annex A of MAS's 29 September 2025 media release accompanying the technical report.

- The banks emphasised both the potential and unresolved challenges. Eugene Huang, Group Chief Information Officer at DBS, described the pilot as providing "a clearer understanding of the security standards and implementation challenges that need to be addressed to build a robust quantum strategy." Tancy Tan, Chief Operating Officer at HSBC Singapore, positioned QKD as part of a defence-in-depth approach, providing added security "in those places where it is most important."

- Lawrence Goh, Head of Group Technology and Operations at UOB, said the sandbox offered "a glimpse of the potential as well as challenges." Praveen Raina, Head of Group Operations and Technology at OCBC, highlighted the importance of strategic investment in "infrastructure, talent development and upskilling."
- Technology providers focused on deployment feasibility. Lum Chune Yang, Co-Founder and Chief Executive Officer of SpeQtral, noted that QKD was already being used by banks internationally and that the sandbox demonstrated its ability to integrate with existing infrastructure and complement PQC through defence in depth.

Both perspectives are valid. QKD can be deployed and combined with PQC, but standards, interoperability and costs remain important considerations. HSBC's emphasis on deploying QKD where protection matters most captures its likely role: securing selected high-value communications rather than serving as a universal replacement for existing cryptography.

National Initiatives and Support for Quantum Readiness

The Roles of Singapore's Key Agencies and Research Institutions

Singapore's quantum-safe efforts involve several agencies, each contributing through regulation, infrastructure, standards, research or technology adoption. This coordinated approach means quantum-readiness expectations may emerge through supervisory guidance, procurement and industry standards.

IMDA leads NQSN+ and the development of quantum-safe network standards, including the IMDA Reference Specification for Quantum Key Distribution Networks (RS QKDN), Issue 1, June 2023. It also collaborated with CSA and GovTech on the Quantum-Safe Migration Handbook and supports standardisation efforts. Its NQSN+ programme describes the direction as "Moving towards a quantum-safe Singapore in 10 years", reinforcing Singapore's long-term transition priorities.

GovTech co-developed the Handbook, participates in the NQSN testbed and supports quantum-safe adoption across government digital services. Its work may also influence future public-sector technology procurement requirements.

CSA provides national cybersecurity guidance through the Handbook, Quantum Readiness Index and migration milestones for Critical Information Infrastructure owners.

MAS leads financial-sector readiness through supervisory guidance, industry experimentation and technology innovation initiatives.

Singapore's research ecosystem, including the National Quantum Office, Quantum Engineering Programme, NUS and the Centre for Quantum Technologies, NTU and SUTD, supports quantum research, infrastructure development and industry collaboration.

Together, these initiatives connect policy, technical standards, infrastructure, research and financial support. For FinTechs, the practical value lies in using these resources to assess cryptographic exposure, plan migration and evaluate suitable technologies rather than treating quantum readiness as a standalone research exercise.

Singapore's approach brings together several complementary efforts: CSA provides national cybersecurity guidance, MAS sets financial-sector expectations and supports innovation, IMDA develops infrastructure and technical standards, and the national quantum research ecosystem builds capabilities. FinTechs serving financial institutions operate at the intersection of these efforts and should consider how each may influence their own quantum-readiness plans.

Funding and Support Available to FinTechs

FSTI 3.0, including its dedicated Quantum Track, concluded in mid-2026. MAS subsequently launched FSTI 4.0 on 31 August 2026, committing up to S$220 million over three years. While FSTI 4.0 does not include a dedicated quantum track, its Institution Project track supports eligible Singapore-based financial institutions and FinTech firms developing and deploying frontier technologies, explicitly including quantum technology. FinTechs considering relevant proofs of concept should therefore assess their eligibility under FSTI 4.0 rather than rely on the former FSTI 3.0 Quantum Track.

CSA also announced the Quantum-Safe Kickstarter Grant on 14 October 2026 to support organisations beginning practical quantum-safe migration. The grant covers up to 70% of qualifying costs and runs from 1 November 2026 to 31 October 2027, with supported pilots lasting up to six months. It is open to non-government organisations incorporated in Singapore, with priority given to CII owners, and includes use cases such as cryptographic discovery and inventory as well as crypto-agility. Eligible FinTechs should assess whether the grant can support relevant discovery, planning or pilot activities.



What Singapore's Quantum-Safe Direction Means for FinTechs

How Quantum-Readiness Expectations Reach Singapore FinTechs

Singapore FinTechs face quantum-readiness expectations through two routes. MAS-regulated FinTechs, including licensed payment institutions, digital payment token service providers, capital-markets licensees, digital banks and insurers, fall within the relevant financial-sector supervisory framework. Unlicensed technology vendors may not be directly subject to MAS's quantum-risk advisory, but can face similar expectations through their regulated customers and, where applicable, Critical Information Infrastructure (CII) procurement requirements.

- The first mechanism is MAS's financial-sector guidance. Since February 2024, MAS has encouraged financial institutions to engage third-party IT vendors on quantum-related supply chain risks and request quantum-resistant solutions under measure (c) of its advisory. For FinTech vendors, these expectations may appear in security questionnaires, vendor due diligence and contractual requirements.
- The second mechanism is CSA's CII migration milestones. The Quantum-Safe Migration Handbook states that CII owners should submit migration plans by 31 March 2027. From 1 January 2028, newly procured CII computers and computer systems with digital components should support quantum-safe algorithms or technologies, and/or be quantum-safe ready. These are CSA-stated milestones rather than statutory deadlines, but they may increasingly shape procurement requirements.

For unlicensed technology vendors, the immediate trigger could be an RFP or security assessment requesting evidence of quantum readiness. MAS-regulated FinTechs face broader expectations, as quantum risk is already part of financial-sector technology-risk guidance, with MAS having announced forthcoming supervisory expectations and progressive implementation timelines.

What this means in practice

For MAS-regulated FinTechs, quantum readiness is becoming part of financial-sector technology-risk expectations. For unlicensed technology vendors, it may become a procurement and sales requirement before any direct regulatory obligation applies. In both cases, firms that can demonstrate a cryptographic inventory, clear ownership, vendor engagement and a credible migration plan will be better positioned to respond to customer and regulatory expectations.

Cryptographic inventories are a practical starting point. MAS's 2024 advisory, under measure (e), calls for inventories identifying algorithms, key lengths, system ownership, responsible parties and where cryptography is embedded. Its June 2026 consultation proposes broader IT asset inventories covering cryptographic assets, open-source software and third-party components. For regulated FinTechs, this reinforces the importance of understanding existing cryptographic dependencies before planning migration.

Harvest now, decrypt later exposure depends on data sensitivity and lifespan. As discussed in *Chapter 4*, MAS measure (f) reinforces the need to consider how long information must remain confidential. Short-lived transaction data may present a different exposure profile from identity documents, KYC records and financial histories that require protection for many years. Migration priorities should reflect these differences.

Vendor readiness works in both directions. FinTechs serving banks may face quantum-readiness questions from their customers while needing similar assurances from their own cloud providers, payment gateways, KYC vendors and hardware security module suppliers. MAS measure (c) and CSA's External Engagements guidance reinforce the importance of managing these dependencies throughout the supply chain.

Crypto-agility is a consistent priority across Singapore's initiatives. It features in MAS's advisory, the MAS–Banque de France experiment, the financial-sector QKD sandbox and CSA's guidance. Continued developments in NIST's PQC standards further reinforce the need for systems that can accommodate future algorithm changes. The architectural implications are covered in *Chapter 5*.

PQC remains the primary migration path, while QKD serves specialised use cases. Singapore's investment in quantum-safe networking should not be interpreted as a requirement for every FinTech to deploy QKD. CSA positions QKD as an additional layer of protection for selected applications, while the financial-sector sandbox identified more immediate opportunities within individual institutions. For most FinTechs, adopting standardised PQC and building crypto-agility should take priority over investing in dedicated QKD infrastructure.



Aligning FinTech Readiness with MAS and CSA Guidance

The following actions provide a practical starting point for FinTechs at different stages of quantum readiness. They align with relevant MAS advisory measures and CSA guidance, allowing firms to address overlapping expectations through a coordinated approach.

Action	Effort	Maps to
Name one accountable person for quantum-safe migration	Hours	CSA Governance MAS (b)
Brief the board or leadership on quantum risk and the CSA CII milestones	One session	CSA Training MAS (b)
Complete the CSA Quantum Readiness Index across the five domains	Half a day	CSA QRI
Inventory cryptography in your most critical systems only, recording algorithm and key length, owner, and host system	Weeks	CSA Risk Assessment MAS (e)
Classify data by how long it stays sensitive, to set harvest now, decrypt later priority	Days	MAS (f)
Email your principal vendors and cloud providers for their PQC roadmaps	Days	CSA External Engagements MAS (c)
Assess whether you could change algorithms without re-architecting	Weeks	MAS (g)
Identify assets that cannot migrate and plan contingencies	Weeks	MAS (j)
Review FSTI 4.0 Institution Project track eligibility if running a relevant frontier-technology trial	Days	MAS (k)
Re-run the Readiness Index periodically and report the trend to the board	Ongoing	CSA QRI

Several actions, including appointing an owner, briefing leadership and engaging vendors, can begin quickly with limited expenditure. Cryptographic inventories, data classification and technical assessments require more sustained effort, while eligible technology trials may benefit from FSTI 4.0 support. Together, these steps provide a proportionate foundation for demonstrating quantum readiness to boards, regulators and financial-institution customers.

03

Perspectives from Quantum Resilience Leaders



03

Perspectives from Quantum Resilience Leaders

Post-quantum readiness goes beyond cryptography. It involves governance, technology dependencies, migration planning and operational resilience, particularly for FinTechs that rely on cloud platforms, payment infrastructure, identity systems, third-party vendors and open-source components.

To bring practical industry perspectives into the report, this chapter draws on insights from four practitioners with experience across cryptography, digital assets, financial technology, enterprise architecture and post-quantum migration. While their backgrounds and areas of expertise differ, their perspectives highlight several common priorities: understanding cryptographic dependencies, addressing vendor readiness, building crypto-agility and beginning preparations before quantum threats become immediate.

Perspective	What it adds to the report
Professor Yehuda Lindell - Head of Cryptography, Coinbase	A cryptographer's perspective on migration risk, standards uncertainty, harvest now, decrypt later prioritisation, MPC custody, vendor accountability and the risks of delaying migration until it becomes urgent.
Dr. Tan Teik Guan - Co-Founder and Chief Executive Officer, pQCee	A Singapore FinTech leader's perspective on digital trust, transaction authenticity, vendor readiness, procurement pressure and practical first steps for smaller FinTechs.
Petr Dvorak - Founder and Chief Executive Officer, Wultra	A financial technology leader's perspective on post-quantum migration, with a focus on crypto-agility, authentication, vendor readiness, customer migration and operational implementation.
Winston Chir - Independent Technology Advisor	An independent technology advisor's perspective on cryptographic inventory, cloud dependency, vendor accountability, enterprise risk and the real-world challenges of implementing migration safely.

Professor Yehuda Lindell - Head of Cryptography, Coinbase

As Head of Cryptography at Coinbase, Professor Yehuda Lindell brings an applied cryptography perspective shaped by the realities of protecting high-value digital assets and operating cryptographic systems at scale.

His central message is that post-quantum readiness already matters because migration takes time. As he puts it, “migrations take a very long time” and “there isn’t time to just wait.” His point is not that organisations should immediately replace every cryptographic system, but that the preparation required for a safe migration should already be under way.

He also cautions against allowing uncertainty over timing to become an excuse for delay. Waiting for a definitive deadline could leave organisations trying to migrate complex systems under pressure, competing for resources and disrupting normal product development.

His view of harvest-now-decrypt-later is deliberately nuanced. Not all encrypted information carries the same long-term risk. The more useful questions are whether the information will still be sensitive years from now and how much value could be exposed if a cryptographic key were eventually compromised. Scenarios where one key protects a large volume of data, or where particularly valuable assets such as signing keys are involved, deserve greater attention.

His vendor advice reflects the same pragmatism. Rather than asking whether a supplier is simply “quantum-safe,” FinTechs should determine whether it has a credible plan, a realistic timeline and a clear understanding of the dependencies involved. For smaller FinTechs in particular, vendor preparedness becomes part of technology risk management.

On crypto-agility, he distinguishes between changes that are relatively straightforward and those that are structurally difficult. Key rotation, configuration changes and cipher-suite updates may be manageable. Re-encrypting large datasets, changing database structures, accommodating larger cryptographic objects or coordinating changes controlled by third parties can be significantly harder.

He also warns against both extremes: doing nothing and investing prematurely in proprietary approaches before risks and standards are sufficiently understood. Either can become costly. A delayed migration may eventually consume resources that would otherwise support normal business priorities.

For digital-asset firms, the challenge extends beyond conventional enterprise infrastructure. Signature schemes, custody models, MPC implementations and blockchain protocols may all be affected. Organisations that do not control the underlying protocols need to understand the migration plans of the networks and service providers on which they depend.

His board-level message is straightforward: “The discussion around timelines needs to be put aside.” Rather than trying to predict the exact arrival of a cryptographically relevant quantum computer, organisations should ask whether they are sufficiently confident that such capability will remain outside their planning horizon.



Professor Yehuda Lindell
Head of Cryptography, Coinbase

Dr. Tan Teik Guan - Co-Founder and Chief Executive Officer, pQCee

Dr. Tan Teik Guan brings a Singapore-based technology and FinTech perspective, connecting post-quantum readiness with digital trust, transaction authenticity, procurement and the practical constraints faced by smaller organisations.

His starting point is trust. In his words, "cryptography is the foundation of this trust," making post-quantum readiness more than a technical upgrade. For FinTechs, cryptography helps establish confidence in customers, counterparties, transactions, identities and digital interactions.

> He also believes the discussion can become too narrowly focused on harvest-now-decrypt-later. In financial services, confidentiality is only one concern. The authenticity of transactions, identities and digitally signed actions may be equally important if future cryptographic weaknesses make forgery or impersonation possible.

His assessment of harvest-now-decrypt-later is therefore proportionate rather than alarmist. FinTechs should examine the potential business consequence of exposure, including regulatory impact, reputational damage, customer loss and wider operational disruption, rather than assuming every encrypted dataset carries the same level of risk.

On vendor readiness, he emphasises the depth of the technology supply chain. A FinTech's own target date may depend on suppliers becoming ready earlier, and those suppliers may themselves rely on underlying providers or open-source components. Smaller open-source projects may create particular challenges where maintainers do not have the resources to implement major cryptographic changes quickly.

> His view on responsibility captures the issue clearly: "You can outsource the work to become quantum-safe, but the FinTech cannot outsource the responsibility." Smaller organisations may reasonably depend on external expertise and technology providers, but accountability for those dependencies remains with the FinTech.

For organisations with limited budgets, he recommends standards-based approaches, targeted pilots and disciplined procurement rather than broad transformation programmes. Starting small allows teams to understand implementation issues and scale their response based on actual experience.

He sees Singapore as still being in an "awareness" phase, although awareness is "relatively good" compared with many other markets. Existing adoption of major cloud platforms may also allow some FinTechs to benefit from underlying quantum-safe technology improvements without having to develop those capabilities independently.

For digital-asset firms, he highlights issues around key generation, signing, wallet migration and network-level dependencies. Migration may be easier in centrally governed environments than in decentralised networks where changes require coordination across a broader ecosystem.

His final advice comes down to awareness, procurement and internal ownership. Teams need enough understanding to ask better questions, procurement processes need to account for future migration, and organisations need people who can distinguish necessary action from unnecessary complexity or, in his words, "what's need-to-have, what's good-to-have and what's snake-oil."



Dr. Tan Teik Guan
Co-Founder and
Chief Executive Officer, pQCee

Petr Dvorak - Founder and Chief Executive Officer, Wultra

Petr Dvorak brings a financial-technology and implementation perspective shaped by Wultra's work with banks and financial institutions. His contribution focuses on how post-quantum migration affects crypto-agility, authentication, technology dependencies and customer-facing services in practice.

He says organisations often underestimate the effort involved because cryptography is embedded across many parts of the technology environment. Authentication, identity, databases, cloud services, network security, code signing, HSMs and end-user devices may all contain dependencies that eventually need to be understood and addressed.

He also highlights that the industry can focus too heavily on harvest-now-decrypt-later and overlook other forms of exposure. He describes these as "trust now, forge later" and "buy now, waste later." The first concerns future threats to signatures and historical evidence of authenticity. The second highlights the risk of investing in technology today that may have a shorter useful life if it cannot adapt to changing cryptographic requirements.

That is where crypto-agility becomes important. Post-quantum migration should leave systems easier to change as standards and requirements evolve, rather than creating another one-off algorithm replacement exercise.

On vendor readiness, his recommended question is practical: "What is your quantum-readiness timeline, and what will the migration require from us?" A credible answer should explain what is already supported, what remains on the roadmap, which external dependencies exist and what has been tested.

He also points out that a technology supply chain will rarely migrate at the same pace. A FinTech may depend on certificate infrastructure, identity providers, HSM vendors, mobile platforms and other technology providers operating on different timelines. One unresolved dependency can therefore delay an otherwise well-prepared migration.

For smaller organisations, he recommends what he calls the **"Top 10 Rule":** begin with the ten most critical systems or services, understand their dependencies and determine whether each should be retained, upgraded, replaced or eventually retired. This provides useful visibility without turning readiness into an exhaustive mapping exercise.

He also cautions against allowing discovery itself to become the objective. A detailed cryptographic inventory is only valuable if it informs priorities and action. For an organisation with limited time and no additional budget, the focus should be on identifying material exposure, understanding supplier roadmaps and completing at least one practical improvement.

Authentication illustrates why implementation needs to be considered at the service level. Moving customers from existing cryptographic credentials to new ones may require user participation, particularly where credentials are tied to registered devices. This makes enrolment, transaction approval, recovery and the risk of customer lockout part of the migration problem.

Technical constraints can also appear outside the cryptographic algorithm itself. Larger cryptographic objects may affect database behaviour and performance, while HSM support and mobile key-management capabilities such as iOS Keychain and Android Keystore introduce their own dependencies.

His practical conclusion is that organisations should test complete customer journeys rather than isolated algorithms. A cryptographic primitive may perform well in a benchmark while the surrounding application, infrastructure, device or recovery process becomes the real constraint.

Based on his experience with European financial institutions, he says regulatory attention often begins by raising awareness and later evolves into more specific expectations around ownership, supplier readiness, dependencies and evidence of progress. Singapore FinTechs should therefore expect quantum readiness to increasingly surface through institutional customers, procurement requirements and supervisory discussions.



Petr Dvorak
Founder and
Chief Executive Officer, Wultra

Winston Chir - Independent Technology Advisor

Winston Chir brings an enterprise technology and architecture perspective, with a particular focus on cryptographic inventory, cloud dependencies, vendor accountability, governance and the practical challenges of implementing migration across complex technology environments.

His starting point is that waiting for a precise "Q-Day" is the wrong approach. As he puts it, "Nobody knows that date." The concern is not whether the necessary quantum hardware exists today, but whether organisations are basing migration plans on a level of certainty that does not exist.

He argues that one of the most underestimated challenges is identifying where RSA and ECC are actually used and changing those dependencies without disrupting payments, identity systems, PKI or customer traffic. The difficult part is often not choosing a new algorithm, but finding embedded cryptography and changing it safely.

> His harvest-now-decrypt-later test is equally practical: "The key question is not how long the network session lasts; it is how long the information inside that session needs to remain secret." A TLS connection may exist for seconds while the personal, financial or commercial information transmitted through it remains sensitive for years.

He also distinguishes confidentiality risk from integrity risk. Harvest-now-decrypt-later primarily concerns information collected today and decrypted in the future. Certificates, trust anchors and code-signing mechanisms raise different concerns because future cryptographic weaknesses may enable impersonation or signature forgery.

His vendor-management advice focuses on evidence rather than broad assurance. FinTechs should expect vendors to understand their cryptographic dependencies, explain how those dependencies are maintained and provide a credible migration roadmap. A claim that a cloud provider will handle everything, or that strong symmetric encryption alone solves the issue, does not address the wider dependency problem.

> He makes a similar distinction between inherited technology and inherited accountability. Major cloud providers, operating systems, browsers and cryptographic libraries are already doing substantial underlying work, but FinTechs remain responsible for their own client versions, application libraries, keys, certificates, configurations and third-party integrations. His summary is direct: "You can inherit capabilities from the cloud; you do not inherit accountability."

For organisations starting without additional budget, he recommends using existing sources to build visibility, prioritising systems according to business criticality and data lifetime, and then testing a limited number of representative migration paths. The purpose is to discover where real constraints emerge rather than attempting immediate algorithm replacement across the organisation.

He also cautions that mathematically secure cryptography does not automatically produce a secure or workable system. Architecture, routing, interoperability, performance, network appliances and legacy assumptions all influence whether migration succeeds in practice.

His view of governance is similarly pragmatic. Policies, inventories and procurement clauses establish direction, but they do not prove that applications, PKI, HSMs, clients and suppliers will work together after cryptographic changes are introduced. Readiness ultimately has to be demonstrated through testing.

For Singapore FinTechs, this means taking advantage of capabilities delivered by major technology platforms without assuming that those platforms eliminate the FinTech's own responsibilities. Organisations still need to understand what they control, what they depend on and where coordination with payment, identity, banking and clearing partners will be necessary.

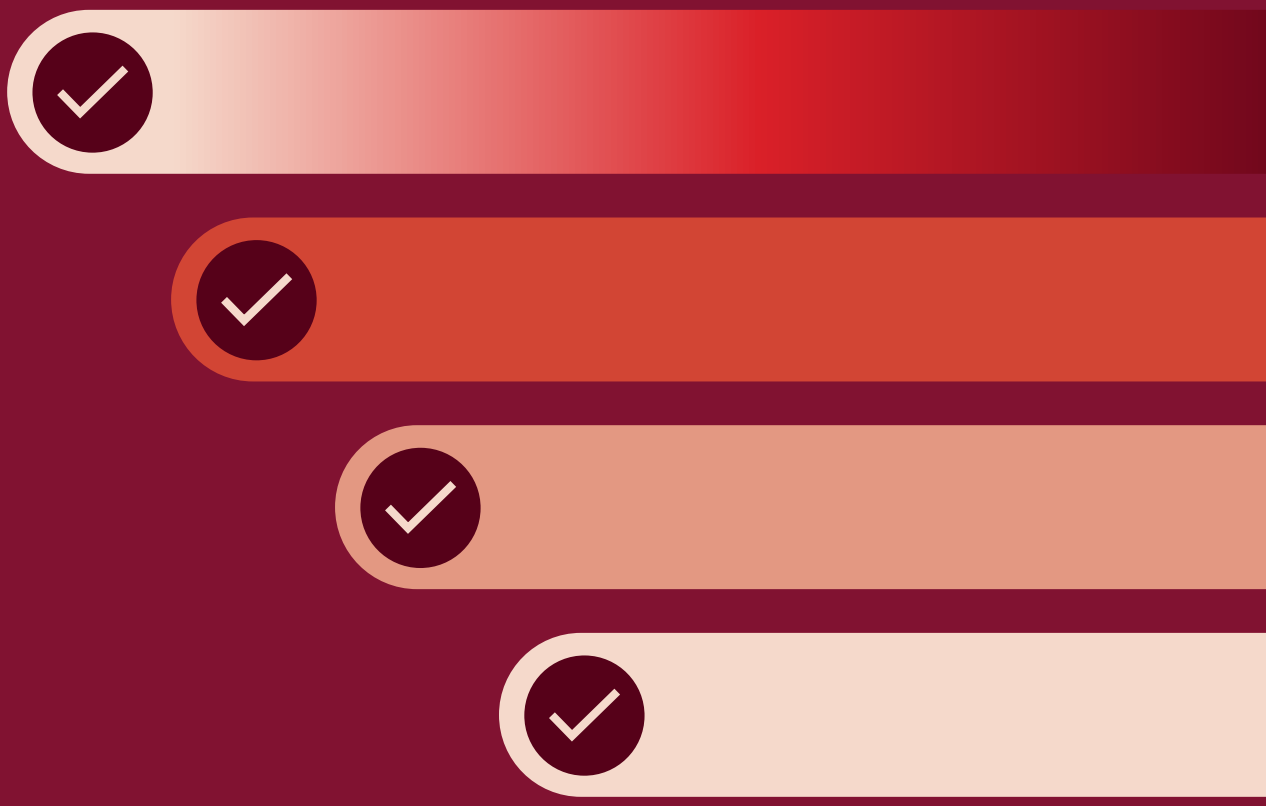
His final board-level question captures the issue well: "MAS aims for financial institutions to achieve quantum resilience before the end of this decade, and since you cannot migrate cryptography you cannot find, the question for this board today is simple: who owns your cryptographic inventory, and when will it be complete?"



Winston Chir
Independent Technology Advisor

04

Vendor and Third-Party Readiness Checklist



04

Vendor and Third-Party Readiness Checklist

A FinTech can prepare its own systems and still be constrained by suppliers. Cloud platforms, payment processors, identity providers and other critical vendors may determine when cryptographic changes become possible, so third-party readiness must be treated as part of the migration plan.

This chapter provides a practical approach to vendor due diligence, procurement and ongoing oversight. The aim is not to ask whether a vendor is simply "quantum-safe," but to establish its cryptographic dependencies, migration roadmap, customer impact and supporting evidence.

How to use this chapter

Start with critical vendors and business-critical services. A small fintech will not receive bespoke assurance from every hyperscaler or global platform. The aim is to ask proportionate questions, collect useful evidence, identify gaps, and know when a vendor issue should be tracked as a material third-party risk.

The Vendor Dependency Problem

FinTechs depend on cloud, payments, identity, PKI, HSM/KMS, cybersecurity, SaaS, SDK and open-source providers. These services often control cryptographic functions that a FinTech cannot change independently.

> Dependencies also extend beyond direct suppliers to cloud platforms, libraries, certificate authorities and other fourth parties. These hidden dependencies can become migration bottlenecks even when the FinTech and its direct vendor are prepared.

Rather than assessing every supplier equally, FinTechs should prioritise critical vendors, identify material cryptographic dependencies and determine where deeper assurance is needed.



"Dr. Tan Teik Guan captures the accountability issue succinctly: 'You can outsource the work to become quantum-safe, but the FinTech cannot outsource the responsibility.' Smaller firms may rely heavily on external technology and expertise, but they remain responsible for understanding and managing the dependencies those providers introduce."

Dr. Tan Teik Guan

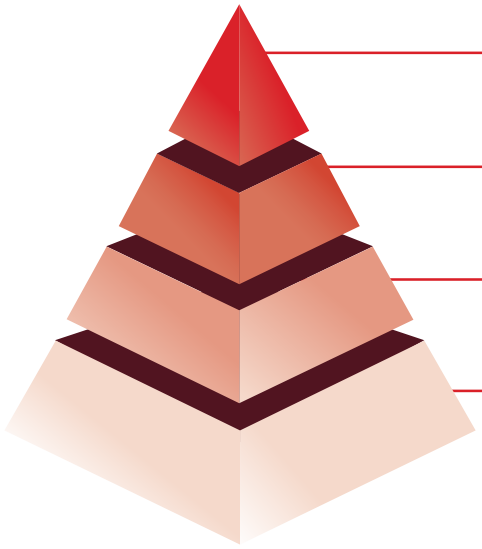
Co-Founder & CEO, pQCee

Mapping the FinTech Technology Supply Chain

Vendor reviews should begin by identifying which suppliers present the greatest operational and cryptographic risks. Low-risk services may require only basic monitoring, while providers handling sensitive data, payments, identity, authentication, cryptographic keys or regulated operations warrant closer assessment.

Prioritise reviews using five factors: service criticality, data sensitivity and longevity, cryptographic dependency, difficulty of replacement and fourth-party exposure.

A simple approach is to group vendors into four tiers.



	Description	Assessment approach
Critical	Supports customer-facing, payment, identity, authentication, cryptographic trust, sensitive-data or regulated services.	Full review, evidence request, roadmap discussion and active risk tracking.
High	Supports important operational or data processes where short disruption is manageable.	Targeted questions, roadmap monitoring and annual review.
Medium	Limited sensitive-data or operational exposure and low cryptographic dependency.	Light questionnaire and periodic monitoring.
Low	No material sensitive-data, cryptographic or operational dependency.	Manage through standard third-party risk processes.

What Vendors Need to Demonstrate

Vendors do not need to have completed migration today. They should, however, be able to identify relevant cryptographic dependencies, name accountable ownership, provide a dated roadmap, explain customer actions and show how interoperability and performance will be tested.

For critical vendors, seek proportionate evidence such as cryptographic inventory summaries, published roadmaps, release notes, assurance reports, migration guidance and change-notification processes. Smaller FinTechs may not receive bespoke assurance from major providers, but they should still expect enough evidence to understand timing, dependencies and customer responsibilities.

Domain-Specific Vendor Considerations

> "Winston Chir highlights 'You can inherit capabilities from the cloud; you do not inherit accountability.' ***Cloud providers*** may deliver underlying quantum-safe capabilities, but FinTechs remain responsible for their own libraries, certificates, keys, configurations and integrations."
>
> **Winston Chir**
> Independent Technology Advisor

The same questions apply across vendors, but the dependency to examine differs by domain.

Vendor domain	What is different in this domain	Example FinTech question
Cloud providers	Clouds may add PQC capabilities, but customers still control configurations, certificates, keys, client versions and integrations.	Which services support post-quantum or hybrid operation, and what must we change?
Payment processors and financial infrastructure	Payment flows depend on APIs, certificates, HSMs, signing and settlement links.	Which payment and signing dependencies change, and how will partner compatibility be tested?
Identity, authentication and trust providers	Authentication, token signing, device identity, PKI, passkeys, mTLS and recovery may migrate at different times.	How will authentication and recovery migrate without disrupting users or fraud controls?
Cybersecurity vendors	Security products may terminate encryption, validate signatures, issue certificates or verify updates.	How will these functions behave with post-quantum or hybrid traffic?
SaaS, APIs and software supply chain	SDKs, libraries, webhooks and API certificates can hide cryptographic dependencies.	Which embedded components require customer action?
HSM, KMS, PKI and certificate providers	These services anchor key management, signing and trust chains; larger objects can affect formats and performance.	How will you support post-quantum or hybrid keys, certificates and interoperability?

Assessing and Managing Vendor Readiness

Assess responses according to both evidence and business criticality. A weak response from a low-risk supplier may require monitoring; the same response from a critical cloud, payment, identity, HSM or PKI provider may require escalation.

Rating	Typical response	What the FinTech should do
Green	Vendor can identify relevant cryptographic dependencies, has named ownership, provides a dated roadmap, shows evidence of testing and explains customer impact.	Track through normal third-party risk processes, request periodic updates and align internal plans to vendor milestones.
Amber	Vendor recognises the issue and has some roadmap activity, but evidence, dates, customer impact or testing detail is incomplete.	Request clarification, set follow-up dates, include in renewal discussions and consider compensating controls where exposure is material.
Red	Vendor gives vague, dismissive or inaccurate answers, has no owner, cannot identify dependencies or treats readiness as someone else's problem.	Escalate as a third-party risk issue, consider risk acceptance, compensating controls, contract escalation, reduced dependency or alternative suppliers.

Where readiness is insufficient, use proportionate actions: request clearer milestones, apply compensating controls, reduce long-lived data exposure, escalate through procurement or contract management, and consider alternatives where no credible migration path exists.

Procurement, Contracts and Third-Party Risk

Integrate post-quantum readiness into existing procurement, architecture review, third-party risk and contract-renewal processes rather than creating a separate control framework.

Start now	Add progressively at renewal or major change
Include readiness questions in RFIs, RFPs and due diligence for critical vendors.	Add notification obligations for cryptographic changes, deprecations and customer action.
Request dependency summaries and roadmap evidence for services you use.	Add migration support, test support, documentation and backward-compatibility expectations.
Track critical-vendor readiness in periodic third-party risk reviews.	Where appropriate, align contract milestones and assurance rights with customer or regulatory timelines.

Reassess critical vendors periodically as standards, products and roadmaps evolve; readiness is a moving risk, not a one-time questionnaire.

Continuous Monitoring and Migration Testing

Vendor readiness must ultimately be demonstrated through testing. Cryptographic changes can affect certificates, message sizes, TLS handshakes, APIs, SDKs, HSM/KMS operations and partner integrations.

For critical vendors, test interoperability, performance, backward compatibility, rollback and business continuity before production deployment.

- Establish baseline performance and error metrics before changes are introduced.
- Use controlled pilots and test existing, hybrid and post-quantum configurations together.
- Document fallback and rollback procedures without creating lasting security weaknesses.
- Validate operational support, escalation and customer or partner communication plans.

Practical Vendor PQC Readiness Checklist

This checklist can be used during vendor due diligence, procurement and periodic reviews. It focuses on specific evidence of readiness rather than general assurances.

Area	Question to ask	Evidence or good response
Scope & inventory	Which services we use contain RSA, ECC, Diffie-Hellman, certificates, signing or other cryptography?	Affected-product list, inventory summary, owner and update process.
Roadmap & standards	What post-quantum or hybrid support is planned, when, and against which recognised standards?	Dated roadmap, versions, standards-monitoring process and expected customer impact.
Customer action	What must we change: certificates, SDKs, app versions, APIs, HSM/KMS, configuration or partner links?	Migration guide, release notes and compatibility documentation.
Testing	What interoperability, performance and rollback testing has been completed or planned?	Test results or pilot plan, known issues and production-readiness criteria.
Data exposure	What long-lived sensitive data do you process or transmit for us, and how is it protected?	Data-flow and retention view showing confidentiality-lifetime exposure.
Fourth parties	Which suppliers or open-source components affect your readiness?	Relevant cloud, HSM/KMS, PKI, payment, SDK and infrastructure dependencies.
Evidence & notification	What evidence can you provide, and how will customers be notified of material cryptographic changes?	Assurance material, roadmap evidence and a clear customer-communication process.
Risk & ongoing review	What happens if your timeline misses our needs, and how often is readiness reassessed?	Mitigation or escalation options, named owner and periodic review cadence.

05

Ignition Guide: Practical First Steps and Readiness Roadmap



05

Ignition Guide: Practical First Steps and Readiness Roadmap

The challenge is turning awareness into a manageable programme of work. The following 12-month approach starts with ownership and visibility, then moves into prioritisation, vendor engagement, testing and migration planning.

Guiding principle

Start with the work that remains useful regardless of the exact quantum timeline: awareness, ownership, inventory, vendor engagement, data lifetime assessment, crypto-agility and staged testing. Avoid both panic buying and passive waiting.

From Awareness to Readiness: A 12-Month Action Plan

First 30 Days: Create Ownership and Awareness

The first month should establish accountability and leadership awareness; technical migration can wait.

- Appoint an accountable owner and identify the core security, technology, risk, product and vendor-management stakeholders.
- Brief leadership on long-lived data, vendor dependencies and future customer or regulatory expectations.
- Agree that the initial objective is discovery and planning, not immediate replacement.



Days 30 to 60: Build an Initial Cryptographic Inventory

Start with business-critical systems rather than attempting a complete inventory. Expand coverage as dependencies become clearer.

> "For smaller organisations, Petr Dvorak recommends a 'Top 10 Rule': begin with the ten most critical systems or services, understand their dependencies and decide whether each should eventually be retained, upgraded, replaced or retired. This creates useful visibility without turning the first inventory exercise into an exhaustive mapping programme."
>
> **Petr Dvorak**
> Founder & CEO, Wultra

- Start with the most critical customer, payment, authentication, identity, API and sensitive-data systems.
- Record algorithms, key lengths, certificates, protocols, owners, vendors and business criticality.
- Use existing certificate, cloud, CMDB, code and vendor records, and record unknown dependencies for follow-up.

Days 60 to 90: Prioritise Risk and Engage Vendors

Use the initial inventory to identify the systems and dependencies requiring earlier attention.

- Prioritise systems by criticality, data sensitivity, confidentiality lifetime and migration complexity.
- Identify long-lived sensitive data and distinguish confidentiality risks from signature, authentication and integrity risks.
- Request roadmaps and evidence from critical vendors, including dependencies outside the FinTech's direct control.

Months 3 to 6: Assess Crypto-Agility and Test Representative Paths

Move from documentation to practical testing, focusing on whether cryptographic changes can be introduced without disrupting services.

- Select one or two representative customer-facing or partner-facing systems.
- Assess whether algorithms, keys, certificates and protocols can be changed through configuration, software updates or vendor support.
- Test suitable hybrid or post-quantum configurations and document performance, compatibility and architectural constraints.

Months 6 to 12: Build the Readiness Roadmap

Translate inventory findings, vendor responses and testing results into a phased migration plan.

- Prioritise systems using criticality, long-lived data exposure, customer impact and migration dependencies.
- Build a phased roadmap covering inventory expansion, vendor engagement, testing and future migration.
- Integrate crypto-agility into procurement and architecture reviews, estimate resource needs and track progress through a simple dashboard.

Readiness Roadmap Summary

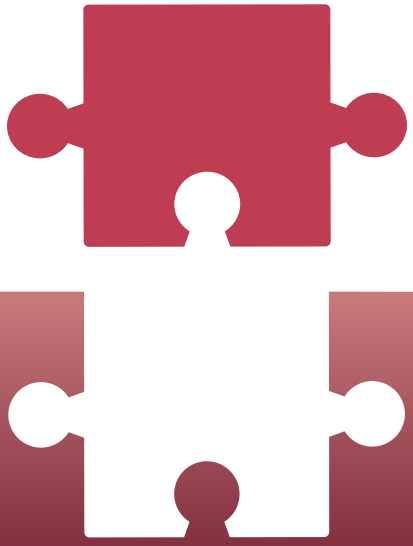
Phase	Timeframe	What to do	Main output
1	0 to 30 days	Assign ownership, brief leadership, identify stakeholders and agree the scope of the first readiness effort.	Named owner, stakeholder map and leadership briefing.
2	30 to 60 days	Build an initial cryptographic inventory for critical systems and record algorithms, key lengths, owners, vendors and business criticality.	Initial cryptographic inventory and list of unknowns.
3	60 to 90 days	Prioritise systems by data lifetime, business criticality and migration difficulty. Start vendor outreach.	Risk-prioritised inventory and vendor question set.
4	3 to 6 months	Assess crypto-agility and test representative hybrid or post-quantum paths in controlled environments.	Test findings, dependency map and initial migration issues.
5	6 to 12 months	Build a phased roadmap, update procurement and governance processes, and identify budget or resource needs.	Readiness roadmap, procurement updates and board/reporting dashboard.
6	Ongoing	Monitor standards, vendor roadmaps, regulatory expectations and production readiness. Reassess periodically.	Updated roadmap and measurable readiness trend.

What Fintechs Should Avoid in the First Year

- Investing in proprietary post-quantum solutions before understanding actual risks, standards and migration requirements.
- Attempting to inventory every system immediately instead of prioritising critical services.
- Assuming cloud providers remove customer responsibility, or accepting vendor lock-in that limits future cryptographic flexibility.
- Focusing only on encryption or treating QKD as the default path; signatures, authentication, certificates and crypto-agility also matter.
- Waiting for specific regulatory mandates before beginning governance, inventory and vendor engagement.

Practical Deliverables

Start now	Add progressively at renewal or major change
Ownership	Named accountable owner and cross-functional stakeholder group.
Inventory	Critical-system cryptographic inventory covering algorithms, certificates, protocols, owners and vendors.
Data lifetime view	Sensitive-data classification by required confidentiality period.
Vendor view	Critical vendors, responses received and roadmap gaps.
Crypto-agility assessment	Systems that can change cryptography easily versus those needing vendor, architecture or hardware change.
Testing plan	One or two representative hybrid or post-quantum test paths and findings.
Roadmap	Phased 12-month plan with actions, owners and dates.
Reporting	Simple dashboard of inventory coverage, key gaps, vendor readiness and decisions required.



Quick Reference: What FinTechs Should Take Away

Message	Implication
Quantum computers are not replacing FinTech infrastructure.	The relevant issue is future cryptographic risk, not replacement of core FinTech systems.
Public-key cryptography is the main area of concern.	Identify RSA, Diffie-Hellman and elliptic curve cryptography across products, APIs, certificates, signatures, authentication and vendors.
The risk is not immediate, but migration will take time.	Start with awareness, ownership, cryptographic inventory, vendor engagement and governance before the threat becomes urgent.
Harvest-now-decrypt-later brings the timeline forward.	Prioritise sensitive data that must remain confidential for many years, and assess where it is stored, transmitted and processed.
Crypto-agility is the practical bridge.	Design systems, processes and vendor relationships so algorithms, keys, certificates and protocols can be changed with minimal disruption.
Hybrid readiness supports transition.	Plan for a period where classical and post-quantum cryptography may operate together, and test interoperability, performance and rollback before production use.
Vendor readiness is part of FinTech readiness.	Prioritise critical vendors, ask for evidence rather than broad assurances, understand fourth-party dependencies, and track roadmaps, testing and customer migration requirements.
Singapore has published dates even though Q-day timing remains unknown	CSA has set quantum-safe migration milestones for CII owners, including submission of migration plans by 31 March 2027 and completion of migration by 31 December 2031.
For most FinTechs, commercial pressure will arrive through customers and procurement before direct regulation.	From 1 January 2028, new CII computers and computer systems with a digital component should support quantum-safe algorithms and technologies or be quantum-safe ready. FinTechs serving CII owners should expect this to appear in RFPs and procurement gates.
MAS has specified what a cryptographic inventory should contain.	Record the algorithm and key length, ownership and responsible parties, and the specific system or application where the cryptography is embedded, in line with measure (e) of the February 2024 advisory.
MAS guidance and the CSA roadmap align.	One readiness programme can support both: use the MAS measures for concrete controls, the CSA domains for structure, and the Quantum Readiness Index to assess and report progress over time.
For FinTechs, PQC is the primary migration path.	Prioritise PQC, cryptographic inventory and crypto-agility. Treat QKD as a specialised infrastructure or defence-in-depth option to monitor rather than a default FinTech migration path.
Readiness should be phased and measurable.	Assign an accountable owner, start with critical systems, engage key vendors, test representative migration paths, and build a 12-month roadmap that can evolve as standards, technology and market expectations mature.

Closing Perspective

Quantum computing is advancing, and while we cannot say exactly when it will pose a serious threat to today's cryptographic systems, there is enough progress to make preparation worth starting now.

For Singapore's FinTech community, this does not mean rushing to replace existing technologies or making major investments before they are needed. It means taking the time to understand where cryptography is used, which systems and services may be exposed, and how dependent the organisation is on technology providers to make future changes.

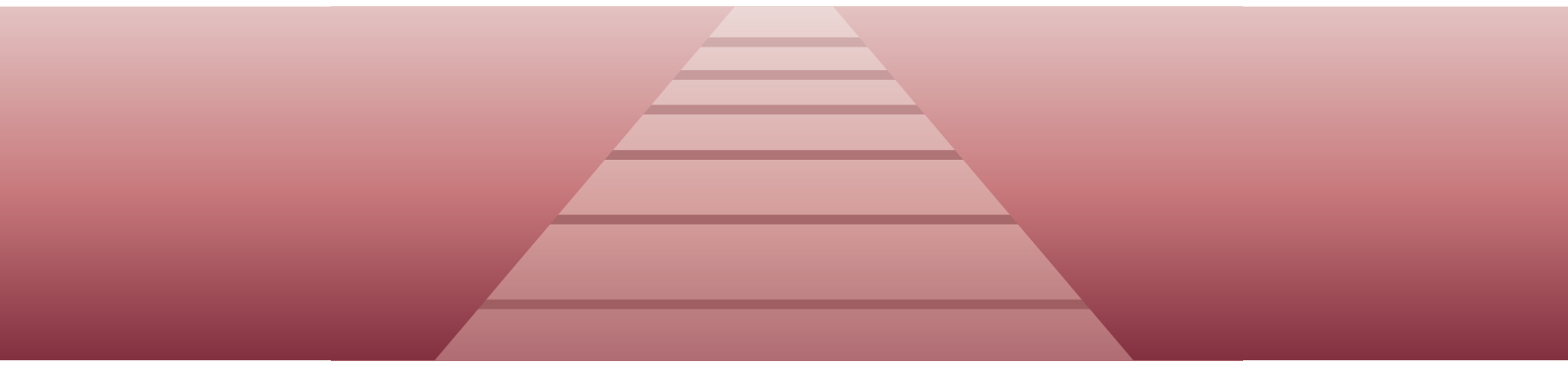
Many of these steps are already part of good cybersecurity and technology risk management. What changes with the quantum threat is the need to look further ahead, particularly where sensitive information must remain protected for years or where systems cannot be easily upgraded.

Throughout this report, we have tried to bring together the developments, industry perspectives and practical considerations that matter most to FinTechs. We recognise that organisations will be at different stages of readiness, with different resources and priorities. There is no single approach that will work for everyone.

As standards mature and Singapore's regulatory expectations continue to develop, the decisions FinTechs make today will influence how smoothly they can adapt in the years ahead. Starting with a clear understanding of their risks, engaging vendors early and building a realistic migration plan will put organisations in a much stronger position.

The SFA Cybersecurity & Quantum Computing Subcommittee hopes this report will help FinTechs take those first steps with greater clarity and confidence.

The aim is not to predict when quantum computing will change the way we secure digital trust, but to make sure Singapore's FinTech ecosystem is prepared for that change.



Sources / References

Primary

Source	Publisher / Organisation	URL
Circular MAS/TCRS/2024/01, Advisory on Addressing the Cybersecurity Risks Associated with Quantum	Monetary Authority of Singapore (MAS)	MAS Advisory
Post-Quantum Cryptography Report	Banque de France and Monetary Authority of Singapore (MAS)	Banque de France / MAS report
Quantum Key Distribution Proof-of-Concept Sandbox for the Financial Sector, Post-Implementation Report	Monetary Authority of Singapore (MAS), with DBS, HSBC, OCBC, UOB, SPTel and SpeQtral	MAS QKD Sandbox report
Quantum-Safe Migration Handbook V1	Cyber Security Agency of Singapore (CSA), GovTech and IMDA	CSA Quantum-Safe Migration Handbook page
Quantum Readiness Index V1	CSA with A*STAR, Accenture, Deloitte, evolutionQ, SGTech, SpeQtral and World Economic Forum	CSA Quantum Readiness Index page
NQSN testbed topology, partners and layer architecture	National Quantum-Safe Network	NQSN Testbed
National Quantum-Safe Network Plus (NQSN+) programme page	Infocomm Media Development Authority (IMDA)	IMDA NQSN+ page
Round 3 Additional Digital Signature Schemes (updated July 2026)	NIST Computer Security Resource Center (CSRC)	NIST Round 3 page
Post-Quantum Cryptography project and standardisation process (FIPS 203-206; HQC selection)	NIST Computer Security Resource Center (CSRC)	NIST PQC project
Simulating Physics with Computers	Richard P. Feynman, International Journal of Theoretical Physics	Feynman paper DOI
Quantum theory, the Church-Turing principle and the universal quantum computer	David Deutsch, Proceedings of the Royal Society A	Deutsch paper DOI
Algorithms for Quantum Computation: Discrete Logarithms and Factoring	Peter W. Shor, IEEE Symposium on Foundations of Computer Science	Shor paper DOI
A Fast Quantum Mechanical Algorithm for Database Search	Lov K. Grover, ACM Symposium on Theory of Computing	Grover paper DOI
IBM Quantum 2030 Roadmap; Starling technical announcement (10 Jun 2025); quantum investment announcement (2 Jun 2026)	IBM	IBM Quantum 2030 Roadmap
IBM Starling / fault-tolerant quantum roadmap	IBM	IBM Quantum hardware and Starling roadmap
IBM quantum investment announcement: more than US$10 billion over five years (2 Jun 2026)	IBM	IBM quantum investment announcement
Timelines for Migration to Post-Quantum Cryptography (20 Mar 2025)	UK National Cyber Security Centre	NCSC PQC migration timelines
RFC 10024: Post-Quantum Traditional (PQ/T) Hybrid Key Agreement Mechanisms for TLS 1.3 (August 2026)	IETF	RFC 10024
NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption (11 Mar 2025)	NIST	NIST HQC selection
Advisory on Quantum-Safe Migration for Organisations, 14 October 2026	CSA	CSA Advisory

Source	Publisher / Organisation	URL
Quantum-Safe Migration Timeline and Grant Announcement, 14 October 2026	CSA	CSA Announcement
Quantum-Safe Kickstarter Grant	CSA	Grant Details
FSTI 4.0 Announcement, 31 August 2026	MAS	MAS Announcement
Ignition Guide: How to Switch to Post-Quantum Authentication	Wultra	Wultra Post-Quantum Ignition Guide
White Paper: Post-Quantum Authentication: The Best Time to Switch Was Yesterday	Wultra	Wultra Post-Quantum Authentication White Paper
Consultation Paper P012-2026: Proposed Amendments to Notices on Technology Risk Management (10 Jun 2026)	Monetary Authority of Singapore (MAS)	MAS Consultation Paper P012-2026
Remarks by Managing Director Chia Der Jiun at the MAS Annual Report 2025/2026 Media Conference (28 Jul 2026)	Monetary Authority of Singapore (MAS)	MAS Managing Director remarks
NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards (Nov 2024)	NIST	NIST IR 8547
Frequently Asked Questions about Post-Quantum Cryptography	NIST Computer Security Resource Center (CSRC)	NIST PQC FAQ

Standards and Guidance Referenced

Reference	Organisation	Relevance to this report	URL
NIST FIPS 203	NIST	ML-KEM post-quantum key-encapsulation standard.	FIPS 203 / NIST PQC publications
NIST FIPS 204	NIST	ML-DSA post-quantum digital-signature standard.	FIPS 204 / NIST PQC publications
NIST FIPS 205	NIST	SLH-DSA post-quantum digital-signature standard.	FIPS 205 / NIST PQC publications
ETSI GS QKD 014, 016 and 020	ETSI	QKD interface and interoperability specifications referenced in the Singapore financial-sector sandbox and network discussion.	ETSI GS QKD 014 directory ETSI GS QKD 016 directory ETSI QKD standards page
ITU-T Y.3800 (2019): Overview on networks supporting quantum key distribution	International Telecommunication Union (ITU-T)	Framework referenced in relation to quantum key distribution networks.	ITU-T Y.3800
IMDA Reference Specification for Quantum Key Distribution Networks (RS QKDN), Issue 1 (June 2023)	IMDA	Singapore reference specification for quantum key distribution networks.	IMDA Reference Standards page
ISO/IEC 23837-1:2023	ISO/IEC	Security requirements and evaluation methods for quantum key distribution referenced in the Singapore financial-sector QKD sandbox.	ISO/IEC 23837-1:2023
MAS Technology Risk Management Guidelines	MAS	Broader technology-risk management context for the MAS quantum-risk advisory.	MAS Technology & Cyber Risk guidance

About Singapore FinTech Association (SFA)

SINGAPORE FINTECH ASSOCIATION

Singapore FinTech Association (SFA), a cross-industry, non-profit initiative, is a premier platform designed to facilitate collaboration among all market participants and stakeholders in the fintech ecosystem. Our mission is to support the development of Singapore's financial technology sector by bridging connections between startups, established institutions, and regulators to drive sustainable innovation.

For more information, please visit www.singaporefintech.org

About the SFA Cyber Security & Quantum Computing Subcommittee

The SFA Cyber Security & Quantum Computing Subcommittee comprises industry leaders who contribute their expertise and experience on a pro bono basis to strengthen and grow Singapore's cybersecurity and quantum computing ecosystem within the financial services sector.

The Subcommittee promotes awareness of quantum computing and cyber risks and their potential financial, operational and reputational impact, while encouraging the adoption of industry-recognised frameworks, standards and best practices to assess, monitor and mitigate technology-related risks.

Through engagement with regulators and industry stakeholders, fostering collaboration and knowledge sharing, supporting the growth of cybersecurity and data protection companies, and nurturing talent, the Subcommittee seeks to advance cyber resilience, support responsible technological innovation and represent the interests of the financial services ecosystem in Singapore and internationally.

Acknowledgements

We would like to extend our sincere appreciation to the following individuals for their valuable contributions, insights and support in the development of this report.



Professor Yehuda Lindell
Head of Cryptography,
Coinbase



Dr. Tan Teik Guan
Co-Founder and
Chief Executive Officer, pQCee



Petr Dvorak
Founder and
Chief Executive Officer, Wultra



Winston Chir
Independent Technology Advisor

SFA Cyber Security & Quantum Computing Subcommittee



Pramodh Rai
Chair, SFA Cyber Security &
Quantum Computing Subcommittee
and Co-founder & CEO, Cyber Sierra



Vinod Kumar Arora
Senior Vice-President,
Bank of America



Sanjeev Kumar Velayuthan
Sr. Regional Lead - Digital Identity,
ASEAN, Wultra Pte Ltd



Erika Zhang
Enterprise Account Director,
softScheck Singapore Pte Ltd



Joel Lee
CEO and Co-founder,
Protos Labs



Jay Prakash
CEO and Co-founder,
Silence Laboratories



Shishir Kumar Singh
Group Head of Information Security,
Advance Intelligence Group



Swati Sodhani
Program Lead – Subcommittees,
Singapore FinTech Association



Muralidharan Sundaramurthy
BISO, APAC,
Coinbase

© 2026 Singapore FinTech Association.
All rights reserved.

SINGAPORE FINTECH ASSOCIATION