EPA ASIA

WORKING GROUP FOUNDING MEMBERS

IBM

KPMG



FROM AWARENESS TO ACTION: WHAT QUANTUM-SAFE READINESS REQUIRES NOW

NOVEMBER 2026

From Awareness to Action: What Quantum-Safe Readiness Requires Now

A year ago, the question in many boardrooms was whether the quantum threat was real. Today, the more useful question is: are we prepared, and have we started?

In EPAA's 2025 workshops, only 20% of participants said their senior stakeholders were very familiar with the quantum threat, while 44% said they were not very familiar or not familiar at all. Those were professionals who had already chosen to attend a session on the topic.

Awareness is now moving quickly. Regulators are turning broad warnings into more concrete expectations. In July 2026, the Monetary Authority of Singapore published that it was issuing formal supervisory expectations, including progressive milestones for cryptographic inventories, migration prioritisation, and capability building. That same month, the Hong Kong Monetary Authority published its first Quantum Preparedness Index. Hong Kong's banking sector scored 2.3 out of 10. Half of authorised institutions had no structured plan for cryptographic upgrades, and half had not assessed whether technical infrastructure was ready for post-quantum security requirements. Among institutions with transition plans, the average implementation timeframe was 5.6 years. The HKMA expects the sector to achieve full readiness by 2030.

In August 2026, the US Treasury launched a Quantum-Readiness Task Force to coordinate the sector, examine the readiness of vendors and other third parties, and consider risks involving digital assets.

These findings suggest that progress begins when someone becomes accountable for quantum safe readiness, rather than presuming it as an issue for technology teams to oversee. Senior leadership needs to assign clear ownership and authorise a limited first assessment. That assessment provides the evidence needed to set priorities, engage vendors, and develop a credible roadmap.

> ***"The question is no longer whether quantum is a real issue. It is what we are learning as we progress, what is working, and what we need to do differently."***



Do not wait for a perfect inventory

The instinct may be to identify every cryptographic asset across the enterprise before making any changes. In practice, this can leave organisations mapping indefinitely while the environment continues to change.

A cryptographic inventory is a record of where and how cryptography is used across an organisation. It is not a one-off deliverable and will need to develop as systems, vendors, standards, and threats evolve. The practical approach is to build knowledge and action together.

The first assessment does not need to become a large technology programme. A small team can begin by identifying where cryptography is used within a few important systems. It can then consider the business and security risks to decide what to examine next.

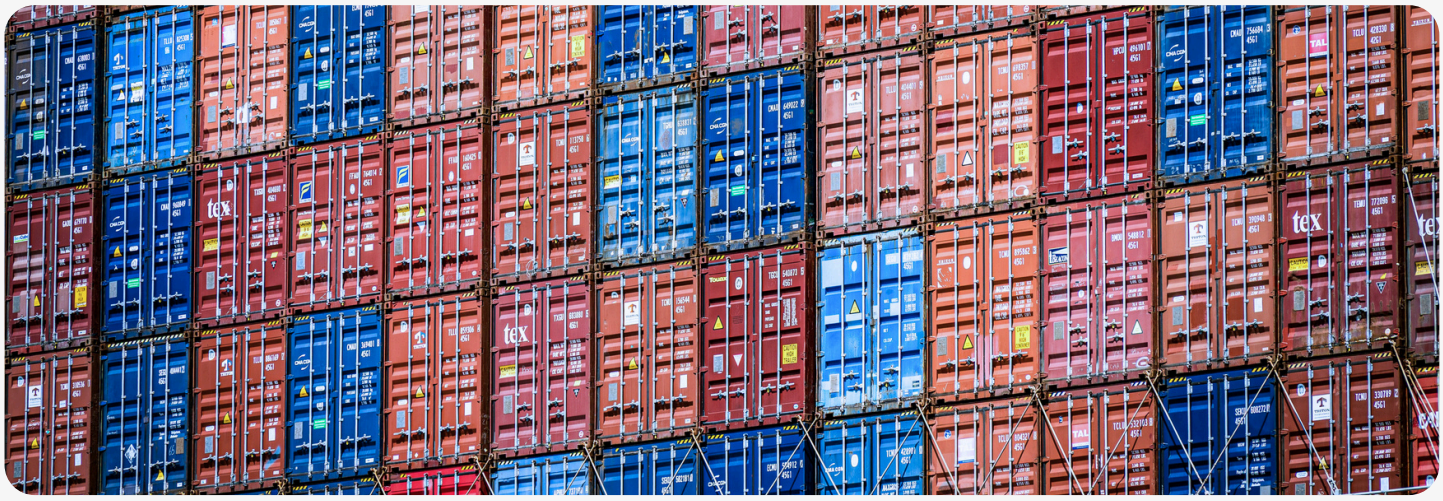
Begin with a clearly defined payment flow or service, selected according to risk and practical feasibility. Consider the consequences if its security were compromised or the service disrupted, how long its data must remain confidential, and whether its systems and dependencies can be meaningfully assessed.

Trace it from initiation through clearing and settlement. Identify where cryptography is used, which data and assets require protection, where the greatest consequences may sit, and which internal and external parties are involved.

The starting point should be informed by risk, but it must also be workable. For some organisations, the best place to start may be where the potential loss of sensitive information would be greatest. For others, it may be better to choose an area where the systems are well understood, responsibility is clear, and the relevant vendors can be readily identified.

For sensitive information, prioritisation should consider how long it must remain confidential. Information captured in encrypted form today could potentially be decrypted in the future. The relevant question is therefore whether the information will still be sensitive by the time that becomes possible, and how long it will take to upgrade the systems protecting it.

The objective is not to select one payment rail and ignore the rest. It is to create a repeatable method that can be expanded across the wider estate.



What examining one payment flow can reveal

Following one payment flow from initiation through clearing and settlement often exposes dependencies that are not visible from the payment application alone.

Identity, keys, and certificates may be the first indication. The flow may depend on public key infrastructure services, certificate authorities, hardware security module providers, certificate management tools, and outsourced cryptographic services. A useful test is whether the bank could rotate the certificates supporting the flow without coordinating with multiple third parties or clients.

Interoperability may prove more difficult than the cryptography itself. API gateways, SWIFT interfaces, network providers, and messaging platforms operate according to their own technology and upgrade cycles. Migration may therefore move at the pace of the least-ready participant exchanging signed or encrypted messages.

Vendor roadmaps can quickly become programme roadmaps. Middleware, managed services, fraud platforms, and other third-party products may contain cryptographic dependencies the bank does not control.

Shared infrastructure may become the critical path. Clearing houses, real-time gross settlement operators, payment schemes, correspondent banks, and their certification windows can ultimately determine when an end-to-end payment flow is ready to migrate. Within the institution, both the upstream and downstream flows must be reviewed as any and all technology efforts impact the business.

> ***"Quantum-safe readiness is not plug and play. Organisations cannot simply buy a solution off the shelf and expect it to work. Their partners and suppliers have a critical role to play."***

Readiness crosses organisational boundaries

Quantum-safe migration cannot be owned by the technology function alone. It requires technical and business judgement to come together. Architecture and security teams need to understand the systems and cryptographic dependencies, while business and risk leaders need to assess the operational consequences, priorities, and investment required.

> ***"One of the biggest risks is treating quantum readiness as something reserved for cybersecurity teams. It needs to be understood and addressed across the organisation."***

For a national payments infrastructure operator, migration is also a coordination challenge. Banks, payment providers, and vendors will have different capabilities and upgrade cycles. A dated roadmap should explain what each group needs to deliver, when testing and certification will be available, and how participants can migrate in stages. Common technical requirements should specify which cryptographic methods are permitted during the transition and when support for existing methods will end.

The first stage should give participants a clear and achievable entry point, such as testing a defined connection or service. Where traditional and post-quantum methods are combined, or existing and upgraded systems operate alongside each other, the operator should explain how interoperability will be maintained and how problems will be managed.

Mapping one payment flow makes these dependencies more visible. It shows why procurement, third-party risk management, and network management must be part of the readiness programme.

Organisations need to distinguish between the changes they control, those that depend on vendors or payment participants, and those that cannot proceed until shared infrastructure is ready. Without that visibility, the least-prepared participant or supplier may determine the pace of migration for everyone connected to the flow.

> ***"Legal and procurement teams need to understand what is happening. Quantum-safe migration is a long-term investment, and the regulatory and legal implications need to be considered alongside the technology."***

Act where the path is clear

Not every part of the migration has a settled answer. Some systems have a clearer route to post-quantum cryptography, while other environments may lack suitable implementations or depend on protocols that are still developing.

Organisations can still act by separating what can be changed now from what can only be prepared for. They should also identify which decisions require coordination with vendors and counterparties, and which areas must be monitored and revisited as standards mature.

Standards published by the US National Institute of Standards and Technology provide an important foundation, but organisations operating across the Asia-Pacific cannot assume that every market will adopt the same algorithms, requirements, or timetable.

This variation may not be limited to implementation timelines. Some jurisdictions may favour their own cryptographic standards or place different levels of reliance on standards developed elsewhere.

Geopolitical considerations could reinforce those differences as post-quantum requirements develop. For cross-border payments, cryptographic agility may therefore mean more than preparing for future updates. Systems may also need to support different algorithms or standards across the markets in which they operate.

What can organisations do in the next 90 days?

Appoint an accountable executive. Give that person sufficient authority to coordinate the work and bring decisions to the board. Agree initial milestones and funding for discovery and testing, with a process for developing the longer-term investment plan.

Begin targeted discovery. Use available tools to identify cryptography within a limited number of high-value systems rather than waiting for an enterprise-wide inventory.

Ask critical vendors for specific commitments. Request their post-quantum roadmaps, expected support dates, testing arrangements, and dependencies. Identify where supplier delays could affect your own migration plan and what interim measures may be needed.

Assess current readiness. Review progress across risk, governance, technology, organisational capability, and external dependencies to identify the most immediate gaps.

Review upcoming contracts. For agreements approaching renewal, consider requirements for cryptographic agility, migration support, and evidence of compatibility with your systems. Agree how suppliers will communicate changes to plans and support the transition.

"When a supplier tells you they are quantum-safe ready, how do you verify that? What evidence should organisations be asking for, and what criteria should they use to assess readiness?"

Coexistence will expose the constraints

Organisations will not move from existing cryptography to post-quantum cryptography in a single step. For a period, old and new methods will need to coexist. How that is achieved will vary according to the system, its architecture, and the capabilities of each endpoint.

Project Leap Phase 2, led by the Bank for International Settlements Innovation Hub, offers a useful illustration. The project tested post-quantum digital signatures in the Eurosystem's T2 wholesale payment environment. The cryptographic tests succeeded, and different national configurations and software libraries interoperated. However, the existing system was not designed to run the traditional and post-quantum approaches side by side without further work. Post-quantum signature verification also required materially more processing time.

The findings show why assumptions about coexistence should be tested early. Organisations should test whether their payment applications, networks, security devices, and interfaces can accommodate the key, certificate, and signature sizes of the proposed algorithms. Testing should also examine processing capacity and the ability to maintain service while participants use different configurations. A successful cryptographic test is only one part of establishing that the wider payment flow is ready.

Some of those constraints will be within an organisation's control; others will not. A readiness programme needs clear governance so that trade-offs can be identified, escalated and resolved, and decisions made about what can proceed and when.

> ***"As the industry develops tokenised payments and new payment architectures, we need to make sure quantum risks are considered from the outset, rather than becoming something we address after the infrastructure has been built."***



Ensure the capability for continued change

PQS is not a one-time investment. Maintaining security requires ongoing investment, oversight, and upkeep, with the ability to adapt as requirements change.

The longer-term goal is cryptographic agility and business security: the ability to discover where cryptography is used, replace or update it without extensive disruption, and repeat that process as standards and threats change.

Experience from a global financial messaging provider illustrates why this matters. Early in its post-quantum programme, the organisation selected cryptographic approaches that it later needed to reconsider. A migration programme must be able to accommodate changes in algorithms, standards, and implementation choices without requiring the underlying services to be redesigned each time.

This capability cannot be bought as a finished product or added after technical decisions have been made. Quantum readiness affects architecture, operating processes, supplier relationships, governance, and the people who understand how payment services work in practice. Organisations need to build resilience into technology decisions from the outset and retain the expertise required to adapt.

The cost of waiting is therefore not only a larger or more expensive migration later. As new security requirements are implemented across the payments ecosystem, organisations that cannot accommodate them may become a constraint on their partners or be unable to interoperate with new infrastructure.

Quantum-safe readiness does not require every answer to be available today. It does, however, require someone to take responsibility, choose a practical place to begin, and identify the dependencies that may affect progress. Starting with a limited payment flow allows the organisation to develop an approach that can expand as it learns, while standards, technologies, and regulatory expectations continue to evolve.

Quantum in a global ecosystem

Quantum readiness cannot be addressed in isolation. We are asking organisations to collaborate across regions, sectors, and the many participants involved in moving money and data, while adapting to other technological changes.

For executives, understanding the upstream and downstream effects of a cryptographic migration means considering how AI, cyber threats, and regulation are changing the same systems. As organisations introduce AI models and agents into payment processes, they need to identify any cryptographic dependencies those changes introduce and keep their inventory current.
This requires coordination within organisations and with the partners, providers, and networks they depend on across the global ecosystem.

EPAA members were involved in the development of this white paper through the working group process. However, any views expressed in this white paper are solely the views of EPAA and do not necessarily represent the views of individual working group members, their organisations, EPAA Ambassadors or EPAA Members.

Working Group Founding Members

Working Group Members

- Alastair Thompson - KPMG
- Alejandro Montblanch - HSBC
- Amaanie Hakim - Idemia
- Andreas Deppeler - Monash Univeristy
- Ankit Shah - KPMG
- Anton Ruddenklau - KPMG
- Avij Kumar - PayPal
- Bing Zhu - HSBC
- Camilla Bullock - EPAA
- Clarissa Ai Ling Lee - Monash Univeristy
- Cody Kieltyka - Australian Payments Plus (AP+)
- Danelle Denny - EPAA
- James Hutton - IBM
- Jasper Poos - CBA
- Jianing Song - KPMG
- John Buselli - IBM
- John Yuen - Monash Univeristy
- Katherine Brown - Australian Payments Plus
- Kyle Harrison - KPMG
- Lory Thorpe - IBM
- Markus Hasibuan - Idemia
- Mary Ann Francis - EPAA
- Maxim Neshcheret - CMA
- Maxwell Denega - Quantum Chain
- May Lam - Australian Payments Plus
- Michael Egan - KPMG
- Monica Jasuja - EPAA
- Phoram Mehta - Paypal
- Pieter Bos - CBA
- Preetpal Walia - CBA
- Ray Harishankar - IBM
- Reggie Kartha - IBM
- Ricardo Toledo - Quantum Chain
- Sacha Hess - Paypal
- Sebastien Rousseau-Bedouch - HSBC
- Shilpa Shetty - IBM
- Umut Cikla - IBM
- Vikas Phogat - Idemia
- Waqas Khalid Obeidy - PayNet
- Will Collison - HSBC

Appendix: Post-Quantum Cryptography Guidance and Reference Resources

From Awareness to Action: What Quantum-Safe Readiness Requires Now

Government guidance, regulatory publications, technical standards, financial-sector research and industry resources relevant to post-quantum cryptography migration. Resources are grouped by issuing organisation and publication type.

A. Government and National Cybersecurity Authorities

Australian Signals Directorate (Australia) — Planning for Post-Quantum Cryptography
Open publication

Canadian Centre for Cyber Security — Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada (ITSM.40.001)
Open publication

UK National Cyber Security Centre — Timelines for Migration to Post-Quantum Cryptography
Open publication

NIST — Migration to Post-Quantum Cryptography, NIST SP 1800-38 (Preliminary Draft)
Open publication

NIST — Transition to Post-Quantum Cryptography Standards, NIST IR 8547 (Draft)
Open publication

Taiwan, Post-Quantum Cybersecurity Industry Alliance and Institute for Information Industry — Post-Quantum Cryptography Migration Guidelines (後量子密碼遷移指引), April 2025; government-supported industry guidance
Open publication

CRYPTREC (Japan) — Cryptographic Technology Guidelines (Post-Quantum Cryptography), 2024 edition, published April 2025
Open publication

CRYPTREC (Japan) — Survey of Technology Trends in Migration to Post-Quantum Cryptography (2025)
Open publication

B. Central Banks and Financial Regulators

Monetary Authority of Singapore — Advisory on Addressing the Cybersecurity Risks Associated with Quantum (MAS/TCRS/2024/01, February 2024)
Open publication

MAS and Banque de France — Post-Quantum Cryptography: Quantum-Safe Experiment Report (2024)
Open publication

Hong Kong Monetary Authority — Quantum Preparedness of Hong Kong's Banking Sector (July 2026)
Open publication

Bank of Thailand — Emerging Payment Technologies: Post Quantum Cryptography
Open publication

Bank of Japan, Institute for Monetary and Economic Studies — Toward the Realisation of Quantum-Resistant Systems: Initiatives and Recommended Responses in the Financial Sector (April 2026); Japanese-language research
Open publication

C. Global Financial-Sector and Payment System Organisations

Bank for International Settlements — Quantum-Readiness for the Financial System: A Roadmap (2025)
Open publication

BIS Innovation Hub — Project Leap Phase 2: Quantum-Proofing Payment Systems (2025)
Open publication

G7 Cyber Expert Group — Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector (January 2026)
Open publication

FS-ISAC — Preparing for a Post-Quantum World by Managing Cryptographic Risk
Open publication

PCI Security Standards Council — FAQ 1491: TLS and Strong Cryptography
Open publication

SIFMA — Quantum Migration: Mapping the Emerging Landscape (October 2025)
Open publication

D1. Research Agencies and Independent Organisations

CSIRO (Australia) — Planning the Cyber Quantum-Safe Transition for Australia's Financial Sector: A National Use Case (2026)
Open publication

CSIRO (Australia) — The Quantum Safe Transition: Reality, Hurdles and Pathways (2025)
Open publication

AIVD, CWI and TNO (Netherlands) — The PQC Migration Handbook (2024)
Open publication

ENISA — Post-Quantum Cryptography: Integration Study
Open publication

Jiangsu Financial Society (China) — Guidelines for Quantum-Resistant Cryptography Migration Management in the Banking Industry (T/JPSFFB 001—2026); 银行业抗量子计算密码迁移管理指南
Open publication

Xi'an Jiaotong-Liverpool University — Global Financial Banking Post Quantum Security Migration White Paper (2025)
Open publication | Additional link

D2. International Standards and Technical Specifications

NIST — FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (2024)
Open publication

NIST — FIPS 204: Module-Lattice-Based Digital Signature Standard (2024)
Open publication

NIST — FIPS 205: Stateless Hash-Based Digital Signature Standard (2024)
Open publication

ETSI — TR 104 016: A Repeatable Framework for Quantum-Safe Migrations
Open publication

ETSI — TS 103 744: Quantum-Safe Hybrid Key Establishment, V1.2.2 (February 2026)
Open publication

ETSI — TR 103 619: Migration Strategies and Recommendations to Quantum-Safe Schemes (2020)
Open publication

IETF — RFC 10024: Post-Quantum Traditional Hybrid Key Agreement Mechanisms for TLS 1.3 (2026)
Open publication

IETF — RFC 9954: Hybrid Key Exchange in TLS 1.3 (2026)
Open publication

IETF — RFC 9958: Post-Quantum Cryptography for Engineers (June 2026)
Open publication

E1. EPAA Member Publications

IBM Quantum — IBM Quantum Safe Roadmap
Open publication | Additional link

IBM Research — Quantum Threat and Quantum-Safe Migration
Open publication

Mastercard — Migration to Post-Quantum Cryptography (2025)
Open publication

KPMG — What Is the Cyber Security Risk from Quantum Computing?
Open Publication

PwC — Preparing for Q-Day: The Business Imperative Leaders Can't Afford to Delay
Open publication

Amazon Web Services — Migrating to Quantum-Resistant Cryptography
Open publication

E2. Other Industry Publications

Palo Alto Networks — NIST PQC Migration: Strategies, Steps, Standards and Tips
Open publication

Palo Alto Networks — What Is Post-Quantum Cryptography (PQC)?
Open publication

Cisco — Getting Started on Your Post-Quantum Cryptography Journey (infographic)
Open publication

Cloudflare — Post-Quantum Cryptography (developer documentation)
Open publication

F. Academic Research on PQC Migration in Financial Services

Muzenda & Ndlovu (2026) — Post-Quantum Migration in the Financial Sector: A Systematic Review of Readiness, Risks, and Transition Frameworks
Open publication

Kuka, Muhyaddin, Teh & Davies (2026) — Global Roadmaps for Post-Quantum Era in Finance: Policies, Timelines, and a Pragmatic Playbook for Migration
Open publication

Nellipudi (2025) — Cryptographic Agility for Real-Time Payment Systems: A Post-Quantum Architecture and Performance Evaluation
Open publication

Jančiūtė (2025) — Cybersecurity in the Financial Sector and the Quantum-Safe Cryptography Transition: In Search of a Precautionary Approach in the EU Digital Operational Resilience Act Framework
Open publication

2026 research article — Securing Financial Transactions in the Quantum Era: A Critical Review of Hybrid Cryptographic Innovations
Open publication

G. EPAA Quantum Safe Cryptography Working Group Publications

EPAA (2026) — Quantum Risk in Payments: Defining Responsibility and Action — EPAA Connect roundtable pre-read
Open publication

EPAA (2025) — Quantum Safe Payments: Why the Payments Industry Must Act Now — QSC Working Group white paper
Open publication

EPAA (2025) — Challenges the Payments Industry Faces in Migrating to Quantum Safe Cryptography
Open publication

EPAA (2025) — Quantum Mythbusters — educational series
Open publication

EPAA (2024) — The Road to Quantum Safe Payments — executive briefing note
Open publication

EPAA (2023) — Quantum Safe and Payments — roundtable report
Open publication

Further EPAA resources: EPAA Quantum Safe Cryptography Working Group



EPA ASIA

The Emerging Payments Association Asia (EPAA) is a leading industry platform shaping the agenda for payments across Asia Pacific.

EPAA convenes members and organisations across the payments ecosystem to turn industry priorities into action through collaboration, policy engagement and thought leadership. Through Working Groups, industry forums, roundtables and collaborative outputs, EPAA provides a platform for organisations to contribute expertise, influence discussion and shape frameworks defining what comes next across the region's payments landscape.

This paper provides general information. It does not constitute legal, financial or professional advice, and should not be relied upon as such. While care has been taken in preparing this material, EPAA and the authors make no representations or warranties as to its accuracy, completeness or currency.

CONTACT US