Quantum-Safe Readiness: A First-Assessment Checklist for Payment Firms

20 steps from awareness to action, built on the EPAA's November 2026 white paper

Sebastien Rousseau

November 2026

Contents

Quantum-Safe Readiness: A First-Assessment Checklist **1**
Why this matters . . . 1
Section A: Ownership . . . 2
Section B: Scope the first assessment . . . 2
Section C: Trace the flow end to end . . . 2
Section D: Sort what you find . . . 3
Section E: Vendors and contracts . . . 3
Section F: Cross-border and agility . . . 3
Section G: Report and repeat . . . 3
If you operate payments infrastructure . . . 3
Sources . . . 4

Quantum-Safe Readiness: A First-Assessment Checklist

20 steps from awareness to action for banks, payment providers and the vendors that serve them.

Why this matters

Supervisors have stopped treating post-quantum cryptography as a research topic. In July 2026 the **Monetary Authority of Singapore** published that it was issuing formal supervisory expectations, with progressive milestones for cryptographic inventories, migration prioritisation and capability building.

Hong Kong's banking sector scored **2.3 out of 10** on the Quantum Preparedness Index. Half of authorised institutions had no structured plan for cryptographic upgrades. Institutions that did have plans reported an average implementation timeframe of **5.6 years**, and the **HKMA expects full readiness by 2030**.

The EPAA's white paper, *From Awareness to Action: What Quantum-Safe Readiness Requires Now*, argues that firms don't get there by finishing a cryptographic inventory first. They get there by naming an accountable executive, tracing one payment flow end to end, and letting what the trace reveals about vendors, counterparties and shared infrastructure decide what comes next.

This checklist turns that approach into a tracker a team can work through. It is my own reading of the paper, not an EPAA publication.

Section A: Ownership

1. Name an accountable executive. One person, with enough authority to coordinate architecture, security, procurement and risk teams and to bring decisions to the board. An owner who can't convene those teams has a title and nothing else.

2. Authorise a limited first assessment. Not a multi-year programme. A bounded piece of discovery whose purpose is to produce the evidence needed to set priorities, engage vendors and build a credible roadmap.

3. Put business and risk leaders in the room. Architecture and security teams understand the systems and their cryptographic dependencies. Business and risk leaders weigh the operational consequences, priorities and investment. Neither can do the other's half.

4. Record who owns which decision. Write down which decisions sit with the accountable executive, which go to the board, and which belong to procurement and third-party risk. The dependencies in Section D land on their desks, not only on the technology team's.

Section B: Scope the first assessment

5. Don't make the full inventory a gate. An inventory is never finished: it changes as systems, vendors, standards and threats change. Treat it as something that grows with the work, not a precondition for starting.

6. Pick a few high-value systems. Use available tools to identify where cryptography is used in a limited number of important systems, rather than waiting for an enterprise-wide inventory.

7. Choose one payment flow. Select a clearly defined flow or service by **risk** (where exposure justifies the effort) and **feasibility** (so the first attempt doesn't collapse under its own ambition). Flows that carry sensitive data come early: information captured in encrypted form today could potentially be decrypted in the future.

8. Write down the method as you go. The goal is not to fix one rail and ignore the rest. It is a repeatable method. Keep the questions you asked, the people you needed and the places where the trail went cold.

Section C: Trace the flow end to end

9. Follow it from initiation through clearing and settlement. An application inspected on its own shows its own cryptography. The whole flow shows everything the application relies on and everyone it talks to.

10. Ask the certificate-rotation question. *Could we rotate the certificates supporting this flow without coordinating with multiple third parties or clients?* If the answer is no, you've found a dependency.

11. List every third-party product in the path. Middleware, managed services, fraud platforms and other third-party products may contain cryptographic dependencies you don't control.

12. List every external participant. Clearing houses, RTGS operators, payment schemes and correspondent banks, with their certification windows. They can decide when an end-to-end flow is ready to

migrate.

Section D: Sort what you find

13. Put each finding in one of three buckets.

- **We control it**: a planning problem.
- **It depends on a vendor or payment participant**: a negotiation.
- **It waits on shared infrastructure**: a waiting game where the right response is preparation.

14. Separate "change now" from "prepare for". Some systems have a clear route to post-quantum cryptography. Others lack suitable implementations or depend on protocols still being developed. For those, prepare: know what's affected and what it depends on, so you aren't starting from zero when a route exists.

15. Find your least-ready participant. Signed or encrypted messages move at the pace of the least-ready party exchanging them. Name that party for the traced flow.

Section E: Vendors and contracts

16. Ask critical vendors four questions. Their post-quantum roadmap, expected support dates, testing arrangements, and their own dependencies.

17. Use the next renewal. For contracts approaching renewal, consider requirements for cryptographic agility, migration support and evidence of compatibility with your systems, while the contract is still open.

Section F: Cross-border and agility

18. Don't assume one standard everywhere. NIST standards are an important foundation, but firms operating across Asia-Pacific can't assume every market will adopt the same algorithms, requirements or timetable.

19. Design for running algorithms side by side. For cross-border payments, cryptographic agility may mean supporting different algorithms or standards in different markets at the same time, not only swapping one algorithm for another later.

Section G: Report and repeat

20. Take the findings to the board, then pick the next flow. Report the named owner, the first findings, the vendor answers and any contract language. Each one feeds the next round of questions. Repeat the method on the next flow.

If you operate payments infrastructure

Scheme and infrastructure operators also have a coordination job, because participants have different capabilities and upgrade cycles. The paper asks operators for:

- a **dated roadmap**: what each group delivers, when testing and certification open, and how participants migrate in stages;
- **common technical requirements**: which methods are permitted during the transition and when support for existing methods ends;
- a **clear first entry point**, such as testing one defined connection or service;
- an explanation of how **hybrid and parallel running** will work.

Sources

- Emerging Payments Association Asia (2026). *From Awareness to Action: What Quantum-Safe Readiness Requires Now.* EPAA Quantum Safe Cryptography Working Group. Free to download: https://emergingpaymentsasia.org/wp-content/uploads/2026/11/From-Awareness-to-Action-What-Quantum-Safe-Readiness-Requires-Now.pdf
- My full reading of the paper: https://sebastienrousseau.com/2026-11-16-quantum-safe-readiness-epaa/

I'm a member of the EPAA Quantum Safe Cryptography Working Group. This checklist is my own reading of the paper. The paper's views are EPAA's, and neither the paper nor this checklist necessarily represents the views of individual working group members or their organisations. Errors are mine.

Sebastien Rousseau, November 2026
https://sebastienrousseau.com