

Coordinating with an indefinite future

Why waiting for certainty on quantum computing creates systemic risk

OLIVER WYMAN
A MARSH BUSINESS

Quantum computing readiness is not an institution-by-institution exercise. When the time comes, central banks around the world will have to determine whether critical financial services, shared providers, and cross-border infrastructures can migrate together. Based on current evidence, few in the financial world seem ready: Almost three-quarters of Swiss institutions have not planned or implemented any quantum-related measures, and Hong Kong's banking sector scored 2.3 out of 10 in the sector's first Quantum Preparedness Index.

The lack of preparation is probably not surprising, given the uncertainty of the quantum timetable. It could be ready to scale five years from now or 10. But what should motivate central banks and the sector are estimates that it could take institutions anywhere from five to 10 years to build the necessary infrastructure.

Quantum computing is different from classical computing and is not a general replacement for classical systems. For finance, it creates two distinct agendas. Computational applications in optimization, simulation, and machine learning merit continued experimentation but remain exploratory and longer-term. On the other hand, cryptographic resilience presents a different challenge. A sufficiently capable quantum computer could compromise widely used public-key cryptography, while replacing that cryptography across the financial system will take many years. The greatest risk, therefore, is not simply that a quantum computer arrives earlier than expected, but that institutions begin preparing too late for a transition that will itself be lengthy and complex. Given the uncertainty around when the threat will materialize — and the long lead time required to address it — this article focuses on the agenda that requires decisions and action today.

For critical financial services, quantum readiness is an end-to-end system property because no bank, payment infrastructure, or technology provider controls the full transaction chain. An institution may upgrade its own systems and still be unable to authenticate a payment, settle a transaction, or connect securely if a shared provider, financial market infrastructure, or cross-border counterparty is not ready.

For central banks, this systemwide dependency creates a challenge for governors who must answer the critical question of whether the financial system can make a coordinated transition safely and in time. The real test will not be whether individual institutions are prepared, but rather whether critical services, shared providers, and cross-border infrastructures can migrate without losing interoperability or continuity.

The real test of quantum readiness is not whether individual institutions are prepared, but whether critical services, shared providers, and cross-border infrastructure can migrate without losing interoperability or continuity.

© Oliver Wyman

FOUR QUESTIONS DETERMINE WHETHER THE FINANCIAL SYSTEM CAN MAKE A COORDINATED TRANSITION SAFELY AND IN TIME

1. What turns delay into systemic risk?

Identify which critical services and transaction chains face the greatest mismatch between information lifetime, migration lead time, and dependency readiness, and understand why fragmented preparation can leave the system unready before the threat date is known.

2. How does quantum risk become a financial stability risk?

Trace how the loss of confidentiality, authenticity, or secure access could impair payments, settlement, supervisory judgment, market confidence, and operational control.

3. Can migration plans work together?

Assess whether institutions, financial market infrastructures, shared providers, and cross-border counterparties have compatible standards, timelines, testing, and fallback arrangements, and where their roadmaps could fail to align.

4. What does coordination look like in practice?

Clarify who owns systemwide readiness and how common milestones, comparable evidence, collective testing, and escalation mechanisms will identify and resolve sequencing conflicts.

These four questions guide the analysis. Section 1 explains how the combination of an uncertain threat date, long migration lead times, and fragmented preparation turns delay into systemic risk. Section 2 examines how a loss of cryptographic protection could create financial stability risk. Section 3 tests whether migration plans across institutions, infrastructures, providers, and borders can work together. Section 4 considers the practical requirements of effective coordination in practice. Section 5 translates the answers into four decisions governors cannot delegate.

Taken together, the overarching question and four supporting questions point to the core issue: quantum readiness is fundamentally a financial stability and coordination problem, not a technology problem. Central banks and relevant financial authorities are uniquely placed to set common expectations, demand evidence, coordinate end-to-end testing, and resolve systemwide dependencies. They do not need to prescribe every cryptographic choice; they do need to know whether the system can migrate safely, coherently, and on time.

© Oliver Wyman

1 | What turns delay into systemic risk?

The first question is what turns delay into systemic risk. The answer lies in the mismatch between when exposure begins, when the threat may materialize, and how long migration takes. A cryptographically relevant quantum computer (CRQC) could eventually defeat widely used public key algorithms. No one can date its arrival with confidence, but the work required to replace those algorithms is already visible: cryptographic discovery, target architecture, provider support, testing, coexistence, migration, and retirement.

Official roadmaps already reflect that mismatch. The National Institute of Standards and Technology (NIST) and Bank of International Settlement (BIS) both call for early, phased migration: NIST has finalized the first core post-quantum standards, while BIS describes migration as a multiyear program. The UK National Cyber Security Centre expects planning by 2028, migration of the highest-priority systems by 2031 and broad completion by 2035. The European Union has similarly called for transition to begin by the end of 2026, with critical infrastructure migrating by 2030.

Dates are no longer in the distant future, given EU calls for transition to begin this year and critical infrastructure to migrate by 2030. In the coming months, planning must become execution, and the available evidence suggests most of the financial system is not yet at that point.

Understanding what turns delay into systemic risk requires three timelines rather than a single arrival-date forecast. The exposure clock is already running because encrypted information can be collected today and retained for decryption in the future.

The technology clock remains uncertain because no one knows when a CRQC will become operationally viable. The migration clock is measured in years because institutions must locate vulnerable cryptography, agree with new designs, secure provider support, test interoperability and performance, and migrate critical systems without disrupting services.

The clocks do not move in sequence. Together, they create a timing mismatch. By the time the threat is certain, the safest window for an orderly transition may have narrowed. Moving too late leaves vulnerable mechanisms in place; moving in a fragmented way can itself disrupt authentication, payments, and settlement. Central banks do not need to predict the arrival date. They need to use the available lead time to protect long-lived information, avoid new vulnerable dependencies, and align migration with technology-renewal cycles.

The practical stance is to prepare now and migrate proportionately. Governance, cryptographic discovery, assessment of long-lived information, mapping of critical transaction chains and shared dependencies, provider engagement and crypto-agility are low-regret actions. Larger migration waves should be driven by information lifetime, service criticality, migration lead time, technology-refresh cycles, and provider readiness - not by a prediction of Q-day.

The supervisory evidence shows why the governor-level question cannot yet be answered with confidence. Authorities need comparable information that distinguishes awareness from executable readiness; surveys suggest baselines are still missing.

© Oliver Wyman

THE READINESS GAP IS MEASURABLE, NOT HYPOTHETICAL

The gap between what needs to get done and executable readiness is already visible. In July 2026, the Hong Kong Monetary Authority reported a Quantum Preparedness Index score of **2.3 out of 10 for its banking sector.** Around half of authorized institutions had no structured plan; among those with plans, the average implementation timeframe was **5.6 years.** About 50% had not assessed their technical infrastructure migration readiness.

The authority intends to refresh the index and work toward full sectoral readiness by 2030. The index scores four dimensions: awareness, planning, pilots, and practical preparedness. Around **68%** of banks showed awareness or had reached planning or piloting, while **32%** had not begun. Around half had discussed quantum at the board level, and about a third had started exploring or piloting.

The authority attributes the gap to the absence of established risk-assessment methodologies and industry-standard frameworks, the technical complexity of building cryptographic inventories, legacy infrastructure and technical debt, uncertainty over standards and regulatory timelines, and a shortage of expertise.

A European supervisor reports the same pattern. FINMA surveyed 60 authorized banks, insurance companies, managers of collective assets, and financial market infrastructures between November 2025 and January 2026. Around two-thirds expect to be directly affected by quantum cyber risks within seven years, and around two-thirds expect that within 10 years at the latest a quantum computer will break RSA-2048 within 24 hours.

Yet **72%** had not planned or implemented any measures relating to quantum-safe encryption, only **8%** had a specific roadmap, and **43%** had not yet decided when to produce one. At the same time, **76%** saw high value in a cryptographic inventory, and **73%** considered crypto-agility important or very important. FINMA now recommends a post-quantum cryptography (PQC) roadmap by mid-2027 at the latest.

An earlier market survey points the same way. In a Bank of Finland survey of around 30 financial institutions in early 2025, **80%** said they were monitoring quantum developments from an information security perspective, but only half had identified the business-critical functions or systems that could be affected, and just under half had planned a cryptographic inventory without yet starting one. Only about **10%** had run any test or trial. Where innovation teams existed, the average effort was **under one person-year.** One-third could not estimate how long a transition would take.

These findings show three distinct gaps: awareness without discovery, plans without capability, and timelines without evidence.

Source: Hong Kong Monetary Authority, Whitepaper on Quantum Preparedness of Hong Kong's Banking Sector and first Quantum Preparedness Index, 27 July 2026.

Sources: FINMA Guidance 05/2026, Quantum computing, 9 July 2026; Bank of Finland, Quantum computing is coming — Is the financial sector ready? 26 August 2025, a voluntary survey of approximately 30 respondents whose authors write in a personal capacity.

© Oliver Wyman

2 | How quantum risk becomes a financial stability risk

The second question is how quantum risk could translate into financial stability risk. The financial system uses public-key cryptography to protect sensitive information, verify identities and instructions, secure software, and establish trusted connections. A failure can undermine more than confidentiality: It can call into question whether a payment is genuine, whether software is trusted, whether a counterparty is who it claims to be, and whether critical systems can be accessed safely.

Because these functions are shared across institutions and infrastructures, the consequences can propagate quickly. Payment and settlement infrastructures process high-value transactions continuously; even a temporary loss of trust in certificates, signatures or secure connections could impair liquidity, settlement, and market operations. Common protocols and shared providers can then amplify disruption across institutions and borders. The risk unfolds through three distinct channels.

Waiting creates systemic risk because the financial system cannot first observe the threat and then migrate safely. The transition itself must preserve trust and continuity across institutions, infrastructures, and providers while vulnerable and quantum-safe mechanisms coexist.

Exhibit 1: Quantum risk can undermine confidentiality, authenticity, and operational control

Harvest now, decrypt later	Authentication and identity spoofing	Quantum-enabled lateral movement
Attackers capture encrypted information today and store it. A future CRQC could break vulnarable public-key protection and expose information that is still sensitive.	Breaking vulnerable certificates and digital signatures could allow attackers to impersonate trusted parties, forge financial instructions, or sign malicious software undetected.	Breaking the public-key mechanisms that protect secure connections could give attackers access to internal networks and critical systems.

Source: Oliver Wyman analysis

Exhibit 1 shows how quantum risk could translate into financial stability risk by distinguishing three channels. The first channel is already active: adversaries can capture encrypted information today and retain it for decryption in the future. The other two depend on a CRQC: vulnerable certificates and digital signatures could be forged, while compromised authentication or key-exchange mechanisms could provide access to internal networks and critical systems.

© Oliver Wyman

Not every quantum-enabled breach would be systemic. The risk becomes a financial stability concern when a common cryptographic weakness — or a poorly coordinated replacement of it — affects multiple critical services at the same time. Financial institutions and infrastructures rely on many of the same public-key algorithms, certificate chains, messaging protocols, and specialist providers. Their correlated compromise, or incompatible migration, could interrupt authentication and settlement across multiple participants, generate liquidity and confidence effects, and force simultaneous remediation. Quantum therefore introduces the possibility of a common-mode failure in the financial system's trust layer, in addition to familiar cyber and third-party risks.

Each channel can translate a technical failure into a mandate-level problem for central banks. Long-lived policy and supervisory information may remain sensitive beyond its current protection; forged identities or instructions could undermine payment authentication and settlement finality; and compromised communications could affect market, reserve, and supervisory operations. The scenario below shows how the confidentiality channel could become a market event years after interception.

ILLUSTRATIVE SCENARIO: TODAY'S SUPERVISORY INFORMATION BECOMES TOMORROW'S MARKET EVENT

A central bank and a supervised institution exchange confidential information during a period of stress. An adversary captures the encrypted communications but cannot read them today. Years later, quantum-enabled decryption exposes details of capital vulnerabilities, liquidity assumptions, supervisory assessments, and possible contingency actions while they remain commercially or market sensitive.

Selective disclosure could undermine market confidence or intensify pressure on the institution. Knowledge of supervisory methods and contingency plans could also constrain future judgement and crisis response. Institutions may become less willing to communicate candidly if they doubt that supervisory information will remain confidential.

The financial stability exposure begins when the information is intercepted, not when the quantum computer arrives.

© Oliver Wyman

3 | The system readiness test: Can migration plans work together?

The third question is whether migration plans can work together across the full transaction chain. That cannot be assessed, institution by institution. The transition to post-quantum cryptography affects certificates, digital signatures, key exchange, hardware security modules, protocols, applications, and third-party products — all while critical financial services continue to operate. Operationally, it resembles a real-time gross settlement modernization or ISO 20022 migration: a multiyear ecosystem transformation. Unlike those programs, however, the deadline is uncertain, and every link in the transaction chain must continue to trust the others throughout.

A central bank has two related responsibilities: migrating its own internal and operated systems and orchestrating systemwide readiness across supervised institutions, financial market infrastructures, and critical providers. This article focuses on the second, while treating internal migration as one workstream within the same program.

Institutional readiness

Can each institution change its own systems and controls?

Dependency readiness

Can critical providers and counterparties support the change?

System readiness

Can the end-to-end transaction chain migrate without losing interoperability or continuity?

The three levels are cumulative rather than competing tests. Institutional readiness shows whether each participant can change its own systems and controls; dependency readiness shows whether providers and counterparties can support the transition; system readiness is the governing test — whether the end-to-end transaction chain can migrate without losing interoperability, continuity, or trust. The first two are necessary inputs; only system readiness answers whether migration plans can work together.

System readiness is not the sum of institutional readiness. No participant controls the full transaction chain. If institutions and providers adopt incompatible solutions or move on different timelines, systems may no longer recognize or trust one another. Payment instructions could fail to get validated, performance could deteriorate, and temporary workarounds could introduce weaker controls. Individual readiness is necessary, but it is not sufficient; the governing test is whether the transaction chain can migrate.

That has a distributional consequence that is easy to miss. Large institutions can fund discovery, target architecture, and testing from their own budgets. Midsize banks, custodians, clearinghouses, and national payment operators often cannot, and in many cases have neither the specialist staff nor a supervisory prompt to begin. Because the chain migrates at the pace of its least-ready participant, capability at the weaker end of the chain is a systemic variable rather than a question of fairness. Shared tooling, common templates, and pooled expertise improve system readiness faster than they improve any single institution.

© Oliver Wyman

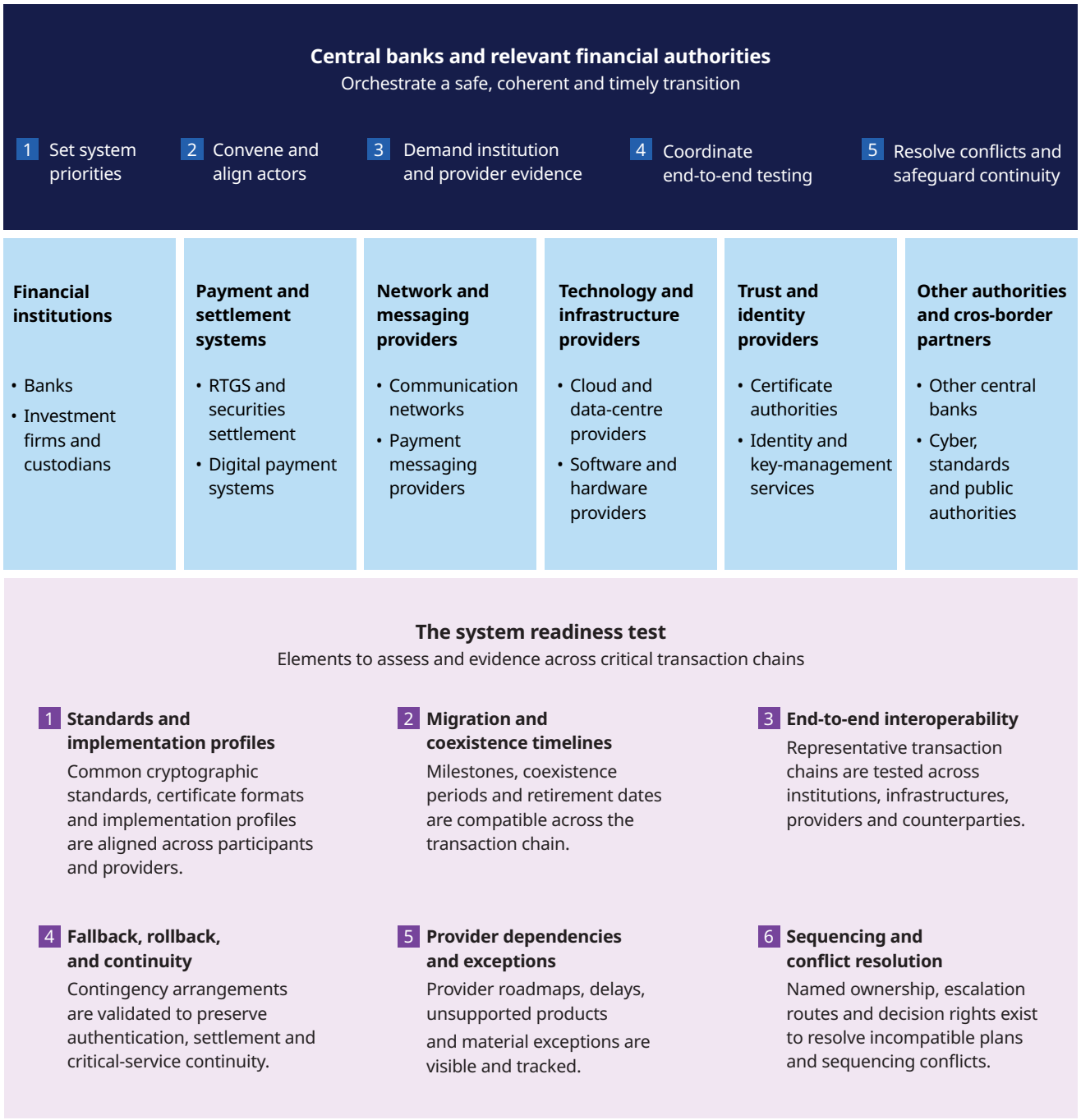
Dependency readiness also has a concentration dimension. If the system migrates onto a small number of hardware security modules, public-key infrastructure, and post-quantum library providers, a cryptographic single point of failure will have been replaced by a commercial one. Open tooling, vendor-neutral procurement guidance, and interoperability testing across competing implementations are practical mitigations. FINMA notes that migration creates dependencies on external service providers, who must themselves move to quantum-safe cryptography, and that responsibility for an outsourced function remains with the outsourcing institution in all cases. It recommends making crypto-agility a prerequisite for all new outsourcing arrangements in software and data and incorporating it into existing arrangements at the earliest opportunity. In its survey, 60% of institutions were already in contact with software suppliers or planned to be, which is the one dependency-readiness metric a supervisor can collect immediately.

Exhibit 2 sets out six elements a central bank should assess to determine whether migration plans can work together across critical transaction chains. These are standards and implementation profiles; migration and coexistence timelines; end-to-end interoperability; fallback, rollback, and continuity arrangements; provider dependencies and exceptions; and sequencing and conflict-resolution mechanisms. Together, they provide a regular system-level readiness view — not a collection of disconnected institution-level updates.

Individual readiness is necessary, but it is not sufficient; The governing test is whether the transaction chain can migrate.

© Oliver Wyman

Exhibit 2: Central bank system-readiness test



Source: Oliver Wyman analysis

© Oliver Wyman

4 | What coordination looks like in practice: convene, require, disclose

Central banks are not starting from an empty field. NIST has standardized the first algorithm. BIS has published a quantum-readiness roadmap and, through Project Leap, tested quantum-safe communication in payment contexts. The European Commission and the NIS Cooperation Group have issued a coordinated implementation roadmap.

In January 2026, the G7 Cyber Expert Group, which advises G7 finance ministers and central bank governors, published a coordinated roadmap for the financial sector's transition, stating explicitly that it sets neither guidance nor regulatory expectations.

In the same month, Europol, cybersecurity nonprofit FS-ISAC, and the Canadian Forum for Digital Infrastructure Resilience published a risk-based method for prioritizing migration activities in financial services, following an earlier call to action from Europol's Quantum Safe Financial Forum. In August 2026, the US Treasury launched a Quantum-Readiness Task Force spanning government, institutions, infrastructures, and providers. Operational resilience frameworks, such as the EU Digital Operational Resilience Act, already provide levers for third-party assurance and reporting. What is missing is not standards, research, or convening. It is a system-level readiness view: no authority yet publishes whether the migration plans of the institutions, infrastructures and providers in its own jurisdiction can work together.

The final analytical question is what coordination looks like in practice. The immediate issue is ownership: who sees the whole chain, and who can resolve a conflict when plans diverge? Existing efforts provide standards, roadmaps, and component-level tests, but they do not assign a single owner for end-to-end transaction-chain readiness. The gap is most visible across borders: an early-moving jurisdiction cannot retire vulnerable mechanisms while a critical counterparty still depends on them, and there may be no single operator able to mandate a common cutover.

Convene, require, and disclose are three practical instruments for building that systemwide view and turning identified conflicts into action.

© Oliver Wyman

Exhibit 3: Three instruments are available to build that layer

		Limit	Delivers
1	**Convene** A standing sector platform of central banks, supervisors, infrastructures, major institutions, cybersecurity authorities and vendors.	Voluntary, so uptake is uneven without a follow-on instrument.	Common crypto-inventory method, comparable milestones, shared pilots, published playbooks.
2	**Require** Supervisory expectations for systemic institutions and infrastructures: completed inventories, migration plans by a fixed date, progress reported through existing supervisory dialogue.	Narrow scope; needs proportionality and technical support to avoid compliance activity that does not reduce risk.	Accountability where systemic exposure is largest.
3	**Disclose** A standardised, non-binding readiness reporting framework, comparable to climate and cyber risk disclosure.	No minimum standard; value depends on comparability of the underlying data.	Aggregate system-level visibility and board-level attention.

Source: Oliver Wyman analysis

None of the three instruments is hypothetical any longer. Rung one is occupied, by the G7 roadmap, the Europol and FS-ISAC prioritization work, and the new US Treasury task force, although the newest of these launched without a published membership, budget, deliverables, or enforcement mechanism.

Rung two is arriving. FINMA recommends that Swiss institutions prepare a PQC roadmap by mid-2027 and give the topic greater prominence in ongoing supervision. MAS has said it will issue formal supervisory expectations, aiming for sector-wide quantum resilience before the decade ends. The Bank of Israel required transition preparedness plans from banks by January 2026. The HKMA is pairing its index with a post-quantum toolkit and workshops, targeting full sectoral readiness by 2030. Rung three, comparable public disclosure, is not yet in use anywhere.

Used together, the three instruments move the system from voluntary coordination toward comparable evidence, targeted accountability and, eventually, transparent system-level reporting. Together, they provide evidence needed to answer the four questions. The next step is for governors to decide how the institution will act on those answers.

5 | Four decisions governors cannot delegate

The article began with one governor-level question: Do we know whether the financial system can make a coordinated transition — safely and in time? The four supporting questions establish what governors need to understand.

The four decisions below translate those answers into action. Taken together, they determine whether the central bank can answer the overarching question with evidence rather than assurance.

Exhibit 4: Four decisions governors cannot delegate

	Supporting question	Governor decision	What the decision covers
1	**What turns delay into systemic risk?**	Set the system ambition and sequencing	Decide which long-lived information, critical services and transaction chains require earlier action; which low-regret measures should begin immediately; and under what conditions larger migration waves, coexistence, fallback and retirement should proceed.
2	**How does quantum risk become a financial stability risk?**	Define the mandate and accountability	Decide how responsibility for the identified risks is allocated across internal operations, payments, supervision and financial stability; appoint the executive sponsor and programme owner; and define how material dependencies, exceptions and residual risks will be escalated.
3	**Can migration plans work together?**	Set the evidence and coordination requirements	Decide what inventories, migration roadmaps and provider evidence are required; which interoperability, performance, fallback and continuity tests must be completed; and how incompatible standards, timelines and implementation choices will be identified and resolved.
4	**What does coordination look like in practice?**	Choose and resource the coordination model	Decide how the authority will combine convening, supervisory requirements and disclosure; which domestic and cross-border infrastructures and corridors require priority attention; and what funding, specialist capability, international engagement and communication are needed.

Source: Oliver Wyman analysis

Together, these decisions provide the basis for answering the governor-level question with evidence rather than assurance. A credible decision requires more than individual institutional plans: it requires mapped critical transaction chains, visible shared dependencies, compatible milestones, tested interoperability and fallback, and an accountable mechanism for resolving sequencing conflicts. Because the threat date remains uncertain while migration takes years, central banks should prepare now and sequence migration proportionately to information lifetime, service criticality, migration lead time, and provider readiness. That is the difference between a collection of isolated projects and a system-wide readiness program.

© Oliver Wyman

Oliver Wyman, a Marsh (NYSE: MRSH) business, is a management consulting firm driven by deep industry insight, bold innovation, and a collaborative approach that cuts through complexity to help organizations navigate their most defining transformative moments. Marsh is a global leader in risk, reinsurance and capital, people and investments, and management consulting, advising clients in 130 countries. With annual revenue of $27 billion and more than 95,000 colleagues, Marsh helps build the confidence to thrive through the power of perspective.

For more information, visit oliverwyman.com, or follow us on LinkedIn and X.

Americas	Europe	Asia Pacific	India, Middle East & Africa
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700	+971 (0) 4 425 7000

AUTHORS

Dominik Weh
Partner, Global Head of Central Banks and Financial Authorities Platform
dominik.weh@oliverwyman.com

Yaroslav Zakharov
Principal, Central Banks and Financial Authorities Platform, Middle East and Central Asia
yaroslav.zakharov@oliverwyman.com

Hany Mesha
Principal, Solutions Architect and Performance Transformation
hany.mesha@oliverwyman.com

CONTRIBUTORS

Alexander Ovsepyan Global Chief of Staff of Central Banks and Financial Authorities Platform

Louis Bourbouze, Engagement Manager, Financial Services, IMEA

Liudmyla Kurnosikova, Principal, Finance, Risk, and Restructuring, Europe

Maria Fernandes , Partner, Government and Public Institutions, Europe

Martin Stolz, Partner, Banking and Financial Services, Europe

Copyright 2026 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.