香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

HONG KONG MONETARY AUTHORITY
香港金融管理局

PQC Accountability and Controlled Transition

A post-quantum cryptography transition framework for the banking industry

Reference Manual



Authors

Allen H. HUANG	Head and Professor, Department of Accounting, HKUST
Terrance FUNG	Senior Manager, Banking Supervision Department (Supervisory Technology), HKMA Adjunct Associate Professor, Department of ISOM, HKUST
Bruce JIN	PhD candidate, Department of ISOM, HKUST
Dimitrios PAPADOPOULOS	Associate Professor, Department of Computer Science and Engineering, HKUST

Acknowledgement

This is a joint effort of The Hong Kong University of Science and Technology (HKUST) and the Hong Kong Monetary Authority (HKMA), bringing together academic and regulatory perspectives to support banks in planning and managing their transition to post-quantum cryptography (PQC).

We are grateful to Mr Arthur Yuen, Deputy Chief Executive, and Ms Carmen Chu, Executive Director (Banking Supervision), of the HKMA for their guidance and support in the development of this work.

We also thank HSBC for sharing its industry perspectives and practical insights. These contributions have helped inform the framework and its consideration of the challenges banks face in preparing for and implementing the PQC transition.

We thank Prof. James Kwok of the Department of ISOM, HKUST, for his valuable comments on an earlier draft of this manual.

Disclaimer

This work, jointly developed by The Hong Kong University of Science and Technology (HKUST) and the Hong Kong Monetary Authority (HKMA), provides general information and a reference framework for banks' transition to post-quantum cryptography. It does not itself create or amend regulatory requirements or supervisory expectations, or replace applicable laws, regulations or official guidance. Use of the framework does not itself establish regulatory compliance or cryptographic security, or replace institution-specific risk assessment and professional advice.

The framework is informed by academic research and industry guidance; its effectiveness, implementation cost and scalability across banks have yet to be established empirically. The hypothetical case study and its results are illustrative and do not represent actual deployments or performance benchmarks. References to third-party organisations, products or services do not imply endorsement.

The material reflects information available at the time of writing. Readers should consult current authoritative sources as technologies, standards and regulatory approaches evolve. HKUST, the HKMA, and the authors make no representation or warranty as to its accuracy, completeness or suitability for any particular purpose. To the extent permitted by law, they accept no liability for loss or damage arising from use of or reliance on this work.

© November 2026 HKUST and HKMA.

All Rights Reserved.

Executive summary

Banks depend on cryptography to protect information, authenticate customers and systems, and verify transactions and records. A sufficiently capable quantum computer could compromise many of the public-key mechanisms supporting these protections. Although the timing remains uncertain, preparation is already necessary: encrypted information collected today may remain sensitive when future decryption becomes possible, and changing cryptography across interconnected systems and external providers takes time. Post-quantum cryptography (PQC) provides replacement algorithms designed to resist known conventional and quantum attacks (Moody et al., 2026; Auer et al., 2025).

Adopting PQC requires coordinated changes across business, technology and operating arrangements while preserving security and service continuity. This manual presents **PACT (PQC Accountability and Controlled Transition)**, a proposed framework for managing that work in banks. PACT starts with the protection required for the bank's services, critical operations and information, and the obligations it must meet. It connects these needs to the relevant cryptographic uses and dependencies, the people responsible for managing them, and the decisions and evidence needed to direct the transition and assess its results.

In Hong Kong, the HKMA launched the Quantum Preparedness Index (QPI) in July 2026 as a sector-wide benchmark for quantum readiness (HKMA, 2026a, 2026b). The QPI assesses Awareness, Planning, Pilots and Practical Preparedness, and supports the HKMA's expectation of full sectoral readiness by 2030. While the QPI establishes a common benchmark and destination, PACT provides a proposed management framework for the journey. It translates the QPI's readiness dimensions into prioritised actions, accountable ownership, decisions, evidence and controlled pilots.

The framework organises the work into four mutually supporting pillars:

Pillar	Intended result
Govern the transition	Establish institutional direction, accountable ownership and decision authority, supported by common requirements, sufficient resources and demonstrated capability.
Assess and plan	Establish the current cryptographic position and dependencies, assess exposure and timing, develop migration designs supported by evidence, and bring plans and commitments together in an integrated transition roadmap.
Implement and retire	Deliver authorised changes under controlled operating conditions, manage coexistence with earlier arrangements, complete required retirement and verify achievement of the approved target.
Maintain and adapt	Keep knowledge and controls current, respond to changing conditions and demonstrate the continuing ability to make further cryptographic changes.

Work across the pillars can proceed concurrently, with governance and adaptation continuing throughout. Different services and systems can progress at different speeds within a coordinated institutional transition. Requirements and authorised decisions guide the work; findings from assessment, testing and operation inform revisions to designs, plans and commitments.

Clear accountability connects institutional direction with delivery and operations. PACT groups related cryptographic uses into estates, each with an accountable owner for ongoing management. Executive sponsors provide direction, secure resources and resolve or escalate material issues within their remits. A transition manager coordinates the integrated roadmap and follows up agreed actions. Decisions on designs, production changes and acceptance of residual risk follow the bank's existing delegations, with identified approvers and required independent controls. Internal owners remain responsible for managing the bank's dependencies on suppliers, counterparties and group entities.

Responsibilities operate at three levels: institutional portfolio governance; outcome and cryptographic estate management; and engineering delivery and operations. External coordination connects the bank's work with suppliers, counterparties, financial infrastructures and group entities.

Two information rails link these arrangements: direction and decisions communicate requirements and authorised choices, while evidence and feedback communicate findings, limitations and reasons to reconsider earlier decisions. Existing records can carry both flows, provided their scope, status and relationships remain clear.

Planning distinguishes how urgently protection is needed, when work must begin and the order in which changes can be delivered. Protection needs, exposure and consequences establish urgency. Applicable deadlines, migration duration and a contingency allowance inform required start dates, while dependencies and available capacity shape delivery order. Difficult migrations may require earlier preparation or interim protection. Quantum-threat dates remain planning assumptions requiring reassessment. Where timing remains uncertain or infeasible, the roadmap keeps the exposure, responsible owner and next action visible.

A bank can make useful early progress by investigating priority services, resolving enabling dependencies and testing a practicable change before a complete institutional inventory exists. These activities create candidates and delivery capability for subsequent work. Progress reporting should identify the evidence and preparation achieved separately from changes that have established the required protection.

Progress is assessed through evidence of the protection and operating conditions achieved. Supplier commitments, successful tests and deployed changes support different conclusions. Completion requires evidence that the approved target has been achieved for a defined scope, including any required withdrawal of earlier arrangements. The completion decision also confirms that records reflect the resulting state and that continuing owners have accepted their responsibilities with the necessary resources. Management reporting distinguishes protection achieved, remaining exposure, delivery progress and operating capability, keeping unfinished work and temporary departures from the target visible.

PACT can be tailored to a bank's size, complexity and starting position through existing governance, risk management, technology change and operating arrangements. Established programmes can use it to identify gaps in responsibilities, evidence and decisions. Banks with limited visibility can begin with a material protection need and trace the cryptographic uses and dependencies that support it. Investigation, prerequisite work and implementation can advance in parallel, allowing useful work to proceed before discovery across the whole bank is complete, while wider coverage gaps remain explicit.

The framework is informed by industry guidance and academic research. It does not constitute a regulatory requirement or itself establish cryptographic security or compliance; technical choices still require applicable standards, specialist assessment and evidence from the relevant environment. Its effectiveness, implementation cost and scalability across banks have yet to be established empirically. The lasting objective is to retain the knowledge, ownership and tested capacity to maintain protection and carry out further cryptographic change (Barker et al., 2025).

Contents

Executive summary 3

1 Purpose and banking context 7
1.1 Cryptography in banking 7
1.2 The quantum transition 8
1.3 The institutional management problem 9
1.4 Purpose, audience and scope 9

2 The PACT framework 11
2.1 Governing principles 11
2.2 Core concepts 12
2.3 The four pillars 14
2.4 Three operating levels and external coordination 15
2.5 The two information rails 17

3 Govern the transition 19
3.1 Establish executive leadership and transition coordination 21
3.2 Establish the mandate, scope and goals 22
3.3 Assign accountable ownership 24
3.4 Establish decision authority and independent control 26
3.5 Set common policy and architecture requirements 28
3.6 Secure resources and demonstrate capability 30
Pillar review – Govern the transition 32

4 Assess and plan 34
4.1 Establish the current cryptographic position 36
4.2 Establish dependency requirements and readiness 38
4.3 Assess exposure, migration constraints and timing 40
4.4 Select the migration approach and proposed target state 43
4.5 Test design feasibility and suitability 46
4.6 Approve the design and interface profiles 48
4.7 Agree the integrated transition roadmap 50
Pillar review – Assess and plan 52

5 Implement and retire 54
5.1 Prepare the change package 56
5.2 Establish readiness and authorise the proposed action 58
5.3 Deploy and establish controlled operation 60
5.4 Control coexistence, remaining work and exceptions 62
5.5 Retire predecessor arrangements 64
5.6 Verify completion and establish continuing ownership 66
Pillar review – Implement and retire 68

6 Maintain and adapt 70
6.1 Maintain current knowledge and effective controls 72
6.2 Measure protection, exposure, progress and capability 73
6.3 Review findings and adapt decisions and arrangements 76
6.4 Demonstrate continuing cryptographic agility 78
Pillar review – Maintain and adapt 80

7 PACT in practice 82
7.1 Govern the transition 83
7.2 Assess and plan 85
7.3 Implement and retire 89
7.4 Maintain and adapt 92

8 Conclusions and practical implications 96

References 98

Appendix A Glossary and abbreviations 103
A.1 Terms and definitions 103
A.2 Abbreviations and algorithm names 104
Appendix B Technical primer on post-quantum cryptography 106
B.1 Cryptographic functions and quantum exposure 106
B.2 Keys, certificates and trust 107
B.3 PQC standards, parameters and system effects 108
B.4 Hybrid protection, agility and implementation patterns 110
B.5 Cryptographic uses across a bank 111
Appendix C Jurisdictional PQC transition landscape 113
C.1 Reading guide and coverage 113
C.2 Comparative table and source maintenance 113

1 Purpose and banking context

Banks rely on cryptography to protect the confidentiality of information, authenticate customers and systems, and verify transactions and records. A sufficiently capable quantum computer could compromise many of the public-key mechanisms supporting these protections. Banks need to prepare before that capability becomes available. Encrypted information collected today may still be sensitive when future decryption becomes possible, and replacing cryptography across interconnected systems and external providers takes time.

Post-quantum cryptography (PQC) provides algorithms designed to resist both known conventional and quantum attacks, giving banks a technical basis for addressing this threat. Adopting these algorithms requires coordinated changes across the systems and services that use them. Banks therefore need to manage the transition as an institutional change programme, preserving security and service continuity while developing the capacity to respond to future cryptographic requirements (Auer et al., 2025).

In Hong Kong, the HKMA launched the Quantum Preparedness Index (QPI) in July 2026 as a sector-wide benchmark for banks' readiness for the quantum era (HKMA, 2026a, 2026b). The QPI considers four dimensions—Awareness, Planning, Pilots and Practical Preparedness—and supports the HKMA's aim of full sectoral readiness by 2030. While the QPI indicates a bank's state of quantum preparedness, PACT provides a proposed management framework for organising the work needed to improve it. It connects the QPI's readiness dimensions with accountable ownership, prioritised migration activity, controlled implementation, evidence of achieved protection and the continuing capability to adapt. PACT is aligned with the QPI and is intended to help banks progress towards full quantum readiness by 2030, while maintaining the security, resilience and continuity of critical banking services.

1.1 Cryptography in banking

Cryptography provides distinct but complementary protections. Encryption protects confidentiality by making information unreadable without the appropriate key. Integrity protection enables unauthorised changes to information to be detected, while authentication provides assurance about the identity of a participant or the origin of a message (Barker, 2020).

These protections rely on cryptographic keys, the numerical values that control cryptographic operations. Symmetric encryption, such as the Advanced Encryption Standard (AES), uses the same secret key to encrypt and decrypt information. When systems communicate, they also need a way to establish the keys used to protect their exchange. Public-key cryptography can support this process. It uses a related pair of keys: a public key that can be shared and a private key that must be protected. Mechanisms such as Diffie–Hellman (DH) and elliptic-curve Diffie–Hellman (ECDH) establish shared secrets from which systems derive encryption keys (Barker, 2020; Rescorla, 2026).

Public-key cryptography also supports digital signatures. A signature is created with a private key and verified with the corresponding public key, allowing the origin and integrity of the signed information to be checked. Common signature mechanisms include Rivest–Shamir–Adleman (RSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA). Signing does not conceal the information (Barker, 2020).

To rely on a signature, a system needs assurance about whose public key it is using. A digital certificate links a public key to an identity through an issuer's signature. The system validates the certificate and any chain of issuing authorities leading to a trusted authority (Cooper et al., 2008, §§3.1, 6, 8).

An online banking connection illustrates how these mechanisms work together. Transport Layer Security (TLS), a protocol for securing communications, can use ECDH to establish shared secrets, RSA or ECDSA signatures to authenticate the bank, and AES to encrypt the information exchanged. TLS also combines cryptographic hash functions with secret keys in mechanisms for deriving keys and authenticating the messages used to establish the connection. These hash functions, such as SHA-256 from the Secure Hash Algorithm 2 (SHA-2) family, produce fixed-length summaries of information, called digests. The customer's application and the bank's systems need to support compatible combinations of these mechanisms. The connection's security therefore depends on the complete arrangement of algorithms, keys, certificates and implementation controls (Rescorla, 2026).

1.2 The quantum transition

Many widely used public-key mechanisms, including RSA, DH, ECDH and ECDSA, derive their security from mathematical problems that are difficult for conventional computers to solve. A sufficiently capable quantum computer could solve these problems and compromise the protections that depend on them. The timing of this capability remains uncertain, and its implications differ for confidentiality and for authentication and digital signatures (Moody et al., 2026). Meanwhile, symmetric encryption and cryptographic hash functions face different quantum effects: Grover's algorithm gives at most a quadratic speed-up against them, and with adequate key and output lengths they are not considered broken. Their algorithms and security parameters require separate assessment (National Institute of Standards and Technology [NIST], 2026).

For confidentiality, an adversary may collect encrypted information today and decrypt it in the future by defeating the public-key mechanisms used to establish or protect its encryption keys using Shor's algorithm. This "harvest now, decrypt later" exposure matters if the information must remain confidential when such attacks become possible. Preparation therefore needs to account for both the required confidentiality period and the time needed to change the relevant systems. Subsequent upgrades cannot protect copies that an adversary has already captured under vulnerable arrangements (Moody et al., 2026).

For authentication and digital signatures, the main threat is future impersonation or forgery once the relevant mechanisms can be defeated. Systems expected to remain in use for many years may need early changes to support replacement mechanisms. Banks also need to consider how they will preserve confidence in the origin and integrity of retained signed records as their signature algorithms become insecure (Moody et al., 2026; Barker et al., 2025).

PQC provides replacement algorithms designed to resist known attacks by both conventional and quantum computers. These algorithms run on conventional computing systems and provide functions such as key establishment and digital signatures. They use mathematical foundations different from those of the common public-key cryptographic algorithms in use today. Lattice-based mechanisms rely on difficult problems involving structured arrangements of points in many dimensions. Hash-based signatures build signing and verification mechanisms from cryptographic hash functions. These two approaches underpin the first three PQC standards finalised by NIST in August 2024, published as Federal Information Processing Standards (FIPS).

Standard	Algorithm and function	Mathematical basis
FIPS 203 – Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)	ML-KEM establishes a shared secret that can be used to derive keys for symmetric encryption and other protections.	Structured lattices (NIST, 2024a).
FIPS 204 – Module-Lattice-Based Digital Signature Algorithm (ML-DSA)	ML-DSA creates and verifies digital signatures.	Structured lattices (NIST, 2024b).
FIPS 205 – Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)	SLH-DSA creates and verifies digital signatures.	Cryptographic hash functions (NIST, 2024c).

The online banking example in section 1.1 illustrates what adoption involves. A connection may use ML-KEM to establish a shared secret while continuing to use AES to encrypt application data. Both ends need to support compatible rules for establishing that secret. Introducing a PQC signature similarly requires the systems that create and verify signatures, and any supporting certificate infrastructure, to handle the new format.

These changes can also affect the resources needed to operate the service. Some PQC mechanisms have substantially larger keys, signatures or messages, with implications for storage, transmission and processing. Migration therefore requires testing across the complete service, including its protocols, supporting products and external connections, to establish that the new mechanisms work together and meet protection and operating requirements (Barker et al., 2025). Further technical background is provided in Appendix B.

1.3 The institutional management problem

The knowledge and responsibilities needed to manage the transition are spread across the bank. The people who understand the information and services being protected may differ from those who operate the systems, manage suppliers or authorise changes. Existing records may identify products and assets without showing how cryptography is used or which business activities depend on it. Building a reliable institutional view therefore means connecting technical findings with business knowledge and identifying who is responsible for the affected information, services and systems (Barker et al., 2025). Research on financial institutions shows that sharing information across teams that cover connected areas improves the quality of their analysis (Huang et al., 2022).

The changes required often extend across several systems and teams. Several services may depend on a shared platform, while one service may rely on multiple internal teams, group entities and external providers. Even when one team is ready, implementation may depend on another party's delivery, testing or operating arrangements. A workable migration plan therefore needs to coordinate these dependencies and commitments across organisational boundaries (European Telecommunications Standards Institute [ETSI], 2024).

These plans develop under uncertainty. Supplier delivery dates and estimates of implementation effort may change, while migration competes with other demands on funding and specialist staff. The most urgent exposures may also be the hardest to address. This requires decisions on what preparatory work to fund, how to sequence dependent changes and when to revisit earlier decisions, while keeping critical operations within the bank's tolerance for disruption (ETSI, 2024; Basel Committee on Banking Supervision [BCBS], 2021a).

Accountability for these choices depends on knowing what each decision covers, who is authorised to make it and whether the supporting evidence is sufficient in view of its consequences. Where exposure remains, management needs to know who is responsible for addressing it and which decisions or dependencies determine the next action. Progress reporting connects completed work with evidence of the protection achieved and the work still required, allowing management to assess how far the transition has addressed the bank's exposure.

The QPI creates a common reference point for assessing preparedness, but a rating alone does not determine how a bank should manage its transition. Banks need arrangements that convert identified gaps into owned actions, funded commitments, tested changes and evidence of outcomes. PACT addresses this management challenge by linking institutional direction and QPI-informed priorities to the cryptographic estates, dependencies, decisions and operating responsibilities through which the transition is delivered.

1.4 Purpose, audience and scope

This manual presents PACT (PQC Accountability and Controlled Transition), a proposed framework for banks to organise and manage their transition to post-quantum cryptography. It is written for technical and non-technical professionals who direct, deliver, operate or oversee that transition. The framework provides a common basis for coordinating work across business, technology and control functions.

PACT covers the cryptography that banks use to protect information, support business services and critical operations, and meet their defined obligations. Its scope includes shared infrastructure and dependencies on group entities, suppliers and other external parties. Quantum key distribution, which relies on specialised physical links rather than algorithm replacement, is outside the report's scope. Its use for particular connections is a separate design decision.

PACT is designed to operate through a bank's existing governance, risk management, technology change and operational resilience arrangements. Banks can tailor its roles and records to their size, complexity and exposure while preserving clear accountability and necessary independent controls. The framework is intended for use alongside applicable technical standards and regulatory requirements. PACT itself does not constitute a regulatory requirement.

Sections 1–2 establish the context and introduce the framework. Readers can use the relevant workstreams in sections 3–6 to identify the required results, responsibilities, evidence and decision criteria for their work. The pillar review at the end of each of these sections provides a basis for assessing

the work or decision under consideration. Section 7 demonstrates how the pillars apply together, and section 8 explains tailoring and limitations.

Appendix A provides a consolidated glossary and list of abbreviations. Appendix B provides a technical primer with selected comparisons and banking-use examples. Appendix C compares selected jurisdictional requirements, guidance and milestones, with their scope and status as of 22 October 2026.

2 The PACT framework

PACT connects what a bank needs to protect with the responsibilities, decisions and evidence needed to manage its PQC transition. It organises this work into four mutually supporting pillars: *Govern the transition*, *Assess and plan*, *Implement and retire*, and *Maintain and adapt*. These pillars provide a common structure for coordinating responsibilities and dependencies across the bank and with external parties, while allowing individual systems and services to progress at different speeds within a coordinated institutional transition.

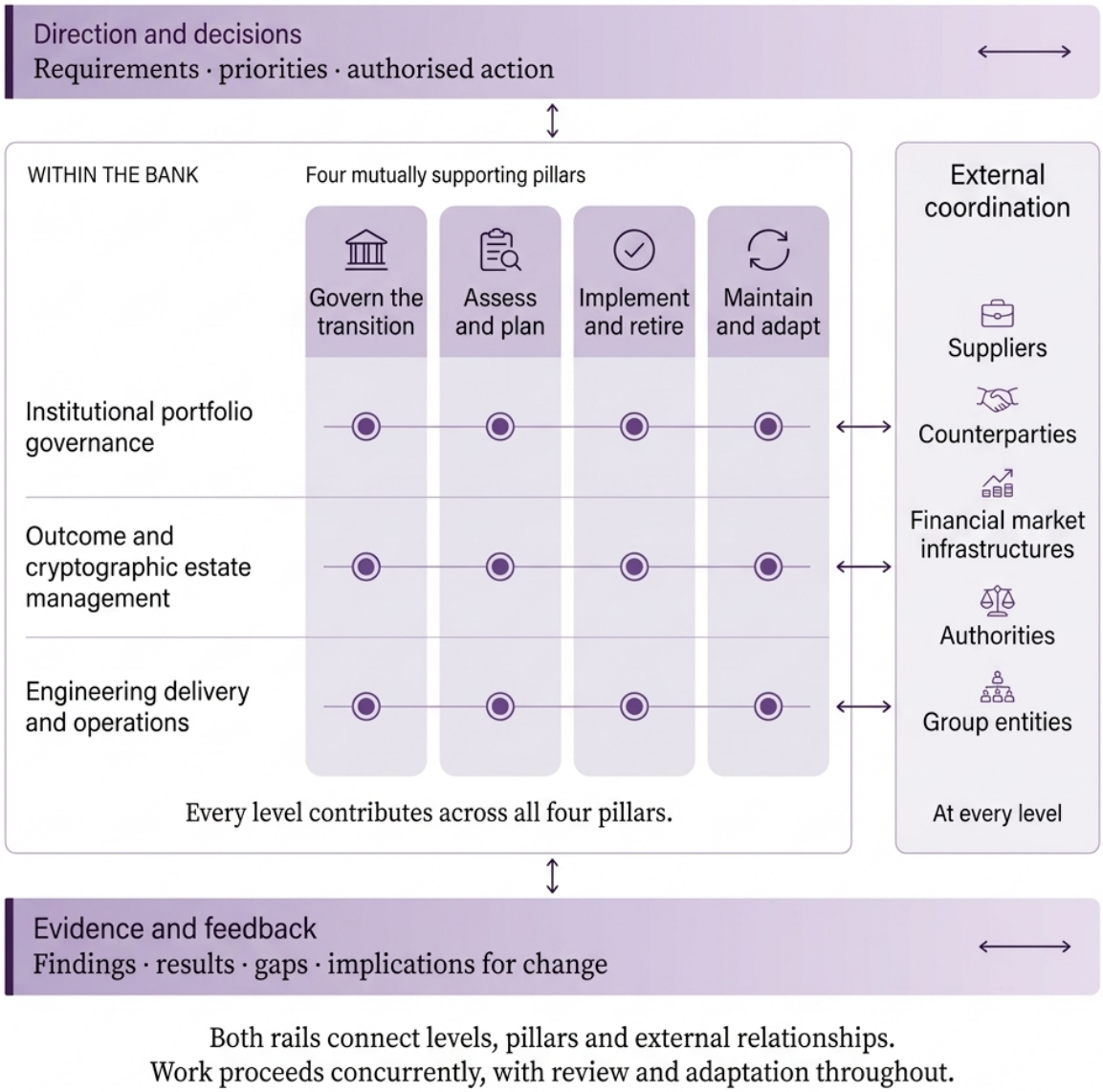

Figure 1 PACT framework at a glance

2.1 Governing principles

Banks can adapt PACT to their organisational structures and circumstances while preserving the following seven principles. These principles apply across all four pillars and draw on established guidance on banking governance, operational resilience, PQC migration and cryptographic agility.

1. **Scope and ownership**. Each material cryptographic use should be linked to the service, operation, information or obligation it protects, with named owners for the relevant responsibilities, to preserve the connection between technical change and business consequences. This scope includes shared infrastructure and external dependencies. Where an external party controls delivery, an internal owner remains accountable for managing the dependency and its consequences for the bank (BCBS, 2021a, Principles 4–5).

2. **Explicit authority**. Responsibility should be matched by sufficient authority, resources and access to expertise. The bank's mandates should identify who may approve changes, accept remaining exposure and resolve conflicts, and where to escalate matters beyond an owner's authority. Preparation, review and approval retain distinct responsibilities, preserving the independent controls required under the bank's existing governance arrangements (BCBS, 2021a, Principle 1; BCBS, 2021b, paras. 6–12).

3. **Risk and timing**. Risk assessment establishes the protection required and the consequences of compromise. Plans should distinguish how urgently protection is needed, when work must start and the order in which changes can be delivered. Dependencies and implementation constraints may alter that order without reducing the underlying exposure. A difficult migration may therefore require early preparation or interim protection. Timing commitments should state their assumptions and known uncertainties and be reviewed when these change (ETSI, 2024, §§6.7–6.9, 6.11).

4. **Evidence-based decisions**. The evidence needed depends on the action being considered and its consequences. A supplier commitment, a laboratory test and observed production use support different conclusions. The bank should assess whether the evidence is sufficient for the proposed action, considering its source, scope, limitations and whether it remains current. Gaps should remain explicit, with review proportionate to the consequences and uncertainty involved (Barker et al., 2025, §5). Evidence informs judgement; the designated authority authorises action.

5. **Controlled change**. Cryptographic change needs to preserve security, service continuity and the operation of dependent systems. Before implementation is authorised, the bank should assess the effects of the proposed change and establish testing, monitoring and recovery arrangements proportionate to the consequences of failure. Where critical operations are affected, the bank should establish how they will remain within its tolerance for disruption during transition and recovery (BCBS, 2021a, Principles 2–3).

6. **Demonstrable completion**. Completion is judged against a defined scope and an approved target (ETSI, 2024, §§5.2 and 6.10). Evidence should show that the target has been achieved: continuing uses operate satisfactorily, earlier arrangements have been withdrawn where required, and records and ownership reflect the resulting state. Authorised temporary departures from the target remain visible as unfinished work.

7. **Continuing adaptability**. Cryptographic requirements may continue to change during and after the initial PQC transition. Banks therefore need to retain the knowledge, skills and operating arrangements to change cryptography again within defined security, service and timing requirements. Findings from tests, incidents and migration should inform improvements and prompt review of affected decisions, while unaffected work continues. Exercises and operating experience should demonstrate the bank's ability to carry out further cryptographic change (Barker et al., 2025, §§5 and 6.5).

2.2 Core concepts

PACT uses the following concepts to connect a bank's protection needs with the cryptography that supports them and the work required to manage and change it.

A **protected outcome** states the result the bank needs cryptography to support, such as maintaining the confidentiality of customer records or preserving the ability to verify retained signed agreements. It may concern a business service, critical operation, protected information or another defined obligation. Critical operations are those whose disruption would materially impair the bank's continued operation or its role in the financial system (BCBS, 2021a). The protection requirements and consequences of failure associated with that outcome provide the basis for assessing technical choices.

A **cryptographic use** is an application of cryptography for a specific security purpose in an identifiable operating context, such as signing certificates within an internal certification authority (CA), authenticating an application to its users, or encrypting stored customer records. The same algorithm, product or certificate can support several uses with different protection needs and transition requirements. A use may cover a defined group of similar deployments where their security purpose, protection needs, responsibilities and transition arrangements can be assessed and managed together. Identifying these uses connects technical inventory information with the activities and information being protected (Barker et al., 2025, §5).

A **cryptographic estate** groups related cryptographic uses under an accountable owner for ongoing management. It may cover a business service, a group of applications or a shared platform. The estate's scope reflects protection needs, operating responsibilities and practical arrangements for change, and includes relevant recovery, fallback and inactive capabilities. It identifies the supporting keys, certificates, protocols, software and hardware managed within its scope, together with dependencies on components and services managed elsewhere. An estate can span several systems, and one system can support uses managed in several estates.

A **dependency** is a reliance on a component, service or party for protection, operation or completion of a change. Dependencies may be internal or external, direct or indirect. Ongoing operation may depend on a shared key-management service, while migration may require a supplier update or a counterparty's readiness to support compatible mechanisms (ETSI, 2024, §§6.3 and 6.5). An internal owner manages the bank's reliance on each material external dependency and response to delays or inadequate delivery.

A **change package** defines a set of transition work with an accountable owner and a delivery plan. The plan covers testing, implementation, recovery arrangements and any required retirement, and identifies the cryptographic uses and dependencies affected. A package may span several estates, and an estate may require several packages. Existing change-management records can document the package.

How the concepts fit together

A protected outcome may depend on several cryptographic uses, and one use may support several outcomes. Each use is assigned to one cryptographic estate for ongoing management, with all the outcomes that depend on it recorded. This assignment establishes accountability for managing the cryptographic use and coordinating its dependencies. Owners of shared components and services retain responsibility for the elements they manage, and responsibility for each protected outcome remains with its owner.

Dependency records link each cryptographic use to the components, services and parties needed to maintain or change it, including the relevant operating arrangements. Where several estates rely on the same component or service, they refer to a common record of its identity, ownership and status. This information helps the responsible teams assess the effects of a shared change, define change packages and coordinate work within and across estates.

Example: authenticating a payment gateway

Consider a bank whose internal public key infrastructure (PKI) issues certificates that a payment gateway uses to authenticate itself to connecting internal systems. The following illustrates one possible arrangement for managing these uses and their transition.

Concept	Application in the example
Protected outcome	Internal systems have assurance that they are communicating with the intended payment gateway. This depends on trustworthy certificate issuance and effective authentication arrangements.
Cryptographic use	The issuing certificate authority (CA) signs certificates for internal services. The payment gateway uses its certificate and corresponding private key to authenticate itself to connecting internal systems. The certificate signing and the authentication are distinct uses, linked through the internal PKI.
Cryptographic estate	The CA's certificate-signing use is assigned to the shared PKI estate, and the gateway's authentication use to the payments estate. Each estate has an accountable owner responsible for the ongoing management of its assigned uses.
Dependency	The payments estate records its reliance on the PKI service for certificate issuance and renewal, referring to a common record of that service's identity, ownership and status. The PKI owner remains responsible for the issuance service. The gateway's authentication also depends on compatible certificate-validation and protocol arrangements in the connecting systems.

Concept	Application in the example
Change package	A package brings together the PKI and gateway work needed to change the authentication arrangements, with an accountable delivery owner and a coordinated plan. It covers the relevant CA and gateway changes, certificate replacement, compatibility testing with connecting systems, deployment, recovery and required retirement of earlier arrangements.

Each use has one estate responsible for its ongoing management, while the dependency connects their transition work. Completing the CA upgrade alone does not establish that the gateway's authentication use has completed its transition; supporting evidence must also cover the gateway and its connections.

2.3 The four pillars

The four pillars organise the cryptographic transition into complementary areas of work. Their activities can proceed concurrently within and across cryptographic estates, with governance and adaptation continuing throughout.

Pillar	Scope of work
Govern the transition	Establish the scope, direction, accountability and decision authority for the transition. Provide common architecture and control requirements, and sufficient resources and capability. Coordinate work across the bank and with external parties.
Assess and plan	Identify cryptographic uses and dependencies, define estate boundaries, assess exposure and timing, select migration approaches and target states, resolve design uncertainty through pilots, and combine feasible plans into an integrated transition roadmap.
Implement and retire	Define, prepare and test change packages, confirm internal and external readiness, and implement changes with monitoring and recovery arrangements. Manage coexistence and remaining exposure, retire earlier arrangements where required, and verify completion against the approved target.
Maintain and adapt	Keep knowledge and controls current, measure progress, outcomes and remaining exposure, respond to changed conditions and operating experience, and demonstrate the continuing ability to make further cryptographic changes.

How the pillars work together

The pillars support a coordinated response as evidence develops and the basis of earlier decisions changes. For example, a migration plan may assume that a supplier update will work with the bank's recovery arrangements. Testing under **Implement and retire** may show that this assumption is incorrect. The responsible teams then revise the migration approach and schedule under **Assess and plan**, seeking any necessary decisions on scope, resources or accepted exposure under **Govern the transition**. The revised change returns to testing before implementation can proceed. Under **Maintain and adapt**, the bank incorporates the findings into its assessment and testing practices so that future changes examine recovery compatibility earlier. Work that does not depend on resolving the problem can continue.

The concurrency can be visible in the roadmap: one set of services is being investigated, another is receiving enabling upgrades, and a third is implementing an approved change. Early testing of potential mitigation or migration approaches can also proceed within a defined scope while discovery continues elsewhere. Findings move between these streams as prerequisites and evidence become usable. Section 4.7 explains how the bank can organise this flow without making the pillars additional sequential approval gates.

Pillar reviews

Pillar reviews assess whether the evidence supports the work, decision or operating condition under consideration. Each review covers a defined scope and brings together the relevant requirements and findings from across the affected pillars.

Reviews recur at material commitments, after consequential changes and at suitable intervals. They can form part of existing governance, planning or change reviews, with one review addressing several pillars. The placement of review guidance at the end of each pillar chapter does not require an entire pillar to be completed before other work proceeds.

Reviews should use existing records and follow the bank's assigned authority and independence requirements, including independent assessment where required. They inform the specific approvals required for design, deployment and retirement. Those approvals remain necessary for the relevant action to proceed.

Each review addresses four questions:

1. What is being reviewed? Identify the affected outcomes, estates, change packages or institutional arrangements, the relevant date or period, and the action, commitment or operating condition under consideration.

2. What does the evidence establish? Determine which required results are demonstrated and whether findings across the affected sections and pillars support a consistent conclusion.

3. What remains unresolved? Identify material gaps, remaining exposure and dependencies, and explain how they constrain the work or conclusion under review.

4. What action or decision follows? Establish what can continue, what should change and what requires further approval, with responsible parties, conditions and follow-up dates.

Review conclusions should remain linked to their supporting evidence and required action. The bank may accept an operating state within a defined scope while work towards the approved target continues. Completion requires evidence that the target has been met, including any required retirement of earlier arrangements.

2.4 Three operating levels and external coordination

The four pillars describe the work involved in the cryptographic transition. PACT's three operating levels organise responsibility for the bank's overall transition, its protected outcomes and cryptographic estates, and engineering delivery and operations. Each level contributes across all four pillars. Banks map these responsibilities onto their existing governance, management and operating arrangements.

Institutional portfolio governance

This level ensures that individual plans collectively address the bank's protection needs and can be delivered within available capacity. It sets institutional scope, common requirements, priorities and resource commitments, and oversees overall exposure and progress.

An integrated view links estate assessments and plans with their protected outcomes, dependencies and resource needs. It reveals gaps in coverage, conflicting priorities, shared constraints and uncertain or infeasible timing. Matters beyond individual estate mandates are addressed through the relevant institutional authority, while work within existing delegations proceeds. Oversight also considers whether coordination arrangements and delivery capacity remain adequate as the transition expands.

Outcome and cryptographic estate management

This level translates institutional direction into plans for defined protection needs and cryptographic scope. Outcome owners establish the protection required, how long it is needed and the consequences of compromise. They also identify the operating conditions changes need to preserve, including tolerance for disruption and recovery requirements for critical operations (BCBS, 2021a, Principles 1–3). Estate

owners use these requirements to assess their cryptographic uses and dependencies and develop migration approaches, schedules and target states.

The assessment should consider the complete arrangement supporting each protected outcome. Where several estates contribute to an outcome, readiness is assessed across the full arrangement of uses and dependencies needed. Evidence for an individual component is considered in that wider context. An estate supporting several outcomes accounts for all their relevant requirements. The responsible owners reconcile these assessments to coordinate change packages and identify matters beyond the estate's authority or resources.

Engineering delivery and operations

This level establishes how the required changes can be implemented and sustained. Engineering and operations teams develop designs and bounded change packages, test their suitability, confirm practical prerequisites, implement authorised changes and perform required retirement. Feasibility analysis and test results contribute while plans are being developed, allowing technical constraints, missing dependencies and unrealistic estimates to be addressed before larger commitments are made.

Operating requirements shape this work from the outset. Monitoring, support, incident response and recovery arrangements need to remain usable under the expected operating conditions. After implementation, operating observations show which cryptographic mechanisms are actually used, how systems behave and which earlier capabilities remain available. The resulting records support assessment against the approved target and identification of remaining work. Continuing maintenance and exercises preserve the ability to operate, recover and make further cryptographic changes.

Working across the levels

Institutional decisions, estate plans and engineering work inform one another. Protection requirements guide assessment and delivery; feasibility and test findings inform plans and commitments; and operating results inform subsequent decisions. Teams also coordinate directly where estates share components, suppliers, implementation windows or specialist capacity. Common methods, evidence requests and test facilities can support several estates, while conclusions about protection and readiness remain specific to the scope assessed.

Business ownership, independent risk and control challenge, and independent assurance apply across all three levels through the bank's existing arrangements (BCBS, 2021b, paras. 6–12). Specialist expertise also supports work at each level.

These levels can be supported by the federated arrangement in section 3.1. Shared expertise and coordination connect their work; implementation remains with the responsible application, platform and infrastructure teams.

Decision authority follows the applicable mandate. Matters that cannot be resolved within existing arrangements are escalated with their consequences and feasible responses. These responsibilities continue as transition work becomes part of routine management.

External coordination

External coordination connects the bank with suppliers, counterparties, financial market infrastructures, authorities and, where applicable, other group entities whose decisions or capabilities affect the transition. Coordination of common technical choices, significant migration milestones and testing helps interconnected participants prepare compatible changes (Auer et al., 2025, §3.1; G7 Cyber Expert Group, 2026; Hui et al., 2017).

Operating level	Focus of external coordination
Institutional portfolio governance	Address applicable requirements, sector initiatives, shared constraints and material commitments.

Operating level	Focus of external coordination
Outcome and cryptographic estate management	Identify the external capabilities, interface arrangements and delivery dates needed by the bank's plans.
Engineering delivery and operations	Support representative joint testing, coordinated deployment and required retirement, operational support and recovery.

The resulting arrangements should establish each party's agreed deliverables, when they are needed, what evidence supports readiness and how the bank will respond to delay or inadequate delivery.

A group-led programme should preserve the local institution's protection requirements, relevant evidence and applicable decision authority. A group-controlled change remains a dependency where the local institution cannot direct its delivery. The local institution assesses the implications for its transition and determines whether additional action is needed (BCBS, 2021a, Principles 4–5).

Sector coordination helps identify shared obstacles and supports common evidence requests, testing and lessons that reduce duplicate effort and improve compatibility. Information exchange should respect confidentiality and preserve the scope and limitations of evidence shared. Each bank assesses what the shared findings establish for its scope and retains responsibility for its decisions and protected outcomes.

Example: responding to supplier delay

Suppose a supplier postpones an update needed to change the online banking website's authentication. Engineering and operations teams assess alternatives and their testing and recovery implications, while the dependency owner seeks a credible supplier response or establishes what an alternative would require. Outcome and estate owners assess the effect on protection requirements, dependencies and the transition plan. Institutional portfolio governance addresses any resulting decisions on priorities, resources or commitments that exceed existing delegations. The agreed responses are reflected in the affected plans and change packages, while work unaffected by the delay can continue.

2.5 The two information rails

PACT connects decisions, work and results through two continuing flows of information across the four pillars, the three operating levels and external relationships. The **direction and decisions rail** communicates requirements and authorised choices. The **evidence and feedback rail** communicates findings and their implications for those choices. Together, they allow those responsible for the transition to guide work, assess its results and respond when circumstances change.

Direction and decisions

This rail gives teams the basis for planning and acting. It carries the requirements and policies that apply, the protection objectives and target states to be achieved, and the priorities, resource commitments and authorised actions that guide delivery. Proposals and requests for decisions remain distinguishable from approved direction.

The record of a decision identifies what is permitted, its scope and conditions, when it takes effect and the authority under which it was made. A policy establishes continuing requirements, while approval for a particular change permits specified work within defined limits. Estate plans and change packages preserve the meaning and limits of both.

External inputs also retain their source and status. An applicable obligation, a recommendation, a draft standard and a supplier forecast provide different bases for action.

Evidence and feedback

This rail carries the information used to assess protection, readiness and progress. It brings together inventory findings, dependency assessments, supplier information, risk and timing analyses, test results, operational observations and retirement evidence. Feedback explains what these findings mean for an

existing plan, decision or practice and whether a response is needed. This flow supports the continuing inventory, assessment and monitoring of cryptography described in NIST's guidance on cryptographic agility (Barker et al., 2025, §5).

Evidence needs to identify what was examined, how and when it was examined, which conclusions it supports and what remains uncertain. Different sources answer different questions. A supplier statement may describe a claimed capability; a configuration record may identify permitted mechanisms; and a traffic observation may show actual use during a particular period. These findings should be interpreted according to the claim being assessed (Huang et al., 2018).

Evidence also relates to the state that was examined. A component can retain its identity while its release, configuration, interfaces or recovery arrangements change. Before using earlier evidence to support a decision about that changed state, the responsible teams assess whether it remains applicable. Material gaps, conflicting findings and limitations remain visible until resolved or explicitly qualified. Evidence informs authorisation; permission to act comes from the relevant decision authority.

Connecting information with actions

Both rails connect work across organisational levels, cryptographic estates and institutional boundaries. A common requirement may affect several estates, while a finding in one estate may reveal a problem in a shared dependency. Supplier information can affect technical plans, institutional commitments and external testing arrangements at the same time. Information therefore needs to reach those responsible for each affected decision and activity, with enough context for them to use it.

The bank should be able to trace a protected outcome to the cryptographic uses, dependencies, decisions and changes that support it. It should also be able to trace a material finding back to the outcomes and decisions it affects. These connections help the responsible owners assess the implications of new information across the transition.

When findings change the basis of a decision, the responsible owner assesses the affected scope and coordinates the response, obtaining any approval required from the relevant authority. The resulting decision and subsequent evidence remain linked to the finding and the earlier decision and its basis, showing what changed and whether the response achieved its purpose. Section 6.3 develops this cycle that uses the migration status and lessons to inform subsequent work (ETSI, 2024, §§6.10–6.11).

Institutional summaries draw on these links. They preserve access to supporting detail, keep consequential uncertainty and remaining exposure visible, and distinguish completed activities from evidence that the required protection has been achieved.

Using existing records

Existing inventory, risk, architecture, supplier, testing and change records can carry both rails. A record can show what was found, what was authorised and what has been done, provided these remain clearly distinguishable. Consistent references connect related records across different systems, with a clear basis for reconciling the information they contain. Relevant history remains accessible when names, configurations or operating arrangements change.

Access and integrity controls protect this information while allowing its authorised use. Records should refer to protected cryptographic material without containing private keys, passwords or other secrets.

Example: recovery testing before deployment

Suppose an approved change package for the online banking website requires recovery testing before deployment. That condition forms part of the direction and decisions rail. A subsequent test report demonstrates successful authentication in normal operation, while leaving recovery untested. The evidence and feedback rail communicates the result and makes clear that the recovery-testing condition remains unmet.

A decision to complete the missing testing and revise the deployment date then returns through the direction and decisions rail. The additional results support the subsequent deployment decision, while operational observations provide evidence of the resulting state.

3 Govern the transition

The *Govern the transition* pillar establishes how the bank directs and oversees its PQC transition. Through existing governance arrangements, the bank defines the mandate and scope, assigns accountability and decision authority, sets common requirements, and secures the resources and capability needed for the work. Coordination connects internal and external contributions, with clear routes for resolving issues beyond individual teams' authority. These arrangements support work within delegated limits and preserve independent controls. As evidence, requirements and delivery conditions change, the bank revisits commitments, responsibilities and resources.

Pillar outcome: The transition has a clear institutional mandate, accountable owners, effective decision and escalation arrangements, and sufficient supporting resources and capability.

PACT / PILLAR 1

Govern the transition

Clear mandate, accountable responsibilities, usable decision arrangements and sufficient support.

Six connected areas of work

3.1 Establish executive leadership and transition coordination

Actors Board or senior-management authority appoints; executive sponsors direct; transition manager coordinates.

Result Recognised remits and coordination authority; current integrated roadmap and responsibility map.

3.2 Establish the mandate, scope and goals

Actors Transition manager assembles; business, technology and control functions validate; sponsors approve within remit.

Result Approved scope, goals and initial priorities; gaps and exclusions with owners and review dates.

3.3 Assign accountable ownership

Actors Sponsors secure coverage; transition manager maintains the map; role holders confirm assignments.

Result Named owners with clear boundaries, authority, expected results and responsibilities, including shared work.

3.4 Establish decision authority and independent control

Actors Owners propose and act; reviewers challenge; assigned approvers decide; independent assurance assesses controls.

Result Usable approval and escalation routes; recorded conditions and accountable follow-through.

3.5 Set common policy and architecture requirements

Actors Specialist domain owners maintain requirements; assigned approvers decide; estate, change package and dependency owners apply them.

Result Approved requirements and design patterns; explicit treatment of departures and revisions.

3.6 Secure resources and demonstrate capability

Actors Sponsors secure commitments; transition manager coordinates; functions demonstrate capability; reviewers assess evidence.

Result Committed resources, capability demonstrated within its tested scope, and owned responses to gaps.

Evidence ↓ ↑ Decisions and follow-through

Recurring pillar review

Can the bank direct, support and control the work under consideration?

Scope
Which arrangements, entities, shared functions and work are being reviewed?

Evidence
Do mandate and ownership, authority and requirements, and resources and capability work together?

Unresolved matters
Which gaps or conflicts in ownership, authority, requirements, access or capacity constrain the work?

Action or decision
Continue supported work; revise arrangements or secure support; limit or defer affected work.

Sponsors obtain decisions; the transition manager coordinates changes and follow-through.

Ownership responsibilities (3.3)

Outcome · cryptographic estate · change package · operations · dependency · specialist domain

Governance continues throughout; findings can revise any affected arrangement.

Figure 2 Govern the transition at a glance

3.1 Establish executive leadership and transition coordination

PQC transition involves interdependent work across business, technology and control functions. Some decisions exceed individual teams' authority, while their implementation requires sustained coordination across organisational boundaries. Executive leadership and a defined coordination function should connect institutional direction with coherent plans, resolve competing demands and ensure that decisions lead to accountable action.

Establish executive responsibility

The board or appropriate senior-management authority should appoint one or more **executive sponsors** and ensure that a **transition manager** function is established through the bank's existing delegations. These responsibilities can be assigned to existing positions and teams.

Each sponsor's remit defines the organisational coverage, authority and reporting relationship. The sponsor secures institutional support and resources, reviews material exposure and progress, and resolves or escalates conflicts that individual teams cannot settle. Decisions on architecture, budgets, risk and production changes follow the bank's existing delegations. The board retains oversight, and senior management is responsible for implementation (BCBS, 2021a, Principle 1).

Where sponsorship is shared, the remits collectively cover the agreed organisational scope, with identifiable executive responsibility for each material commitment and unresolved issue. The appointment arrangements establish how matters spanning those remits reach an authority able to resolve them.

Where a group or head office leads the programme, the local bank retains identified executive responsibility and access to the evidence needed for its own scope and decisions.

Coordinate the work and dependencies

The transition manager brings planned work, commitments and dependencies together in the integrated transition roadmap and maintains a responsibility map identifying ownership and decision authority. Maintaining these shared views involves reconciling contributors' plans and identifying inconsistencies, resource constraints and unresolved dependencies. Contributing functions remain accountable for their assessments, evidence and delivery.

To coordinate this work, the manager needs timely access to relevant information and authority to convene contributors, obtain agreed updates and escalate unresolved issues. Contributing business, technology and control functions maintain contacts and cover arrangements, validate their inputs, confirm commitments, and report changes or shortfalls affecting the wider plan. Review cycles and response times reflect the pace of work and the consequences of delay.

A federated arrangement can combine central coordination with delivery through the responsible application, platform and infrastructure teams. Common methods, specialist advice, reusable guidance and consolidated reporting can be shared centrally. Estate and change-package owners remain answerable for the work and evidence within their scopes. The arrangement should secure access to expertise and resolve shared constraints without assuming a new permanent organisation is required.

Group and external contributions form part of the planning arrangements. The manager incorporates relevant commitments, supporting evidence and dates from group functions, suppliers, counterparties and financial infrastructures into the roadmap, and coordinates assessment of changes affecting the bank's plans. Commitments on the bank's behalf are made through authorised representatives.

Turn issues into decisions and action

Working meetings can resolve technical and delivery issues, consolidated updates can expose dependencies across estates, and senior forums can decide matters outside the contributing owners' authority. Use existing management arrangements for these purposes. The frequency and detail of review should respond to delivery activity, unresolved constraints and the decisions needed, rather than remain fixed throughout the programme.

When an issue requires a decision, the transition manager explains the affected scope, supporting evidence and uncertainties, available options and consequences of delay. The responsible sponsor decides within their authority or obtains the required decision through the arrangements in section 3.4. The manager communicates the decision, coordinates the resulting updates to the roadmap and responsibility map, and tracks agreed actions with their owners. Reporting distinguishes confirmed results from work still planned, underway or unresolved.

Example: competing testing needs across two teams

For example, two teams may need the same testing specialists during overlapping periods. The transition manager works with both teams to establish feasible alternatives. The sponsor obtains a decision from the authority controlling that capacity, and the manager confirms the revised commitments and follows up delivery.

Key accountable party and responsibility	Expected result	Evidence of achievement
Board or appropriate senior-management authority: appoint sponsors and establish the coordination function through existing delegations.	Executive leadership and coordination have recognised authority, clear coverage and reporting relationships.	Approved appointments and remits identify responsible parties, authority, reporting relationships and arrangements for resolving matters across sponsors' remits.
Executive sponsors: provide direction, secure institutional support and resources, and resolve or escalate material issues within their remits.	The transition receives consistent direction and authorised decisions addressing material constraints.	Decisions and commitments identify supporting evidence, responsible owners and dates. Unresolved matters have an identified decision-maker and escalation route.
Transition manager: maintain the roadmap and responsibility map, prepare matters for decision and coordinate follow-through.	Contributors work from a current, consistent view of commitments, responsibilities and dependencies.	Plans reflect confirmed internal, group and external contributions. Issue and decision records link findings to authorised decisions, assigned actions and implementation status.

3.2 Establish the mandate, scope and goals

A bank needs a common basis for deciding what its PQC transition should cover and what protection and operating results it should achieve. Without agreed boundaries and goals, teams may work to different assumptions or leave material areas unexamined. The mandate, scope and goals should establish an authorised basis for investigation and planning, while making uncertainties and exclusions explicit.

Define the scope and applicable requirements

The scope identifies the business services, critical operations and information to be protected, the obligations to be met, and the legal entities and jurisdictions covered. Information retained after a service ends remains within scope while protection or verification obligations continue.

Existing service, asset, information and supplier records provide the starting boundaries, including known supporting systems, shared infrastructure and external interfaces. Subsequent discovery refines the cryptographic uses, estate boundaries and dependencies. Where the cryptography is not yet fully understood, the proposal identifies the need for investigation (FS-ISAC Post-Quantum Cryptography Working Group, 2023b, pp. 15–19, 28–31).

The proposal identifies applicable legal, regulatory and contractual requirements and distinguishes binding deadlines from internal targets and external planning references. Group arrangements are assessed against local requirements to establish where further local action is needed. For Hong Kong

banks, the Hong Kong Monetary Authority's aim of full sectoral readiness by 2030 provides a planning reference (HKMA, 2026b). Individual protection needs and migration constraints may justify earlier action. The HKMA's July 2026 circular also expects authorized institutions to assess their quantum exposure, establish a cryptographic inventory and formulate a transition roadmap (HKMA, 2026c). Appendix C supports this assessment of jurisdictional applicability.

Set assessable goals

Goals define the protection and operating results sought, their scope and how achievement will be judged. For critical operations, they reflect the bank's tolerance for disruption and recovery requirements (BCBS, 2021a, Principles 1–3). To support protection over time, the goals also address the ability to make subsequent cryptographic changes.

The goals reflect the bank's existing risk appetite—the types and level of risk it is willing to accept—and applicable limits. Any proposal to accept risk beyond those limits follows the bank's established escalation and approval arrangements (BCBS, 2021b, Principle 4).

Where a measure, target or date cannot yet be established, the proposal identifies the investigation needed, its responsible owner and a review date.

Select areas for early investigation

Within the overall transition scope, an initial screen identifies where investigation should begin. It considers required protection periods, harm from compromise, likely migration duration and the bank's approved quantum-threat assumptions.

Severe consequences can justify early investigation even where migration appears straightforward. Long protection needs and lengthy supplier, hardware, integration or validation cycles can also require early preparation (Canadian Centre for Cyber Security, 2025, §§3.1.2, 3.2; Cybersecurity and Infrastructure Security Agency [CISA], 2024, pp. 5–6). These priorities are provisional; formal risk and timing assessments follow under *Assess and plan*.

For early investigation, success criteria can concern usable evidence for priority services, identified owners for material blockers, demonstrated discovery access, initial supplier information and a technically credible option for further testing. The mandate should state which of these results it seeks and the evidence required. These are legitimate preparation outcomes; they do not demonstrate institution-wide visibility, delivery readiness or completed protection.

Lower-priority areas remain within the transition scope, and areas not yet examined remain visible as coverage gaps. Any explicit exclusion has a recorded justification, an accountable party and a review date or trigger.

Approve the mandate and keep it current

The responsible sponsor approves the mandate within delegated authority and obtains any further required approval. The decision identifies the accepted scope, goals and initial priorities, the investigation and planning work authorised, and any conditions attached.

The transition manager maintains the approved position and coordinates follow-up on unresolved issues. Contributing functions provide findings from their investigations and validate proposed changes. Changes in protection needs, consequences of compromise, supplier commitments, equipment lifetimes or evidence quality prompt reconsideration of the affected scope and priorities. Revisions requiring approval return to the responsible sponsor under the applicable delegation and approval arrangements.

Example: early investigation of online banking within customer-facing digital service scope

For example, a bank may include all customer-facing digital services within its transition scope but begin by investigating an online banking service that handles loan applications. Long confidentiality requirements and potentially lengthy supplier upgrades justify early investigation. The goal is to preserve

confidentiality while maintaining agreed service levels during change. Other digital services remain in scope. If the cryptography in a supplier-operated component is unknown, the proposal names an investigator and sets a review date. The sponsor authorises this focused investigation within the broader transition scope.

Key accountable party and responsibility	Expected result	Evidence of achievement
Executive sponsors: approve the mandate, scope, goals and initial priorities within their remits, obtaining further approval where required.	Investigation and planning have an authorised scope, intended results and conditions.	Approval records identify the supporting evidence, accepted scope and goals, initial priorities, applicable risk limits, material assumptions, authorised work and conditions.
Transition manager: assemble and maintain the proposal and initial screen; coordinate validation, review and follow-up.	Overall coverage, early priorities and outstanding investigations form a coherent, current basis for planning.	Scope and screening records link goals and priorities to their supporting inputs. Exclusions and unresolved questions have responsible parties and review dates or triggers.

3.3 Assign accountable ownership

PQC transition work spans business functions, technology teams and external parties. Without explicit ownership, responsibilities for shared components, individual changes and continuing operation can fall between teams.

Accountable ownership establishes who is answerable for the required results within the transition scope and how responsibilities connect across teams and external relationships. PACT distinguishes six ownership responsibilities covering different aspects of the same work. Several may apply to the same service, component or change.

The bank assigns these functions through existing management arrangements. Roles may be combined where their scope and authority remain clear, capacity is sufficient and required independence is preserved. Owners may delegate tasks while remaining accountable for their assigned responsibilities. Technical contributors are the people and teams assigned to discovery, design, configuration, testing, implementation and other technical work.

Connect protection needs with cryptographic estates

The **outcome owner** establishes the protection needs of a business service, critical operation, protected information or other obligation. This includes the consequences of compromise, required protection or verification periods, applicable obligations and service constraints. For critical operations, the constraints reflect the bank's tolerance for disruption and recovery requirements (BCBS, 2021a, Principles 1–3). The owner assesses whether these needs are met using evidence across the supporting estates and dependencies, and obtains action on shortfalls. The assessment covers the protected outcome as a whole.

The **cryptographic estate owner** manages a defined estate and its transition. This owner maintains the estate's boundary, current-state evidence and links to protected outcomes and dependencies, and coordinates exposure assessment, transition planning and responses to unresolved issues. Even where technical work is distributed across teams, the estate owner remains able to explain the estate's current position, the evidence supporting it and the action still required.

Where an estate supports several outcomes, one estate owner manages that defined scope and each outcome owner retains responsibility for its own protection needs and consequences. The responsibility map records these relationships and identifies ownership of shared components.

Manage change delivery and continuing operation

The **change package owner** delivers a defined package of transition work, which may affect one or several estates. This includes coordinating contributors, prerequisites, testing, implementation, recovery arrangements and any retirement work within the package. Closure requires evidence that the completion criteria have been met and that the relevant owners have accepted continuing responsibilities. Delivery accountability does not itself confer authority to approve deployment or accept residual risk; those decisions follow the arrangements in section 3.4.

The **operations owner** maintains controlled operation within an assigned scope of systems or services. The owner contributes monitoring, support, incident-response and recovery requirements during planning and design, and establishes the capability needed to operate the changed environment. Operational acceptance rests on usable procedures, prepared personnel and demonstrated monitoring and recovery capability. This responsibility continues after the change package closes.

Manage dependencies and common requirements

The **dependency owner** manages the bank's reliance on an internal provider, group function, supplier, counterparty or financial infrastructure. Working with the affected estate and outcome owners, this owner establishes what is needed, who controls delivery, the required dates and available evidence, and coordinates the response to delay or inadequacy (Hui et al., 2019). For third-party service relationships, accountability to authorities and customers remains with the financial institution and its board and senior management (Financial Stability Board, 2023, p. 12).

The **specialist domain owner** maintains common expertise, methods and requirements in a defined area, such as cryptographic architecture, key management or the cryptographic inventory data model. The owner maintains guidance, supports its application and addresses inconsistencies across estates. For example, an inventory domain owner maintains the common data model and quality rules, while estate owners remain accountable for the adequacy of their estate records. This allocation supports the coordination of policy and technical implementation described in NIST's crypto-agility guidance (Barker et al., 2025, §§5.2, 5.4).

Confirm assignments and resolve gaps

The transition manager consolidates the assignments in the responsibility map, with role holders and contributing functions confirming their scopes and commitments. Each assignment identifies a named person or a position with a current holder, the responsibility's boundary, expected results, delegated authority, supporting contributors and continuity arrangements. The responsible executive sponsor confirms coverage within their remit and secures any required assignments through the appropriate management authority.

Role holders need access to the information, expertise and capacity required to fulfil their responsibilities; section 3.6 explains how that capability is secured and demonstrated. The transition manager coordinates review of the map when boundaries, dependencies, personnel or delivery arrangements change.

Where ownership is missing or disputed, the responsible sponsor resolves or escalates the matter before a material decision relies on it. Authorised discovery may continue to clarify the boundary, with a named investigator and defined reporting arrangements.

Ownership allocation should be part of interpreting discovery output. Findings concerning a common platform should reach its estate owner, with the dependent applications and outcomes retained in the record. Findings within an application's own delivery boundary should reach its application or estate owner. Technical contributors should propose the allocation, the receiving owners should confirm their boundaries, and disputed cases should follow the existing escalation route. Investigation may continue under the arrangements already specified for unresolved ownership.

Example: accountable ownership around the change of a key-establishment mechanism

For example, a bank may group the cryptographic uses protecting its online-banking connections into one estate and initiate a package to change the key-establishment mechanism. The outcome owner

confirms confidentiality and acceptable service disruption, while the estate owner identifies the affected uses and dependencies. The change package owner coordinates delivery and evidence, and the operations owner demonstrates monitoring and recovery capability. The dependency owner obtains and tracks the commitment for any required supplier upgrade, and the architecture domain owner provides common design requirements. Outcome, estate and operating responsibilities continue after the package closes.

Key accountable party and responsibility	Expected result	Evidence of achievement
Executive sponsors: confirm ownership coverage and resolve or escalate gaps within their remits.	Material responsibilities have recognised owners with appropriate authority and support.	Confirmed assignments and decisions addressing missing or disputed ownership. Unresolved gaps remain identified and are addressed before material decisions rely on them.
Transition manager: consolidate and maintain the responsibility map and coordinate follow-up on ownership issues.	Teams can identify who is responsible and how their responsibilities connect.	A current map with confirmed scopes, commitments and relationships, together with recorded changes and follow-up on unresolved assignments.
Outcome owner: establish protection needs, assess their fulfilment and obtain action on shortfalls.	Protection is assessed across the whole outcome and its supporting environment.	Requirements and assessments link evidence across estates and dependencies to protection needs, remaining exposure and required action.
Cryptographic estate owner: manage the estate's current position and transition.	The estate's exposure, planned response and remaining work are understood and managed.	Defined boundaries, current-state evidence, exposure assessments and plans linked to affected outcomes, dependencies and outstanding actions.
Change package owner: deliver the defined work and substantiate completion.	The package achieves its required results and continuing responsibilities are accepted.	Applicable test, implementation and retirement evidence against completion criteria, together with acceptance by the relevant continuing owners.
Operations owner: maintain controlled operation within the assigned scope.	Systems and services can be supported, monitored and recovered.	Operational acceptance and subsequent observations demonstrate usable procedures, prepared personnel and effective monitoring and recovery.
Dependency owner: manage the bank's reliance on another party.	Dependency requirements and shortfalls receive an accountable response.	Dated commitments and delivery evidence, with shortfalls linked to responsible actions and updates to affected plans.
Specialist domain owner: maintain common expertise, methods and requirements, and support their application.	Estates can apply consistent, current specialist requirements.	Maintained guidance and records showing its application, the treatment of inconsistencies and necessary revisions.

3.4 Establish decision authority and independent control

PQC transition decisions may affect several protected outcomes and require approvals beyond a single owner's remit. Review and approval arrangements connect accountable ownership with the authority to decide what may proceed. They provide for challenge of the supporting evidence, define the scope and conditions of approval, and establish how decisions are carried into action. These arrangements are particularly important where a proposal affects several protected outcomes or extends beyond an individual owner's authority.

Assign approvers and preserve independent control

Executive sponsors ensure that each material decision has an identified approver acting within the bank's existing delegations and approval limits. The responsibility map records the standing arrangements for defined types and scopes of decision: who prepares the proposal, which reviews are required, who approves and who carries out the resulting action. It also identifies the applicable delegations and decision requirements. The transition manager maintains these assignments and brings gaps or conflicting responsibilities to the responsible sponsor for resolution.

Preparation, review and approval remain sufficiently separate to provide effective challenge (Fauver et al., 2017). Material decisions do not rely solely on unreviewed evidence from those proposing or carrying out the work (Ke et al., 2013). Responsibility for initiating an exception request remains separate from authority to accept the associated residual risk—the risk remaining after controls are applied.

The bank also identifies who provides independent assurance over the adequacy and effectiveness of controls, with a defined scope and reporting route (Bhambhwani and Huang, 2024). Internal audit retains its independent mandate and does not develop, implement or operate the processes it assesses (BCBS, 2021b, paras. 6–12).

Define proposal and review requirements

The owner seeking approval identifies the proposed action, affected outcomes and cryptographic estates, supporting evidence and significant uncertainty. Where several domains are affected, the owner obtains the contributions needed to assess the combined technical, business and operating effects. These may cover key and certificate management, applications and communication protocols, and governance requirements (FS-ISAC Post-Quantum Cryptography Working Group, 2023a, pp. 26–29).

Reviewers assess whether the evidence supports the requested action and identify findings or uncertainties that need a response. The responsible owner presents unresolved issues with the available options and consequences of delay. The response reflects the nature of the issue: competing demands for testing capacity call for a resource decision, while disagreement about recovery capability calls for evidence and agreement on operating requirements. This reflects the distinction between resource constraints and concerns about a change's fit with organisational needs (Tsai et al., 2023). Unaffected work may continue within existing permissions.

Specify decision scope, records and conditions

Each decision links the proposal, review and approval records, identifying the people involved and the authority under which they act. Following review, the assigned approver decides what is approved, deferred or rejected within the relevant delegation. The record identifies the supporting evidence, rationale, permitted scope, conditions, responsible parties and relevant dates. Matters beyond the approver's delegation follow the applicable escalation arrangements.

The decision distinguishes work that may proceed immediately from work requiring further evidence or approval. Permission extends only to the stated action; approving a design does not itself authorise production deployment. Where permission has continuing conditions or an expiry date, the decision identifies the responsible owner, the permitted response and the required escalation if a condition fails or permission expires.

Example: approval route for online-banking cryptographic changes

For example, when establishing the approval route for online-banking cryptographic changes, a bank may find that the proposed arrangements allow the change package owner both to request a departure from recovery requirements and to accept the associated residual risk. The executive sponsor obtains confirmation of a separate authorised risk acceptor under the bank's existing delegations. The relevant functions confirm the required technical and operating reviews, with sufficient separation for effective challenge, and identify the delegated authority for design approval and production deployment. Matters beyond those limits have a defined escalation route. The scope and reporting route for independent assurance over these controls are also confirmed under the relevant assurance mandate. The transition

manager records the agreed arrangements in the responsibility map, giving subsequent proposals an established route for review, decision and any necessary risk acceptance.

Key accountable party and responsibility	Expected result	Evidence of achievement
Executive sponsors: ensure that decision authority is established, responsibilities are appropriately separated, and gaps are resolved.	Material decisions have identified approvers, defined authority limits and usable escalation routes.	Confirmed assignments specify applicable delegations and approval limits. Gaps have an authorised resolution.
Transition manager: maintain and coordinate the review and approval arrangements.	A current responsibility map connects proposal preparation, required reviews, approval, resulting action and escalation.	The map identifies responsibilities for defined decisions, references applicable delegations and records routes for unresolved matters. Changes to assignments are reflected in the map.

3.5 Set common policy and architecture requirements

Individual PQC designs need a common basis for deciding which cryptographic choices are acceptable and how they are implemented. Common policy and architecture requirements provide usable criteria for design, procurement and operation while accommodating justified differences between uses. This helps estates avoid incompatible approaches and dependencies that make later changes difficult.

Establish and approve the common requirements

Relevant specialist domain owners prepare and maintain the requirements, drawing on outcome owners' protection needs and the technical, operating and supplier constraints identified by estate, operations and dependency owners. Following the required reviews under section 3.4, the assigned approver decides whether to approve the requirements within their mandate. Each requirement identifies its owner, scope of application, effective version and review triggers, and is accessible to the teams that use it.

The requirements identify permitted mechanisms and settings for key establishment, signatures, symmetric encryption, hashing and authentication, together with relevant protocol, certificate and implementation requirements. They identify applicable jurisdictional or sector requirements and distinguish the status of supporting sources, including final standards, drafts, research candidates and superseded guidance. A published algorithm standard does not by itself establish a compatible protocol, a validated implementation or the bank's approval for a particular use. NIST identifies standards, protocol and validation maturity as interdependent conditions affecting delivery of cryptographic products and services (Barker et al., 2025, §§5.1–5.3).

Where hybrid key establishment is permitted, the requirements specify the permitted combination of traditional and post-quantum mechanisms within the same key-establishment process, together with controls against unauthorised selection of a weaker alternative. NIST emphasises that the security of a combined scheme requires assessment for its intended application (NIST, 2026, "Transition and Migration"). Retirement requirements distinguish an approved traditional component within such a construction from a vulnerable standalone use. NIST typically expects hybrid solutions to be temporary measures leading to a second transition to post-quantum-only mechanisms (Moody et al., 2026, §3.2).

Support controlled cryptographic change and recovery

Architecture requirements preserve the ability to change cryptography under policy control. Where practical, applications use replaceable cryptographic components through defined interfaces, allowing algorithms and settings to change with limited alteration to business functions. Making this separation usable depends on knowing where components are deployed, governing their configuration and maintaining supported replacement paths (Barker et al., 2025, §§4–5). Hardware, certification and supplier constraints inform the permitted approaches and their limits. Research on software architecture

supports the underlying rationale: early design choices shape later adaptability, and modularity, which separates components to limit the effects of change, can slow its decline, although that benefit weakens as systems age (Agarwal and Tiwana, 2015; Tiwana and Safadi, 2024).

Common requirements also cover key and certificate lifecycles, trusted issuers and the ability to retain necessary decryption or signature-verification capabilities. Requirements for key protection, backup, recovery and destruction reflect the function and type of key (Barker, 2020, §8 and Appendix B). Approved patterns, which provide reusable descriptions of acceptable designs, specify permitted operating and recovery arrangements, including how prohibited cryptographic use is prevented from returning through fallback or restoration.

Apply the requirements to designs and supplier arrangements

Estate and change package owners apply the requirements to designs and changes. Dependency owners incorporate them into supplier engagement, procurement and renewal, covering cryptographic use, supported upgrade paths, compatibility and evidence of performance. FS-ISAC recommends incorporating cryptographic usage and agility into procurement processes and relevant contractual provisions (FS-ISAC Post-Quantum Cryptography Working Group, 2023b, p. 17).

The requirements specify the evidence expected for design and implementation review, such as configuration records and security, interoperability and recovery test results. An approved pattern provides a reusable basis for assessment; suitability and readiness still need to be demonstrated for the intended use.

The requirements should also reduce avoidable new transition work. For new purchases and designs, reviewers should examine supported upgrade routes, dependence on fixed algorithms or interfaces, and the ability to change key and certificate arrangements. Existing estates may need a different treatment because replacement, certification or supplier constraints cannot be removed immediately. A design can improve future changeability before a suitable post-quantum implementation is available; that improvement should be described within its actual scope.

Decide departures and manage revisions

The owner responsible for a proposal identifies any departure from the applicable requirements before relying on it and refers it for decision. The relevant domain owner assesses the implications, and the assigned approver decides whether to permit the departure and on what conditions. The decision and any required acceptance of residual risk follow the authority arrangements in section 3.4.

When requirements change, the domain owner identifies affected uses and proposes how existing approvals, work in progress and new proposals should be treated. The assigned approver confirms that treatment within their mandate. The transition manager coordinates consequential changes across plans and commitments, while the relevant owners carry out the assigned actions. The domain owner retains earlier versions and reasons for revision to preserve the basis of prior decisions.

Implementation of common requirements can develop progressively. Initial work can improve purchasing decisions and architecture review, identify upgrade constraints and establish guidance for current delivery. As supported approaches are demonstrated, incorporate appropriate checks into development and change processes, maintain reusable patterns and test them on the technology stacks that will use them. Broader automation should follow validation of the relevant requirements and patterns. Each stronger requirement needs an effective scope, usable guidance and treatment of existing approvals and constrained legacy systems.

Example: common cryptographic library across new applications

For example, a bank may require new applications to use an approved cryptographic library that can be updated independently of application releases. A proposed supplier product can update its embedded library only through a full product release. The dependency owner obtains evidence of the supplier's update capability and support commitments, while the architecture domain owner assesses the departure. The assigned approver then decides whether a conditional departure is justified or a different product is needed. The recorded decision gives the estate owner a clear basis for further design and procurement.

Key accountable party and responsibility	Expected result	Evidence of achievement
Specialist domain owners: prepare and maintain common requirements and approved patterns, and assess the effects of revisions.	Teams can identify the applicable requirements and the changes that affect their work.	Accessible requirements identify ownership, scope, effective version, supporting sources and review triggers. Revision assessments identify affected uses and proposed treatment; earlier versions and reasons for revision are retained.
Assigned approvers: approve requirements, decide departures and confirm the treatment of revisions within their mandates.	Permitted choices and conditions have an explicit basis and scope.	Decisions record the evidence, rationale, scope and conditions, including the treatment of existing approvals, work in progress and new proposals where requirements change.
Transition manager: coordinate the consequences of changes to common requirements.	Affected plans and commitments reflect approved revisions.	Updated plans, commitments and assigned actions show how the relevant owners have addressed the changes.

3.6 Secure resources and demonstrate capability

Assigned responsibilities become workable only when people have the competence, time, access and support to fulfil them. The bank needs both confirmed resources and practical evidence that the relevant functions can perform their assigned work. Establishing these conditions supports credible commitments and exposes capability gaps before they undermine delivery.

Identify needs and secure commitments

The transition manager consolidates capability and resource needs with the responsible owners and contributing functions, starting with the work being authorised. Together, they identify which existing arrangements can be reused and where additional expertise, capacity, access, tools or test facilities are needed. Initial needs include locating cryptographic uses, establishing their business significance, obtaining supplier evidence and assessing technical and operating constraints. As work expands, the assessment also covers the ability to enforce approved settings, implement changes, recover from failures, preserve service continuity and automate repeated work where appropriate. Reported capability, planned improvements and demonstrated results remain distinguishable.

In particular, the assessment evaluates the capacity to analyse inventory and delivery information and turn it into usable reporting. It identifies the support needed to prepare learning materials, communicate changed practices and help teams adopt them. These contributions can be supplied through existing data, reporting, learning and change functions; naming a new role does not itself secure the capability.

Executive sponsors secure resource commitments through the bank's management and budget arrangements. The functions providing people or facilities confirm what will be available, when and for how long, taking account of competing work and shared specialist capacity. Funding covers the relevant investigation, engineering, review, testing, training and continuing operating support. Commitments match the work being authorised and are revised as its scope becomes clearer. An indicative budget alone does not establish that the necessary people and facilities are available. These arrangements reflect the BIS roadmap's emphasis on cross-functional preparation, early funding and sustained investment (Auer et al., 2025, §§3.2.1–3.2.2).

Prepare people for their responsibilities

Preparation is tailored to the responsibilities being performed. Outcome owners and decision-makers need to interpret exposure, uncertainty and evidence. Technical and operations personnel need practical knowledge of discovery, configuration, testing and recovery, while dependency owners need to obtain and assess relevant external commitments. Specialist domain owners help identify learning needs and suitable methods. FS-ISAC similarly distinguishes technical training from awareness for nontechnical

stakeholders and recommends a controlled test environment (FS-ISAC Post-Quantum Cryptography Working Group, 2024, p. 11).

Participating teams should have short induction materials tied to their immediate work, maintained reference guidance and an identified route for specialist help. Such guidance helps when it is actively used: in a large finance organisation, rich use of a knowledge management system improved job performance, with the effect depending on the task, available support and leadership (Zhang, 2017). Scheduled advice sessions or paired work can support initial assessments and implementations. Capacity commitments should cover this assistance as well as specialist design and review, so that several teams do not rely on the same unallocated time.

Demonstrate capability within a defined scope

A practical demonstration establishes whether the resources and working arrangements can produce evidence suitable for a decision. The evidence may come from relevant work already performed, where its scope and conditions remain applicable, or from a bounded practical exercise.

Where an exercise is needed, the transition manager coordinates it with the relevant estate owner, agreeing its question, scope, participants, success criteria and limits before work begins. For initial discovery and assessment, participants use a priority protected outcome and its supporting cryptographic uses to connect protection needs with observed configurations, dependencies and initial supplier evidence, and to identify material uncertainty. This tests whether the required access, tools and expertise are usable in practice. An independent reviewer assesses whether the findings substantiate the capability claimed and identifies its limits.

The demonstration remains proportionate to the assigned work. An initial discovery and assessment exercise establishes capability within its tested scope; it does not establish institution-wide readiness or authorise production deployment. Design feasibility, release readiness and continuing cryptographic agility are examined in sections 4.5, 5.2 and 6.4 respectively. NIST's illustrative maturity guidance likewise treats training, tools and testing of practices as complementary aspects of capability (Barker et al., 2025, §6.5).

Address gaps and decide what can proceed

Each material capability gap has an owner, a funded or otherwise credible response, a target date and defined evidence of resolution. The transition manager tracks these actions and brings unresolved shortfalls to the responsible sponsor. The sponsor makes or obtains the required decision through the arrangements in section 3.4. The decision specifies what can proceed, what requires additional support and whether scope or sequencing needs to change. Bounded work can continue within existing permissions where its own requirements are satisfied, while wider gaps are addressed.

Example: resources and capabilities to obtain and interpret cryptographic configuration

For example, a bank may use an exercise to test whether staff can obtain and interpret cryptographic configuration evidence for the estate supporting online-banking connections. Staff can inspect the primary system, but have no agreed route for examining the recovery system managed by the supplier. The dependency owner arranges a supervised session with the supplier to collect evidence, and the sponsor secures the specialist capacity required for that work. Staff obtain and interpret the configurations, and an independent reviewer checks whether the findings answer the agreed question. The reviewed results demonstrate capability for the defined discovery task under the agreed access conditions. The estate owner can continue the authorised assessment within the access arrangements and capacity confirmed for it.

Key accountable party and responsibility	Expected result	Evidence of achievement
Executive sponsors: secure resources and make or obtain decisions on material shortfalls.	Confirmed resource commitments match the scope and timing of authorised work.	Resource commitments identify funding, capacity, timing and duration. Material shortages lead to decisions on additional support, limits on work, or changes to scope and sequencing.
Transition manager: consolidate needs, coordinate the demonstration and track capability gaps.	Plans reflect confirmed support, demonstrated capability and the work needed to address gaps.	Commitments, demonstration findings and assigned actions identify affected work and dates, distinguishing reported capability, planned improvements and demonstrated results.
Responsible owners and contributing functions: confirm availability, prepare personnel and demonstrate capability for assigned work.	Relevant functions can perform the specified work under the conditions covered by the evidence.	Commitments specify resources and timing. Results from exercises or applicable prior work show that personnel can perform the defined tasks using the required access, tools and facilities; limitations remain explicit.

Pillar review — Govern the transition

The pillar review brings together the findings from sections 3.1–3.6 to assess whether the bank can direct, support and control the work under consideration. It examines whether the mandate, ownership, decision arrangements, common requirements and demonstrated capability work together for the defined scope. Following the review approach in section 2.3, the conclusion identifies the work these arrangements can support, any remaining constraints and the actions or decisions needed.

Review question	Review focus
1. What is being reviewed?	Identify the work or commitment under consideration and the institutional arrangements needed to support it, including relevant legal entities, group relationships and shared functions. Establish the applicable scope, goals, exclusions and initial priorities, and the date or period covered. Make clear whether the review concerns preparation for new work or the adequacy of arrangements already in use.
2. What does the evidence establish?	**Direction and coverage (3.1–3.3)**: The mandate and responsibility map connect agreed goals, scope and initial priorities to accountable owners, including across sponsor remits and shared components. Goals have a basis for judging achievement; exclusions and unresolved scope questions have owners and remain subject to review. **Authority and requirements (3.4–3.5):** Assigned responsibilities have usable decision and escalation routes, reviews that provide effective challenge and defined arrangements for independent assurance. Owners can identify the approved policy and architecture requirements applicable to their work. Where group arrangements are used, they provide the authority and evidence needed to discharge local responsibilities. **Practical capability (3.6):** Confirmed funding, staff availability, access and facilities match the scope, timing and duration of the assigned work. Exercises or applicable prior work demonstrate the ability to obtain and interpret evidence, have it reviewed and respond to findings. Conclusions remain within the scope and conditions demonstrated.

Review question	Review focus
3. What remains unresolved?	Identify material gaps affecting the work under review, including disputed ownership, conflicting mandates or requirements, unavailable expertise or facilities, and weaknesses in review or escalation. Explain which responsibilities cannot be fulfilled or which activities and conclusions are limited as a result. Distinguish information to be obtained through planned investigation from missing access, authority or capability that prevents the investigation itself.
4. What action or decision follows?	Identify changes needed to mandates, assignments or requirements, and any additional capacity, access or training. Responsible owners address matters within their existing authority; executive sponsors make or obtain the necessary decisions under section 3.4. Where support remains insufficient, the decision specifies the work to be limited or deferred and the conditions for reconsidering it. The transition manager coordinates agreed changes and tracks assigned actions. Bounded work can continue within existing permissions where its own requirements are satisfied.

4 Assess and plan

The *Assess and plan* pillar establishes what needs to change to meet the bank's protection needs, and how the work can be delivered. It establishes the current cryptographic position and dependencies as a basis for assessing exposure, migration constraints and timing. These findings guide the choice of migration approach and target state, while proportionate testing or relevant existing evidence supports design approval. The integrated roadmap brings estate plans and delivery commitments together, addressing dependencies, resources and the sequence of work through required retirement.

These assessments, designs and plans develop as evidence becomes available. Findings from testing, implementation and operation may require earlier conclusions or commitments to be revised. Unresolved assumptions and delivery constraints remain visible in the affected plans.

Pillar outcome: The bank understands its current position and protection needs, has approved migration designs supported by evidence, and can explain how the required changes and retirement will be delivered.

PACT / PILLAR 2

Assess and plan

Understand the current position, justify migration designs and establish how required protection will be delivered.

Seven connected areas · key actors and results

4.1 Establish the current cryptographic position

Actors Estate owner substantiates records; technical contributors collect evidence; outcome owners confirm needs; specialist domain owner maintains methods.

Result Dated inventory links uses, deployments, outcomes and evidence; coverage gaps have owners.

4.2 Establish dependency requirements and readiness

Actors Estate owner defines needs; dependency owners obtain commitments and evidence; transition manager reconciles shared constraints.

Result Readiness assessed for a defined action; forecasts, commitments and demonstrated capability remain distinct.

4.3 Assess exposure, migration constraints and timing

Actors Outcome owners confirm needs and limits; estate owner assesses exposure and timing with technical, operations and dependency contributors.

Result Traceable urgency, required starts and owned responses; uncertainty distinguished from infeasibility.

4.4 Select the migration approach and proposed target state

Actors Estate owner compares options; technical contributors design; outcome, operations and dependency owners substantiate requirements and constraints.

Result Justified target and route specify acceptance criteria, recovery, coexistence and required retirement.

4.5 Test design feasibility and suitability

Actors Estate owner defines questions; technical contributors assess and test; outcome and operations owners assess findings; reviewers challenge conclusions.

Result Applicable test evidence supports design choices; limits, retests and remaining release validation are explicit.

4.6 Approve the design and interface profiles

Actors Estate owner assembles the baseline; dependency owners secure interface agreements; specialist domain owners and reviewers assess; assigned approvers decide.

Result Versioned approved design and agreed profiles, with scope, conditions and remaining validation explicit.

↕

4.7 Agree the integrated transition roadmap

Actors Transition manager integrates; responsible owners substantiate plans and commitments; executive sponsors agree priorities and secure resources.

Result Dated roadmap reconciles priorities, deadlines, dependencies, critical paths, capacity, funding and required retirement; uncertainty remains visible.

Evidence ↓ ↑ Decisions and follow-through

Recurring pillar review

Is the response justified by exposure, applicable evidence and credible delivery arrangements?

Scope
Which outcomes, estates, connections and proposed investigation, design decision or delivery commitment are being reviewed?

Evidence
Do inventory, dependency and timing findings, design evidence and delivery commitments support that work?

Unresolved matters
Which evidence, interface or capacity gaps affect feasibility? Is timing uncertain or already infeasible?

Action or decision
Obtain evidence; revise designs or sequencing; secure resources or safeguards; define supported work and conditions.

Design approval and roadmap agreement do not authorise production deployment.

Assessment and planning continue as evidence and delivery conditions change.

Figure 3 Assess and plan at a glance

4.1 Establish the current cryptographic position

Assessment and planning require a clear account of where cryptography is used, what it protects and what the available evidence establishes about its deployed state. The **cryptographic inventory** provides this account by linking cryptographic uses and deployments to protected outcomes, owners, dependencies and supporting evidence. Its purpose is to support decisions about exposure and change within a clearly identified scope. The cryptographic estate owner is accountable for the adequacy of this account within the estate's approved scope.

Define the scope and protection context

Within the approved scope, the estate owner identifies the systems, applications, information and connections to be examined. Coverage includes relevant recovery environments, fallback arrangements and inactive capabilities that could affect protection or operation. Where a component's internal cryptography cannot be inspected, the component remains visible in the inventory, together with the party controlling it and the limits of available information.

Outcome owners confirm the required protection, how long it is needed and the consequences of failure. Each material cryptographic use is linked to these requirements and to its estate, responsible owners and dependencies. These links give the technical findings their business context (FS-ISAC Post-Quantum Cryptography Working Group, 2023c, pp. 2–4).

The technical record identifies the cryptographic function, algorithms and parameters, protocols, implementation and version, deployed configuration, and relevant keys and certificates. Certificate records distinguish the algorithm of the holder's public key from the algorithm used by the issuer to sign the certificate, since these may require separate changes (Cooper et al., 2008, §§4.1.2.3, 4.1.2.7).

Gather and interpret the evidence

Discovery may begin with existing enterprise records, specialist tooling, targeted investigation or a combination suited to the bank's circumstances. Available sources may include application and infrastructure inventories, configuration records, certificate and key systems, vulnerability tools, application-security results and software-supply-chain records. A source catalogue identifies each source's purpose, owner, covered population, collection method, refresh arrangements, known omissions and basis for confidence. It explains what the source can establish for a particular decision and where corroboration or further investigation is needed.

The inventory distinguishes what a product supports, which capabilities are installed, what configuration permits and what has been observed in use. These distinctions guide how findings from different sources are interpreted.

The inventory can be populated in successive levels of detail. Initial records can locate systems, owners and relevant business services; further investigation can establish connections and dependencies, followed by the cryptographic functions and configurations needed for the decision. Retain explicit unknowns and coverage gaps at every level. The common model supplies a consistent destination for that information, rather than a requirement to complete every field across the institution before useful assessment begins.

Technical contributors, supported by the operations owner, select discovery methods suited to the environment and combine their findings with relevant enterprise records where available (FS-ISAC Post-Quantum Cryptography Working Group, 2023c, pp. 7–11; Newhouse et al., 2023, §§1.4, 3.2). These methods may include examining code and installed software, observing running applications and network traffic, and targeted manual investigation. The dependency owner obtains relevant supplier or group evidence. Together, these sources populate and enrich the cryptographic inventory.

Before relying on a discovery tool, technical contributors check it against known cases in the intended environments, recording missed or incorrect findings and coverage limits. With the operations owner, they establish safe collection conditions and assess possible operating effects, particularly for active scanning or tracing running applications.

For example, build inspection may identify an available mechanism, deployed-software inspection may locate the library and configuration carrying it, and a connection trace may show which mechanism was selected. An included capability with no supporting deployed-state evidence remains a question for investigation. A deployed library with no observed traffic may reflect an unexercised path.

An established endpoint or enterprise-management service may offer a suitable deployment route for discovery tooling. Assess its population coverage, access arrangements, communication paths and operating effects, including environments it cannot reach. Reusing the channel can simplify distribution, but it does not replace assessment of the discovery tool or the permission required for its collection activity.

Repeated observations require careful interpretation. Several tools may report the same component in one deployment, while the same component identity may also appear in genuinely separate deployments. Keep these relationships explicit, retain the source observations and record the reason for consolidation or separation. Shared-platform ownership remains linked to each dependent use.

Keep records consistent and traceable

Findings may be recorded or exchanged through a **cryptographic bill of materials** (CBOM), a structured record of cryptographic assets and their dependencies (Hess, 2026). A CBOM may represent some or all of the inventory information; its scope, contents and supporting evidence determine what it establishes. When incorporating or linking a CBOM, contributors identify whether it describes, for example, a software release or a particular deployment, and add or verify the bank's deployment, outcome and ownership information as needed.

Each finding retains its source, collection date, method, relevant version and limitations. Code findings may identify unused capabilities, while observations cover only the paths and periods examined. Failure to observe a use does not, by itself, establish its absence. Technical contributors reconcile findings about the same deployment and keep conflicting observations visible until their differences are explained.

To allow findings to be combined across estates, the specialist domain owner responsible for inventory methods maintains common definitions, identifiers and quality rules. Shared components have consistent identifiers linked to each affected use, while separate deployments remain distinguishable. Existing systems can hold the records, provided their relationships and supporting evidence remain traceable.

The definitions are maintained independently of any exchange format, with documented mappings to the formats and versions used. When records are imported, exported or converted, checks confirm that material findings, their meaning, source information and dependency links are preserved. Any material loss or change is assessed before the transferred records support a decision.

Establish what the inventory supports

For a material assessment, the estate owner preserves a dated, versioned inventory snapshot identifying the scope and evidence relied upon. The owner assesses whether the coverage, traceability, currency of evidence and treatment of conflicting findings support the proposed conclusions. Unexamined areas remain explicit. Each material gap has an owner, a response and a due date, together with an explanation of its effect on the assessment.

Assessment may proceed within existing authority for the scope supported by sufficient evidence while further discovery addresses outstanding gaps. The conclusions remain limited to that scope. Earlier snapshots are retained so that the bank can distinguish changes in deployed cryptography from changes in its knowledge or coverage. Continuing inventory maintenance is addressed in section 6.1.

Example: CBOM for banking gateway

For example, a supplier provides a CBOM for software installed on a banking gateway. The CBOM lists a post-quantum key-establishment algorithm in an included library, while configuration records and observed connections show use of a traditional mechanism. The estate owner links these findings to the same deployment, distinguishing what the installed software contains from what the gateway is configured and observed to use. The recovery configuration remains unexamined. The estate owner

records the gap and its effect on the assessment, and the operations owner arranges inspection with a due date. Assessment may proceed within existing authority for the examined scope, with the recovery gap explicit. Conclusions covering the full estate require evidence addressing that gap.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate owner: establish the estate's current position and assess whether the inventory supports the proposed conclusions.	Assessments have a clear scope and an adequate evidence base, with limitations understood.	A dated, versioned inventory snapshot links material uses to outcomes, deployments, owners and dependencies; gaps identify their effects, responses, owners and due dates.
Specialist domain owner: maintain common inventory definitions, methods and quality rules.	Information can be consistently combined and interpreted across estates and exchange formats.	Applied definitions, identifiers, format mappings and quality checks preserve meaning and relationships, distinguish deployments and expose conflicts.
Operations and dependency owners, with technical contributors: establish deployment facts and obtain relevant provider evidence within their remits.	Findings distinguish supported and installed capabilities, permitted settings and observed use.	Discovery and tool-check results, collection conditions, configuration records, observations and supplier evidence retain sources, dates and limitations; discrepancies have follow-up actions.

4.2 Establish dependency requirements and readiness

Transition work may depend on a supplier release, a shared internal platform or coordinated action by another organisation. Dependency assessment establishes what each material dependency needs to provide, when it is needed and whether the available evidence supports the bank's intended next step. This helps the bank identify what work can proceed and what remains conditional in its transition plan.

Define the required contribution and who controls it

Using the inventory under section 4.1, the cryptographic estate owner identifies the internal, group and external dependencies that materially affect the estate's transition. These may include shared certificate and key-management services, technology platforms, suppliers, counterparties and financial market infrastructures. Existing operational-resilience maps provide a starting point for dependencies supporting critical operations (BCBS, 2021a, Principle 4).

For each material dependency, the estate owner defines the required contribution with relevant outcome, operations and specialist domain owners. An identified dependency owner within the bank works with the party controlling that contribution to establish its scope, prerequisites, proposed delivery date and available evidence. Requirements may concern a particular product version, compatible protocol, hardware replacement, testing access or joint testing window. The date needed by the bank remains distinct from the date offered by the controlling party.

For cloud services and hosted software, the record identifies how control over algorithms, keys, trust arrangements, configuration and updates is divided between the bank and provider, including changes only the provider can make. This allocation is established for the particular service (FS-ISAC Post-Quantum Cryptography Working Group, 2024, pp. 16–17). Requirements and dates are refined as migration options and designs develop, with links maintained to every affected estate and outcome.

Assess readiness for the intended action

Readiness is assessed for a specified action, such as beginning joint testing. With operations and specialist contributors, the estate owner assesses whether the available evidence supports that action for the bank's product, version and intended use, and identifies any further integration or testing needed. A supplier's

successful test establishes what was demonstrated within its stated scope; its relevance to the bank's environment still needs to be assessed.

An application-wide readiness label can conceal differences between cryptographic uses and their dependencies. Assessment therefore addresses the material uses involved in the intended action, with scope and priorities informed by their protection needs, exposure and consequences (section 4.3). These uses may concern communications, stored information, authentication or signatures. Records identify the relevant components and controlling parties, current evidence, intended change and next feasible action. For communications, they also identify endpoints and termination points. Outstanding prerequisites remain linked to the parties able to resolve them.

A forecast estimates future delivery. A commitment identifies an agreed contribution and date. Test or validation evidence establishes demonstrated capability within a defined scope. Records preserve these distinctions, together with the source, date, applicable product or service, conditions and limitations.

For supplier-controlled cryptography, the dependency owner obtains evidence relevant to the bank's use, including controls and changes the bank cannot inspect directly. The evidence covers supported cryptographic capabilities, compatibility constraints, upgrade or replacement arrangements, testing access, continuing support and material upstream dependencies.

Early supplier engagement helps the bank understand delivery timelines and secure the information and support needed as work develops. Through existing procurement and supplier-management arrangements, the bank seeks proportionate PQC provisions in contracts and service-level agreements covering evidence, change notification, testing, support, remediation and escalation (Cross Market Operational Resilience Group, Cyber Coordination Group, 2025, §6).

Initial engagement need not wait for a detailed supplier roadmap; it identifies the critical products and services, the bank's uses that they support, the parties controlling change and whatever transition information is available. Record indicative plans and unanswered questions with their limitations. A missing roadmap requires an owned response; it does not establish either compatibility or permanent inability to migrate.

Address shared constraints and practical alternatives

Several estate plans may rely on the same supplier, platform, upstream component or testing facility. A delay or failure in that shared dependency can therefore affect several plans together (Hui et al., 2012). The transition manager brings the owners' findings together to identify these common constraints and coordinate their treatment across the affected estates.

Where the constraint is material, responsible owners assess practical alternatives, including their lead time, compatibility, cost and continuity implications (Financial Stability Board, 2023, §§3.7–3.8). A contractual exit right requires a practical means of exercising it. For material third-party service dependencies, the assessment establishes whether exit or substitution can be carried out with the available time, people, infrastructure, knowledge and data. Relevant arrangements are tested proportionately (BCBS, 2025, Principle 9, paras. 61–66).

Manage uncertainty and keep plans current

Where readiness remains uncertain, the dependency owner identifies what is missing and coordinates the response, with responsible contributors and a review date. The response may involve further investigation, prerequisite work, safeguards, escalation or assessment of an alternative. The estate owner identifies what work the evidence supports and any necessary conditions. Unaffected work may continue within existing authority. Required review and decisions to accept residual risk or depart from approved requirements follow the arrangements in section 3.4.

The dependency owner communicates material changes in scope, evidence or dates to affected owners and the transition manager so that assessments and plans can be revised. The resulting dependency assessment informs the timing analysis under section 4.3 and the integrated roadmap under section 4.7. Forecasts, unresolved conditions and confirmed commitments retain their distinct status in those plans.

Existing supplier-management arrangements are used to review significant dependencies and convene technical sessions when a specific decision needs them. As products and requirements become

supportable, obtain more precise release commitments, interface evidence, test participation and support arrangements. Purchasing and contractual expectations can likewise develop from transparency and future transition support towards specific deliverables and evidence. When the position changes, previous statements and dates should be preserved.

Example: dependency on supplier's gateway software for interoperability testing

For example, two cryptographic estates use the same supplier's gateway software and need an upgraded release before interoperability testing can begin. The supplier's roadmap gives June as the release date, but access to the release for testing remains unconfirmed. The dependency owner records June as a forecast, seeks a commitment covering both the required release and testing access, and sets a review date. The transition manager reflects the shared constraint in both estate plans. Test preparation can continue within existing approvals, while the testing dates remain provisional until confirmed.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate owner: define dependency requirements and assess readiness for the intended action.	Dependencies reflect the estate's protection and transition needs, with planned reliance bounded by the evidence.	Requirements link affected uses and outcomes to capabilities, prerequisites and dates; assessments identify the supported action, applicable evidence and outstanding conditions.
Dependency owner: obtain commitments and evidence, coordinate follow-up and communicate changes.	Each material dependency has a supported readiness position and an owned response to outstanding constraints.	Records identify controlling parties, required and offered dates, forecasts, commitments and demonstrated capabilities; gaps have actions, responsible parties and review dates.
Transition manager: bring together shared dependencies and coordinate their treatment across estates.	Common constraints and concentration are reflected consistently in transition planning.	Plans identify affected estates, shared constraints and their consequences; material changes are incorporated and conflicts are escalated.

4.3 Assess exposure, migration constraints and timing

A credible transition plan should connect the bank's protection needs with the work required to address its exposure. It establishes how urgently action is needed, how long the change is likely to take and when work needs to begin. The findings guide the choice of migration approach and identify where further investigation, prerequisite work or interim protection is needed.

Establish protection needs and exposure

Using the inventory evidence, the cryptographic estate owner identifies the vulnerable mechanism, how it could be compromised and the outcomes that would be affected. For each material cryptographic use, the assessment considers three factors:

- **Protection or trust period**: how long confidentiality, authenticity or integrity needs to remain effective, including later reliance on retained records.
- **Exposure**: how readily an attacker could obtain the protected material or reach the relevant function, considering live, stored and recovery environments.
- **Consequences**: the potential harm from disclosure, forgery, false authentication or disruption, including effects on customers and critical operations.

Together, these factors establish the urgency of a response. Outcome owners confirm the protection periods and consequences, distinguishing uses with materially different needs within the same estate. For

confidential information, the relevant period is how long disclosure would remain harmful. The record-retention period may inform that judgement but does not determine it.

Assess the work and time required

The estate owner examines what addressing the exposure would involve, with technical, operations and dependency contributors. The assessment covers solution availability, implementation effort and cost, operating constraints and the dependency requirements established under section 4.2.

Separate ratings can help compare protection urgency and migration difficulty (Europol, 2026, pp. 8–10). The specialist domain owner responsible for the assessment method maintains common criteria that keep the underlying evidence, severe consequences and material uncertainty visible. These ratings support comparison; they do not measure compromise probability or establish elapsed migration time.

A simple preliminary screen may be useful before detailed evidence exists. Existing service-criticality records, information classifications and connectivity information can act as labelled proxies for a stated question. Record their dates, owners, limitations and any conflicting information. A proxy-based priority should trigger appropriate investigation and remain open to revision; it should not be reported as a quantified reduction in business risk.

Scheduling requires an estimate of the remaining elapsed time for a defined protection target. The estate owner's estimate covers preparation, supplier lead times, engineering, testing, deployment, stabilisation and any retirement needed to meet that target. It accounts for available capacity, dependencies and activities that can proceed concurrently. Initial estimates may compare candidate approaches, with assumptions recorded and refined as design and testing provide better evidence.

Establish the applicable completion limits

The estate owner identifies the applicable dates and the actions they constrain: beginning work, completing protection, procurement or new use. A completion deadline specifies when the required protection needs to be in place. Each date retains its source, scope and authority, distinguishing binding requirements, bank commitments and external planning references under section 3.2.

For quantum-threat timing, the relevant specialist domain owner maintains the supporting evidence and proposes a common range of credible dates at which a quantum computer could defeat the relevant cryptography. Appendix B provides evidence that can inform this range. The authority assigned under section 3.4 approves the range, with the covered mechanisms and assumptions recorded.

PACT recommends using the earliest date in the approved range as a conservative planning basis. Estate assessments record any justified difference in applicability. Using a different planning basis requires a recorded rationale, its consequences and the decision required under section 3.4. The selected date is a planning assumption, not a prediction, and does not override binding requirements.

The effect of this assumption on the completion limit depends on the protection concerned.

Continuing flows of confidential information. Each new transmission needs protection for its required confidentiality period. Subtracting that period from the quantum-threat date establishes when the bank needs to stop sending new information under vulnerable cryptography (Mosca, 2018; ETSI, 2024, §6.8). This addresses the risk that encrypted traffic collected now could be decrypted later. Migration cannot undo the exposure of vulnerable ciphertext already collected by an attacker.

Fixed archives and backup copies. The outcome owner identifies when disclosure of the existing information would cease to cause harm. The estate owner compares this sensitivity end date with the selected quantum-threat date and examines the exposure of the stored ciphertext and any route to recovering its protecting keys. The response and timing follow that assessment. The subtraction used for continuing flows does not apply automatically. Ongoing creation of backups may introduce new information with different protection periods.

Authentication and signatures. The assessment establishes how long credentials, signatures or retained signed records need to remain trustworthy, when continued reliance on the existing mechanism becomes unacceptable, and whether earlier action is needed to preserve evidence of authenticity. Long-term signature preservation may, for example, require renewal of supporting evidence before its cryptographic

protection becomes unreliable (Gondrom et al., 2007, §§1.1–1.2). The completion limit follows these requirements; a record-retention period is not automatically subtracted from the quantum-threat date.

The governing completion deadline is the earliest applicable limit for the scope and protection target being assessed. It may arise from these protection needs, a binding obligation, an authorised commitment, end of support or planned retirement. Each limit is assessed against the same scope and completion condition.

Determine when work needs to begin

The estate owner works back from the governing completion deadline to establish the latest credible start under the stated assumptions. The calculation deducts the remaining migration duration and a separate contingency allowance for credible delay and rework, while observing any earlier binding start deadline:

Required start = earlier of (governing completion deadline minus remaining migration duration minus contingency allowance) and any applicable binding start deadline.

Where no binding start deadline applies, the calculation based on the completion deadline governs. Procurement and new-use restrictions continue to constrain their respective activities separately. The contingency allowance remains distinct from the duration estimate so that the same allowance is not counted twice.

The result identifies the date by which work needs to begin under the assessed approach. The urgency of the exposure or the need to resolve prerequisites may justify earlier action.

Act on the findings and keep plans current

Where inputs are uncertain, supported ranges or scenarios show how earlier quantum capability or delivery delays would affect the result. If a material input cannot be bounded credibly, the assessment states that timing remains unresolved and identifies the missing evidence, its owner and a response date. Known urgency and completion limits remain visible. Where evidence shows that the assessed approach cannot meet a completion limit under the stated assumptions, the estate owner records the cause and obtains the required residual-risk decision under section 3.4.

The estate owner coordinates the response within existing authority. This may involve progressing a supported approach, initiating prerequisite work, investigating alternatives or applying interim protection. A required-start date that has passed prompts immediate reassessment and any necessary residual-risk decision. Each resulting action has an owner, a date and clear conditions.

The transition manager incorporates shared constraints and required dates into the integrated roadmap under section 4.7. Changes to protection needs, dependency evidence or delivery assumptions lead to coordinated revisions across the affected assessments and plans.

Example: confidential information sent through a banking connection

For example, suppose information sent through a banking connection needs six years of confidentiality. The selected quantum-threat date in this illustrative assessment is ten years from now, leaving four years to stop sending new information under vulnerable cryptography. The estate owner estimates three years for the complete change, with a further year of contingency. Assuming no earlier completion or binding start deadline applies, the required start is now.

The estate owner coordinates preparation and prerequisite work within existing authority, referring additional resource or risk decisions to the relevant approvers. If supplier evidence subsequently lengthens the migration estimate under the same assumptions, the calculated start falls in the past. This prompts immediate reassessment of the approach, timing and interim protection.

Key accountable party and responsibility	Expected result	Evidence of achievement
Outcome owners: confirm protection needs, consequences and applicable limits.	The assessment reflects what needs protection, for how long and with what consequences of failure.	Confirmed protection or trust periods, sensitivity end dates where relevant, consequences and applicable limits are linked to the affected outcomes.
Cryptographic estate owner: assess exposure, migration constraints and duration, and coordinate or escalate the response.	Urgency and timing have a clear basis and lead to action, with uncertainty and infeasibility explicit.	Evidence supports the assessment, applicable deadlines, duration estimate and required-start calculation, or explains why timing remains unresolved or infeasible; actions identify owners, dates and conditions.
Relevant specialist domain owners: maintain assessment methods and evidence, and propose common quantum-threat assumptions.	Assessments use consistent criteria while preserving material differences and uncertainty.	Criteria and supporting evidence are maintained; the approved threat range and planning basis retain their version, scope, assumptions and justified differences in applicability.
Transition manager: incorporate shared constraints and timing implications into institutional planning.	The integrated roadmap reflects the assessments governing delivery.	Plans retain material drivers and required dates; changed assumptions lead to coordinated updates across affected estates.

4.4 Select the migration approach and proposed target state

The assessment of exposure and timing establishes what needs protection and when action is needed. The bank should translate those findings into a justified migration approach and a proposed target state: the cryptographic arrangements and operating conditions it intends to achieve. The proposal explains the choice, the route to the target and the criteria for assessing its suitability. It provides the basis for investigation or testing under section 4.5 and subsequent design approval under section 4.6.

Compare the practicable approaches

The cryptographic estate owner compares practicable approaches with technical contributors and relevant specialist domain owners. Options may include modifying a system, obtaining a supplier upgrade, moving to a supported platform or shared service, replacing components, protecting specified connections through a gateway, isolating or restricting an exposed function, or retiring the affected use. Continued use until an approved retirement date is also an option to assess.

The comparison considers protection needs, operating fit, support life, dependencies, delivery time and lifecycle costs, including parallel operation, legacy support and withdrawal. It also examines technical or organisational dependencies that could obstruct the withdrawal of earlier arrangements (Furneaux and Wade, 2011; Rinta-Kahila et al., 2023). The reasons for preferring an approach should follow from this comparison. System changes and cryptographic choices are developed together because each affects which options are practicable.

Define the proposed target state

For the preferred approach, the proposal identifies the affected cryptographic uses and connections, their intended protection and the supporting components. It specifies algorithms and parameter sets, together with the protocol and certificate profiles governing how connected systems will use them. Candidate implementations are identified by product, version and configuration. Their current validation status and scope, including algorithm or cryptographic-module validation, are recorded with supporting evidence, limitations and unmet requirements.

Technical contributors, supported by relevant specialist domain owners, define the key, certificate and trust arrangements. These cover how keys are generated, protected, used and destroyed, with recovery

where appropriate; how certificates are issued, renewed and revoked; and the trusted issuers, relying systems and hardware involved (ETSI, 2020, §6). Dependency owners substantiate supplier and counterparty assumptions using the evidence under section 4.2. Vulnerable connections and continuing obligations outside the immediate change remain explicit.

The controls also reflect the particular cryptographic functions being used:

Cryptographic function	What the design establishes
Key establishment	How public keys are linked to intended parties, how working keys are derived from the shared secret, whether and how agreement on those keys is confirmed, and how failures are handled (Alagic et al., 2025, §§3.3, 4.2–4.4).
Stateful hash-based signatures	How the record of one-time signing keys already used is protected and updated to prevent reuse during both normal operation and recovery (Cooper et al., 2020, §§8.1, 9.1).
Long-lived signed records	How verification evidence is preserved and renewed where necessary, including renewal of archival timestamps before the earlier protection becomes unreliable (Gondrom et al., 2007, §§1.1–1.2).

Where hybrid protection is proposed, the design explains how traditional and post-quantum algorithms contribute jointly to the same cryptographic operation. Operating the mechanisms alongside each other does not, by itself, establish hybrid protection (Driscoll et al., 2025, §2). A hybrid key-establishment design identifies the combiner—the method joining the component contributions—and substantiates its suitability (Alagic et al., 2025, §4.6). A hybrid signature design specifies which component signatures must verify, how failures are handled and why the acceptance rule provides the intended protection (Driscoll et al., 2025, §§5–6).

Where mechanisms are negotiated, the design explains how negotiation is authenticated and unauthorised weaker choices are prevented (Barker et al., 2025, §3.2.3).

The design also preserves a practicable route for later cryptographic change. Applying section 3.5, technical contributors explain how components or configurations can be replaced, permitted choices controlled and actual use observed, with relevant specialist domain owners supporting the application of common requirements. The proposal identifies responses to hardware, certification and supplier constraints (Barker et al., 2025, §§5.2–5.4). Any proposed departures from common requirements identify the safeguards, review or remediation conditions and decisions required under sections 3.4–3.5.

Explain the transition and retirement arrangements

The proposal describes how the bank will move from its current arrangements to the target. Where predecessor and replacement mechanisms coexist, it identifies the purpose, scope, permitted uses, expected duration or continuing justification, and the withdrawal conditions required by the target. Continued use until retirement requires an approved end date and operating conditions justified by the exposure and timing assessment.

Fallback and recovery arrangements define their triggers, permitted configurations and conditions for returning to the intended operating state. These arrangements prevent recovery from silently reintroducing prohibited cryptographic use. Legacy capabilities retained solely to decrypt historical information or verify earlier signatures remain confined to those purposes.

The route can contain enabling changes before the intended cryptographic replacement. A protocol or platform upgrade, including a move to TLS 1.3 where relevant to the chosen implementation, may improve current security and provide a basis for later post-quantum deployment. Each change identifies the later action it enables and the evidence that its own objectives have been met. Reporting recognises these benefits and the completion of enabling work, while distinguishing them from the post-quantum protection demonstrated for the affected use. That protection depends on the mechanisms actually used and the scope of the evidence; the protocol version alone does not establish it.

Retirement requirements follow section 3.5. They distinguish traditional components retained within an acceptable hybrid target from vulnerable uses that require withdrawal.

Set the acceptance criteria

The proposed protection and operating arrangements determine what needs to be demonstrated. Outcome owners confirm the required protection and service behaviour. The operations owner and technical contributors translate these requirements into measurable criteria for compatibility, message handling, latency, capacity, availability and recovery, as relevant.

The criteria reflect the intended systems and workloads, including peak demand and recovery conditions. They account for changes in key, signature, ciphertext and certificate sizes, and establish how the design will demonstrate its security controls, continuing access to encrypted information and verification of retained records.

Prepare the proposal for assessment and testing

The estate owner brings together the proposed design, alternatives considered, selection reasons, supporting evidence and unresolved assumptions for review. Review identifies the questions to resolve through investigation or testing under section 4.5. Final design and interface-profile approval follows section 4.6.

Material changes in exposure, cost, support or timing prompt reconsideration of the approach and roadmap. Earlier assumptions and the reasons for revision remain available, and the transition manager coordinates the consequences across affected estates.

Example: legacy payments application migration

For example, a legacy payments application cannot directly support a proposed protocol, so the estate owner proposes a gateway while the application is replaced. The proposal distinguishes the intended protection of the gateway's external connection from the protection and remaining exposure of its internal connection to the application. It identifies the gateway configuration, available validation evidence, support costs and conditions for ending the interim arrangement.

Review identifies compatibility and recovery questions for a bounded test, which the estate owner arranges within existing authority. The findings inform the proposal and subsequent design approval. Production deployment remains subject to the release evidence and authorisation under section 5.2.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate owner: compare approaches and assemble the proposed target and transition route.	The preferred approach connects protection needs to a practicable route to completion.	The proposal records alternatives, selection reasons, lifecycle costs, dependencies, interim arrangements, withdrawal conditions and questions for assessment.
Outcome owners: confirm protection and service requirements.	The proposed change addresses the outcomes it is intended to protect.	Requirements and acceptance criteria identify the protection, service behaviour and continuing obligations to be demonstrated.
Technical contributors with specialist domain owners: develop and substantiate the design, and guide the application of common requirements.	Technical choices and controls are sufficiently defined for assessment, testing and later change.	Mechanisms, profiles, implementations, controls for relevant cryptographic functions, validation evidence, constraints and proposed departures are recorded with their supporting basis.

Key accountable party and responsibility	Expected result	Evidence of achievement
Operations owner and dependency owners: establish operating requirements and substantiate contributions controlled by other parties.	The proposal accounts for operating conditions, recovery, support and dependencies.	Measurable operating and recovery criteria, provider evidence and unresolved prerequisites inform the design and the questions for testing.

4.5 Test design feasibility and suitability

Practical evidence is needed to determine whether a proposed design can meet its protection and operating requirements. This step uses existing evidence and, where needed, further investigation or testing to resolve questions that could affect the design or its acceptance. The findings support a decision to retain, revise or discontinue the proposed approach and inform design approval under section 4.6.

Identify the questions and assess existing evidence

Based on the acceptance criteria under section 4.4, the cryptographic estate owner and technical contributors identify what needs to be demonstrated and which uncertainties could affect the design, priority, cost, timing or conditions for acceptance. The scope and depth of assessment reflect the consequences of failure, the novelty of the approach, its dependencies and remaining uncertainty. Relevant specialist domain owners guide the assessment methods and application of common requirements.

Technical contributors first assess available internal results, supplier evidence and relevant external experience against the proposed requirements and intended operating conditions. The assessment considers material differences in versions, configurations, profiles, hardware, interfaces and workloads. It explains what the evidence supports, how differences limit its use and what questions remain unresolved.

Algorithm or cryptographic-module validation is used within its defined scope; it does not by itself establish that the bank's connected systems will meet their requirements. Published experience can help identify questions for investigation, but conclusions about the bank's design require evidence applicable to its intended use.

Plan and conduct proportionate investigations or tests

For questions requiring further practical assessment, technical contributors select conditions that can provide a useful answer. A pilot, where needed, is a bounded trial addressing a stated design uncertainty. For example, Europol suggests trials on representative but non-critical websites to assess performance and interoperability before implementation (Europol, 2026, p. 20). The test record states the question and explains why the selected scope, environment, build, configuration, interface profiles and workload can answer it. It also specifies the evidence to collect, stopping conditions and recovery arrangements.

Outcome and operations owners confirm the relevant protection and service thresholds before execution. Dependency owners secure the necessary counterparty participation and configuration evidence. A pilot affecting production remains subject to the controls and approvals for that production action.

A path-based pilot can extend the existing test record with the connection's baseline, intended change, responsible controlling parties, unresolved prerequisites, test findings and the action now supported. This allows evidence from a feasible connection to inform the design while a different connection remains under investigation or awaits an enabling contribution. A key-establishment result retains that function-specific scope.

Testing exercises the components and connections needed to answer the stated questions. Depending on the proposed use, this may include security controls, certificate and trust handling, interoperability, message-size limits, capacity, performance, failure behaviour, fallback and recovery, including relevant peak-demand conditions. Structured risk mitigation of this kind pays off most where technical project risk is high, as field evidence from IT project teams shows (Maruping et al., 2019).

Security assessment includes relevant side-channel exposure, where observable implementation behaviour, such as execution time or power consumption, may reveal secret information. The assessment considers safeguards suited to the intended implementation and possible attacker access, using applicable supplier or independent evidence and additional testing where material questions remain (Alagic et al., 2025, §3.3).

Performance measurements distinguish algorithm execution from the behaviour of the full protocol and certificate processing on the intended hardware and workload. The recorded build, configuration and workload allow results to be reproduced. Any comparison identifies its baseline: the configuration or results used as the reference.

Interpret the findings and revise the proposal

Technical contributors record results against the stated criteria, including unsuccessful or inconclusive tests, defects, resource use, relevant effort and costs, limitations and retests. The estate owner explains which design assumptions are supported, rejected or unresolved and whether the findings support retaining, revising or discontinuing the approach. Outcome and operations owners assess the protection, service and recovery implications, with relevant specialist domain owners supporting technical interpretation.

Material design changes trigger reassessment of the supporting evidence and retesting of affected requirements. Earlier evidence may continue to be used where its applicability to the revised design is justified. If acceptance criteria are revised, the record preserves the earlier criteria, explains the change and includes any necessary approval.

Each unresolved question has an owner, a proposed response and a target date. Material effects on exposure, cost or timing feed into reassessment and roadmap updates.

Establish support for design approval

Reviewers assess whether the evidence supports the conclusions drawn and whether its limitations are adequately reflected, with independent assurance where required under section 3.4.

The estate owner consolidates the findings and review results for the design decision under section 4.6. The record distinguishes questions that must be resolved for that decision from testing still needed for the actual release intended for deployment. Where evidence is insufficient for the proposed design scope, the record identifies the further work or narrower scope to be considered.

For the remaining release work, the record identifies the tests, thresholds, dependencies and responsible owners. A pilot result supports only the scope and conditions examined; wider deployment requires applicable evidence and the necessary authority.

Example: testing of proposed payment gateway

For example, a bank tests the gateway proposed in section 4.4 using a recorded configuration and representative payment workload. Normal operation meets the agreed performance criteria, but recovery restores an earlier configuration that permits a prohibited cryptographic choice. The estate owner requires the recovery design to be corrected. Technical contributors repeat the affected recovery and negotiation tests, while the operations owner assesses the revised recovery procedure. Successful earlier results are retained only where their applicability to the revised design is justified. The findings support review of the revised design, while the actual release intended for deployment still requires qualification.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate owner: define the questions and consolidate the findings, their implications for the design and the remaining work.	The proposal reflects what the evidence establishes and the uncertainty remaining.	Findings linked to design choices, revised planning assumptions and outstanding questions, with proposed responses, owners and dates. Remaining release tests, thresholds and dependencies are identified.
Technical contributors: assess existing evidence, conduct investigations or tests and record results.	The assessment is reproducible, applicable to the proposed use and consistent with common requirements.	The selection rationale, test conditions, configurations, workloads, comparison baselines, criteria, results, relevant costs, limitations and retests substantiate the conclusions.
Dependency owners: coordinate supplier and counterparty contributions.	Relevant dependencies are represented and the limits of their contribution are understood.	Participation and configuration evidence, joint-test results and unresolved dependencies are recorded.
Reviewers: assess the adequacy of test evidence and the limits of its conclusions.	Conclusions are supported within the examined scope and conditions.	Review findings identify supported conclusions, evidence limitations and further work needed.

4.6 Approve the design and interface profiles

Design and testing establish a basis for deciding what the bank should implement. Approval turns that work into a defined design baseline: the versioned design, settings and requirements against which subsequent changes are prepared and assessed. Design approval establishes which design and interface profiles the bank may use to prepare a change, and the conditions that apply.

Bring the design and evidence together

The cryptographic estate owner brings together the design developed under section 4.4 and the findings from section 4.5. Technical contributors update the proposal to reflect those findings, so the version submitted for approval is supported by the available evidence. The proposal identifies the affected uses and connections, the acceptance criteria and any limits on the products, versions or configurations covered. It also retains the operating, recovery and retirement conditions. Material changes to the tested design require reassessment and retesting of the affected requirements.

Relevant specialist domain owners assess conformity with the common requirements in section 3.5, including applicable jurisdictional requirements. The supporting references identify the standards and guidance used, their editions, status and what they establish for the proposed design. Publication status should be interpreted alongside purpose. NIST's draft key-generation guidance proposes methods for deriving and regenerating key pairs from secret values, with associated protection and device-boundary conditions (Dang et al., 2026, §4.2). The final version of NIST's first call for multi-party threshold schemes concerns techniques that distribute cryptographic operations and secret-key control among several parties; it invites submissions and analysis, without establishing approved schemes (Brandão and Peralta, 2026). Any reliance on draft or exploratory material should be explicit, with recorded assumptions and conditions for review.

Confirm the interface profiles and agreements

The interface profiles specify how the systems on each connection will work together. Technical contributors confirm the profiles developed under section 4.4 against the configurations and evidence assessed under section 4.5. Each profile covers the protocol, algorithms and parameters, certificate and trust arrangements, negotiation, and permitted fallback and recovery behaviour. For example, RFC 9954 provides an Informational construction for hybrid key exchange in TLS 1.3, while RFC 10024 specifies particular combinations of traditional elliptic-curve key agreement and ML-KEM as a Proposed

Standard, a published specification on the Internet Standards Track (Stebila et al., 2026; Kwiatkowski et al., 2026). Naming an algorithm alone is insufficient to establish compatibility.

Profiles should also identify their applicable jurisdictions and requirements. Different connections may require different approved profiles. For example, where mainland Chinese requirements apply, SM2 elliptic-curve public-key cryptography should be distinguished from SM3 hashing and SM4 symmetric encryption (State Cryptography Administration, 2020). An informational RFC specifies how these algorithms are used in TLS 1.3 (Yang, 2021). SM2 is exposed to the public-key quantum threat described in section 1.2; SM3 and SM4 require separate assessment according to their functions and security parameters. Relevant specialist domain owners should track applicable official developments and assess their implications for affected profiles.

When a connection requires coordinated change, the dependency owner obtains agreement from the relevant internal provider, supplier, counterparty or infrastructure operator. The record links the agreed profile to available test evidence, remaining joint tests, and the transition and support commitments. Any unresolved agreement remains a dependency in the roadmap, with an owner, next action and review date. Safeguards and escalation arrangements are recorded where needed.

Decide the scope and conditions of approval

Outcome and operations owners confirm whether the proposal addresses their protection and operating requirements. Reviewers assess whether the evidence supports the proposed scope. The assigned approver then decides what is approved, deferred or rejected. Departures from common requirements and decisions to accept residual risk follow the relevant authorities.

The decision should identify the approved design version, permitted scope and reasons, together with any conditions, responsible owners and review dates. Where evidence is insufficient for the design decision, the response is further investigation or a narrower approval. Tests required for the eventual release may remain outstanding, provided their criteria, dependencies and responsible owners are recorded and the decision makes clear what may proceed before they are completed.

Keep the approved design current

The estate owner maintains the approved version and its links to evidence and decisions. When changes to standards, validation status, supplier commitments, interface agreements or material design assumptions could affect the basis of approval, the relevant domain and dependency owners assess the implications, including consequential changes to common requirements, procurement commitments and tests. Revisions preserve earlier versions and the reasons for change, with renewed approval where required under section 3.4. The transition manager coordinates the consequences for shared dependencies and the integrated roadmap.

Example: approving a gateway redesign

For example, the corrected gateway design from section 4.5 has supporting recovery evidence and an agreed profile for one counterparty connection. A second counterparty has yet to confirm compatible settings but the two connections can be changed independently. The approver permits change preparation for the first connection and leaves the second outside the approved scope. The dependency owner follows up the missing agreement.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate owner: consolidate the proposal and maintain the approved design.	A defined design provides the basis for change preparation.	A versioned design linked to findings, acceptance criteria, approval conditions and outstanding work.

Key accountable party and responsibility	Expected result	Evidence of achievement
Specialist domain owners: assess conformity with applicable requirements.	The proposed technical choices are supported for their intended use.	Profiles and configurations linked to source editions and status, validation evidence, test findings and any departures.
Reviewers and assigned approvers: assess support for the proposal and decide its permitted scope within their mandates.	The decision establishes what may proceed and under what conditions.	Review and decision records identifying the design version, scope, reasons, conditions, owners, dates and further approvals required.

4.7 Agree the integrated transition roadmap

Individual estate plans may be feasible on their own but compete for the same people, platforms or change windows. The integrated transition roadmap reconciles those plans into a coherent institutional response, linking protection priorities to an achievable sequence of work and the resources needed to deliver it. Agreement establishes the bank's commitments for defined work, while keeping unresolved matters visible. The plan establishes how the bank will deliver the required protection while maintaining controlled operation through required retirement.

Bring together the estate plans

The transition manager assembles the roadmap from the assessments, designs and dependency evidence developed under sections 4.1–4.6. Cryptographic estate owners substantiate their plans, with change package owners specifying the work to be delivered where packages have already been defined. Outcome and operations owners confirm completion deadlines and operating constraints within their respective remits, while dependency owners substantiate internal, group and external contributions.

Each planned activity links to the affected outcomes and estates and identifies its responsible owner, prerequisites, relevant dates and evidence needed to demonstrate completion. Required dates, delivery forecasts and confirmed commitments remain distinguishable, as do proposed and approved designs.

Reconcile priorities, dependencies and delivery order

The transition manager develops proposed priorities and sequencing with the responsible owners, drawing on the urgency and required-start findings under section 4.3, shared dependencies and available actions. Priority guides choices between competing demands; delivery order reflects prerequisites and what can feasibly happen first. A shared platform upgrade may therefore precede a more urgent application change. Ease of delivery alone does not justify allocating capacity needed to meet a more consequential transition's required dates. Where several uses are planned together, their material consequences and earliest required dates remain visible.

The schedule identifies dependencies that constrain preparation, testing, deployment or retirement, and work that can proceed in parallel. It also identifies critical paths: sequences of dependent activities that determine the earliest feasible completion dates under the stated duration and resource assumptions. Technical prerequisites are distinguished from constraints such as staffing or change windows since they may require different responses. Additional capacity may ease a staffing constraint, while a technical dependency may require a revised design or sequence. Where connected systems cannot change independently, owners establish a compatible intermediate arrangement or coordinated transition (ETSI, 2024, §6.9).

Where useful, **migration waves** group changes around shared prerequisites, interfaces, resources or delivery periods. Each wave has a stated purpose, membership, sequence and conditions; it need not require simultaneous deployment. Independent changes can retain their own plans. The transition manager reconciles shared work and resource allocations across the affected plans so that the same specialist capacity or supplier contribution is not committed to incompatible schedules.

A roadmap can distinguish investigation waves, enabling work and remediation waves. Investigation establishes the posture, dependencies and credible route for a bounded set of services; enabling work resolves prerequisites; remediation delivers the authorised changes. Link the work across these streams so that sufficiently understood candidates are available when delivery capacity can use them. Institution-wide discovery need not finish first, and an investigation wave does not itself authorise implementation.

Confirm resources and address shortfalls

Resource estimates cover preparation, assessment, procurement, testing and deployment (National Cyber Security Centre [NCSC], 2025; Canadian Centre for Cyber Security, 2025, §3.3). They also include, where relevant, review and assurance, training, customer and counterparty communications, recovery, stabilisation, temporary support for predecessor and replacement arrangements, and required retirement.

Responsible functions confirm resource availability for the proposed dates and identify outstanding funding or capacity decisions. The plan aligns contract dates, supplier commitments, hardware refresh cycles and testing windows with the proposed sequence, and identifies contingency for delay and rework. Cost estimates and indicative allocations remain distinguishable from confirmed funding and delivery capacity.

The roadmap preserves work whose solution or timing remains unresolved, with its exposure, known deadlines, owner, next action and review date visible. Useful preparation can continue within existing authority, including further discovery, key-management improvements, configurable cryptographic interfaces, lifecycle automation and procurement requirements (FS-ISAC Post-Quantum Cryptography Working Group, 2024). The roadmap records completion of this preparatory work separately from migration of the affected cryptographic uses.

If the integrated schedule cannot meet a required date, the responsible owners identify the resulting exposure and present options for acceleration, an alternative approach or interim protection, together with the decisions needed. Required dates remain visible alongside revised forecasts.

For the stated next action, an optional candidate classification may be ready, conditionally ready or blocked. Define ready by the evidence and conditions for that action; list the unmet conditions or blocking prerequisite otherwise. Revisit candidates when evidence changes, and allow further packages for the same application as other paths or functions become feasible.

Agree the roadmap and record commitments

The transition manager presents the reconciled roadmap, including material conflicts, shortfalls and options, to the responsible executive sponsors. Sponsors agree priorities and delivery commitments within their remits and make or obtain the necessary funding and capacity decisions under the bank's existing delegations.

The resulting commitments identify the authorised work, responsible owners, dates, conditions and unresolved matters. The transition manager records these decisions in a dated roadmap and communicates their consequences to affected owners. Agreement may cover defined work while other areas remain under investigation. It does not supply a missing design approval or authorise production deployment.

Maintain the roadmap as conditions change

The roadmap is revised when changes in protection needs, designs, support arrangements, dependencies, capacity or lifecycle costs affect its priorities or feasibility. Owners report consequential changes and use observed delivery results to improve later estimates.

Use early delivery to measure effort, waiting, defects, support demand and the evidence needed to proceed. Revise readiness criteria and later estimates from these observations. Increase the size or concurrency of groups only when the method is sufficiently repeatable and the required capacity is confirmed. This is a planning option to be evaluated in use; any volumes used are not validated benchmarks or common targets for other institutions.

The transition manager coordinates revisions across affected plans and records the revised position, preserving earlier assumptions and dates with the reasons for change. Where renewed decisions are required, the manager brings the affected commitments and proposed responses through the arrangements under section 3.4.

Example: resolving test scheduling conflicts in the integrated roadmap

For example, two estates require the same certificate-platform upgrade and testing specialists. One has an earlier completion deadline. Using the supplier's confirmed upgrade date, the transition manager proposes a combined sequence in which the shared upgrade precedes both sets of integration tests and the earlier-deadline estate receives the first testing slot. The responsible sponsor makes or obtains the capacity decision, and affected owners confirm that both schedules remain feasible. Independent preparation proceeds in parallel. If the supplier later withdraws its date commitment, the dependency owner obtains a revised position and assesses alternatives with the estate owners. The transition manager records the resulting uncertainty, coordinates reassessment of the affected dates and identifies any further decisions needed.

Key accountable party and responsibility	Expected result	Evidence of achievement
Transition manager: integrate plans, reconcile shared constraints and maintain the roadmap.	The institutional plan is coherent, current and explicit about uncertainty.	A dated roadmap links priorities, dependencies, critical paths, resources, commitments and unresolved actions; revisions retain their reasons.
Cryptographic estate and change package owners: substantiate plans and delivery commitments within their respective scopes.	Defined work has credible sequencing, completion conditions and an owned response to shortfalls.	Estimates and schedules link to assessments, designs and prerequisites, with capacity, dates, completion evidence and remaining work identified.
Executive sponsors: agree priorities and commitments, make or obtain resource decisions, and resolve or escalate material conflicts within their remits.	Authorised commitments support an achievable institutional plan, with outstanding decisions and conditions explicit.	Decisions identify funded work, committed capacity, responsible owners, dates and conditions. Matters beyond delegation reach the appropriate authority.

Pillar review — Assess and plan

The review establishes whether the findings under sections 4.1–4.7 support a proposed investigation, design decision or delivery commitment. It examines whether the proposed response addresses the bank's exposure and whether the evidence and delivery arrangements are sufficient for the scope under consideration.

Review question	Review focus
1. What is being reviewed?	State the proposed investigation, design decision or delivery commitment and identify the affected outcomes, cryptographic estates and connections. Establish the relevant date or period and the inventory, assessment, design and roadmap versions being used. This scope determines which evidence and prerequisites the review needs to examine.

Review question	Review focus
2. What does the evidence establish?	**Current position and dependencies (4.1–4.2):** Material cryptographic uses link to protected outcomes, deployments and dated evidence, including relevant recovery and fallback paths. Dependency records identify the contribution needed, who controls it, the responsible bank owner and the relevant date. Forecasts, commitments and demonstrated capability remain distinguishable. **Exposure and timing (4.3):** Protection needs, consequences and migration constraints support the proposed response and timing. Required start dates can be reproduced from the applicable completion deadlines, remaining work duration and a separately recorded contingency allowance. Severe consequences and unresolved timing remain visible. **Approach and design evidence (4.4–4.6):** The chosen approach and target address the protection and operating requirements. Applicable evidence supports the design against its acceptance criteria, with material changes reflected in reassessment and retesting of affected requirements. Where approval is required, the design version and agreed interface profiles correspond to the supporting evidence and approval conditions. Remaining validation for the intended deployment release is identified. **Delivery commitments (4.7):** The roadmap reconciles completion deadlines, prerequisite dates, shared capacity and funding for the commitment under review. Operating support, recovery, coexistence and required retirement are included in the planned work and resources.
3. What remains unresolved?	Identify gaps or inconsistencies that could change the response or its feasibility. These may include an unconfirmed supplier release, recovery behaviour not covered by testing, an unresolved interface agreement or competing plans relying on the same capacity. Explain which protection needs, activities or commitments are affected. Where timing cannot yet be established, identify the missing assumptions or evidence. Where a forecast already shows that a required deadline will be missed, record the known shortfall and its consequences. These positions remain distinguishable in the review findings.
4. What action or decision follows?	Identify the response needed: further evidence, a revised approach or design, different sequencing, additional resources or interim safeguards. Where change preparation is proposed, assess whether the approved design, prerequisites, acceptance criteria, operating support, recovery arrangements and funding support that scope. If the evidence supports only narrower work, identify that scope and the conditions governing further progress.

5 Implement and retire

The *Implement and retire* pillar puts approved designs and the transition roadmap into effect through defined change packages. For each package, the bank prepares the implementation and supporting arrangements, establishes readiness and obtains the required authorisation for the proposed action. Deployment proceeds within the approved limits, with observations used to confirm which cryptography is actually in use and whether protection, service and recovery requirements are met.

Where predecessor and replacement arrangements coexist, the bank controls their permitted use, remaining exposure and unfinished work. Completion is established for a defined scope when evidence shows that the approved target has been achieved, required retirement has been carried out, records reflect the resulting state and continuing responsibilities have been accepted. Findings during implementation or operation may require the design, roadmap or permitted action to be reconsidered.

Pillar outcome: Changes achieve their approved protection and operating objectives, with remaining exposure controlled, required retirement verified and continuing responsibilities accepted.

PACT / PILLAR 3

Implement and retire

Authorised changes achieve their intended results, with remaining exposure controlled and retirement and completion demonstrated.

Six connected areas · key actors and results

5.1 Prepare the change package

Actors Change package owner integrates the package; technical contributors prepare the candidate; operations and dependency owners confirm arrangements and prerequisites.

Result Reproducible candidate and versioned plan link approved design, completion criteria, assigned tasks and remaining tests.

5.2 Establish readiness and authorise the proposed action

Actors Change package owner assembles evidence; technical contributors validate the candidate; reviewers challenge findings; assigned approvers define permission.

Result Permission defines the candidate, action, prerequisites, limits, and stop or recovery conditions.

5.3 Deploy and establish controlled operation

Actors Change package owner coordinates deployment; technical contributors implement; operations owner monitors and responds; estate and outcome owners assess results.

Result Actual cryptographic use and service behaviour are evidenced; tested, authorised and deployed states are reconciled.

5.4 Control coexistence, remaining work and exceptions

Actors Estate and outcome owners assess exposure; change package and dependency owners resolve gaps; operations maintains controls; approvers decide departures.

Result Coexistence, remaining work, transition debt and exceptions remain distinct, with owned actions and controls.

5.5 Retire predecessor arrangements

Actors Estate owner defines scope; dependency owners confirm readiness; approvers authorise; change package owner coordinates withdrawal.

Result Specified predecessor paths, including fallback and recovery, are unavailable; retained uses serve only permitted purposes.

5.6 Verify completion and establish continuing ownership

Actors Change package owner reconciles evidence; estate and outcome owners assess achievement; assigned approver confirms completion; continuing owners accept responsibilities.

Result Approved target and required retirement achieved for the stated scope; records and continuing ownership confirmed.

Evidence ↓ ↑ Decisions and follow-through

Recurring pillar review

Does the evidence support the proposed action, continued operation or completion claim?

Scope
Which action or operating state, approved target, configuration, affected scope and observation period are being reviewed?

Evidence
Do permissions, actual use, service behaviour, remaining exposure, retirement and accepted ownership substantiate the claim?

Unresolved matters
Which discrepancies, unverified paths, predecessor dependencies or failed conditions prevent action, operation or completion?

Action or decision
Proceed within permission; restrict or recover operation; correct and retest; authorise retirement or confirm completion within scope.

Decisions and follow-through identify responsible owners, conditions and follow-up dates.

Deployment, operation, retirement and completion require their own evidence and decisions.

Figure 4 Implement and retire at a glance

5.1 Prepare the change package

An approved design establishes the intended cryptographic arrangement, but implementation requires a specific release and coordinated work across the affected systems and parties. The change package brings together the implementation to be tested and the tasks, dependencies and operating arrangements needed to introduce it. It turns the approved design and agreed roadmap into a defined proposal for validation and the authorisation decision under section 5.2.

Define the scope and prepare the implementation

The change package owner brings the package together, using the bank's existing change records where suitable. The package identifies what will change, where the change will apply and the criteria for completing its scope. It links the affected outcomes, cryptographic estates, uses, components and environments to the approved design and interface-profile versions. The cryptographic estate owner confirms how the package contributes to the estate's target. Related work outside the package remains linked to its responsible owners, keeping unfinished estate work visible when the package is completed.

Technical contributors prepare the implementation candidate: the particular hardware, firmware, software, libraries and configuration intended for the change. Recorded versions, settings and build or installation instructions make the candidate reproducible and allow subsequent deployments to be compared with it. Contributors check the candidate against the approved design and common requirements, with relevant specialist domain owners assessing conformity within their remits. Findings and departures are recorded, with material departures addressed through the design and decision arrangements in sections 4.6 and 3.4.

Where automation is used, its versioned instructions or rules form part of the supporting records, together with restricted execution access, test evidence, monitoring and recovery arrangements.

Coordinate the work and dependencies

The change plan translates the roadmap into assigned tasks, prerequisites, sequencing and change windows. It also identifies necessary communications with customers and connected parties. Activities involving libraries, keys, certificates, trust arrangements and interfaces may require separate steps because they have different owners or replacement cycles. Changes to key-establishment and signature uses may also proceed separately. The plan shows how these activities fit together and coordinates them with other packages where needed.

Required retirement tasks and conditions are included from the outset, with their owners and timing. The plan also assigns updates to the inventory, relevant CBOMs, dependency records and decision records as implementation and retirement proceed.

Dependency owners confirm the arrangements for the particular release with internal providers, suppliers, counterparties or infrastructure operators, using current release information, available joint-test results and commitments for test access, delivery and support. The records distinguish confirmed arrangements from unresolved prerequisites. Each unresolved prerequisite identifies the activity it prevents, together with an owner, next action and review date. Prerequisites for validation are established before the affected tests begin; conditions for later deployment remain explicit for the readiness decision under section 5.2.

Prepare operating and recovery arrangements

The operations owner prepares monitoring, support, incident and recovery arrangements for the change. These identify operating criteria, warning and intervention conditions, responsible personnel and the actions they are authorised to take. Recovery procedures specify the configuration to be restored, its permitted cryptographic behaviour and any resulting exposure. The package retains available monitoring and preproduction recovery results and identifies the further demonstrations needed for the intended operating environment.

These arrangements also depend on usable, protected key material. Technical contributors prepare the applicable procedures for key generation, protected transfer and storage, rotation and destruction,

together with certificate issuance, renewal and revocation. Backup requirements depend on the key's purpose and application (Barker, 2020, §§8.2.2.1–8.2.2.2). Where backup or regeneration forms part of the approved recovery approach, the package identifies the protected material, procedures and tests needed to demonstrate safe restoration and use.

Where the implementation uses secret seeds to generate or regenerate key material, the procedures cover their generation or derivation, protection and permitted handling across devices in line with the approved design (Dang et al., 2026, §4.2). The package references controlled procedures and records, while secret values remain in their protected systems.

Bring the package and evidence together

Before presenting the package for validation, the change package owner checks that its scope, implementation candidate, plan and supporting evidence are consistent. Earlier findings are linked to the configurations and requirements they address, so their applicability to the prepared candidate can be assessed. Remaining tests, acceptance thresholds and unresolved conditions establish what is ready to be tested and what still needs to be demonstrated.

Example: preparing a gateway change package

For example, the bank prepares the gateway change for the first counterparty connection covered by the design approval in section 4.6. The package identifies the gateway release, agreed connection settings and corrected recovery configuration, with confirmed test access and support. It assigns deployment, monitoring and retirement tasks, links earlier findings to the configurations tested and identifies the remaining tests for this release. The second connection remains outside the package, with its unresolved profile agreement linked to the dependency owner. Validation can therefore proceed for the first connection while the second remains outstanding.

Key accountable party and responsibility	Expected result	Evidence of achievement
Change package owner: bring together the scope, implementation, assigned work and evidence.	A defined package is ready for validation within its stated scope.	A versioned package links the candidate, tasks, prerequisites, completion criteria, available results and remaining tests.
Cryptographic estate owner: confirm the package's contribution to the estate's target and retain visibility of related work.	Package boundaries and remaining estate work are clear.	Affected outcomes and uses are linked to the estate's target and to work outside the package, with responsible owners identified.
Technical contributors: prepare the candidate and procedures. **Specialist domain owners:** assess conformity within their remits.	A reproducible candidate reflects the approved design, with departures explicitly addressed.	Versions, settings, build instructions and conformity findings identify the implementation, supported by relevant key-management procedures, automation records and test evidence.
Operations owner: prepare monitoring, support, incident and recovery arrangements.	Operating responsibilities, procedures and remaining demonstrations are defined.	Procedures identify personnel, criteria, permitted actions and recovery configurations, with available results linked to remaining demonstrations.
Dependency owners: confirm supporting arrangements and manage unresolved prerequisites.	Confirmed arrangements and conditions affecting testing or deployment are distinguishable.	Current change notices, joint-test evidence and commitments establish test access, dates and support; unresolved prerequisites identify blocked activities, owners, actions and review dates.

5.2 Establish readiness and authorise the proposed action

The preparation of a change package does not establish that a change is ready for production. The bank assesses whether the implementation prepared under section 5.1 and its supporting arrangements can meet the requirements of a specified action. The assigned approver uses the validation evidence and required reviews to decide what may proceed, within which limits and subject to what conditions.

The candidate view in section 4.7 should identify the action to which its classification applies. Evidence sufficient to investigate a connection, complete a prerequisite or conduct a bounded test does not establish readiness to activate a production profile. This section supplies the release-specific assessment and permission needed for the proposed implementation action, including any conditions remaining from the candidate record.

Define the action and validate the implementation

The change package owner defines the action for which approval is sought and the change it would make to the current state. The proposal identifies the candidate release and configuration, cryptographic mechanisms, key and trust arrangements, environment and affected interfaces, systems and uses, including users or traffic where relevant. Installing a capability, activating a profile and expanding its use may each require different evidence.

Technical contributors validate the exact candidate against the approved design, interface profiles and relevant service and security thresholds in a controlled preproduction environment representative of the intended use. Tests address the requirements applicable to the selected mechanisms, including key-establishment and signature operations, key generation and handling, certificate processing, negotiation and permitted fallback. Where hybrid mechanisms are used, tests also cover the selected combination rules and failure behaviour. NIST's key-encapsulation mechanism (KEM) guidance identifies implementation and secure-use considerations, including input validation, key derivation and confirmation, and the construction and limitations of hybrid combinations (Alagic et al., 2025, §§3–4).

Testing establishes interoperability and acceptable service behaviour under normal operation, peak demand, component or counterparty failure, recovery and resource exhaustion. It accounts for device constraints and relevant supplier or key-management outages, and demonstrates monitoring and safe restoration of required key material. Where rollback is permitted, tests demonstrate restoration of the earlier release or configuration. Test observations establish which cryptography is actually used, including fallback, alongside the service results (NCSC, 2025, "Executing your migration plan").

Each result identifies the tested configuration, dependencies, environment and workload, and the requirement and threshold it addresses. Technical contributors record defects and corrections and repeat the affected tests. Earlier pilot results, supplier evidence and algorithm or module validation are used only within their demonstrated scope and after their applicability to the candidate has been assessed. Differences between tested and proposed conditions, limits on inspection, and any justification for applying findings to another interface or workload remain explicit. Readiness of the connected service requires evidence of its behaviour under the proposed conditions.

Confirm operating readiness and review the evidence

The operations owner demonstrates that the monitoring, support, incident and recovery arrangements are usable for the proposed action, with prepared personnel, necessary access and defined intervention conditions. Dependency owners confirm the necessary internal and external contributions using current commitments for the release and relevant joint-test evidence. Joint testing and evidence gathering can support this work, with sensitive information protected and the bank retaining responsibility for its assessment and decision. HKMA's quantum-preparedness whitepaper similarly connects implementation assurance with supplier commitments, interoperability, coordinated transition and operating resilience (HKMA, 2026a, pp. 42–43, 45–46).

The change package owner brings together the evidence and identifies its limitations. The cryptographic estate owner assesses the implications for the estate's transition, while outcome and operations owners assess whether protection and service requirements are met. Required reviewers challenge whether the evidence is current, sufficiently complete and applicable to the proposed action, comparing supplier

claims with test results and other observations. The depth of review reflects the consequences, novelty and uncertainty of the action. Critical, custom, constrained or supplier-controlled implementations may require closer examination. HKMA's technology-risk guidance provides supporting principles for testing, independent review and change approval (HKMA, 2003, §§4.2.3–4.2.4, 4.3.1).

Decide what may proceed

The assigned approver decides whether to authorise the action, limit its scope, impose conditions or withhold permission, within the applicable delegation. Before the affected action proceeds, each material finding is either:

- resolved with supporting evidence and satisfactory retesting of corrections that affect tested behaviour;
- shown by evidence not to affect a narrower scope proposed for approval; or
- addressed through an authorised departure from an identified requirement, where permissible.

Missing evidence is not itself an approved exception. Approval conditions distinguish prerequisites to be met before action from requirements monitored during operation. Outstanding findings and conditions identify responsible owners, required responses and due dates.

Set the limits for introduction and continued permission

Evidence of the first deployment's live performance becomes available after introduction. Permission for that introduction therefore defines the configuration, permitted users or traffic, observation period, success criteria, stop conditions and recovery action. One approval may cover several increments where the limits, progression conditions and authority to continue are explicit. An increment outside those limits, or new evidence undermining their basis, requires reassessment.

The decision record links the permitted action and its authority to the candidate, applicable requirements, evidence, review findings, limitations and conditions. It identifies responsible owners and relevant dates. Permission remains valid only while its basis and limits hold. Material changes to the release, configuration, environment or dependencies require reassessment; significant findings or incidents that could affect the basis of permission also reopen the affected assessment. Failed conditions or expired permission trigger the specified response and escalation.

The decision provides the authority for controlled deployment under section 5.3. Withdrawal of the predecessor requires separate evidence and authority under section 5.5.

Example: authorising the gateway package

For example, tests of the gateway package from section 5.1 demonstrate the agreed profile, acceptable payment performance and recovery to a permitted configuration for the first counterparty connection. The required review supports a limited production introduction. The assigned approver permits a defined subset of payments during an attended observation period. A breach of the agreed payment-error threshold or use of a prohibited profile triggers the specified stop or recovery action. Wider use follows the approved progression conditions. The second counterparty connection remains outside the permission, and predecessor retirement requires its own supporting evidence and authority.

Key accountable party and responsibility	Expected result	Evidence of achievement
Change package owner: assemble the proposal and evidence. **Technical contributors:** validate the candidate and address technical findings.	The proposed action has a defined scope and a traceable technical basis.	Results link the candidate, configuration, dependencies and workload to the approved design, profiles and thresholds, with defects, corrections, retest outcomes and limitations recorded.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate and outcome owners: assess transition and protection consequences within their respective remits.	The readiness assessment accounts for affected estates and protected outcomes.	Assessments identify supported requirements, scope limits, unresolved consequences and required decisions.
Operations and dependency owners: demonstrate operating capability and confirm necessary contributions.	The proposed action can be supported and recovered within its intended conditions.	Demonstrations, usable procedures, prepared personnel, current commitments and relevant joint-test evidence establish the operating and dependency position.
Required reviewers: challenge the sufficiency and applicability of evidence.	The decision rests on evidence that has received the required challenge.	Review findings compare claims with observed results and identify limitations, material concerns and their treatment.
Assigned approvers: determine permission within delegated authority.	The permitted action, conditions, progression limits and responses to changed circumstances are explicit.	The decision identifies the approver and authority, scope, treatment of material findings, prerequisites, operating conditions, owners, dates and reassessment triggers.

5.3 Deploy and establish controlled operation

Production deployment exposes the change to operating conditions that testing may not fully reproduce. The bank therefore uses observations of cryptographic and service behaviour to control its introduction and invoke any required response when those observations differ from expectations. The purpose is to establish whether the deployed change operates within its authorised and intended limits.

Deploy within the authorised limits

The change package owner coordinates implementation by technical contributors and operations. Before each increment, they confirm that the release, configuration, environment and affected systems, users or traffic remain within the authorised scope. They also confirm that the required keys, trust arrangements and dependencies are available, and that the change window, communications, monitoring, support and recovery provisions are in place. The scope of each increment reflects the consequences of failure and the capacity to recover. Material changes to a prerequisite or the basis of permission receive the specified response before the affected action proceeds. These arrangements apply established change-control disciplines, such as implementation records, rollback and post-implementation verification (HKMA, 2003, §4.3.1).

Dependency owners coordinate the agreed actions and support of internal providers, suppliers and counterparties. Where a change affects public-key infrastructure (PKI, which supports certificate issuance and validation), technical contributors follow the approved sequence for distributing replacement certificates and updating which issuers connected systems trust. The sequence accounts for systems still dependent on earlier arrangements, permitted coexistence, the conditions for withdrawal or continued use, and the recovery route (NCSC, 2025, “PQC migration for enterprise PKI”).

Establish actual cryptographic use and service behaviour

The operations owner, supported by technical contributors, monitors actual cryptographic use alongside service behaviour. Relevant observations include the algorithms and profiles selected, negotiation and fallback events, remaining predecessor use, key and certificate status, processing times, capacity, errors and incidents. The findings are assessed against the agreed security and service thresholds and the outcomes experienced by customers and counterparties. NCSC cautions that systems can appear to work while using traditional cryptography, making actual-use verification essential (NCSC, 2025, “Executing your migration plan”).

The evidence distinguishes a capability being installed, enabled or selected as the normal choice from its demonstrated use in particular interactions. Relevant configuration checks and controlled tests supplement live observations to cover batch, standby, failover and recovery paths that ordinary traffic may not exercise.

Where a supplier-controlled product limits direct inspection, the dependency owner obtains evidence specific to the deployed release and configuration, together with incident and recovery support. The operations owner records what the evidence establishes and what remains unverified. Successful transactions or general supplier assurances do not remove a material gap in that evidence.

A verification view should connect each changed path and cryptographic function to the observed mechanism, collection method, endpoints, releases, settings and conditions examined. Show separately the paths for which the intended behaviour was observed, those with inconclusive or missing evidence, and those awaiting implementation.

Control progression and respond to findings

The change package owner brings together the observations and the operations, outcome and estate owners' assessments to establish whether the authorised progression conditions have been met. These assessments address service stability and continuing support and recovery capability, protection and business requirements, and the implications for the estate's transition. Further increments proceed only where the evidence supports them and they remain within the existing permission.

When a stop or recovery condition occurs, operations invokes the authorised response promptly. Rollback restores an earlier release or configuration. Fallback uses an alternative mechanism or path without necessarily reversing deployment. Recovery restores correct service and data and may involve either. Each response remains within its specified trigger, scope and conditions for returning to the intended operating state.

Any necessary emergency change follows the bank's emergency-change arrangements, including recording, subsequent review and replacement by a properly tested correction (HKMA, 2003, §§4.3.2–4.3.3). If the response reintroduces quantum-vulnerable cryptography, the responsible estate and outcome owners reassess the exposure and record its scope, reason and duration. Emergency recovery does not itself authorise indefinite use; continuing arrangements are addressed under section 5.4.

Record the resulting operating state

The change package owner compares the deployed state with the configurations tested and the permission granted, and explains material differences. Responsible owners update the linked configuration, cryptographic inventory, relevant CBOM, dependency and change records. Material discrepancies have an owner, response and date, with affected assessments or authorisations reopened where necessary.

The resulting record shows what is operating, what the evidence establishes and its limits, the basis for continued operation, and any remaining work or exposure. Predecessor retirement and transition completion require the separate evidence specified in sections 5.5 and 5.6.

Example: gateway package deployment and operational findings

For example, the bank deploys the gateway package authorised under section 5.2 for the permitted subset of payments on the first counterparty connection. Monitoring confirms the agreed profile, but payment errors exceed the approved threshold during the observation period. Operations invokes the specified recovery action and verifies restored service. The change package owner records the deployed and recovered states, while technical contributors investigate the difference from the test results. The outcome and estate owners assess any resulting exposure. Expansion remains on hold until the applicable conditions are met and any required revised permission is obtained.

Key accountable party and responsibility	Expected result	Evidence of achievement
Change package owner: coordinate execution and progression and compare the resulting state with the tested and authorised arrangements. **Technical contributors:** implement and verify the change.	Deployment remains within permission, and material discrepancies receive an appropriate response.	Records link actual releases, configurations and actions to the permission and progression conditions, with discrepancies, responsible owners and responses identified.
Operations owner: monitor cryptographic and service behaviour, assess stability, and maintain support and authorised response capability.	The operating state and its evidence limits are understood, with support and response arrangements available.	Observations establish actual cryptographic use and service performance, with coverage limits, incidents and stop or recovery actions recorded.
Cryptographic estate and outcome owners: assess transition, protection and business consequences within their remits.	Continued or expanded use has a supported basis, with remaining exposure and consequences explicit.	Assessments link observed results to estate targets and protection and business requirements, identifying required responses and outstanding exposure.
Dependency owners: coordinate connected parties and obtain the necessary support and evidence.	Internal and external contributions support the deployed arrangement.	Current confirmations, coordinated actions and evidence specific to the deployment establish the contributions, incident and recovery support, and any inspection limitations.

5.4 Control coexistence, remaining work and exceptions

Different cryptographic uses and dependencies may migrate at different speeds, so the bank may need to operate predecessor and replacement arrangements together. The task is to keep the remaining exposure controlled, maintain the support those arrangements need and establish a credible route to the approved target. Where a proposed or continuing arrangement would depart from an applicable requirement, the bank obtains a decision specifying whether and on what conditions it may proceed.

Establish what remains and support coexistence

The cryptographic estate owner maintains a view of predecessor mechanisms that remain in use or available, including fallback and recovery paths. The record identifies the affected uses, protected outcomes, dependencies, operating conditions and work needed to reach the target. Temporary coexistence has a defined purpose, expected duration and evidence required for withdrawal (NCSC, 2025, "Developing your migration plan"). Traditional components within an approved hybrid target, or capabilities retained for permitted historical decryption or signature verification, are assessed against those purposes and their applicable controls.

PACT uses three related terms to describe remaining work and departures:

Term	Meaning
Remaining transition work	All work still needed to reach the approved target.
Transition debt	A gap carried beyond an agreed date or event, or outside approved transition conditions.
Exception	An authorised departure from an identified requirement or operating condition, bounded by scope, duration and conditions.

These terms can apply to the same matter. Transition debt describes a condition; an exception records permission for a departure. Planned work and permitted coexistence do not automatically constitute debt or require an exception, although their exposure remains relevant to risk and timing assessments.

When a commitment is missed, the estate owner retains the original date or condition, the resulting gap and exposure, and the current response. Any rescheduling records its rationale and effect on the debt. Granting an exception does not itself change the completion deadline or demonstrate reduced exposure. A timing assessment changes only when its underlying basis changes.

For example, a connection may be unable to adopt the target until its provider supplies a compatible release. The dependency owner should obtain the missing evidence or commitment, while the estate and outcome owners assess the exposure, feasible interim measures and the trigger for reconsideration. Remaining within approved conditions is different from breaching a requirement. Record the former as outstanding work; route the latter through the existing departure process. Neither a backlog entry nor a candidate classification authorises a departure.

The bank provides the funding, personnel and capacity needed to support both arrangements while they remain necessary and to complete the required transition or retirement work. Research on legacy-system discontinuance shows that withdrawal can require temporary additional work on the old system and its connections to the replacement (Rezazade Mehrizi et al., 2019). Change package owners maintain assigned actions and dates; dependency owners substantiate the necessary supplier and counterparty contributions; and the operations owner maintains support and safeguards. The transition manager coordinates material consequences for shared resources and the integrated roadmap.

Assess and decide proposed departures

The responsible owner identifies the requirement or operating condition from which a proposed or continuing action would depart, explaining the operational need, affected outcomes and estates, expected duration, exposure, uncertainty and alternatives. These may include acceleration, narrower use, isolation, another design or cessation. The outcome owner assesses the protection and business consequences. Supplier delay or schedule pressure may explain the request, but does not by itself justify acceptance.

Missing evidence alone does not establish an exception. Where an evidence requirement would be unmet, the request identifies the proposed departure from that requirement.

Compensating controls are safeguards intended to reduce the exposure created by the departure. The proposal explains how each control will operate, who maintains it and the evidence supporting its effectiveness and limitations. Restrictions on an interface or user population, isolation, reduced retention or another protected path may reduce exposure. Monitoring may improve detection and response, but does not provide confidentiality that the cryptography lacks. Controls introduced now cannot reverse earlier capture of vulnerable encrypted information.

Following the required review, the approver assigned to the departure first establishes whether the bank has authority to permit it, then decides within the applicable delegation. The approver assesses whether the controls bring remaining exposure and uncertainty within the applicable risk appetite and limits. Requests beyond the approver's delegation are escalated, and any required residual-risk decision follows the relevant authority. Risk acceptance cannot waive a binding obligation. The decision may reject the request, narrow it or permit a bounded departure.

Any permission is limited to the need supported by the evidence. It specifies the scope, rationale, effective period, conditions, accountable owners, monitoring, review or expiry, and the requirements for ending the departure. The plan to end it identifies credible actions, resources, dependencies and evidence of resolution. An unconfirmed supplier roadmap is insufficient by itself.

Monitor conditions and manage expiry

The decision specifies the response to a failed condition or expiry without a replacement decision, identifying who acts, under what authority and when escalation is required. The operations owner maintains the ability to carry out that response. Permission does not extend automatically.

Monitoring tests whether the controls and assumptions supporting the decision remain valid. Incidents, control failures, changed exposure or dependencies, and missed dates prompt reassessment. Renewal

requires current evidence of continued need, control performance, progress and a credible plan to end the departure. Repeated renewal without progress is escalated to the authority able to address the underlying resource, design or governance problem.

Close work and exceptions on evidence

The responsible owner closes remaining work or transition debt only when evidence meets its resolution criteria, or an authorised revision to the target removes the need for that work. An exception closes when evidence establishes that the departure has ended, through meeting the requirement or an authorised revision to it. Expiry of the permission does not by itself establish that the departure has ended.

Any revision preserves the earlier commitment, the reasons for change and the remaining exposure. Temporary controls are safely withdrawn or assigned continuing ownership and review. Linked inventory, change, dependency and exception records reflect the resulting state. Closing an exception does not establish the retirement or transition completion addressed in sections 5.5 and 5.6.

Example: predecessor recovery path remains permitted after deployment

For example, following the production findings in section 5.3, further recovery testing shows that the replacement arrangement cannot yet restore service within the agreed tolerance. The predecessor recovery path remains permitted until an agreed withdrawal date, but correction of the limitation is expected to extend beyond that date. Continued reliance beyond the withdrawal date would create transition debt and depart from the withdrawal requirement. The estate owner therefore seeks a decision before that date, supported by an exposure assessment, controls and a credible plan to correct the replacement recovery arrangement. Any permission specifies the response at expiry. The original commitment remains visible, and the exception closes only when evidence establishes that the departure has ended.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate and outcome owners: establish the remaining work and exposure and assess protection and business consequences.	Unfinished work, transition debt and proposed departures are understood, owned and assessed.	Records identify affected uses, requirements, original commitments, exposure, uncertainty and the basis for the current response or closure.
Change package and dependency owners: deliver resolution work and substantiate necessary contributions.	Remaining work and permitted departures have a credible, resourced route to resolution.	Assigned actions, dates, resources, dependency commitments and delivery evidence support the plan and identify delays requiring action.
Assigned approvers: decide departures and renewals within the applicable authority and delegation.	Any permitted departure has a justified scope, duration and conditions.	Decisions identify the approver and authority and link the departure to reviewed evidence, rationale, scope, duration, conditions, owners, review or expiry, resolution requirements and any escalation.

5.5 Retire predecessor arrangements

A functioning PQC replacement does not eliminate exposure while configuration or fallback can still select the predecessor, and inadequately protected negotiation may allow an attacker to steer selection towards it (NCSC, 2025; Barker et al., 2025, §3.2.3). Retirement establishes that a predecessor arrangement can no longer be selected, negotiated or invoked for a specified use within a defined scope. The bank therefore authorises withdrawal on the basis of readiness evidence and verifies the resulting state, while preserving required protection, service continuity and continuing information obligations.

Define the scope and continuing needs

The cryptographic estate owner defines the retirement scope against the approved target, identifying the affected uses, components, interfaces, environments and dependencies. Deprecation signals that a mechanism is being phased out under stated conditions; it does not establish retirement. Components retained within an approved hybrid target or for another permitted purpose remain distinguishable from the paths to be withdrawn.

The outcome owner establishes any continuing need for historical decryption, signature verification, retention or audit. Technical contributors specify the permitted functions, access, keys, environment, retention and eventual disposal. This assessment distinguishes applying new protection from processing previously protected information and applies the relevant conditions for retaining key material (Barker, 2020, §§7.4, 8.3.1).

Retained capability is limited to its authorised purposes and prevented from enabling prohibited new encryption, signing, authentication or key establishment. Retaining signatures for later verification does not by itself justify keeping the corresponding private signing keys. The continued availability of a decryption or verification capability does not itself demonstrate that historical confidentiality or verification requirements remain satisfied.

Establish readiness and authorise withdrawal

Where the use continues, the operations and outcome owners establish that the replacement has operated satisfactorily against the relevant service and protection requirements. Evidence covers representative business cycles, peak demand, key and certificate events, participant differences and failure conditions as applicable. The observation period reflects the use and its consequences; infrequent events may require controlled tests. Recovery remains possible within the service's tolerance without relying on the capability being retired.

Where ending the use is the approved target, the assessment instead establishes readiness for cessation and the treatment of continuing data, trust and other obligations.

Dependency owners substantiate that affected internal and external consumers meet their requirements without relying on the predecessor capability proposed for withdrawal. Relevant configuration, test and operating evidence covers dependencies through applications, protocols, certificate and trust arrangements, hardware, administrative access and recovery facilities. A delivered supplier release or a counterparty commitment alone does not establish that the dependency has ended. Any continuing dependency is reconciled with the approved target before the affected withdrawal proceeds.

The estate owner brings these assessments together for the required review and retirement decision. The approver assigned to that decision authorises, limits or defers withdrawal within the applicable delegation. The decision identifies the approver and authority, the permitted scope, prerequisites, operating consequences and the permitted response if the action fails.

Deployment and retirement permissions may share a decision record, provided the actions and their supporting evidence remain distinguishable. Permission to introduce the replacement does not itself authorise withdrawal of its predecessor.

Carry out withdrawal and prevent reintroduction

The change package owner coordinates the withdrawal by technical contributors and operations. Depending on the design, the work disables protocol choices, replaces hardware, removes configurations or implementations, alters supplier connections, or withdraws credentials and trust arrangements.

The work prevents key generation and certificate issuance or renewal from enabling the prohibited use and applies the required expiry, revocation or disabling controls. For PKI, NCSC notes that quantum-secure authentication generally requires completion of migration and expiry or revocation of traditional certificates (NCSC, 2025, "PQC migration for enterprise PKI").

Withdrawal controls also cover secondary systems, deployment templates and recovery procedures, including restoration from backups. Where backup contents cannot be changed, the restored environment is brought into the approved state before it resumes the affected use.

Secret and private key copies with no remaining authorised purpose are destroyed under the applicable key-management requirements; revocation and destruction serve different functions (Barker, 2020, §§8.3.4–8.3.5). The disposal assessment also covers secret seeds capable of regenerating those keys. Seeds are destroyed when no authorised purpose remains; any seeds retained for an authorised purpose are prevented from enabling prohibited regeneration.

Verify and record retirement

Technical contributors and the operations owner verify the resulting state through appropriate configuration checks, tests and operating observations. Verification covers relevant dormant, fallback and recovery paths and establishes that prohibited selection, negotiation or invocation is prevented. The absence of observed predecessor traffic alone does not demonstrate this. The operations owner maintains controls that detect relevant attempted use and trigger the specified response.

The estate owner assesses the resulting evidence, and the change package owner coordinates updates to the inventory, relevant CBOM, dependency, change and exception or debt records. The record identifies the verified scope, limitations, retained capability and remaining exposure. A predecessor path that remains available contrary to the target prevents a retirement claim for the affected scope.

Example: withdrawal of predecessor path in payment gateway

For example, after the payment-error fault is corrected and the affected tests are repeated, the bank resumes the permitted introduction and establishes satisfactory operation on the first counterparty connection. The recovery limitation identified in section 5.4 is also corrected and tested, demonstrating restoration within the payment service's tolerance without the predecessor path. The dependency owner confirms that the first counterparty connection can use the replacement during recovery, and the assigned approver authorises withdrawal for that defined scope. Technical contributors disable the earlier profile and update the secondary gateway and recovery configuration. Post-change tests confirm that normal operation and recovery use the approved profile and that the earlier profile cannot be selected. The estate owner assesses the evidence and records retirement of that path. The second counterparty connection remains separately tracked as unfinished estate work.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate and outcome owners: define the retirement scope and assess protection, service and continuing obligations.	Withdrawal has a justified scope, and retained capability has an explicit authorised purpose.	Assessments link the target, affected uses, operating results, continuing needs and retained capability to the retirement decision and verified result.
Change package owner and technical contributors: coordinate and perform the authorised withdrawal and verify its effects.	The specified predecessor use is unavailable within the retirement scope.	Change records, configuration checks and tests substantiate withdrawal, including relevant dormant, fallback and recovery paths, with limitations and unresolved findings explicit.
Dependency owners: substantiate consumer migration and coordinate related actions.	Affected internal and external consumers can meet their requirements without the capability being withdrawn.	Configuration, test and operating evidence confirms the changed dependencies and identifies any capability retained under the approved target.

5.6 Verify completion and establish continuing ownership

The bank confirms completion of a defined transition scope when evidence establishes that its approved target has been achieved and the resulting arrangements can be sustained. The completion decision brings together delivery results and continuing ownership, leaving a clear account of what has been achieved and who remains responsible after the change work ends.

Assess achievement against the approved target

The change package owner assembles the evidence against the approved completion criteria, identifying the scope, target version, resulting configuration, affected uses and dependencies. The assessment draws on design and change records, validation results, observed operation, required retirement evidence and unresolved findings. It explains material differences between planned and actual results and their consequences for completion, keeping alternative, interim and incomplete states distinguishable from achievement of the approved target (ETSI, 2024, §6.10).

The cryptographic estate owner assesses the evidence against the approved target for the scope under review. The outcome owner assesses whether the protection and business requirements have been met, and the operations owner substantiates satisfactory operation and support where the use continues.

Completion requires the necessary retirement under section 5.5 and reconciliation of the relevant records with the verified result. Where cessation is the target, the evidence establishes that the use has ended and that continuing information and other obligations are addressed.

An exception may permit an interim operating state, but it does not satisfy an unmet completion criterion. Any authorised revision to the target preserves the earlier target and the reason for the change; it does not demonstrate that the original work was performed.

Confirm continuing ownership and support

Before delivery responsibilities end, the outcome, estate, operations and dependency owners confirm their continuing responsibilities or an agreed transfer. Any transfer identifies the receiving owner and records acceptance.

The operations owner confirms access to current records, usable procedures, competent personnel and resources for monitoring, key and certificate management, incident response and recovery. Dependency owners substantiate continuing provider support and commitments. These arrangements sustain the operational disciplines needed to support the resulting service and its protection requirements (HKMA, 2003, §§5.1–5.4).

Historical decryption or verification, retention and eventual disposal remain assigned where needed. Such continuing duties are compatible with completion when they conform to the approved target. Work still needed to meet that target remains open; administrative closure or transfer to a continuing owner does not establish that the work has been completed.

Review, decide and record completion

The change package owner coordinates reconciliation of the architecture, configuration, inventory, relevant CBOM, dependency and change records with the verified result. The responsible owners reconcile affected responsibility, roadmap and exception or debt records, preserving a consistent account of achieved results, remaining exposure and unfinished work.

The estate owner brings the assessment, reconciled records and owner confirmations into the required review and completion decision. Following review, the approver assigned to that decision determines whether completion can be confirmed within the applicable delegation. Confirmation is specific to the defined scope and requires evidence that its approved completion criteria and continuing ownership arrangements are met. Where a criterion remains unmet, the decision identifies what must be resolved before completion can be confirmed.

The decision record identifies the approver and authority, scope, target version, supporting evidence and limitations, operating acceptance, retained capability, remaining exposure, continuing owners and the decision with its rationale. The responsible owners reflect the decision in the relevant status and roadmap records. Existing linked records can provide this account.

Keep completion claims within their scope and maintain their basis

A change package may be complete while its estate remains in transition. Completion of one estate does not establish that every cryptographic use supporting a protected outcome meets its target. The outcome

owner therefore considers the relevant estates and shared dependencies before making a broader protection claim.

The transition manager consolidates owner assessments against the programme's defined scope, keeping package, estate and programme status distinguishable and remaining work visible. Broader completion claims remain supported by the assessments for the uses and dependencies they cover.

The verified result and recorded decision provide a basis for the continuing maintenance and adaptation described in section 6, which also operate during transition. Evidence of an omitted recovery path or a reintroduced prohibited configuration prompts the responsible owners to reassess the affected completion claim and take corrective action. The assessment distinguishes gaps in the original completion evidence from later changes to the operating state and updates the recorded position accordingly. A later change in threats, standards or protection needs may require a new transition without automatically invalidating a properly supported earlier decision.

Example: completion of payment gateway package

For example, the gateway package for the first counterparty connection has met its target, including verified retirement of the predecessor path. The change package owner reconciles the records, the outcome owner confirms the specified payment protection, and the operations and dependency owners confirm continuing responsibilities, support and recovery arrangements. The estate owner submits the assessment and owner confirmations for the required review, and the assigned approver confirms completion of that package. The second counterparty connection still uses its earlier arrangement, so the transition manager reports the completed package alongside the remaining estate work. The first connection's completion does not establish that the payment service's entire transition is complete.

Key accountable party and responsibility	Expected result	Evidence of achievement
Change package owner: assemble completion evidence and coordinate record reconciliation.	Achieved results and remaining work are traceable to the approved scope, target and completion criteria.	Linked design, change, validation, operating and retirement evidence supports the assessment and agrees with the resulting configuration and reconciled records; differences and limitations are explicit.
Cryptographic estate and outcome owners: assess target achievement and protection within their remits and confirm continuing responsibilities.	Completion and protection claims are substantiated for their stated scope, with continuing ownership established.	Assessments and owner confirmations link the target to verified results, relevant dependencies, retained capability, remaining exposure and accepted responsibilities.
Assigned approver: decide completion within the applicable authority and delegation.	Completion is confirmed for a defined scope on the basis of reviewed evidence and accepted continuing arrangements.	The decision identifies the approver and authority, the scope and target, supporting assessments and limitations, continuing owners, rationale and any matters preventing confirmation.
Transition manager: consolidate scoped results and remaining obligations.	Programme reporting preserves the distinctions between package completion, estate progress and broader completion or protection claims.	Dated status and roadmap updates trace consolidated claims to owner assessments, shared dependencies and assigned remaining work.

Pillar review — Implement and retire

The review establishes whether the evidence supports the particular action or claim: introduction or expansion, continued operation, predecessor withdrawal, or completion of a defined scope. It connects the approved target and applicable permissions to the implementation under review, its operating

behaviour and any remaining predecessor uses. The relevant checks should reflect the particular action or state under review.

Review question	Review focus
1. What is being reviewed?	The review identifies the action or claim, the affected protected outcomes, cryptographic estates and change packages, the approved target, the relevant configuration and dependencies, and the date or period covered. It states the scope for which a conclusion is sought.
2. What does the evidence establish?	**Implementation and permission (5.1–5.2):** The reproducible candidate, validation results and confirmed operating and dependency arrangements support the particular action. Any permission identifies the candidate, scope, prerequisites, limits and stop or recovery conditions. **Controlled operation (5.3):** Observations establish actual cryptographic use and service behaviour, including relevant fallback and recovery paths. Material differences between tested, authorised and deployed states are explained, with their implications for permission and operation addressed. Operations can support, monitor and recover the service. **Remaining exposure (5.4):** Remaining predecessor uses, exposure and work to reach the target, and associated transition debt or exceptions, are visible. Original commitments remain traceable. Evidence supports claimed exposure reduction and control effectiveness. Required exceptions remain current, their conditions are met and actions to end departures remain assigned. **Retirement (5.5):** Configuration checks, tests and operating evidence establish that the predecessor arrangement can no longer be selected, negotiated or invoked for the retired use within the defined scope, including relevant dormant, fallback and recovery paths. Retained capability has an authorised purpose, and continuing obligations remain supported. **Completion and continuing ownership (5.6):** The approved target and completion criteria are met for the claimed scope, including required retirement. Architecture, inventory and related records agree with the verified result. Continuing owners have accepted their responsibilities and have the resources and support to fulfil them. Broader claims account for relevant estates, shared dependencies and unfinished work.
3. What remains unresolved?	The review identifies discrepancies between permission and deployment, unverified paths, unmet service or protection requirements, continuing predecessor dependencies, breached exception conditions and approaching expiry of permissions. For each finding, the assessment identifies the affected scope and requirement, explains the remaining uncertainty or shortfall, and determines its consequence. The finding may prevent the proposed action, require a response to continued operation, or leave a completion criterion unmet. An exception may permit an interim operating state, but it does not satisfy an unmet completion criterion.
4. What action or decision follows?	The review identifies the supported course of action: proceeding within existing permission, restricting or recovering operation, correcting and retesting the implementation, resolving dependencies, authorising withdrawal, or confirming completion of the defined scope. The recorded conclusion states what may proceed, the applicable conditions, what remains to be resolved, and the responsible owners, actions and follow-up dates. Deployment permission, operating acceptance, retirement and completion remain distinguishable.

6 Maintain and adapt

The *Maintain and adapt* pillar sustains cryptographic protection as systems, dependencies and protection needs evolve. It operates throughout the transition and continues after defined scopes are complete, keeping the bank's understanding of its cryptographic position current and enabling it to respond when further change is needed.

Current records and control checks establish what is deployed, whether controls remain effective and where uncertainty remains (section 6.1). This evidence supports measures of protection achieved, remaining exposure, delivery progress and operating capability (section 6.2). Reviews consider these findings alongside changes in threats, standards and supplier arrangements to determine whether earlier decisions or working practices need revision, and verify the effects of agreed responses (section 6.3). Exercises and operating experience establish whether the bank can make further cryptographic changes within its protection, service and timing requirements (section 6.4).

Pillar outcome: Knowledge of the bank's cryptographic position remains current, controls remain effective, and decisions respond to changing conditions. The bank retains a demonstrated ability to change cryptography again.

PACT / PILLAR 4

Maintain and adapt

Keep cryptographic knowledge and controls effective, adapt decisions to changed conditions and demonstrate the ability to change again.

Four connected areas · key actors and results

6.1 Maintain current knowledge and effective controls

Actors Estate owner reconciles records; operations owner maintains and checks controls; outcome, dependency and specialist domain owners maintain requirements and supporting information.

Result Current records and control evidence support protection and retirement claims; discrepancies, uncertainty and verified corrections remain traceable.

6.2 Measure protection, exposure, progress and capability

Actors Transition manager consolidates measures; responsible owners substantiate protection, exposure, delivery and capability; specialist domain owners maintain measurement definitions.

Result Reporting distinguishes evidence coverage from attained results, keeps material exposure visible and assigns responses to threshold breaches.

6.3 Review findings and adapt decisions and arrangements

Actors Estate owners reassess decisions and timing; specialist domain owners review quantum-threat assumptions and shared practice; responsible owners implement and verify responses.

Result Decisions explain retained or changed arrangements and timing; implemented responses are verified against their intended effects.

6.4 Demonstrate continuing cryptographic agility

Actors Estate and outcome owners define objectives and assess capability; change package, operations and dependency owners exercise changes with technical contributors.

Result Demonstrated capability covers decisions, waiting time, implementation, recovery and required withdrawal, with timing against targets and unproven scope explicit.

Evidence ↓ ↑ Decisions and follow-through

Recurring pillar review

Do earlier conclusions about protection, operation and change capability remain supported?

Scope
Which operating, reporting, timing or capability conclusions are being tested, for which outcomes, estates and period?

Evidence
Do current control and recovery checks, reproducible coverage and attainment measures, verified responses and complete exercise timings support earlier conclusions?

Unresolved matters
Which claims remain unproven or contradicted; which missed targets, overdue responses or expiring exceptions affect continuing operation?

Action or decision
Retain, qualify or reopen conclusions; refresh evidence, correct controls, revise timing or repeat exercises, with owners and dates.

The transition manager coordinates consequences across estates and tracks resulting commitments.

Maintenance and adaptation operate throughout transition and after completion of a defined scope.

Figure 5 Maintain and adapt at a glance

6.1 Maintain current knowledge and effective controls

Systems, dependencies and protection needs continue to change during and after transition. The bank needs current evidence of what cryptography is deployed, what it protects and whether its operating controls remain effective. It connects maintenance of the records established under section 4.1 with checks on actual configurations and behaviour, so that material changes and discrepancies receive a timely and appropriate response.

Keep the records and requirements current

The cryptographic estate owner maintains the inventory and linked records, drawing on routine architecture, development, procurement, change and operating activities. Relevant releases, configuration changes, key and certificate events, ownership transfers and changes to recovery arrangements prompt updates to the affected records, including any relevant CBOM. These updates preserve the links between deployments, protected outcomes, dependencies, decisions and outstanding work. Earlier states remain available so that changes can be traced and explained.

Dependency owners obtain current provider evidence, support commitments and notices affecting the bank's deployments. Outcome owners communicate changes in protection needs, obligations and service constraints. Specialist domain owners maintain common methods and requirements, identify relevant changes in standards or technical guidance, and establish which uses may be affected. This information reaches the responsible estate and operations owners for assessment. New standards or guidance inform that assessment; any resulting change to the bank's approved arrangements follows the applicable decision process.

Maintenance should include the source catalogue introduced in section 4.1. Changes to tools, platforms, collection routes, ownership or source populations can create or remove blind spots even if no known cryptographic configuration has changed. Reassess coverage, refresh arrangements and confidence, then preserve the links between consolidated findings, deployments and dependent applications.

Check the records against actual deployments

The estate owner, supported by technical contributors, reconciles the records with configuration checks, observations and appropriately scoped discovery. Scans can help validate the inventory and identify changes, subject to their access and visibility limitations (FS-ISAC Post-Quantum Cryptography Working Group, 2023c, pp. 4–6). Periodic checks supplement updates triggered by events. Their frequency and coverage reflect the rate of change and consequences of error, while meeting any applicable minimum review frequency.

Each finding retains its scope, source, date, relevant version and limitations. When a release or configuration changes, the estate owner assesses which earlier findings still apply and where renewed inspection or testing is needed. Evidence may remain applicable where its supporting conditions are unchanged. Unresolved conflicts and gaps remain visible. Missing or outdated evidence limits the conclusions that can be supported, but does not by itself establish a control failure.

Check that operating controls remain effective

The operations owner, supported by technical contributors, maintains and checks the controls governing approved cryptographic profiles, key and certificate requirements, fallback limits, and incident-response and recovery arrangements. Checks establish actual behaviour and detect configuration drift, unexpected algorithm selection and the reintroduction of prohibited predecessor paths, including through backups or recovery images. This supports continuing monitoring and enforcement of cryptographic policy (Barker et al., 2025, §5 and §5.2).

Permitted coexistence and retained historical decryption or verification remain subject to their stated purposes, safeguards and applicable time limits. Controls are assessed periodically and after changes or incidents that affect the basis of earlier results. Renewed testing focuses on the requirements and recovery arrangements affected (BCBS, 2021a, paras. 21–22, 35).

Resolve discrepancies and verify the response

The estate owner ensures that each material discrepancy has an identified response owner, an appropriate response and a due date. The record links the finding to the affected requirement or conclusion, supporting evidence and remaining uncertainty. An evidence gap may call for inspection or testing; a demonstrated control failure may require prompt containment or correction by the operations owner within existing authority. The responsible owners verify the resulting state, reassess the affected conclusions and update the linked records.

Where a finding may affect other deployments using the same component or method, it is shared with their responsible owners for assessment. If the response would change permissions, targets or common arrangements, the responsible owner obtains the required decision from the assigned approver, following the review arrangements in section 6.3.

Example: gateway recovery configuration maintenance work

For example, a routine update changes the gateway's recovery configuration for the first counterparty connection discussed in section 5.6. The estate owner identifies that the earlier recovery test no longer establishes how the changed configuration behaves. A targeted test then shows that recovery can re-enable the retired cryptographic profile. The operations owner applies the authorised containment response, while technical contributors correct and retest the configuration. The estate and outcome owners reassess the affected retirement and protection conclusions, and other deployments using the same configuration are checked. The records distinguish the initial uncertainty, the demonstrated failure and the verified correction.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate owner: maintain and reconcile the estate's records and ensure responses are assigned to material discrepancies.	Records and conclusions reflect the current state and its uncertainties.	Dated, linked records identify changes, evidence limitations, unresolved findings, assigned responses and verified results.
Operations owner, supported by technical contributors: maintain and check operating controls and carry out authorised responses.	Operation remains within approved conditions, and failures receive timely action.	Configuration checks, observations and tests establish actual behaviour; containment, correction and verification are recorded.
Specialist domain owners: maintain common methods and requirements and assess relevant technical changes.	Common arrangements remain current, and changes requiring assessment are identified.	Versioned requirements and guidance, with assessments of their basis, applicability and affected owners.

6.2 Measure protection, exposure, progress and capability

Transition activity and technical observations need interpretation before they can support management decisions. To support those decisions, measures need to show what protection has been demonstrated, what exposure remains, what work has been completed and whether the bank can carry out further cryptographic change.

Select measures that support decisions

The transition manager works with the responsible owners to select a small set of measures suited to the bank's current decisions. PACT distinguishes four reporting views:

Reporting view	What it should establish
Protection achieved	Whether actual algorithm and profile use and service behaviour meet specified requirements, including relevant fallback and recovery conditions.
Remaining exposure	Which vulnerable uses remain, their consequences and required protection periods, and whether safeguards and planned responses are credible and timely. Undetermined or infeasible timing, exceptions, transition debt and overdue withdrawal remain visible.
Delivery progress	Results substantiated against agreed commitments, including design, deployment, required retirement, completion of a defined scope and closure of exceptions. Supplier delivery is assessed against the dates needed by dependent work; delays and unfinished work retain their owners and dates.
Operating capability	Whether competent people, available capacity, technology and dependencies support controlled change. Measures may include the time from policy approval to verified enforcement in production, tested recovery, effort, and supplier or hardware replacement lead times.

These views answer different questions. A supplier agreement may complete a planning action while the affected use remains vulnerable. Deployment, required retirement and completion also remain distinct achievements, as established in section 5.

Capability measures draw on assessed competence and demonstrated performance, including the time, effort and operational disruption involved in replacing an algorithm (FS-ISAC Post-Quantum Cryptography Working Group, 2024, pp. 6, 13). Training attendance and workshops record supporting activity; exercises and observed work provide evidence of the capability claimed. Section 6.4 develops the corresponding exercises.

Define the measures and make evidence limits visible

Each measure identifies the decision it supports and what is being measured: the unit, population, scope and exclusions. Its calculation, evidence sources and reporting period make the result reproducible. Definitions also explain how unknown, stale, conflicting and not-applicable items are treated. Relevant specialist domain owners maintain common definitions and methods so that results can be interpreted consistently and compared on a stated basis (Schroeder et al., 2024, §§3.1–3.2).

Coverage measures draw on the records and checks maintained under section 6.1. They show whether protected outcomes are linked to the relevant cryptographic uses and owners, whether supporting evidence remains current, and whether material provider-controlled deployments have evidence specific to the release and configuration used.

For a reported percentage, reporting distinguishes the full identified population in scope, the subset with suitable current evidence, and the subset demonstrated to meet the stated condition. Reporting evidence coverage alongside attainment makes the limits of the conclusion visible. Known but unassessed items remain in the population without being counted as demonstrated successes or failures. Where the population cannot be credibly established, reporting uses bounded counts or justified ranges and describes the blind spots. Sampling and unobserved paths also qualify the result.

Consolidate results and explain changes

The transition manager reconciles owner submissions before consolidating them. Estate and outcome owners substantiate transition, protection and exposure conclusions within their remits. Change package, operations and dependency owners substantiate delivery, operating and provider results.

Aggregation should retain access to the underlying evidence and consequential gaps. Counts should state whether they measure distinct components or dependency relationships. A shared component should be counted once in a component total, while each affected use and its reliance remain identifiable. Estates, uses, connections and change packages should remain distinct units, and any weighting should have an explicit basis. Numerous completed low-consequence changes should not conceal a shared dependency that prevents a critical outcome from meeting its requirements. Metrics also shape where effort goes.

Intensive tracking can draw attention away from important unmeasured work, such as flagging risks (Edwards et al., 2026). Rewarding one task can also reduce contributions to related tasks that are not rewarded (Zhou et al., 2026).

Comparisons over time explain changes in scope, evidence coverage, classifications and calculation methods. Newly discovered vulnerable uses are distinguished from increased exposure in previously assessed uses. Revised dates preserve the original commitments, allowing management to see both the current plan and the extent of delay.

External readiness benchmarks can provide context. Banks may draw on the same evidence when responding to the HKMA's Quantum Preparedness Index, while keeping the resulting scores distinct from protection demonstrated for particular uses (HKMA, 2026b).

A pipeline view can show what is being investigated, what prerequisite work remains, which candidates have evidence for a specified next action and which are blocked. Identify the affected critical services and the owners of material blockers. Keep the counting unit and unknown population explicit, and show verified cryptographic changes separately from preparation activity.

Connect findings to timely action

Each measure identifies its reporting owner, reporting frequency and refresh triggers, together with its target or action threshold and the expected response. Reports connect threshold breaches and other material findings to their consequences, the responsible owner, the required action or decision, and the response date. Decision and action timeliness are tracked against agreed response periods, with overdue items visible.

Threatened completion dates, expiring exceptions, inadequate evidence or unavailable capacity may require a response between reporting dates. Urgent operating responses proceed under existing authority without waiting for the next reporting cycle. Section 6.3 addresses the resulting reassessment.

Example: measure conformance of counterparty connections

For example, a bank assesses 100 counterparty connections against their approved target profiles, including normal and recovery paths. Sixty have sufficient current evidence, and 48 of those meet the requirement:

Measure	Calculation	Result
Evidence coverage	60 assessed connections out of 100 identified	60%
Conformance among assessed connections	48 conforming connections out of 60 assessed	80%
Conformance across the full scope	48 conforming connections out of 100 identified	48%

Twelve connections are known not to conform; 40 remain unassessed. If discovery identifies another 20 connections without further assessments, the identified population increases to 120. Evidence coverage becomes 50%, and conformance demonstrated across the full scope becomes 40% (48 of 120). Conformance among the assessed connections remains 80%. The report explains the expanded population and preserves the earlier results.

These percentages describe conformance with the stated requirement. They do not establish an equivalent reduction in business risk, which also depends on the consequences and dependencies of the affected uses.

Key accountable party and responsibility	Expected result	Evidence of achievement
Transition manager: coordinate measures, reconcile submissions and consolidate reporting.	Management receives a coherent account of results, limitations and matters requiring action.	Dated reports trace results to owner submissions, preserve material gaps and identify required responses or decisions, owners, due dates and overdue items.
Cryptographic estate and outcome owners: substantiate transition, protection and exposure conclusions within their remits.	Reported conclusions are supported for their stated scope and requirements.	Assessments identify the population, demonstrated results, remaining exposure, evidence limitations and consequences.
Change package, operations and dependency owners: substantiate delivery, operating and provider results.	Progress and capability reflect verified results and credible commitments.	Change, operating, exercise and provider records support reported achievement, timing, capacity and unresolved constraints.
Specialist domain owners: maintain common measurement definitions and methods within their remits.	Measures can be interpreted consistently and compared on a stated basis.	Versioned definitions specify populations, calculations, evidence treatment and thresholds; changes in methods are explained.

6.3 Review findings and adapt decisions and arrangements

Findings from sections 6.1 and 6.2, together with changes in assumptions, dependencies or operating conditions, may require the bank to revisit earlier decisions. A local correction may resolve an immediate fault while a shared cause still affects other deployments. This section connects the assessment of those findings to decisions, coordinated action and evidence that the response has achieved its intended effect.

Assess findings and changed conditions

Cryptographic estate owners use existing review arrangements with the relevant outcome, operations and dependency owners. Reviews bring together operating and assurance findings, reported results, and changes in protection needs, obligations, threats, standards, systems, supplier commitments and resources. Review frequency reflects the potential consequences, rate of change, currency of evidence and proximity to important dates. Material events prompt review without waiting for the scheduled cycle. Periodic reviews also examine cumulative weaknesses, such as repeated exceptions, delayed decisions, persistent evidence gaps or unrealistic delivery assumptions.

For each material finding, the estate owner works with those responsible for the evidence and consequences to identify the affected uses, outcomes and decisions. Investigation establishes whether a local correction is sufficient or a shared cause requires changes to common profiles, methods, supplier arrangements, skills, resources or governance. A single consequential finding may justify wider action. Other estates relying on the affected component or arrangement are included in the assessment; unrelated work may continue within existing permissions.

PACT recommends reassessing the quantum-threat planning assumptions used under section 4.3 at least annually, and earlier when credible developments could materially affect them. The relevant specialist domain owner assesses the evidence and proposes any revision through the applicable approval arrangements. A revised assumption becomes the planning basis only after the required approval.

Estate owners use the applicable approved version when revisiting affected completion deadlines and required-start dates, taking account of protection periods, remaining migration duration and contingency. A shorter assumed threat horizon may bring the required start forward even where comparative priority ratings remain unchanged. Assessments retain earlier assumptions and calculations and identify any resulting urgency, uncertainty or infeasibility.

Decide what to retain or change

An earlier decision or arrangement may be retained, revised, suspended, withdrawn or replaced. Retention requires a reason and a next review trigger.

The decision record states the affected scope, supporting evidence and uncertainty, rationale, deciding authority, and resulting actions, owners and dates. An authorised revision specifies its effective version and how work already under way will be treated. Earlier decisions and commitments remain available; changing criteria does not retrospectively establish that an unmet requirement was achieved.

Apply the decision across affected work

The transition manager coordinates consequences that span estates or organisational boundaries, communicates decisions to affected owners and tracks the resulting commitments. Estate, operations, dependency and change package owners implement their assigned actions and update the relevant assessment, design, inventory, supplier, operating and change records. The transition manager reconciles changes to the integrated roadmap and, where needed, the responsibility map, referring unresolved resource or authority issues to the responsible executive sponsor. The updated plans identify who will act, what remains permitted and which commitments have changed.

Where findings support improvements to common practice, specialist domain owners incorporate the agreed changes into the profiles, discovery methods, test procedures, supplier requirements or training used in future work. Each revision identifies its purpose, owner and version, together with its supporting evidence, prerequisites, limitations and review trigger. Receiving estate owners assess its applicability to their configurations, dependencies and protection needs. This connects lessons from actual results to improvements in subsequent work (ETSI, 2024, §§6.10–6.11).

Operational findings can improve specific methods: repeated asset observations can change consolidation rules; a missed environment can change discovery coverage; shared-platform findings can change ownership allocation; and provider constraints can change candidate selection. Feed measured implementation effort and waiting into later estimates and readiness criteria. Keep the original finding, revised method and evidence from its next use linked so that an improvement is tested rather than merely recorded.

Verify that the response worked

Each material corrective or improvement action specifies the intended result and how it will be verified, including the necessary evidence, responsible owner and due date or triggering event. Testing or subsequent operating experience establishes whether the response addressed the cause and preserved the required protection and service behaviour. Outcome owners assess the results against the affected protection and service requirements. Issuing a revised procedure or closing an action does not by itself demonstrate effectiveness. Failed checks or recurrence reopen the response or prompt escalation (BCBS, 2021a, paras. 35–36).

Example: adapting a shared maintenance procedure that omits recovery checks

For example, investigation of the gateway recovery failure in section 6.1 identifies a shared maintenance procedure that omitted recovery checks after supplier updates. Correcting the first gateway resolves the local fault, while other deployments using that procedure require assessment. Through the applicable decision arrangements, the specialist domain owner revises the procedure to require recovery testing before an updated gateway returns to service. Affected estate and operations owners assess and apply the revision. In a controlled test, the revised procedure detects an update that would reinstate the prohibited profile, and the update is withheld from production until corrected. The transition manager records the verified improvement alongside deployments still awaiting the change.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate owners: reassess affected decisions and timing, obtain required decisions and coordinate the estate's response.	Findings lead to justified decisions and responses covering the affected scope.	Linked assessments and decisions explain what is retained or changed, preserve earlier assumptions and calculations, and identify actions, owners, dates, continuing conditions and unresolved matters.
Specialist domain owners: reassess common assumptions, including quantum-threat planning assumptions, and revise shared practices where warranted.	Common assumptions remain justified, and shared weaknesses lead to appropriate improvements.	Dated reviews link retained or revised assumptions to their evidence, approval and version. Revised practices identify their purpose, applicability, prerequisites and limitations.
Transition manager: coordinate consequences across estates and track resulting commitments.	The integrated roadmap and responsibility map reflect authorised changes, and unresolved resource or authority issues reach the responsible executive sponsor.	Linked updates preserve previous and revised commitments, assigned actions and outstanding constraints. Follow-up records distinguish verified responses from work still awaiting implementation or confirmation of effectiveness.

6.4 Demonstrate continuing cryptographic agility

Cryptographic arrangements may need to change again as standards, security findings and supplier products evolve. The bank therefore needs evidence that it can complete a further change within its protection, service and timing requirements. This includes both the technical means to make the change and the ability to obtain decisions, coordinate dependencies and complete the work (Barker et al., 2025, §§5.2, 6.5).

Define the capability to be demonstrated

The cryptographic estate owner works with the relevant outcome owners to identify representative changes and define the protection, service and timing criteria against which capability will be assessed. Each case identifies the cryptographic use and proposed change, affected systems and dependencies, environment and time allowed. Evidence from an actual subsequent cryptographic change can support the assessment where it answers the same questions.

Targets reflect the particular use. Changing an online-banking connection profile and replacing cryptography in a fixed device may involve different work and lead times. Exercise frequency reflects the consequences of failure, the rate of change and gaps in existing evidence. Material changes may require an earlier exercise.

Test the complete change process

Selected scenarios cover planned replacement and urgent change, including changes to algorithms, parameters, certificates, trust anchors or policy, as relevant to the estate. Where critical operations are affected, scenarios examine severe but plausible disruption and material internal, group and external dependencies (BCBS, 2021a, Principle 3 and paras. 23–25).

The estate owner arranges the exercise with the relevant change package, operations and dependency owners and technical contributors. Permissions, stopping conditions and permitted recovery configurations are established before execution. Exercises use an appropriate controlled environment; any production activity remains subject to the bank's change and operating controls.

The exercise establishes whether the bank can identify the affected uses, obtain the necessary decisions, coordinate connected parties and implement the replacement. Tests then establish whether the replacement is actually used, permitted choices are enforced, service behaviour remains acceptable,

recovery works and any required predecessor withdrawal is effective. Where automation supports the change, testing covers its behaviour during failed updates and its capacity at the required scale (FS-ISAC Post-Quantum Cryptography Working Group, 2024, pp. 12–14).

Assess performance and state the limits

Performance is assessed against the agreed criteria over the complete process, from the initiating event to the required result. Records distinguish time spent identifying and deciding the response, implementation time, and waiting or delays outside the bank's direct control. Supporting evidence records effort, defects, rework, service effects, and recovery and withdrawal results.

Supplier releases, counterparty coordination, hardware procurement and certification can determine whether the complete change meets its target. Dependency owners substantiate the relevant steps and distinguish observed delivery from commitments or estimates (FS-ISAC Post-Quantum Cryptography Working Group, 2024, pp. 16–17).

The estate owner assesses the results with the outcome owner and states what capability has been demonstrated and what remains unproven. A discussion exercise can test decisions and coordination; a technical test can demonstrate behaviour in its stated configuration and environment. A claim about completing a change in production requires evidence covering the relevant decisions, implementation, operation, recovery and required withdrawal.

Conclusions identify workloads, parties, recovery paths and other material conditions not exercised. Specialist domain owners support consistent methods and assess whether shared results apply to other estates. Support for several algorithms, a maturity rating or completion of the initial migration does not by itself demonstrate the ability to make a subsequent change.

Use the results to improve subsequent changes

Results inform the capability measures under section 6.2 and lead to assigned responses under section 6.3. Observed durations and constraints inform future timing and capacity estimates. Where a weakness is identified, a subsequent exercise or suitable operating evidence establishes whether the response improved the affected capability.

Example: profile change rehearsal

For example, a bank rehearses a profile change for a supplier-operated file-transfer service. The agreed objective is to request, implement and verify the change in the test environment within ten working days. The supplier's test release arrives on working day twelve, after which the bank completes its configuration and recovery tests in one day. The rehearsal demonstrates the tested change and recovery behaviour but misses the timing objective. The dependency owner seeks revised release arrangements, and a later exercise checks whether the complete process can meet the target.

Key accountable party and responsibility	Expected result	Evidence of achievement
Cryptographic estate and outcome owners: define representative changes and protection, service and timing criteria; assess the resulting capability.	The bank can identify which subsequent changes it has demonstrated, under what conditions and within which limits.	Scenario criteria and assessments identify tested systems, dependencies and conditions, performance against targets and the scope still unproven.

Key accountable party and responsibility	Expected result	Evidence of achievement
Change package, operations and dependency owners: carry out the relevant parts of the exercise and substantiate internal and external results.	The complete change, including recovery and required withdrawal, is assessed against its objectives and constraints.	Dated execution, test and operating records show actual use, enforced choices, service effects, recovery and withdrawal results, effort and elapsed time. Observed supplier delivery remains distinguishable from commitments and estimates.
Specialist domain owners: maintain suitable exercise methods and assess the applicability of shared results.	Exercises cover material ways a later change could fail, and shared evidence is used within its demonstrated scope.	Methods cover relevant policy, compatibility, recovery and scale conditions. Applicability assessments identify the configurations and dependencies covered and where further testing is needed.

Pillar review — Maintain and adapt

The pillar review establishes whether current evidence continues to support the bank's conclusions about cryptographic protection, operation and change capability. It draws together the work under sections 6.1–6.4 to identify what remains supported, what requires qualification or reassessment, and what action follows as deployments, assumptions and dependencies change.

Review question	Review focus
1. What is being reviewed?	Identify the outcomes and estates covered, the review date or period, and the operating, reporting, timing or capability conclusions to be examined. Select the material deployment changes, reported results, findings, completed responses and exercises relevant to those conclusions.
2. What does the evidence establish?	**Deployments and controls (6.1).** Compare current deployments, protection requirements and dependency information with the inventory and evidence supporting earlier protection or retirement conclusions. Examine periodic control checks and findings from releases, configuration changes and key or certificate events. Establish whether fallback and recovery evidence still applies to the changed state. Where it does not, examine targeted retesting, including whether restoration could reintroduce a prohibited profile. **Reported results (6.2).** Trace material measures, including counts, ranges and timing results, to their definitions and current evidence. For percentages, verify the full identified population, the subset with suitable current evidence and the subset demonstrated to meet the stated condition. Distinguish changes in coverage, population or calculation from changes in protection or delivery. Check that shared dependencies blocking critical outcomes remain visible and that threshold breaches and overdue actions or decisions have assigned responses. **Decisions and responses (6.3).** Trace material findings to reasoned decisions and, where action was required, to implementation and verification of its effects. For shared causes, establish which other deployments have been assessed and which remain outstanding. Examine the latest reassessment of quantum-threat assumptions and the resulting timing calculations. A shorter threat horizon or longer migration duration may require an earlier start even where priority ratings remain unchanged. Check that the resulting decisions and roadmap reflect those consequences. **Demonstrated agility (6.4).** Reconstruct elapsed time from the initiating event to the required result, including decisions and supplier or counterparty waiting time. Compare performance with the stated target and examine recovery and required withdrawal results. Limit capability conclusions to the configurations, environments, workloads, parties and paths actually exercised.

Review question	Review focus
3. What remains unresolved?	For each material gap, state which conclusion it prevents or qualifies. An untested recovery configuration may leave a retirement conclusion unsupported; a revised procedure without evidence of its effect leaves the improvement unverified; and a supplier delay may prevent a change from meeting its deadline. Distinguish missing evidence from an observed failure or a missed target. Identify overdue responses and expiring exceptions that affect the conditions for continued operation.
4. What action or decision follows?	Record which conclusions are retained, qualified or reopened, the reasons, and the resulting actions. These may include refreshing evidence, correcting controls, assessing other affected deployments, revising timing or repeating an exercise. Each action identifies its responsible owner, date, intended result, and the conditions under which affected operation or work may continue. Retained arrangements have a recorded reason and a next review trigger. Responsible owners make or obtain the required decisions. The transition manager coordinates consequences across estates.

7 PACT in practice

This hypothetical case follows a bank as it changes the cryptography supporting a corporate payment connection, from initial planning through implementation, retirement and continuing management. The example shows how protection and operating requirements guide decisions, and how findings from testing and operation lead the bank to revisit them. Events are presented chronologically, although work across the four PACT pillars overlaps and recurs.

The payment connection and its dependencies

A corporate customer submits an authorised batch of 500 payment instructions. After validation, the bank's payment engine sends the batch through either its primary or standby gateway to an external payment processor. The processor, referred to as the provider in this case, returns a receipt acknowledgement and individual payment statuses. It operates primary and standby endpoints. A separate gateway software supplier provides the bank's software releases, patches and recovery images.

The case covers two cryptographic estates:

- The **payment-connection estate** covers the cryptographic uses, configurations and recovery arrangements of both bank gateways.
- The **shared-platform estate** covers the cryptographic uses and components supporting certificate issuance and the protection and restoration of identity keys using hardware security modules (HSMs).

The shared services support gateway authentication, so the connection's protection and recovery depend on coordinated work across both estates. The shared platform also serves other bank applications. The processor's endpoints remain external dependencies of the bank's connection. Figure 6 shows the payment flow and the boundaries of the two estates.

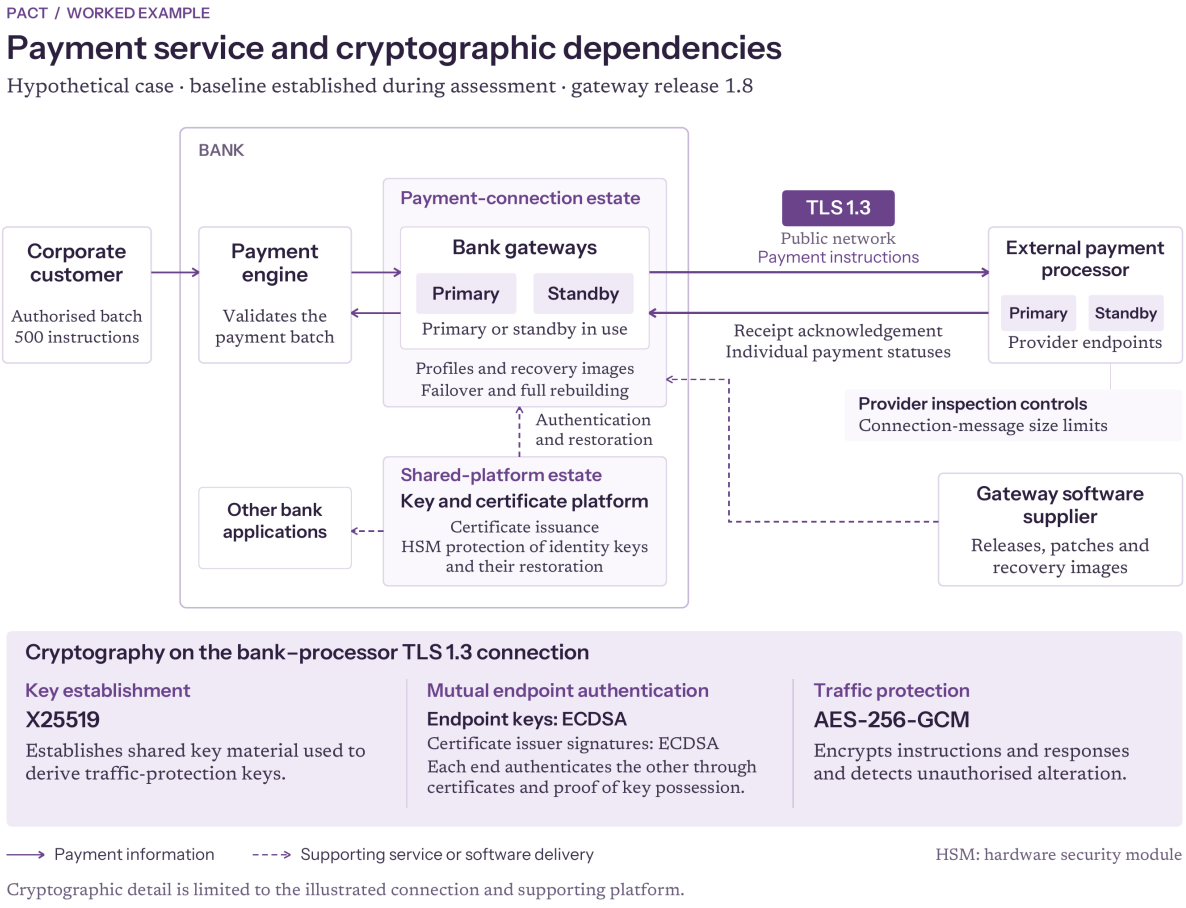

Figure 6 Payment flow and cryptographic estate boundaries in the worked example

Assumptions and measures

All dates, software releases, requirements and results are illustrative. Test and operating results apply to their stated workloads and configurations. The following assumptions and measures apply throughout the case.

Assumption / measure	Meaning in this case
Planning dates	The bank uses 2035 as the conservative quantum-threat date selected from its approved illustrative range. It is a planning assumption, not a prediction. The target for authentication migration is a separate decision by the bank.
Payment performance	The 500-millisecond limit applies to the 95th-percentile time from batch submission to receipt acknowledgement. Individual payment acceptance and payment reconciliation are assessed separately.
Recovery measure	The 30-minute limit applies to restoration of the approved connection, including activation controls and verification. Payment reconciliation is a separate requirement. Failover and complete rebuilding are tested separately.

The case follows senior management, service and estate owners, and delivery and operations teams as they coordinate the work with the processor and gateway supplier. The bank retains responsibility for its decisions throughout.

7.1 Govern the transition

Establish the scope and leadership

The bank proposes six weeks of investigation and planning for the payment connection. Senior management appoints the chief operating officer as executive sponsor for both estates. Within existing delegations, the sponsor authorises preparation of the mandate and an initial capability exercise. A transition manager coordinates the preparation, maintains the integrated roadmap and responsibility map, and escalates unresolved commitments (section 3.1).

The proposed mandate covers both gateways, their supporting key and certificate services, and recovery arrangements. The head of corporate payments sets the protection and operating requirements. Transmitted information requires seven years of confidentiality, and the connection must provide mutual endpoint authentication and protection against undetected alteration. Connection recovery must be possible within 30 minutes, and payments must be reconciled without loss, duplicate execution or incorrect status.

Customer login, payment authorisation, retained records and other applications using the shared platform remain assigned to owners in the wider transition programme. They sit outside this package's delivery scope unless the investigation identifies changes needed to support the connection (section 3.2).

Assign responsibilities and decision authority

The transition manager records the following assignments in the responsibility map, identifying the current role holders, their deputies and the boundaries of their responsibilities (section 3.3).

Responsibility	Assignment and expected contribution in this case
Outcome owner	The **head of corporate payments** assesses evidence from both estates and secures action on protection or service shortfalls.
Payment-connection estate owner	The **payments connectivity manager** is accountable for the cryptographic uses and configurations of both gateways, including failover and rebuilding arrangements.

Responsibility	Assignment and expected contribution in this case
Shared-platform estate owner	The **shared platform manager** is accountable for certificate issuance, key protection and restoration, and assesses the effects of changes on other applications using the platform.
Change package owner	The **payments technology delivery lead** is accountable for the gateway change and supporting shared-platform work, including prerequisites, testing, retirement and completion evidence.
Operations owners	The **payments operations manager** is responsible for gateway monitoring, service recovery and payment reconciliation. The platform operations manager is responsible for continuing key and certificate operations and their restoration.
Dependency owner	The **provider relationship manager** coordinates both the processor and gateway supplier, obtaining configuration or release evidence, named contacts, testing commitments and support arrangements.
Specialist domain owners	The **enterprise cryptography architect** maintains common design requirements. The **inventory standards lead** maintains the common model and rules for identifiers and relationships. Each estate owner maintains the records for their estate.

The same map identifies who can approve the relevant decisions within their respective delegations.

- The **chief architect** approves designs and common architecture requirements.
- The **head of technology operations** authorises production changes and the relevant operating arrangements.
- The **chief risk officer** decides requests to accept residual risk or depart from internal requirements within the applicable remit.

An independent **technology-assurance lead** reviews evidence and control effectiveness, reporting material findings to the sponsor. The delivery lead prepares proposals and executes authorised work; the designated approvers retain decision authority (section 3.4).

Set common requirements and secure capacity

To give both estates a common basis for assessment, the enterprise cryptography architect prepares *Connection transition requirements, version 1*, which the chief architect approves. The requirements distinguish key establishment, authentication and traffic protection, and call for dated evidence of the deployed arrangements.

Their coverage includes primary, standby and rebuild arrangements, together with the protection and restoration of required keys and certificates. Fallback is controlled, and cryptographic settings must be changeable under configuration control while preserving payment-authorisation logic. Assessment and testing will determine the replacement mechanisms and interface profile (section 3.5).

A resource conflict tests the coordination arrangements. Another application has already reserved the shared test HSM and the specialist needed for the investigation. The estate owners report the resulting delay through the **evidence and feedback rail**. The transition manager compares schedules with both application owners and presents the consequences to the sponsor.

Following the sponsor's priority decision, the facility manager confirms two specialist days each week for six weeks, with separate slots retained for the other application. The relevant managers confirm funding and time for engineering, provider support and independent review. These allocations return through the **direction and decisions rail** as commitments recorded in the roadmap (sections 3.1 and 3.6).

Check readiness and authorise the investigation

The capability exercise checks whether the proposed arrangements work in practice. Engineers retrieve dated configurations from both gateways and link their cryptographic uses to the payment requirements

and shared-platform records. The dependency owner obtains a provider capability statement and arranges an evidence-collection session for week two of the investigation.

Independent assurance confirms that the exercise demonstrates the bank's ability to collect and link its own configuration evidence. The provider's statement does not establish the configuration actually in use at its endpoints, and the gateway rebuild image still needs to be examined. These remain assigned investigations for the six-week period (section 3.6).

Pillar review

The *Govern the transition* review brings together the defined responsibilities, approved requirements, confirmed resources and exercise findings. It records the basis and limits of the decision to proceed:

Review question	Case conclusion
What is being reviewed?	Readiness to undertake six weeks of investigation and planning across both estates.
What does the evidence establish?	Named responsibilities and decision authorities, approved common requirements, confirmed capacity and demonstrated ability to collect and link bank configuration evidence support the investigation.
What remains unresolved?	The dependency owner is responsible for obtaining evidence of the provider's active settings. The payments connectivity manager is responsible for investigating the gateway rebuild image. Both investigations are due within the six-week period.
What action or decision follows?	The chief operating officer, as executive sponsor, authorises the six-week investigation and planning work within the defined scope. The transition manager reports weekly and escalates access or capacity failures. Design and production decisions remain open.

7.2 Assess and plan

During the six-week investigation, the bank establishes the cryptography currently in use, assesses the timing of the required changes and tests a proposed migration approach. The findings provide the basis for the design and integrated roadmap reviewed at the end of this stage.

Establish current use and dependencies

Before collecting evidence, engineers check the discovery tools against known code and configurations, record their coverage limits and agree safe collection conditions with operations.

The investigation confirms that both gateways run release 1.8 and use TLS 1.3 with X25519 for key establishment and AES-256-GCM for traffic protection. Mutual endpoint authentication uses ECDSA keys, and the corresponding certificates are also signed using ECDSA. The inventory records the certificate public-key and issuer-signature algorithms separately and links the cryptographic uses to the payment requirements and the shared platform's certificate and HSM records.

Examination of the rebuild image confirms that it reinstates the same release and settings. Provider configuration records and joint connection traces confirm the corresponding arrangements at its primary and standby endpoints for the bank's connection. These findings resolve the evidence gaps identified in section 7.1.

The supplier's cryptographic bill of materials (CBOM) also lists an ML-KEM component in evaluation build 2.0-rc1. That information concerns the evaluation build and does not establish ML-KEM use in the deployed connection (section 4.1).

For this hypothetical example, assume also the deployed-software scan and release inventory both report the same gateway library on the primary instance. Engineers retain both observations, resolve them to

one deployment and preserve the standby instance as a distinct deployment linked to the same component identity. Certificate and HSM findings remain allocated to the shared-platform estate and linked to the gateways' authentication uses. Consolidation changes the interpretation of observations, rather than removing the payment connection's dependencies.

The dependency owner secures access to the provider's laboratory endpoint for design testing. The gateway supplier and provider commit to compatible production candidates by 31 March 2027 and joint testing during April–June. Their commitments include named contacts, defect support and notification of changes. The shared-platform owner specifies the required HSM-interface, certificate-operation and recovery tests. These arrangements support planning, with production interoperability still to be demonstrated (section 4.2).

Assess urgency and timing

The outcome owner assesses confidentiality exposure as urgent: sensitive payment traffic crosses a public network and requires seven years of protection. The estate owners separately estimate the time needed to migrate, including supplier lead time, integration, qualification, deployment, stabilisation and retirement.

They compare a supported gateway upgrade, estimated at nine months, with a full replacement requiring approximately fifteen months because of procurement and additional integration. The estimates account for work that can proceed in parallel. Applying the timing calculation in section 4.3 to the upgrade option gives the following result.

Planning input or conclusion	Illustrative case value
Quantum-threat planning date	**1 January 2035**, the earliest date in the bank's approved illustrative range. This is a planning assumption, not a prediction.
Required confidentiality period	Seven years from transmission.
Latest date for stopping new vulnerable transmissions	**1 January 2028**: the threat-planning date less seven years.
Remaining migration duration and contingency	Nine months for the upgrade, plus a separate two-month contingency allowance.
Required start	**1 February 2027**: 1 January 2028 less nine months of work and two months of contingency. No earlier binding start deadline applies.

The calculation concerns future transmissions. Migration cannot remove the exposure of traffic already captured under vulnerable cryptography. The timing of endpoint-authentication migration requires a separate assessment.

The full replacement would not fit the window, even before contingency. The owners therefore propose the supported upgrade, which also preserves existing operational interfaces and supplier support.

Define the proposed change

The first change replaces standalone X25519 key establishment with **X25519MLKEM768**, a hybrid mechanism combining X25519 and ML-KEM-768. TLS 1.3 and AES-256-GCM are retained. The hybrid mechanism is specified in RFC 10024 (Kwiatkowski et al., 2026).

This sequencing addresses the risk that future traffic could be recorded and decrypted later. ECDSA mutual authentication remains in use, with its replacement recorded as separate work. The first package therefore addresses only part of the connection's quantum transition (Stebila et al., 2026).

The payments connectivity manager owns the authentication assessment, supported by the cryptography architect and dependency owner. They will present a feasible approach and justified timing by 30 June

2027, drawing on provider, certificate and HSM evidence. Relevant changes will prompt earlier reassessment (section 4.4).

The shared platform retains its existing authentication algorithms for this first package. Its contribution is to demonstrate compatibility and substantiate the required key, certificate and recovery arrangements.

At this stage of the case, key establishment has a candidate for bounded testing, while authentication remains separate assessment work. Shared certificate and HSM services must substantiate compatibility and recovery for the first package; the processor and supplier must supply the release-specific evidence needed later. The view below records these different next actions without assigning one readiness status to the whole payment application.

Scope	Evidence and condition	Next action
Key establishment	Evaluation candidate available; final release and joint qualification still required.	Conduct the bounded pilot and subsequent release-specific qualification under their permissions.
Authentication	ECDSA retained for the first package; a separate approach and timing assessment remains assigned.	Complete that assessment and define the later change.
Shared certificate and HSM services	Compatibility, identity restoration and recovery evidence needed for the connection.	Coordinate and substantiate those contributions without claiming authentication migration.

Test the design and approve the profile

A bounded pilot tests the proposed design using evaluation build 2.0-rc1, the provider's laboratory endpoint, the intended HSM interface and a recorded rebuild configuration. It submits 100 batches of 500 synthetic instructions at one batch per minute. Versions, settings, measurement methods and acceptance criteria are recorded so that the tests can be repeated (section 4.5).

Test	Finding and design implication
Communication compatibility	Initial handshakes fail because of the provider's inspection-device size limit. The provider corrects the laboratory setting, and repeat tests succeed. The corresponding production change becomes a named prerequisite.
Payment behaviour and performance	After correction, all 50,000 instructions reconcile without loss, duplicate execution or incorrect status. Under the same workload and network conditions, the 95th-percentile time from batch submission to receipt acknowledgement rises from 300 milliseconds with the current profile to 330 milliseconds with the proposed profile, within the 500-millisecond limit.
Rejection checks	The target profile rejects standalone X25519 negotiation and a peer certificate issued by an untrusted authority.
Failover	The test connection is restored within 22 minutes, against the 30-minute requirement.
Rebuilding	Rebuilding reinstates the target profile and required authentication material. The result applies to the tested build and image.

The findings pass through the **evidence and feedback rail** to the estate and outcome owners. They accept the evidence for the tested interoperability, payment behaviour and recovery arrangements, subject to the corresponding inspection-device correction in production. The confidentiality assessment also depends on the design and threat assumptions.

The cryptography architect incorporates the correction into *Payment connection profile, version 1*. The profile specifies the hybrid mechanism and retained authentication, together with certificate issuance, renewal and revocation, trust arrangements, HSM interfaces, monitoring and recovery.

For this profile, each new connection requires a fresh hybrid handshake; session resumption and early data are disabled. Recovery restores the approved identity material and configuration before establishing fresh sessions.

During staged deployment, identified configurations awaiting migration may continue to use standalone X25519 until its planned withdrawal in September. The target profile prohibits automatic downgrade. After withdrawal, primary, standby and rebuild configurations will reject standalone X25519, while retaining its contribution within the hybrid mechanism.

The chief architect approves the profile for change preparation, and the provider confirms matching interface requirements. The profile distinguishes the evaluation build from the intended production release. Production permission still requires qualification of the actual release, applicable implementation-validation evidence, production-path tests and release-specific recovery results (section 4.6).

Agree the roadmap and review the plan

The transition manager incorporates the approved profile and remaining conditions into a roadmap with a planned start of **1 January 2027**, one month before the calculated latest credible start.

Period	Planned work
January–March 2027	Candidate delivery and shared-platform preparation.
April–June 2027	Qualification, joint testing and operational rehearsal.
July–August 2027	Deployment subject to production authorisation, followed by observation of operating results.
September 2027	Remaining stabilisation, withdrawal of standalone X25519 and verification of completion.

Planned completion is **1 October 2027**, with two months of contingency available through 1 December 2027, before the scenario deadline of **1 January 2028**. Final candidate delivery enables joint qualification, which in turn supports deployment and retirement. Platform preparation proceeds in parallel (section 4.7).

The sponsor confirms funding for provider testing, training, retirement and contingency. Relevant managers reserve engineering and operations capacity, including two shared-platform specialist days each week during April–June, with the other application's allocation preserved. The approved profile and resource decisions return through the **direction and decisions rail** as dated commitments.

If candidate delivery slips, the remaining duration and ability to meet the protection deadline are reassessed. Any revised schedule continues to allow the time needed for the required tests.

The initial six-week investigation is an upstream preparation stream for the January delivery roadmap. Its findings create the supplier, platform and evidence actions shown in that plan. The separate authentication assessment may generate a later package and remains linked to the same protected outcomes. The dates and allocations illustrate how work connects; they are not evidence of achievable institutional throughput or a recommended wave size.

Pillar review

At the assessment review on 1 December 2026, the owners present the inventory, dependency commitments, tested design proposal and integrated roadmap. The *Assess and plan* review records the following conclusions.

Review question	Case conclusion
What is being reviewed?	The proposed key-establishment change, including its shared-platform, provider and recovery dependencies.
What does the evidence establish?	The initial discovery gaps are resolved. The corrected pilot supports the proposed design within the tested scope, and the timing assessment and resource commitments support the planned start.
What remains unresolved?	The delivery lead owns final-release and recovery qualification. The dependency owner owns evidence for the provider's intended production arrangements. Both are required before the planned July deployment. The payments connectivity manager will present the authentication proposal by 30 June 2027.
What action or decision follows?	Proceed with funded change preparation under the profile approved by the chief architect. Obtain the required release and operating evidence before seeking production permission. Authentication migration remains separately assigned work.

7.3 Implement and retire

The bank implements the approved key-establishment profile and verifies withdrawal of the predecessor arrangements. A payment-status fault and a later recovery limitation require revised decisions on deployment and continued operation. The bank must then establish when the predecessor recovery route can be retired and the package recorded as complete.

Prepare and authorise deployment

The delivery lead prepares the implementation package for final release 2.0, identifying its cryptographic library, configuration, recovery image and installation instructions. It links the approved profile to the provider's production endpoints, the inspection-device correction and the shared-platform interfaces. It also connects the delivery tasks and operating procedures to the September retirement criteria.

The cryptography architect checks the implementation and validation evidence. Operations owners prepare monitoring, support and recovery, while the dependency owner confirms supplier and provider support for the specified release. The sponsor assigns completion authority to the head of technology operations, supported by the affected owners' assessments (section 5.1).

Recovery preparation establishes which cryptographic material must be restored and which must be created afresh. The package records controls for generating, protecting and destroying the implementation's transient ML-KEM keys and secret seeds. Secret values remain outside change records and logs. The ephemeral key pairs are not backed up for session recovery; NIST requires single-use ephemeral KEM key pairs to be destroyed as soon as possible after use (Alagic et al., 2025, §4.2). Recovery instead restores the required ECDSA identity material through the established HSM arrangements and establishes fresh hybrid sessions.

From April to June 2027, qualification tests use the actual release and provider configuration proposed for production. At the agreed peak of five 500-instruction batches per minute, payments reconcile correctly and the 95th-percentile receipt-acknowledgement time is 410 milliseconds, within the 500-millisecond limit. Tests also confirm rejection of unacceptable certificates and standalone X25519 under the target profile.

Further exercises cover provider interruption, loss of HSM access and failover. When both gateway instances become unavailable, a complete rebuild restores the approved connection within 28 minutes, meeting the 30-minute recovery tolerance. Each result identifies its configuration, conditions and limits. Independent assurance challenges reliance on the earlier evaluation build and confirms that the production proposal has evidence for the actual release.

On this basis, the head of technology operations authorises an attended first batch in July and, if its checks pass, a five-working-day pilot covering the identified batches. Wider use requires the outcome and

operations owners to confirm the agreed progression conditions: use of the approved hybrid mechanism, reconciled payments and performance within limits.

An unresolved status discrepancy or prohibited cryptographic selection requires operations to stop submissions and follow the specified recovery response. During coexistence, that response may include controlled recovery to release 1.8. Automatic downgrade within the target profile remains prohibited (section 5.2).

Respond to the payment defect

On 5 July, an interruption between provider acceptance and the gateway's status update exposes a reconnect defect missed by earlier tests. After reconnection, the provider confirms acceptance of all 500 instructions, but release 2.0 incorrectly marks 20 as not submitted. Operations stops further batches and reconciles those instructions using their identifiers, preventing duplicate submission.

Operations follows the authorised procedure to restore release 1.8, coordinating activation of the predecessor profile at both ends. The procedure requires the normal restrictions to be restored when hybrid operation resumes. Operations records the affected traffic and the duration of traditional-only key establishment so that the owners can assess the exposure. Expansion stops, and the supplier reproduces the status-handling defect (section 5.3).

Assess the corrected release and its recovery arrangements

Release 2.0.1 corrects the status-handling defect and passes repeated interruption and reconciliation tests. Testing its new recovery image reveals a separate fault: an automated rebuild reinstates an older connection template that permits standalone X25519. The rebuilt instance remains isolated until the configuration is corrected and verified. This manual work extends recovery to 38 minutes, beyond the 30-minute tolerance.

The successful rebuild test for release 2.0 does not establish recovery performance for release 2.0.1. Release 2.0 also remains unsuitable as a recovery alternative because its payment fault is unresolved.

Before permitting release 2.0.1 in production, the owners assess the available recovery routes. Failover between gateways succeeds under the hybrid profile. For a complete rebuild, supported release 1.8 restores the connection within 24 minutes, including coordinated activation at both ends and verification. The head of technology operations authorises release 2.0.1 with this temporary predecessor recovery arrangement, retaining the same observation and stop conditions.

By August, both gateways operate satisfactorily under the hybrid profile, as shown by observed payment cycles and controlled failover. The delivery lead and supplier remain responsible for correcting the recovery image. At this stage, the correction is unfinished work within the permitted coexistence period, which runs to the agreed 30 September withdrawal date (section 5.4).

Authorise a temporary extension

In September, the supplier confirms that the corrected recovery image will arrive on 5 October, after the withdrawal date. The estate and outcome owners therefore seek a decision before 30 September.

Their assessment explains the remaining dependency. Release 1.8 is the only demonstrated complete-rebuild route that meets both the 30-minute tolerance and the payment-handling requirements. Removing it at the withdrawal date would jeopardise continuity. Retaining it would preserve quantum-related confidentiality exposure for traffic carried if the route were invoked.

The dependency owner substantiates the supplier's delivery commitment and books joint tests. Through the **evidence and feedback rail**, the transition manager presents the delay and additional resource needs to the sponsor, who secures the testing capacity.

After reviewing the exposure, controls and exit plan, the chief risk officer permits departure from the internal withdrawal requirement from 1 to 20 October. The head of technology operations confirms the corresponding temporary operating permission. Both decisions apply only to the identified release 1.8 recovery route, within their respective delegations and under the following conditions.

Condition	Required treatment in this case
Restricted invocation	Keep the image isolated and access controlled. The payments operations manager may invoke it only for the specified recovery need, following the tested procedure with the provider. Automatic downgrade remains prohibited.
Exposure and return	Record each invocation, the affected traffic and its duration. Restore the target profile when the incident permits. Monitoring does not supply quantum-resistant confidentiality.
Credible exit	The delivery lead owns the corrected image and repeat tests. The dependency owner secures supplier and provider participation. The retirement criteria remain unchanged.
Expiry response	Without a further decision, disable the predecessor route at expiry on 20 October. If an incident then prevents hybrid recovery, stop new submissions, preserve and reconcile outstanding instructions, and escalate the service interruption under existing incident arrangements.

The decisions and resource commitments return through the **direction and decisions rail** into the change and operating records. From 1 October, the missed withdrawal is **transition debt**. The exception records permission for that specific departure; the original commitment and the 1 January 2028 protection deadline remain in place. The package remains incomplete even though its normal traffic uses hybrid key establishment.

Verify retirement

On 8 October, tests of the corrected recovery image demonstrate a complete rebuild within 26 minutes, restoration of the approved identity material and establishment of fresh hybrid connections. Repeated payment-interruption tests also pass.

Operations substantiates satisfactory live performance, including peak processing and certificate renewal. The dependency owner confirms that the provider can support normal and recovery operation without standalone X25519. Together, these findings provide the basis for the head of technology operations' separate decision to retire the predecessor route.

By 12 October, technical contributors remove the predecessor configuration and image from active deployment and recovery catalogues. Archived backups remain isolated. A restoration check prevents any instance recovered from those backups from reconnecting until the approved release and profile have been restored and verified.

Tests across primary, standby, rebuild and provider paths confirm successful hybrid operation and rejection of standalone X25519. Combined with observed use, these tests verify actual cryptographic behaviour, consistent with NCSC's migration guidance (NCSC, 2025).

X25519 remains part of the hybrid mechanism, and ECDSA identity keys remain necessary for the separately retained authentication. Verified withdrawal of the predecessor route on 12 October closes the transition debt and exception (section 5.5).

Confirm completion and continuing ownership

With withdrawal verified, the delivery lead reconciles the configuration, inventory, relevant CBOM, dependency, change and decision records. The estate owners substantiate achievement of the target within their respective scopes, and the outcome owner confirms that the specified payment and connection requirements are met.

The operations owners accept the procedures, access, staffing and resources needed for monitoring, certificate management, incident response and recovery. The dependency owner confirms continuing provider support. On the basis of these assessments, the head of technology operations confirms package completion on 15 October, fourteen days after the original 1 October target and within the reserved contingency (section 5.6).

The transition manager reports completion alongside the separate authentication plan delivered by 30 June. That plan sets a bank-approved target of 1 January 2030 based on its own protection requirements, with implementation assigned to the payments connectivity manager. Authentication migration remains open.

Pillar review

The *Implement and retire* review records:

Review question	Case conclusion
What is being reviewed?	The deployed key-establishment package and its required retirement across the defined normal and recovery paths.
What does the evidence establish?	The specified payment and connection requirements are met. Complete rebuilding takes 26 minutes. Verified withdrawal and negative tests establish that standalone X25519 cannot be invoked within the defined scope.
What remains unresolved?	Authentication migration remains separately assigned. Historical confidentiality exposure remains outside the protection achieved.
What action or decision follows?	Record verified withdrawal and closure of the debt and exception on 12 October, and package completion on 15 October. Continue under accepted ownership and controls, retaining the original commitments and actual results in reporting.

7.4 Maintain and adapt

After completing the key-establishment package, the bank continues to check that its protection and recovery arrangements remain effective. A provider change requires renewed evidence, a revised supplier estimate brings authentication work forward, and a controlled exercise tests the bank's ability to make another cryptographic change. These events bring assessment, planning and implementation decisions back under review.

Renew evidence after the provider change

In November 2027, the provider replaces its standby endpoint. Both bank gateways continue to show the approved profile during normal operation, but the earlier provider-failover tests covered the previous endpoint. The payments connectivity manager therefore records the evidence for current provider-failover capability as incomplete. The manager assigns the dependency owner to obtain the new release and configuration records and arrange a joint test within three working days.

After assessing the gap, the estate and operations owners continue normal operation under the enforced profile. They record that provider-failover capability requires verification for the new endpoint. The October completion decision remains supported for the configuration assessed at that time (section 6.1).

The joint test confirms use of the approved profile, correct payment reconciliation and rejection of standalone X25519 during provider failover. The payments connectivity manager links the results to the new endpoint and identifies which earlier results remain applicable. The previous configuration and its supporting evidence remain in the record.

Operations checks negotiated mechanisms, certificates, templates and recovery controls. Selection of a prohibited mechanism triggers the specified stop response. Overdue evidence requests follow the dependency owner's escalation route.

Report the position and improve provider information

The transition manager's weekly report presents four views of the same bank–provider connection, with both gateways and recovery paths identified within scope. The November report draws on dated owner assessments and records both the evidence gap and its resolution (section 6.2).

Reporting view	Case position and implication
Protection achieved	Normal-operation observations and the new provider-failover evidence support the connection's key-establishment claim.
Remaining exposure	ECDSA authentication remains under its separate plan. Any traffic previously captured under vulnerable key establishment retains its confidentiality exposure. The resolved evidence gap is not recorded as a proven cryptographic failure.
Delivery progress	The key-establishment package was completed on 15 October against 1 October planned. Withdrawal and exception closure occurred on 12 October. Authentication implementation remains open. Provider evidence arrived within the three-working-day commitment.
Operating capability	The latest complete bank rebuild took 26 minutes against the permitted 30 minutes. Its date, configuration and applicability after provider maintenance are recorded. A subsequent-change exercise will measure agility.

Review of the evidence gap finds that the provider's maintenance notice named the service but omitted the changed endpoint and the evidence affected by the change. The inventory standards lead revises the common recording method so that notices can be connected to the relevant deployments, versions and supporting evidence.

The dependency owner agrees with the provider what information will be supplied and when. Other estate owners use the shared dependency links to assess their own records. The chief architect approves *Connection transition requirements, version 2*.

The transition manager coordinates implementation and a check of the revised arrangements. The check will establish whether usable information arrives before the next changed endpoint is relied upon (section 6.3).

Reassess the authentication timetable

At the annual review on 1 December 2027, the bank retains its approved threat-planning range and governing 2035 date. Material new evidence remains a trigger for review between annual reviews.

The same review reassesses the separate authentication plan against its established 1 January 2030 target. New supplier evidence increases the estimated remaining qualification and migration work from 18 to 21 months. Adding three months' contingency requires 24 months between the start and the target. The required start therefore advances by three months, from 1 April 2028 to 1 January 2028.

The sponsor secures capacity for the earlier start. The transition manager updates the roadmap, preserving the previous estimate and the reason for revision. This calculation uses the authentication target and the time needed to complete that work; the earlier seven-year confidentiality calculation applies to key establishment.

Prepare the agility exercise

The bank then tests its ability to carry out a further cryptographic change in a controlled replica covering both gateways, their recovery arrangements, the HSM interface and the provider's test endpoint. The exercise instruction is to replace X25519MLKEM768 with **SecP256r1MLKEM768** and verify the resulting state within ten working days.

Both mechanisms are specified in RFC 10024. The change replaces the traditional contribution, X25519, with P-256 while retaining ML-KEM-768 (Kwiatkowski et al., 2026). The requirement is assumed for the exercise; it does not reflect a finding that the production mechanism is insecure (section 6.4).

The payments connectivity manager identifies the affected uses and records. The chief architect approves the exercise profile, while the head of technology operations authorises the bounded test, stopping conditions and permitted recovery. The dependency owner secures the matching provider configuration and test window. Production continues under its existing profile.

The exercise requires the replacement mechanism in use, acceptable payment behaviour, complete rebuilding and withdrawal of the former hybrid group. Standalone X25519 remains prohibited throughout.

Before testing, the provider supplies the endpoint, release and evidence-impact records. Their availability demonstrates the revised information handoff in practice.

Assess the results and use the findings

The exercise takes nine working days. Assessment and decisions occupy the first two days. Provider preparation takes four days, with bank preparation proceeding concurrently. Configuration and joint testing take two further days, followed by one day for complete rebuilding and withdrawal verification. Recorded effort is eight bank person-days and four provider person-days, reported separately from elapsed time.

The workload comprises 100 batches of 500 synthetic instructions, processed at five batches per minute. All 50,000 instructions reconcile correctly. The 95th-percentile receipt-acknowledgement time is 445 milliseconds, below the 500-millisecond limit. Complete rebuilding restores the exercise profile within 27 minutes.

Primary, standby and rebuilt instances use the replacement hybrid group. After the specified withdrawal, attempts to select either the former group or standalone X25519 fail. A deliberately incomplete update leaves the former group enabled in a rebuilt test instance; the configuration check prevents that instance from joining the test connection until corrected. These results verify the exercised change and the relevant enforcement and recovery controls.

The estate and outcome owners conclude that the exercise meets its technical objectives within the required ten working days. The report identifies the tested releases, workload, provider participation and recovery conditions that define the scope of this conclusion. It demonstrates the specified hybrid-group change in that environment. Production deployment, replacement of ML-KEM itself, authentication migration and an unplanned emergency remain unproven.

The exercise assesses both technical enforcement and the coordination needed to deliver the change, consistent with NIST's treatment of policy enforcement and organisational readiness (Barker et al., 2025, §§5.2, 6.5).

The transition manager adds the observed duration, effort and provider lead time to capability reporting and future planning assumptions. The specialist domain owners make the revised method and linked test evidence available for reuse, subject to each estate's assessment of applicability.

Pillar review

The *Maintain and adapt* review records:

Review question	Case conclusion
What is being reviewed?	Continuing connection control, the authentication timetable and the ability to carry out a further hybrid-group change.
What does the evidence establish?	Retesting resolves the provider-failover evidence gap. Timely provision of records demonstrates the revised information handoff. The nine-working-day exercise verifies the specified change, withdrawal and 27-minute rebuilding in the test environment.
What remains unresolved?	Authentication delivery remains open. Production execution of the exercised change, replacement of ML-KEM itself and an unplanned emergency remain untested.
What action or decision follows?	Maintain the production profile and checks. Advance the planned authentication start to 1 January 2028. Use the measured duration, effort and provider lead time in future planning.

Figure 7 summarises the first package's verified changes, the cryptographic functions retained and the continuing work described in this case.

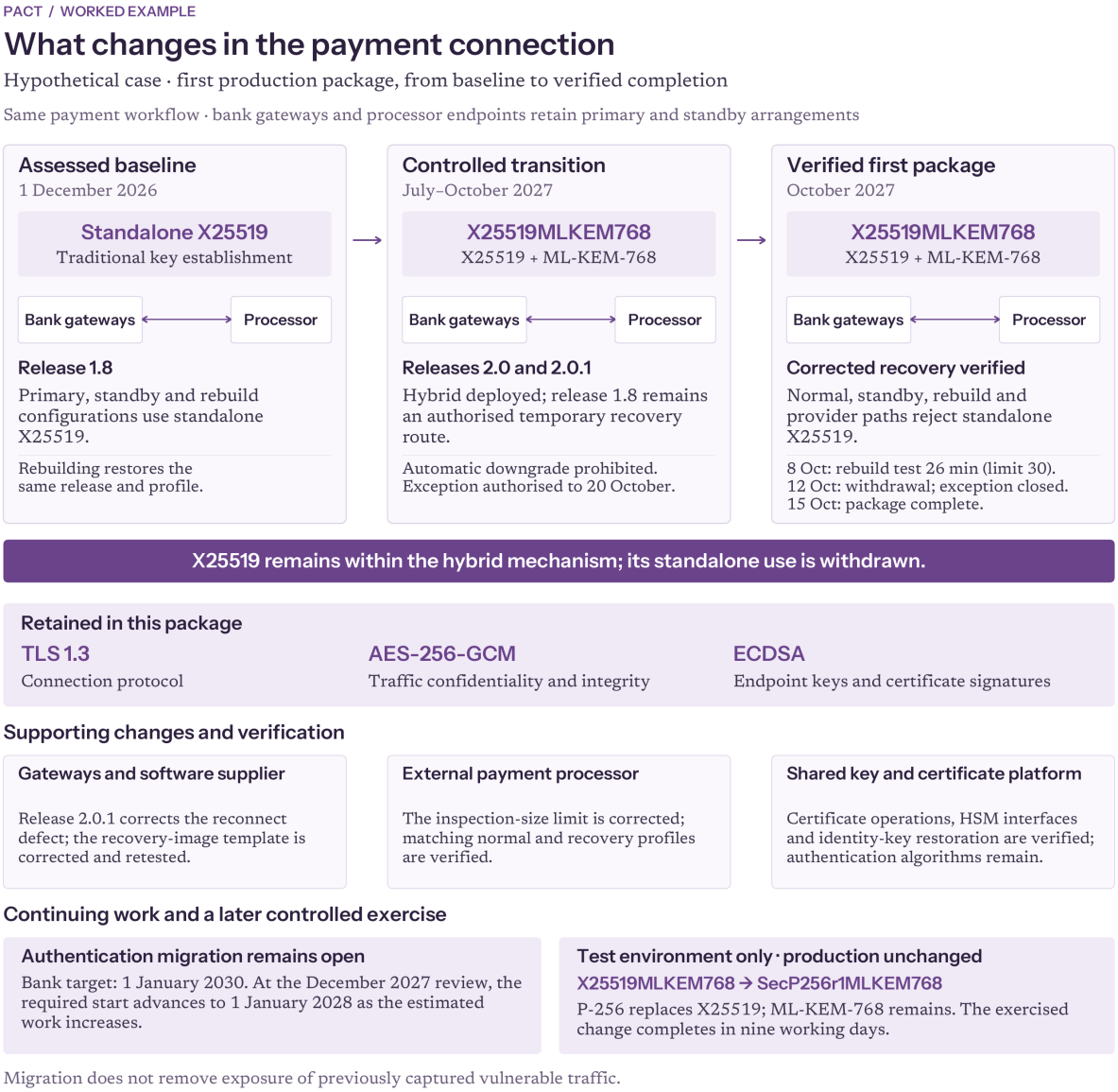

Figure 7 Cryptographic changes and continuing work in the payment-connection example

8 Conclusions and practical implications

What PACT contributes

A bank's PQC transition needs to deliver the required protection while preserving service continuity. PACT provides a common structure for coordinating this work across business, technology and control functions. It connects the services, operations, information and obligations being protected with the cryptographic arrangements they depend on, the people responsible for managing change, and the evidence needed for decisions. This supports oversight of work that progresses at different speeds, while keeping shared dependencies and their consequences for protected outcomes visible.

Progress is assessed through evidence of the protection and operating conditions achieved. A supplier commitment, a successful test and a deployed change support different conclusions, each limited to the scope and conditions it covers. Completion requires evidence that the approved target has been achieved, the earlier arrangements identified for retirement have been withdrawn, and continuing owners have accepted their responsibilities with the necessary resources confirmed. Management can then distinguish protection achieved from remaining exposure, unfinished work and capability still to be demonstrated. These distinctions inform decisions about further resources, changes to the approach, temporary departures from the target and whether completion can be confirmed.

Adopting and tailoring the framework

The starting point for adoption depends on the bank's existing programme and knowledge of its cryptography. An established transition programme can use PACT to examine whether responsibilities, evidence and decisions connect across its current work, addressing gaps through existing plans and records. A bank with limited visibility can begin with a material protected outcome and trace the cryptographic estates and dependencies that support it. This can reveal gaps in ownership, discovery capability, supplier evidence or recovery arrangements while advancing useful transition work.

Starting with a limited scope still requires a clear view of the wider programme. Areas not yet examined remain visible as coverage gaps, and shared dependencies identified locally inform the integrated roadmap. Useful work in one estate can therefore proceed without waiting for discovery across the whole bank to be complete.

Roles and governance can be adapted to the bank's operating model, complexity and exposure, consistent with the Basel Committee's emphasis on existing governance and proportionate implementation (BCBS, 2021a, paras. 9–13 and Principle 1). One person may own both an estate and a change package where authority, capacity and required independence permit. A more distributed bank may need separate owners and several executive sponsors, with clear remits and a route for resolving matters that cross those boundaries. In either arrangement, accountability remains identifiable, decisions follow explicit delegations, and necessary independent challenge is preserved. Assigning titles or separating functions does not, by itself, demonstrate that the responsibilities are being carried out.

Existing inventory, architecture, risk, change and operating records can connect requirements and decisions with evidence of the resulting changes. Their identifiers, scope and status need to be sufficiently consistent to support those links reliably. Reviews can address several pillars together, and evidence can be reused where its applicability has been established. The depth of testing and review depends on the consequences of error, the uncertainty involved and the dependencies affected. A limited change to a familiar configuration may draw on relevant existing evidence; a change to a shared platform supporting several critical operations requires assessment across those operations, including their recovery arrangements. The purpose of tailoring is to reduce duplication while preserving the basis and limits of decisions.

An institution beginning its programme may start by developing ownership and an initial evidence base, targeted investigation and enabling work, and validation of candidates for delivery. These activities overlap and should be revised as findings improve. Useful work can proceed under sufficient existing authority while wider arrangements develop. Expected outputs include usable source and inventory records, owned dependencies, tested approaches and credible next actions.

Working with group and external dependencies

The bank's ability to direct the work may be limited where a head office, supplier or counterparty controls the relevant product, release schedule or technical activity. The bank remains responsible for establishing its requirements, obtaining usable evidence, assessing the consequences and securing the necessary response or escalating unresolved matters. For third-party service relationships, accountability to customers and authorities remains with the financial institution and its board and senior management (Financial Stability Board, 2023, p. 12).

Group or shared assessments can support local decisions where their conditions apply. Differences in deployment, obligations or recovery arrangements still require examination. PACT can make an infeasible dependency or timetable visible, but assigning an owner cannot create a compatible product, additional supplier capacity or an acceptable alternative.

Limitations and further evaluation

PACT is a proposed framework for managing transition and making decisions, informed by industry guidance and academic research. It does not itself constitute a regulatory requirement or establish cryptographic security or regulatory compliance. Algorithm and implementation choices still require applicable standards, technical assessment and evidence from the relevant environment. Inventories may be incomplete, observations may become outdated, and tests demonstrate behaviour only under the conditions examined. Estimates of quantum-threat timing and future delivery remain assumptions that require reassessment. Records and approvals cannot guarantee protection. Material uncertainty therefore remains explicit, together with its implications for what may proceed, the safeguards required and the evidence still needed.

The framework's effectiveness, implementation cost and scalability across banks have yet to be established empirically. The hypothetical case in section 7 illustrates its intended application; its results are not benchmarks for other institutions. Evaluation through use can examine whether PACT helps banks resolve gaps in responsibility, make timely decisions and substantiate operating results at a proportionate cost. That evaluation also needs to consider whether these benefits can be sustained after the initial migration.

Indeed, evaluation can examine whether staged investigation yields usable candidates, whether enabling and supplier constraints are identified early enough to affect decisions, and whether initial implementations improve subsequent effort estimates and repeatability. It can also examine these effects alongside protection, decision timeliness and the cost of collecting and maintaining evidence.

The lasting objective is to retain the knowledge, ownership and tested capacity to maintain protection and carry out further cryptographic change. This continuing capability extends beyond the first PQC migration, consistent with NIST's treatment of cryptographic agility as an organisational and technical capability that must be maintained over time (Barker et al., 2025).

References

Agarwal, R., & Tiwana, A. (2015). Editorial—Evolvable systems: Through the looking glass of IS. *Information Systems Research, 26*(3), 473–479. https://doi.org/10.1287/isre.2015.0595

Alagic, G., Barker, E., Chen, L., Moody, D., Robinson, A., Silberg, H., & Waller, N. (2025). *Recommendations for key-encapsulation mechanisms* (NIST Special Publication 800-227). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-227

Auer, R., Dodson, D., Dupont, A., Haghighi, M., Margaine, N., Marsden, D., McCarthy, S., & Valko, A. (2025). *Quantum-readiness for the financial system: A roadmap* (BIS Papers No. 158). Bank for International Settlements. https://www.bis.org/publications/paper-158-quantum-readiness-financial-system-roadmap

Bank for International Settlements Innovation Hub, Bank of Italy, Banque de France, Deutsche Bundesbank, Nexi-Colt, & Swift. (2025). *Project Leap Phase 2: Quantum-proofing payment systems*. Bank for International Settlements. https://www.bis.org/publ/othp107.htm

Barker, E. (2020). *Recommendation for key management: Part 1 – General* (NIST Special Publication 800-57 Part 1, Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M., Newhouse, B., Housley, R., Turner, S., Barker, W., & Kent, K. (2025). *Considerations for achieving crypto agility: Strategies and practices* (NIST Cybersecurity White Paper 39-upd1; includes updates as of 29 June 2026). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.39-upd1

Basel Committee on Banking Supervision. (2021a). *Principles for operational resilience*. Bank for International Settlements. https://www.bis.org/publications/202103-guidelines-principles-operational-resilience.pdf

Basel Committee on Banking Supervision. (2021b). *Revisions to the Principles for the Sound Management of Operational Risk*. Bank for International Settlements. https://www.bis.org/publications/202103-guidelines-revisions-principles-sound-management-operational-risk.pdf

Basel Committee on Banking Supervision. (2025, December 10). *Principles for the sound management of third-party risk*. Bank for International Settlements. https://www.bis.org/publications/202512-guidelines-principles-sound-management-third-party-risk.pdf

Bashiri, K., Fluhrer, S., Gazdag, S., Van Geest, D., & Kousidis, S. (2025, December). *Internet X.509 Public Key Infrastructure: Algorithm identifiers for the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)* (RFC 9909). RFC Editor. https://www.rfc-editor.org/rfc/rfc9909

Bhambhwani, S. M., & Huang, A. H. (2024). Auditing decentralized finance. *The British Accounting Review, 56*(2), 101270. https://doi.org/10.1016/j.bar.2023.101270

Bouraffa, T., & Hui, K.-L. (2025). Regulating information and network security: Review and challenges. *ACM Computing Surveys, 57*(5), Article 126, 1–38. https://doi.org/10.1145/3711124

Brandão, L. T. A. N., & Peralta, R. (2026, January 20). *NIST first call for multi-party threshold schemes* (NIST IR 8214C). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8214C

Canadian Centre for Cyber Security. (2025). *Roadmap for the migration to post-quantum cryptography for the Government of Canada* (ITSM.40.001). https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (RFC 5280). RFC Editor. https://www.rfc-editor.org/rfc/rfc5280

Cooper, D. A., Apon, D. C., Dang, Q. H., Davidson, M. S., Dworkin, M. J., & Miller, C. A. (2020). *Recommendation for stateful hash-based signature schemes* (NIST Special Publication 800-208). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-208

Cross Market Operational Resilience Group, Cyber Coordination Group. (2025). *Guidance for post-quantum cryptography* (Version 1.0, April 2025). https://www.cmorg.org.uk/artefact/guidance-post-quantum-cryptography

Cybersecurity and Infrastructure Security Agency. (2024). *Post-quantum considerations for operational technology*. https://www.cisa.gov/sites/default/files/2024-10/Post-Quantum%20Considerations%20for%20Operational%20Technology%20%28508%29.pdf

Dang, Q., Moody, D., Regenscheid, A., & Silberg, H. (2026, April 17). *Recommendation for cryptographic key generation* (NIST Special Publication 800-133 Revision 3, Initial Public Draft). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-133r3.ipd

Driscoll, F., Parsons, M., & Hale, B. (2025). *Terminology for post-quantum traditional hybrid schemes* (RFC 9794). RFC Editor. https://www.rfc-editor.org/rfc/rfc9794

Edwards, M. R., Parker, S. L., Okimoto, T., Anseel, F., & Álvarez, B. (2026). Balancing paradoxical outcomes of metricized employee performance systems (MEPS): avoiding de-prioritization of important (non-metricized) job tasks. *The International Journal of Human Resource Management, 37*(10), 1839–1869. https://doi.org/10.1080/09585192.2026.2711061

EMVCo. (2026, August 24). *Security position statement: Update on quantum computing and EMV chip cryptography*. https://www.emvco.com/resources/security-position-statement-update-on-quantum-computing-and-emv-chip-cryptography-2/

European Telecommunications Standards Institute. (2020). *CYBER; Migration strategies and recommendations to Quantum Safe schemes* (ETSI TR 103 619 V1.1.1). https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

European Telecommunications Standards Institute. (2024). *CYBER; Quantum-Safe Cryptography (QSC); A repeatable framework for quantum-safe migrations* (ETSI TR 104 016 V1.1.1). https://www.etsi.org/deliver/etsi_tr/104000_104099/104016/01.01.01_60/tr_104016v010101p.pdf

Europol. (2026). *Prioritising post-quantum cryptography migration activities in financial services*. Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/Post-quantum-cryptography-report.pdf

Fauver, L., Hung, M., Li, X., & Taboada, A. G. (2017). Board reforms and firm value: Worldwide evidence. *Journal of Financial Economics, 125*(1), 120–142. https://doi.org/10.1016/j.jfineco.2017.04.010

Financial Stability Board. (2023). *Enhancing third-party risk management and oversight: A toolkit for financial institutions and financial authorities*. https://www.fsb.org/wp-content/uploads/P041223-1.pdf

FS-ISAC Post-Quantum Cryptography Working Group. (2023a). *Post-Quantum Cryptography (PQC) Working Group current state (crypto agility) technical paper*. Financial Services Information Sharing and Analysis Center. https://www.fsisac.com/hubfs/Knowledge/PQC/CurrentState.pdf

FS-ISAC Post-Quantum Cryptography Working Group. (2023b). *Post-Quantum Cryptography (PQC) Working Group future state technical paper*. Financial Services Information Sharing and Analysis Center. https://www.fsisac.com/hubfs/Knowledge/PQC/FutureState.pdf

FS-ISAC Post-Quantum Cryptography Working Group. (2023c). *Post-Quantum Cryptography (PQC) Working Group infrastructure inventory technical paper*. Financial Services Information Sharing and Analysis Center. https://www.fsisac.com/hubfs/Knowledge/PQC/InfrastructureInventory.pdf

FS-ISAC Post-Quantum Cryptography Working Group. (2024). *Building cryptographic agility in the financial sector: Effective, efficient change in a post quantum world*. Financial Services Information Sharing and Analysis Center. https://www.fsisac.com/hubfs/knowledge/PQC/BuildingCryptographicAgilityInTheFinancialSector.pdf

Furneaux, B., & Wade, M. (2011). An exploration of organizational level information systems discontinuance intentions. *MIS Quarterly, 35*(3), 573–598. https://doi.org/10.2307/23042797

G7 Cyber Expert Group. (2026, January). *G7 Cyber Expert Group statement on advancing a coordinated roadmap for the transition to post-quantum cryptography in the financial sector*. https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf

Gidney, C. (2025). *How to factor 2048 bit RSA integers with less than a million noisy qubits* (arXiv:2505.15917). arXiv. https://doi.org/10.48550/arXiv.2505.15917

Gondrom, T., Brandner, R., & Pordesch, U. (2007). *Evidence Record Syntax (ERS)* (RFC 4998). RFC Editor. https://www.rfc-editor.org/rfc/rfc4998

Hess, B. (2026). The anatomy of cryptography bills of materials: Standardization and practice in CycloneDX. In D. Loebenberger & M. Stöttinger (Eds.), *Migration and agility in cryptographic systems* (CCIS 3002, pp. 1–19). Springer. https://doi.org/10.1007/978-3-032-28946-9_1

Hong Kong Monetary Authority. (2003). *General principles for technology risk management* (Supervisory Policy Manual TM-G-1, Version 1, 24 June 2003). https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20030624-2-EN/TM-G-1.pdf

Hong Kong Monetary Authority. (2026a). *Quantum preparedness of Hong Kong's banking sector*. https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2026/20260727e3a1.pdf

Hong Kong Monetary Authority. (2026b, July 27). *HKMA launches quantum preparedness whitepaper and index to support banking sector's readiness for quantum era*. Government of the Hong Kong Special Administrative Region. https://www.info.gov.hk/gia/general/202607/27/P2026072700527.htm

Hong Kong Monetary Authority. (2026c, July 27). *Results of Quantum Preparedness Index Survey* (Circular B1/15C). https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20260727-1-EN/20260727-1-EN.pdf

Huang, A. H., Lehavy, R., Zang, A. Y., & Zheng, R. (2018). Analyst information discovery and interpretation roles: A topic modeling approach. *Management Science, 64*(6), 2833–2855. https://doi.org/10.1287/mnsc.2017.2751

Huang, A. H., Lin, A. P., & Zang, A. Y. (2022). Cross-industry information sharing among colleagues and analyst research. *Journal of Accounting and Economics, 74*(1), 101496. https://doi.org/10.1016/j.jacceco.2022.101496

Hui, K.-L., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems, 29*(3), 117–156. https://doi.org/10.2753/MIS0742-1222290304

Hui, K.-L., Ke, P. F., Yao, Y., & Yue, W. T. (2019). Bilateral liability-based contracts in information security outsourcing. *Information Systems Research, 30*(2), 411–429. https://doi.org/10.1287/isre.2018.0806

Hui, K.-L., Kim, S. H., & Wang, Q.-H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *MIS Quarterly, 41*(2), 497–523. https://doi.org/10.25300/MISQ/2017/41.2.08

Ke, P. F., Hui, K.-L., & Yue, W. T. (2013). Information security as a credence good. In A. A. Adams, M. Brenner, & M. Smith (Eds.), *Financial cryptography and data security: FC 2013 workshops* (Lecture Notes in Computer Science, Vol. 7862, pp. 83–93). Springer. https://doi.org/10.1007/978-3-642-41320-9_6

Kwiatkowski, K., Kampanakis, P., Westerbaan, B. E., & Stebila, D. (2026, August). *Post-quantum traditional (PQ/T) hybrid key agreement mechanisms for TLS 1.3* (RFC 10024). RFC Editor. https://www.rfc-editor.org/info/rfc10024/

Maruping, L. M., Venkatesh, V., Thong, J. Y. L., & Zhang, X. (2019). A risk mitigation framework for information technology projects: A cultural contingency perspective. *Journal of Management Information Systems, 36*(1), 120–157. https://doi.org/10.1080/07421222.2018.1550555

Massimo, J., Kampanakis, P., Turner, S., & Westerbaan, B. E. (2025, October). *Internet X.509 Public Key Infrastructure: Algorithm identifiers for the Module-Lattice-Based Digital Signature Algorithm (ML-DSA)* (RFC 9881). RFC Editor. https://www.rfc-editor.org/rfc/rfc9881

Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2026). *Transition to post-quantum cryptography standards* (NIST IR 8547). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8547

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy, 16*(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Mosca, M., & Piani, M. (2026, March 9). *Quantum threat timeline report 2025*. Global Risk Institute. https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

National Cyber Security Centre. (2025, March 20). *Timelines for migration to post-quantum cryptography*. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

National Institute of Standards and Technology. (2024a). *Module-lattice-based key-encapsulation mechanism standard* (FIPS 203). https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology. (2024b). *Module-lattice-based digital signature standard* (FIPS 204). https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024c). *Stateless hash-based digital signature standard* (FIPS 205). https://doi.org/10.6028/NIST.FIPS.205

National Institute of Standards and Technology. (2026). *Post-quantum cryptography: FAQs* (updated 5 August 2026). Retrieved 22 October 2026, from https://csrc.nist.gov/projects/post-quantum-cryptography/faqs

National Institute of Standards and Technology. (n.d.-a). *Cryptographic Module Validation Program*. Retrieved 22 October 2026, from https://csrc.nist.gov/projects/cryptographic-module-validation-program

National Institute of Standards and Technology. (n.d.-b). *Hash functions*. Retrieved 22 October 2026, from https://csrc.nist.gov/projects/hash-functions

National Institute of Standards and Technology. (n.d.-c). *Post-quantum cryptography*. Retrieved 22 October 2026, from https://csrc.nist.gov/projects/post-quantum-cryptography

Newhouse, W., Souppaya, M., Barker, W., Brown, C., Kampanakis, P., Manzano, M., McGrew, D., Dames, A., Soukharev, V., Lafrance, P., Hu, A., Hook, D., Garcia, R., Gervis, E., Kim, E., & Lee, C. (2023). *Migration to post-quantum cryptography: Quantum readiness—Cryptographic discovery. Volume B: Approach, architecture, and security characteristics of public key application discovery tools* (NIST SP 1800-38B, preliminary draft). National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

Ounsworth, M., Gray, J., Pala, M., Klaußner, J., & Fluhrer, S. (2026, April 21). *Composite Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for use in X.509 Public Key Infrastructure* (Internet-Draft draft-ietf-lamps-pq-composite-sigs-19). Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/19/

Perlner, R. (2025, September 25). *FIPS 206: FN-DSA (Falcon)* [Conference presentation]. Sixth PQC Standardization Conference, National Institute of Standards and Technology. https://csrc.nist.gov/presentations/2025/fips-206-fn-dsa-falcon

Rescorla, E. (2026, July). *The Transport Layer Security (TLS) protocol version 1.3* (RFC 9846). RFC Editor. https://doi.org/10.17487/RFC9846

Rezazade Mehrizi, M. H., Rodón Mòdol, J., & Zafar Nezhad, M. (2019). Intensifying to cease: Unpacking the process of information systems discontinuance. *MIS Quarterly, 43*(1), 141–165. https://doi.org/10.25300/MISQ/2019/13717

Rinta-Kahila, T., Penttinen, E., & Lyytinen, K. (2023). Getting trapped in technical debt: Sociotechnical analysis of a legacy system's replacement. *MIS Quarterly, 47*(1), 1–32. https://doi.org/10.25300/MISQ/2022/16711

Schroeder, K., Trinh, H., & Pillitteri, V. Y. (2024). *Measurement guide for information security: Volume 1—Identifying and selecting measures* (NIST Special Publication 800-55 Vol. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-55v1

State Cryptography Administration. (2020, March 4). *Cryptography policy questions and answers (58)* [In Chinese]. https://www.nca.gov.cn/sca/xxgk/2020-03/04/content_1060664.shtml

Stebila, D., Fluhrer, S., & Gueron, S. (2026, July). *Hybrid key exchange in TLS 1.3* (RFC 9954). RFC Editor. https://www.rfc-editor.org/info/rfc9954/

Tiwana, A., & Safadi, H. (2024). Atrophy in aging systems: Evidence, dynamics, and antidote. *Information Systems Research, 35*(1), 66–86. https://doi.org/10.1287/isre.2023.1218

Tsai, J. C.-A., Jiang, J. J., Klein, G., & Hung, S.-Y. (2023). Task conflict resolution in designing legacy replacement systems. *Journal of Management Information Systems, 40*(3), 1009–1034. https://doi.org/10.1080/07421222.2023.2229120

Turner, S., Kampanakis, P., Massimo, J., & Westerbaan, B. E. (2026, March). *Internet X.509 Public Key Infrastructure: Algorithm identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)* (RFC 9935). RFC Editor. https://www.rfc-editor.org/rfc/rfc9935

Ward, M. (2025, June 3). *Quantum computing and EMV® chip: What's the threat?* EMVCo. https://www.emvco.com/news-publications/quantum-computing-and-emv-chip-whats-the-threat/

Yang, P. (2021, March). *ShangMi (SM) cipher suites for TLS 1.3* (RFC 8998). RFC Editor. https://www.rfc-editor.org/rfc/rfc8998

Zhang, X. (2017). Knowledge management system use and job performance: A multilevel contingency model. *MIS Quarterly, 41*(3), 811–840. https://doi.org/10.25300/MISQ/2017/41.3.07

Zhou, J., Hui, K.-L., & Kwon, O. (2026). Incentivizing crowds and intergroup spillovers: Evidence from the Internet Bug Bounty program. *Management Science*. Advance online publication. https://doi.org/10.1287/mnsc.2024.04544

Appendix A Glossary and abbreviations

This glossary defines PACT terms and lists abbreviations and algorithm names. Section references lead to fuller explanations and sources. Sections 3.1 and 3.3 define the roles, and a single person may hold several of them.

A.1 Terms and definitions

Term	Meaning in this manual	Section
Change package	A bounded set of work under an accountable plan, including testing, implementation, recovery arrangements and required retirement.	2.2
Cryptographic agility	The capability to organise and complete subsequent cryptographic change within the required protection, service and timing conditions.	6.4
Cryptographic estate	A bounded set of cryptographic uses and supporting elements managed together under defined accountability. Its scope includes relevant recovery, fallback and inactive capabilities.	2.2
Cryptographic inventory	The maintained account linking cryptographic uses and deployments to protected outcomes, ownership and supporting evidence.	4.1
Cryptographic use	A specific application of cryptography for a security purpose in an identifiable operating context.	2.2
Exception	An authorised departure from an identified requirement or operating condition, bounded by scope, duration and conditions.	5.4
Fallback	Use of an alternative mechanism or path without necessarily reversing deployment.	5.3
Information rails	The two continuing flows of information across the pillars, operating levels and external relationships. The direction and decisions rail carries requirements and authorised choices. The evidence and feedback rail carries findings that support those choices or indicate a need to reconsider them.	2.5
Integrated transition roadmap	The institutional plan connecting protection priorities, estate plans, dependencies, resources and dates, with agreed sequencing and unresolved commitments distinguished.	4.7
Interface profile	The mechanisms, settings and operating rules that connected systems need to use compatibly.	4.6
Mandate	The statement establishing what the bank intends to protect, where the transition applies and the results it seeks.	3.2
Migration duration	The elapsed time needed to complete the remaining work for the assessed protection target, accounting for dependencies, available capacity and activities that can proceed concurrently.	4.3
Protected outcome	The result that cryptography needs to support, concerning a business service, critical operation, protected information or another defined obligation.	2.2
Protection or trust period	The period for which confidentiality, authenticity or integrity needs to remain effective, including later reliance on retained records.	4.3

Term	Meaning in this manual	Section
Quantum-threat planning assumption	The evidenced planning basis for when a quantum computer could defeat the relevant cryptography, including the approved credible range and the selected date governing the assessment. It is not a prediction.	4.3
Required start	The latest credible start that meets applicable completion deadlines and any binding start deadlines under stated assumptions, allowing for remaining migration duration and contingency.	4.3
Retirement	The condition in which an arrangement can no longer be selected, negotiated or invoked for a specified use within the defined scope.	5.5
Sensitivity end date	The date at which disclosure of specified information would cease to cause harm; it is distinct from the date on which retention ends.	4.3
Transition debt	A gap carried beyond an agreed date or event, or outside approved transition conditions. Examples include overdue withdrawal, deferred recovery migration or evidence not provided when required.	5.4

A.2 Abbreviations and algorithm names

The table lists abbreviations and selected algorithm names used in the report. Numbers in algorithm names do not always denote key length or security strength. For example, the 256 in AES-256-GCM is a key length in bits, whereas the 768 in ML-KEM-768 identifies a parameter set.

Abbreviation or name	Meaning
AES	Advanced Encryption Standard
AES-256-GCM	AES with a 256-bit key, used in Galois/Counter Mode to provide encryption and integrity protection
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CBOM	Cryptographic bill of materials
CISA	Cybersecurity and Infrastructure Security Agency (United States)
DH	Diffie–Hellman
ECDH	Elliptic-curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
FS-ISAC	Financial Services Information Sharing and Analysis Center
HKMA	Hong Kong Monetary Authority
HSM	Hardware security module
KEM	Key-encapsulation mechanism
ML-DSA	Module-Lattice-Based Digital Signature Algorithm

Abbreviation or name	Meaning
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism
NCSC	National Cyber Security Centre (United Kingdom)
NIST	National Institute of Standards and Technology (United States)
P-256	An elliptic curve, also named secp256r1, used for traditional public-key cryptography
PACT	PQC Accountability and Controlled Transition
PKI	Public-key infrastructure
PQC	Post-quantum cryptography
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman
SecP256r1MLKEM768	A TLS hybrid key-establishment group combining elliptic-curve Diffie–Hellman using P-256 with ML-KEM-768
SHA-2	Secure Hash Algorithm 2
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SM2	A set of elliptic-curve public-key algorithms specified in Chinese standards
SM3	A cryptographic hash function specified in Chinese standards
SM4	A symmetric encryption algorithm specified in Chinese standards
TLS	Transport Layer Security
X25519	An elliptic-curve Diffie–Hellman mechanism for establishing a shared secret
X25519MLKEM768	A TLS hybrid key-establishment group combining X25519 with ML-KEM-768

Appendix B Technical primer on post-quantum cryptography

This primer explains cryptographic mechanisms and their implications for compatibility, key management, performance and protection. Designs should be assessed against each service's needs, dependencies and applicable requirements. Standards status was checked on 22 October 2026.

A bank uses cryptography across nine banking-use classes, grouped here for scoping purposes and described in Table B4 (section B.5). These classes are payment connections, public channels, cards and ATMs, identity services and stored information. They also include external and cloud connections, software supply chains, hardware roots of trust, and constrained systems. A single service may span several classes and share components with other services.

B.1 Cryptographic functions and quantum exposure

Banking services combine public-key mechanisms for establishing secrets or authenticating parties with symmetric mechanisms for protecting data. The bank should identify each function and the information or trust that depends on it. Table B1 summarises five common functions and the quantum exposure of each.

Table B1 Cryptographic functions and protection

Function	What it does	Quantum exposure to examine
Key establishment	Creates a shared secret from which working keys can be derived. Examples include ECDH and ML-KEM.	RSA, DH and ECDH rely on problems that sufficiently capable quantum computers could solve. An attacker who captures an exchange may later recover the working keys derived from it.
Symmetric encryption	Conceals application data or stored information using a secret key. AES is a common example.	Assess key length, mode and key management, including any vulnerable public-key mechanism protecting or distributing the key.
Digital signature	Links a message to a signing key and enables public verification of origin and integrity.	Vulnerable RSA or ECDSA signing keys enable forgery. Consider active identities, software acceptance and later reliance on signed records.
Message authentication code	Uses a shared secret to detect changes and authenticate a message among key holders.	Assess the algorithm, tag length and key establishment. Every holder of the shared key has the ability to generate a valid tag.
Cryptographic hash	Produces a digest used in integrity checks, signatures and key derivation.	Assess the hash property required by its use and the digest length, alongside the security of the surrounding construction.

Sources: Barker (2020) and Moody et al. (2026). The table assesses each function on its own, and the complete service needs its own security assessment.

A key-encapsulation mechanism establishes a secret in three steps. First, the receiving party generates a public encapsulation key and a private decapsulation key. Second, the sending party uses the public key and fresh randomness to produce a shared secret and a KEM ciphertext, and sends the ciphertext. Third, the receiving party uses its private key and that ciphertext to recover the shared secret. The KEM ciphertext carries only information for establishing the secret, while application data is encrypted separately (NIST, 2024a).

The surrounding protocol binds this exchange to the intended participants and derives working keys for specific purposes. In TLS, the handshake combines key establishment with authentication, and the record layer protects application data using authenticated encryption, which provides confidentiality and

integrity together. A change to key establishment should therefore be checked alongside certificate authentication, key derivation and record protection (Rescorla, 2026).

The separation between key establishment and data encryption explains harvest-now-decrypt-later exposure. An attacker can retain encrypted traffic together with its public key-establishment messages. A future attack on the vulnerable key-establishment mechanism may recover the secret needed to decrypt that traffic, even when the symmetric cipher remains secure. Migrating key establishment protects new exchanges, but previously captured traffic retains the exposure of the mechanism used when it was sent (Moody et al., 2026).

Hash functions have three relevant properties. Preimage resistance makes it difficult to find an input matching a given digest. Second-preimage resistance makes it difficult to find a different input with the same digest as a given message. Collision resistance makes it difficult to find any two different inputs with the same digest. Signature schemes commonly depend on collision resistance, while other uses may depend on different properties. A digest provides useful integrity evidence when its reference value is authenticated or otherwise trusted (NIST, n.d.-b).

A sufficiently capable quantum computer running Shor's algorithm could solve the factoring and discrete-logarithm problems behind traditional public-key mechanisms. Such an attack would allow future forgery and the decryption of previously captured information. Symmetric encryption and hashes require a separate assessment. Grover's algorithm offers a theoretical speed-up for exhaustive search, but practical costs and limits on parallelisation reduce its effect. NIST continues to permit AES with 128-, 192- and 256-bit keys under its existing guidance. The required security margin should be assessed for the intended use and protection period (Moody et al., 2026; NIST, 2026). Regarding hash digests, current practice typically uses SHA-256, which provides 128 bits of classical security strength where a use depends on collision resistance, as digital signatures do. NIST accepts 128 bits for applying protection both through 2030 and beyond, so SHA-256 remains acceptable after 2030, whereas, for uses that depend on collision resistance, hash functions providing only 112 bits, such as SHA-224, do not (Barker, 2020; NIST, n.d.-b). Quantum considerations do not currently alter this guidance. The SHA-2 and SHA-3 families remain approved, and NIST has issued no quantum-driven transition requirement for hash functions (Moody et al., 2026; NIST, 2026).

Published estimates of when such a computer may exist vary and serve as evidence for the bank's planning assumption rather than as predictions. In a survey conducted in 2025 and published in March 2026, 26 experts assessed the likelihood of a quantum computer able to factor RSA-2048 within 24 hours as quite possible (28–49%) within the survey's ten-year horizon and likely (51–70%) within fifteen years (Mosca and Piani, 2026). Resource estimates have also fallen. One analysis estimates that a 2048-bit RSA modulus could be factored in under a week with fewer than one million noisy qubits, under stated hardware assumptions (Gidney, 2025). Sections 4.3 and 6.3 explain how the bank approves and reviews its planning range.

B.2 Keys, certificates and trust

Key management covers generation, authorised use, protection, replacement and destruction, with backup and recovery where the key's purpose requires them. Generation needs suitable randomness and the checks specified for the mechanism. Private and secret keys require controlled storage and access. Public keys require authentic association with the intended party. Key recovery for a retained decryption key can preserve access to an archive, while promptly destroying an ephemeral session key limits later exposure. The key-recovery policy should follow the key's function and required lifetime (Barker, 2020).

Some implementations store a seed from which a key pair can be regenerated. For ML-KEM, the two 32-byte key-generation inputs together provide a 64-byte seed representation. ML-DSA can regenerate its key pair from a 32-byte seed. These representations differ from the full encoded private keys compared in Table B2. Anyone holding the seed can regenerate the key pair, so the seed needs the same protection as the private key (NIST, 2024a, 2024b).

Seed handling should cover generation, access, transfer, recovery and disposal, including copies in backups. Where seeds are derived from other secrets, the derivation method and separation between purposes also matter. NIST SP 800-133 Revision 3, an Initial Public Draft dated 17 April 2026, addresses seed handling and derivation. The draft remained current on 22 October 2026 (Dang et al., 2026).

A certificate contains a subject public key and an issuer's signature over the certificate information. The subject key and the issuer signature are separate cryptographic choices, so replacing the subject key still leaves the issuer-signature algorithm to assess. Certificate validation checks the chain of issuers, permitted uses, validity and relevant status information against a locally trusted starting point. A trust anchor supplies that starting point, and a trust store holds the anchors or other trust material accepted by a system (Cooper et al., 2008).

Consequently, a certificate migration may require coordinated changes to issuing authorities, enrolment services, certificate formats, status services and relying applications. The bank should establish which relying applications can process each algorithm and chain, how new trust material reaches them, and how renewal and revocation behave during coexistence. Long-lived signed records may additionally need evidence preserving the validity of earlier signatures, such as archival timestamp renewal before the existing protection becomes unreliable (Gondrom et al., 2007; Cooper et al., 2008).

Certificate profiles for the new algorithms are now largely standardised. RFC 9881 (October 2025), RFC 9909 (December 2025) and RFC 9935 (March 2026) specify how ML-DSA, SLH-DSA and ML-KEM public keys are identified in X.509 certificates (Massimo et al., 2025; Bashiri et al., 2025; Turner et al., 2026). As of 22 October 2026, the specification for composite certificates pairing ML-DSA with a traditional algorithm awaited publication as an RFC (Ounsworth et al., 2026). Issuing authorities, HSMs and relying applications each need to support the chosen profile.

A hardware security module (HSM) protects keys and performs cryptographic operations within a defined boundary. Its suitability depends on the supported algorithm and parameter set, firmware, interfaces, operating mode and relevant validation scope. Assessment should include generation, import where permitted, backup, failover and destruction. The applicable module certificate and security policy establish the validated configuration, while deployed settings and surrounding controls establish how the service uses it (NIST, n.d.-a).

Stateful hash-based signature schemes include the Leighton–Micali Signature system with its Hierarchical Signature System variant (LMS/HSS) and the eXtended Merkle Signature Scheme with its multi-tree variant (XMSS/XMSSMT). These schemes require an additional control that prevents reuse of any one-time signing key. The signer maintains a persistent index of consumed keys. Under NIST SP 800-208, the signer advances and durably stores that index before releasing a signature or accepting another signing request. Crash recovery and concurrent signing need to preserve that progress. Restoring an earlier state or cloning a signer can cause key reuse, so recovery has to follow the scheme's state-preserving design (Cooper et al., 2020).

SP 800-208 also requires conforming key generation and signing to take place in hardware cryptographic modules that meet specified conditions, including preventing the export of private keys. Capacity planning should allow replacement before the available signing keys are exhausted. These controls are specific to stateful schemes. Stateless SLH-DSA avoids a persistent record of consumed one-time keys. Like other PQC signature schemes, it still requires private-key protection and correct implementation (Cooper et al., 2020; NIST, 2024c).

B.3 PQC standards, parameters and system effects

NIST finalised ML-KEM in FIPS 203 and ML-DSA in FIPS 204 on 13 August 2024. Both use structured lattices: ML-KEM establishes shared secrets, while ML-DSA creates signatures (NIST, 2024a, 2024b). SLH-DSA, standardised on the same date in FIPS 205, provides stateless hash-based signatures. Stateful hash-based signatures have their own approved parameter sets and operating constraints under SP 800-208 (Cooper et al., 2020; NIST, 2024c).

A parameter set specifies an algorithm's security and resource choices. NIST categories express comparative attack costs. Categories 1, 3 and 5 use exhaustive key search against AES-128, AES-192 and AES-256 as benchmarks. Categories 2 and 4 use collision search against 256- and 384-bit hashes. A parameter set meets a category when any attack on it, classical or quantum, needs resources comparable to or greater than those of the category's benchmark attack. A category therefore differs from a key length in bits, an encoded size in bytes or a service-performance rating (Moody et al., 2026).

Table B2 Encoded sizes for ML-KEM, ML-DSA and SLH-DSA

Parameter set	NIST category	Public key bytes	Private key bytes	Ciphertext or signature bytes
ML-KEM-512	1	800	1,632	768
ML-KEM-768	3	1,184	2,400	1,088
ML-KEM-1024	5	1,568	3,168	1,568
ML-DSA-44	2	1,312	2,560	2,420
ML-DSA-65	3	1,952	4,032	3,309
ML-DSA-87	5	2,592	4,896	4,627
SLH-DSA-SHA2-128s	1	32	64	7,856
SLH-DSA-SHA2-128f	1	32	64	17,088

Sources: NIST (2024a, 2024b, 2024c). The final column gives KEM ciphertexts for ML-KEM and signatures for ML-DSA and SLH-DSA. Every ML-KEM parameter set produces a 32-byte shared secret. ML-DSA-44 falls to category 1 if used with an approved random bit generator providing less than 192 bits of security (Moody et al., 2026). Private-key sizes are the full algorithm encodings, distinct from seed storage. The SHAKE variants of SLH-DSA, such as SLH-DSA-SHAKE-128s, have the same sizes as the SHA2 variants listed. SLH-DSA also has parameter sets for categories 3 and 5, with signatures of up to 49,856 bytes. Certificates, containers and protocol messages add their own fields to these encodings.

FIPS 203 recommends ML-KEM-768 as the default parameter set, while allowing alternatives where it is impractical or a higher security margin is required. Selection should reconcile the required protection with the protocol profile, peer support and resource limits (NIST, 2024a).

Table B2 shows a practical trade-off. The listed SLH-DSA parameter sets have smaller public keys and larger signatures than the listed ML-DSA parameter sets. Within SLH-DSA, a service that distributes many signed software images may favour the smaller signatures of the s variants. A service that signs messages frequently may instead favour the faster signing of the f variants (NIST, 2024b, 2024c).

As of 22 October 2026, NIST's PQC programme lists the Falcon-derived FN-DSA signature algorithm, associated with the developing FIPS 206, and the code-based Hamming Quasi-Cyclic (HQC) KEM as selected for ongoing standardisation. Because neither mechanism is yet a final standard, deployment planning should use the published status of the exact mechanism and profile at design approval (Perlner, 2025; NIST, n.d.-c).

Larger public keys, ciphertexts or signatures can increase handshake traffic, certificate-chain size, storage and working memory. Effects depend on where the additional bytes occur: a longer handshake can exceed message-size limits or need extra network packets, while larger signatures can affect firmware packaging or retained-record storage. The protocol, peer implementation and intermediate devices all influence the result. For example, a TLS hybrid group defines the component encodings and their placement within the exchange (Kwiatkowski et al., 2026).

Service testing should measure the complete operation on the intended platform under a stated workload. Useful measures include handshake or transaction latency, sustained throughput, CPU and peak memory use, total bytes exchanged, failure rates and recovery behaviour. Record hardware, software versions, parameter sets, message sizes, concurrency and network conditions. Primitive timings for key generation, encapsulation, decapsulation, signing or verification help explain a bottleneck. Service measurements, by contrast, establish whether the deployed design meets its operating needs. Project Leap's payment-system experiments illustrate why integration and operational testing accompany cryptographic changes (Bank for International Settlements Innovation Hub et al., 2025).

B.4 Hybrid protection, agility and implementation patterns

A post-quantum traditional hybrid construction makes both a traditional and a post-quantum mechanism contribute to the same protection. For key establishment, a specified combiner joins their shared-secret contributions, with the goal of preserving secrecy while at least one component remains secure. Whether that goal is met depends on the combiner and protocol. For signatures, the construction specifies how the component signatures bind the message and which verifications are required. Requiring both valid signatures can preserve authenticity when one component becomes vulnerable, subject to the construction's security conditions (Driscoll et al., 2025; Alagic et al., 2025).

Algorithm negotiation is the process by which peers select a supported profile. The protocol should authenticate that choice and enforce the policy on permitted profiles. When a condition triggers fallback, the resulting protection is that of the selected alternative mechanism or path. A bank should specify fallback triggers, permissions, monitoring and return conditions, and test recovery under those rules (Barker et al., 2025).

For TLS 1.3, RFC 9954, published in July 2026 as an Informational RFC, describes the hybrid key-exchange construction. RFC 10024, published in August 2026 as a Proposed Standard, specifies X25519MLKEM768, SecP256r1MLKEM768 and SecP384r1MLKEM1024. These groups combine an ephemeral elliptic-curve exchange with ML-KEM. Certificate and handshake signatures remain separate parts of authentication and require their own assessment (Stebila et al., 2026; Kwiatkowski et al., 2026).

Cryptographic agility, as defined in Appendix A, requires knowledge of deployed uses, together with replaceable components, controlled configuration, testing and observation. Table B3 compares the control points and protection boundaries of five common implementation patterns, which a service can combine (Barker et al., 2025).

Table B3 Implementation patterns and protection boundaries

Pattern	Control point	Dependencies and protection boundary
Central cryptographic service	A shared service manages selected cryptographic operations and keys.	Depends on service availability, authenticated access and supported calls. Assess the client-to-service link, caller permissions and where plaintext or secrets are processed.
Application library	The application invokes a cryptographic library or provider.	Depends on runtime support, interfaces and release ownership. Protection can cover the full path between application endpoints; each deployed copy and data format needs compatibility checks.
Transport proxy or service mesh	Proxies or mesh components control transport protection and identity distribution.	Depends on routing, peer support and control-plane availability. Protection spans the configured transport endpoints; inspect application-to-proxy and proxy-to-proxy segments separately.
Automated public-key infrastructure	Automated authorities and enrolment or validation components manage the certificate lifecycle.	Depends on HSMs, supported formats and trust distribution. Protects the identity and trust lifecycle; relying applications need to support the resulting keys and signatures.
Gateway for a legacy connection	A gateway terminates one connection and establishes another under a different profile.	Depends on gateway trust, availability and protocol compatibility. The external link can gain protection while the internal legacy link retains its own exposure. Plaintext may be processed at the gateway.

For each deployed pattern, the bank should identify termination points, key holders, administrative control and update dependencies. Protection claims should be limited to the boundaries and connections verified.

Side-channel leakage from the implementation also affects security. Timing, memory access, power consumption or electromagnetic emissions can reveal information about secrets, and error behaviour can create further leakage. Relevant checks include constant-time processing where required, secret-memory handling, randomness, input validation and failure behaviour. Tests and specialist review should cover the target hardware and implementation, because algorithm correctness and resistance to such attacks are separate properties (Alagic et al., 2025).

In hosted services, control may be divided between the bank and its provider. The bank should record who selects algorithms, generates and holds keys, configures permitted profiles, distributes trust, deploys updates and supplies evidence of actual use. Customer-managed keys may coexist with provider-controlled protocol and software choices. Product- and version-specific evidence, contractual change notices and an agreed update path help establish what the bank can change directly and what requires provider action (FS-ISAC Post-Quantum Cryptography Working Group, 2024).

B.5 Cryptographic uses across a bank

Table B4 describes the nine banking-use classes. It does not assign risk ratings, which depend on each bank's protection needs and dependencies.

Table B4 Banking-use classes, typical uses and distinctive constraints

Class	Typical cryptographic uses	Distinctive dependencies and constraints
Payment connections	Key establishment and authentication on interbank, settlement, messaging and processor links; message signing	Counterparties, financial market infrastructures and network operators; changes need agreed profiles and coordinated test windows
Public channels	TLS for internet, mobile and API channels; server certificates; application signing	Browsers, operating systems and app stores; the bank controls its servers but not client support
Cards and ATMs	Public-key offline card authentication; remote key loading for ATMs and terminals, often using RSA; symmetric online cryptograms	Card schemes, issuers, acquirers and device vendors; scheme specifications, certification and reissue cycles set lead times
Identity services	Internal PKI, workforce and customer authentication, document signing	Issuing authorities, HSMs and directories; trust material must reach every relying application
Stored information	Database, backup and archive encryption; any public-key mechanism used to transport or recover their keys; retained signed records	Captured ciphertext keeps its exposure; large archives may need re-encryption
External and cloud connections	VPNs, partner APIs, hosted and cloud services	Providers may control protocols, keys and update timing
Software supply chains	Code, package and firmware signing; update verification	Long-lived devices must accept new signature algorithms before vulnerable ones are withdrawn
Hardware roots of trust	HSMs, secure elements, firmware verification keys fixed in hardware	Firmware upgrades, revalidation or replacement

Class	Typical cryptographic uses	Distinctive dependencies and constraints
Constrained or end-of-life systems	Embedded, operational-technology and legacy platforms	Vendor support may have ended; gateways, isolation or replacement may be the only routes

Sources: CISA (2024); EMVCo (2026); FS-ISAC Post-Quantum Cryptography Working Group (2023c); Moody et al. (2026); Ward (2025).

Appendix C Jurisdictional PQC transition landscape

Table C1 compares official PQC requirements, guidance and milestones for seven jurisdictions, verified on 22 October 2026. Hong Kong is the home jurisdiction, where the HKMA readiness aim gives banks a planning reference, and mainland requirements can apply to particular connections (sections 3.2 and 4.6). The other five jurisdictions have issued official PQC timelines or financial-sector guidance that a bank may need to assess where it has legal entities, group arrangements or connections there (section 3.2). Use each instrument's scope and status to assess its relevance to the bank.

C.1 Reading guide and coverage

Security regulation spans national, international and industry regimes that differ in scope and in demonstrated effectiveness (Bouraffa and Hui, 2025). Read each entry in three steps. First, identify the institutions and systems covered. Second, distinguish requirements, guidance, readiness aims and proposals. Third, link each date to the action it concerns, such as planning, procurement or completed migration.

Government entries are relevant to a bank that operates a covered system or has accepted corresponding obligations by contract. Confirm binding obligations with legal and compliance staff and the relevant authority. Record the applicable source, entity, system, action, owner and review date. For advisory guidance, explain how it informs priorities.

C.2 Comparative table and source maintenance

Table C1 Selected jurisdictional instruments and milestones (verified 22 October 2026)

Jurisdiction, instrument and status	Institutions and systems covered	Actions, dates and qualifications
United States, federal direction Executive Order 14412, 22 June 2026 (The White House, 2026) OMB M-26-15, 24 June 2026 (Office of Management and Budget, 2026)	Federal agency information systems outside the national-security system regime. Priority scope includes high-value assets and high-impact systems.	Submit agency migration plans within 120 days of the Office of Management and Budget (OMB) memorandum. Complete priority key-establishment migration by 31 December 2030 and digital-signature migration by 31 December 2031. The OMB roadmap extends the priority scope to highly sensitive and particularly vulnerable systems, with remaining migration by 2035 subject to risk assessment and commercial availability. Agencies must also support TLS 1.3 by 2 January 2030. Relevant to banks mainly as a reference and for government-facing services. The order also directs the Federal Acquisition Regulatory Council to publish a proposed rule requiring covered contractors to comply by 31 December 2030 with NIST Federal Information Processing Standards (FIPS), including all applicable FIPS incorporating PQC-compliant algorithms.

Jurisdiction, instrument and status	Institutions and systems covered	Actions, dates and qualifications
United States, standards transition NIST IR 8547, final, 27 October 2026 (Moody et al., 2026)	Transition from quantum-vulnerable public-key algorithms in NIST-approved standards to post-quantum standards. A technical planning reference that applies through the relevant standards and the requirements that adopt them.	Listed classical public-key algorithms for digital signatures and key establishment are deprecated after 2030 and disallowed after 2035, including those providing at least 128-bit security. Application-specific transition requirements can call for earlier migration, with key establishment in TLS and similar protocols as an early priority. A hybrid key-establishment combination remains eligible for FIPS 140 validation where at least one component is approved, even if another is disallowed.
European Union, coordinated recommendations NIS Cooperation Group roadmap, published 23 June 2025 (NIS Cooperation Group, 2025) Roadmap FAQ, 15 April 2026 (NIS Cooperation Group, 2026) ECB Banking Supervision letter to banks, 7 July 2026 (European Central Bank, 2026)	Recommendations to Member States and stakeholders. Bank-specific obligations follow applicable EU and national law, supervisory measures and implementation arrangements.	By end-2026: establish initial national roadmaps and initiate planning and pilots for high- and medium-risk uses. By end-2030: complete high-risk migration, complete planning and pilots for medium-risk uses and enable quantum-safe software and firmware upgrades by default. By end-2035: complete medium-risk migration and low-risk migration as far as feasible. The FAQ confirms that the milestones concern deployment. In July 2026, ECB Banking Supervision told the significant institutions it supervises directly that the adoption of PQC "must start now" and that it will address quantum risk to encryption in a separate letter.
United Kingdom, technical guidance NCSC migration timelines, 20 March 2025 (NCSC, 2025)	Indicative targets for UK organisations, especially large organisations, critical national infrastructure operators and organisations with bespoke IT.	By 2028: complete discovery and assessment, define goals and prepare an initial migration plan. By 2031: carry out the highest-priority migration work and refine the plan into a thorough roadmap for completing migration. By 2035: complete migration of systems, services and products. NCSC recognises additional difficulty for a small set of rarely used technologies.
Canada, financial-sector sound practices OSFI Quantum Readiness Phases and Timelines, March 2026 (Office of the Superintendent of Financial Institutions [OSFI], 2026a) Bulletin status statement, updated 13 July 2026 (OSFI, 2026b)	Financial institutions supervised by the Office of the Superintendent of Financial Institutions (OSFI). The bulletin describes sound practices for discretionary application.	Build competency and awareness, inventory cryptographic assets, assess risk and create a migration plan, execute the transition, and test, validate and anticipate developments. The bulletin notes that external guidelines generally recommend quantum readiness across all systems by 2035. OSFI states that its technology risk bulletins are not regulatory expectations, so each institution decides how to apply them.
Canada, federal direction Government of Canada roadmap ITSM.40.001, June 2025 (Canadian Centre for Cyber Security, 2025); Security Policy Implementation Notice on migrating the Government of Canada to PQC, effective 9 October 2025 (Treasury Board of Canada Secretariat, 2025)	Federal IT systems covered by the implementation notice. Migration planning covers information up to Protected B; departments handling Protected C or classified information must consult the Cyber Centre.	Departmental migration plans by 1 April 2026; high-priority systems migrated by end-2031; remaining systems by end-2035. Relevant to banks mainly as a reference and for government-facing services.

Jurisdiction, instrument and status	Institutions and systems covered	Actions, dates and qualifications
Hong Kong, sectoral readiness aim HKMA whitepaper and readiness announcement, 27 July 2026 (HKMA, 2026a, 2026b) HKMA circular to authorized institutions (B1/15C), 27 July 2026 (HKMA, 2026c)	Hong Kong banking sector. The Hong Kong Monetary Authority (HKMA) uses a Quantum Preparedness Index (QPI) to assess sectoral preparedness.	HKMA expects authorized institutions to take early and concrete steps, including assessing quantum-related exposure, establishing a cryptographic inventory across systems and critical operations, and formulating a transition roadmap commensurate with their operational complexity and risk profile. HKMA aims for full sectoral readiness, expressed as QPI 10, by 2030. The index covers awareness, planning, pilots and practical preparedness.
Chinese Mainland, standards development ICCS Next-generation Commercial Cryptographic Algorithms Program, launched 5 February 2025; call for public-key algorithm proposals, 9 October 2025 (Institute of Commercial Cryptography Standards, 2025a, 2025b); first-round candidate listings (Institute of Commercial Cryptography Standards, n.d.)	Commercial cryptography standards	The cited ICCS programme announcements do not specify deployment or migration deadlines. New proposals closed on 30 April 2026; updates to existing proposals were accepted until 30 June 2026. First-round candidates have been published for evaluation. Track for connections where mainland requirements apply (section 4.6).
Singapore, financial-sector advisory and announced direction MAS/TCRS/2024/01, 20 February 2024 (Monetary Authority of Singapore [MAS], 2024) MAS annual-report remarks, 28 July 2026 (Chia, 2026)	All financial institutions addressed by the Monetary Authority of Singapore (MAS). The advisory supplements MAS notices and guidelines.	Monitor quantum developments, raise management and supplier awareness, maintain an inventory and prioritise critical assets. Develop cryptographic agility and staff capabilities. Prepare risk mitigation strategies for assets that cannot migrate to PQC and contingency plans for an earlier quantum threat. Consider trials where resources permit. The advisory's measures support ongoing preparation, with timing driven by exposure and solution availability. On 28 July 2026, MAS announced forthcoming expectations covering inventories, migration prioritisation, technical capabilities and governance, with progressive milestones. The stated aim is quantum resilience before the end of the decade. Treat the remarks as an announcement until MAS publishes the supervisory instrument and its operative dates.

Jurisdiction, instrument and status	Institutions and systems covered	Actions, dates and qualifications
Singapore, critical-infrastructure milestones CSA Quantum-Safe Migration Handbook V1, 16 July 2026 (Cyber Security Agency of Singapore et al., 2026) CSA guidelines for sector leads and CII owners, June 2026 (Cyber Security Agency of Singapore, 2026b) CSA advisory, 14 October 2026 (Cyber Security Agency of Singapore, 2026a)	Owners of designated critical information infrastructure (CII). Banking applicability follows the designation of the particular system.	Submit a quantum-safe migration plan to the Cyber Security Agency of Singapore (CSA) through the sector lead by 31 March 2027. From 1 January 2028, new CII systems with a digital component procured under contracts awarded from that date must support quantum-safe algorithms or technologies, or be quantum-safe ready, meaning able to support them by 31 December 2031; systems without cryptographic assets are exempt. Earlier contracts are not subject to this requirement, even if implementation starts later. Complete quantum-safe migration across CII systems by 31 December 2031. The handbook presents these dates as milestones, and CSA's June 2026 guidelines state them as requirements for CII owners, but neither cites a legal instrument that makes them binding. The bank should confirm detailed requirements and their legal basis with CSA and the sector lead. For other organisations, CSA's October 2026 advisory recommends a migration plan by end-2027 and encourages completion by 2035.

Earlier action: The bank's protection periods, migration duration and consequences of compromise may justify moving ahead of the milestones in Table C1.

Source maintenance: Entries identify official sources and their dates. Full entries appear under Sources for Table C1 below. Recheck entries when issuers change instruments or publish relevant sectoral guidance, and before material investment or deployment decisions. Record the verification date and effects on obligations, procurement and migration timing.

Sources for Table C1

Sources also cited in the main text (Canadian Centre for Cyber Security, 2025; HKMA, 2026a, 2026b, 2026c; Moody et al., 2026; NCSC, 2025) appear in the References.

Chia, D. J. (2026, July 28). *Remarks by Mr Chia Der Jiun, Managing Director, MAS, at the MAS Annual Report 2025/2026 Media Conference on 28 July 2026* [Speech]. Monetary Authority of Singapore. https://www.mas.gov.sg/news/speeches/2026/md-remarks-for-mas-ar-2025-2026

Cyber Security Agency of Singapore. (2026a, October 14). *Advisory on quantum-safe migration for organisations*. https://www.csa.gov.sg/alerts-and-advisories/advisories/advisory-on-quantum-safe-migration-for-organisations/

Cyber Security Agency of Singapore. (2026b, June). *Guidelines to sector leads and CIIOs for adoption of quantum-safe requirements and migration plan outline*. https://isomer-user-content.by.gov.sg/36/226284f1-4fbd-4a0f-9ec3-4cc0700cb6b0/Annex%20A%20-%20Guidance%20on%20Quantum-safe%20Requirements%20and%20Migration%20Plan%20Outline.pdf

Cyber Security Agency of Singapore, Government Technology Agency, & Infocomm Media Development Authority. (2026, July 16). *Quantum-safe migration handbook* (Version 1). https://isomer-user-content.by.gov.sg/36/350e4bd5-fa25-4609-8e78-5e159d9da245/CSA%27s%20Quantum-Safe%20Handbook%20V1%20Dtd%2016%20Jul%2026.pdf

European Central Bank. (2026, July 7). *Addressing AI-enabled cybersecurity threats* (Letter to banks SSM-2026-0301). https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2026/ssm.2026_letter_on_AI_enabled_cybersecurity_threats.en.pdf

Institute of Commercial Cryptography Standards. (n.d.). *Round 1 candidates*. Retrieved 22 October 2026, from https://www.niccs.org.cn/niccs/Round1Additional/pc/list.html

Institute of Commercial Cryptography Standards. (2025a, February 5). *Announcement on launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC)*. https://www.niccs.org.cn/niccs/Notice/pc/content/content_1937428197396713472.html

Institute of Commercial Cryptography Standards. (2025b, October 9). *Call for proposals for the next-generation public-key cryptographic algorithms*. https://www.niccs.org.cn/niccs/Notice/pc/content/content_1975896137741635584.html

Monetary Authority of Singapore. (2024, February 20). *Advisory on addressing the cybersecurity risks associated with quantum* (MAS/TCRS/2024/01). https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/mas-quantum-advisory/mas-quantum-advisory.pdf

NIS Cooperation Group. (2025, June 23). *A coordinated implementation roadmap for the transition to post-quantum cryptography*. European Commission. https://ec.europa.eu/newsroom/dae/redirection/document/117507

NIS Cooperation Group. (2026, April 15). *Frequently asked questions on the EU roadmap for the transition to post-quantum cryptography*. European Commission. https://ec.europa.eu/newsroom/dae/redirection/document/132120

Office of Management and Budget. (2026, June 24). *Execution of the migration to post-quantum cryptography* (Memorandum M-26-15). Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2026/06/M-26-15-Execution-of-the-Migration-to-Post-Quantum-Cryptography.pdf

Office of the Superintendent of Financial Institutions. (2026a, March). *Quantum readiness phases and timelines* (Technology risk bulletin). https://www.osfi-bsif.gc.ca/en/risks/technology-cyber-risk-management/technology-risk-bulletin/quantum-readiness-phases-timelines

Office of the Superintendent of Financial Institutions. (2026b, July 13). *Technology risk bulletin*. https://www.osfi-bsif.gc.ca/en/risks/technology-cyber-risk-management/technology-risk-bulletin

Treasury Board of Canada Secretariat. (2025, October 9). *Migrating the Government of Canada to post-quantum cryptography: Security Policy Implementation Notice*. https://www.canada.ca/en/government/system/digital-government/policies-standards/spin/migrating-government-canada-post-quantum-cryptography.html

The White House. (2026, June 22). *Securing the nation against advanced cryptographic attacks* (Executive Order 14412). https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/