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

## Practitioner Guide

A companion to the Reference Manual



## Purpose

This Guide explains how banks can apply the PQC Accountability and Controlled Transition Framework, or PACT. It is a companion to the Reference Manual, which provides the full specification. It is intended for those who direct, deliver, operate and oversee a bank's transition to post-quantum cryptography, helping them understand the work and the decisions involved.

PACT can be applied through existing governance, risk management, technology-change and operating arrangements. Supporting tools may facilitate adoption, but use of a particular toolkit, data model, template or software product is not a condition for applying PACT.

## Authors


| | |
|---|---|
| Allen H. HUANG | Head and Professor, Department of Accounting, HKUST |
| Terrance FUNG | Senior Manager, Banking Supervision Department (Supervisory Technology), HKMA<br>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 work 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 work.

## 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 work does not itself establish regulatory compliance or cryptographic security, or replace institution-specific risk assessment and professional advice.*

*The work 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.*

# CONTENTS

About this Guide ..... 4
1. Preparing for quantum change ..... 5
2. Getting started ..... 6
3. Govern the transition ..... 9
4. Assess and plan ..... 11
5. Implement and retire ..... 17
6. Maintain and adapt ..... 22
7. Applying PACT across the bank ..... 25
8. Working terminology ..... 26
9. Reference Manual navigation ..... 27
Sources ..... 29

ABOUT THIS GUIDE

# Using the Guide and Reference Manual

The Guide explains the PQC Accountability and Controlled Transition (PACT) framework through the decisions banks face and a continuing payment example. The Guide accompanies the Reference Manual, which sets out the full workstreams, responsibilities and criteria. Readers can move between the two according to their role and the issue under consideration.

The routes below suggest starting points, rather than allocating responsibilities.

| Your role | Guide pages | Reference Manual sections |
|---|---|---|
| **Board and senior management** | Direction and authority p. 9<br>Timing p. 13<br>Reporting p. 23 | **3.1–3.2** Leadership and mandate<br>**3.4** Decision authority<br>**3.6** Resources<br>**4.3** Exposure and timing<br>**6.2** Reporting |
| **Programme and transition teams** | Starting work p. 6<br>Responsibilities pp. 8–9<br>Integrated planning p. 16 | **3.1** Coordination<br>**3.3** Ownership<br>**4.7** Integrated roadmap<br>**6.3** Responding to findings<br>**8** Practical application |
| **Business and information owners** | Protection needs pp. 6–8<br>Acceptance criteria p. 14<br>Completion p. 21 | **3.3** Outcome ownership<br>**4.3** Exposure and protection periods<br>**4.4** Target and acceptance criteria<br>**5.6** Completion and continuing responsibilities |
| **Security, architecture, engineering and operations** | Discovery p. 11<br>Design and testing pp. 14–15<br>Controlled change pp. 17–21<br>Agility p. 24 | **3.5** Common requirements<br>**4.1** Discovery<br>**4.4–4.6** Design, testing and approval<br>**5.1–5.6** Implementation and retirement<br>**6.1, 6.4** Maintenance and agility<br>**Appendix B** Technical primer |
| **Procurement, supplier and group coordinators** | Dependencies p. 12<br>Commitments p. 16<br>Continuing responsibilities pp. 21–22, 25 | **4.2** Dependency requirements and readiness<br>**4.7** Commitments<br>**5.6** Continuing support<br>**6.1–6.3** Current evidence, reporting and response |
| **Risk, compliance and internal audit** | Decision authority p. 9<br>Exceptions p. 19<br>Evidence and reporting pp. 21–24 | **3.4** Authority and independent control<br>**5.4** Exceptions<br>**5.6** Completion evidence<br>**6.2–6.3** Reporting, review and response |

References at the end of each topic lead to the relevant Manual sections. The workstream map on pages 27–28 covers all 23 workstreams, while Manual Section 2 provides a shared introduction to the framework and core concepts; Manual Section 7 develops the payment example in full. Appendix A explains the terminology. Appendix B provides technical background for readers who need it. Appendix C compares selected jurisdictional approaches and milestones.

1. PREPARING FOR QUANTUM CHANGE

# Why preparation matters now

Banks use cryptography every day to protect information, verify identities and support trust in transactions and records. These protections are embedded in applications, networks, shared platforms and services supplied by other organisations. Changing them requires coordinated work across the bank and its dependencies.

A sufficiently capable quantum computer could defeat many widely used public-key cryptographic mechanisms. Its arrival date remains uncertain. Preparation is nevertheless necessary because migration takes time and information captured today may remain sensitive when future decryption becomes possible. Post-quantum cryptography provides replacement algorithms designed to resist known conventional and quantum attacks, using conventional computers. [1]

### The Hong Kong preparedness agenda

The HKMA's first Quantum Preparedness Index, published in July 2026, placed the banking sector at 2.3 out of 10. The QPI considers Awareness, Planning, Pilots and Practical Preparedness. The HKMA aims for full sectoral readiness, expressed as a QPI score of 10, by 2030. This is a preparedness objective; individual protection needs and delivery constraints can require earlier action. [2, 3]

Banks are expected to take early, concrete steps: assess quantum exposure, establish a cryptographic inventory across systems and critical operations, and develop a roadmap proportionate to operational complexity and risk. The HKMA's July 2026 circular points banks to the critical operations identified under SPM OR-2 when establishing that inventory. [4, 6]

PACT helps banks organise that work. It connects the protection required for a service or information with the people responsible, the changes needed and the evidence supporting each decision. It can help a bank substantiate its preparedness, but it does not assign QPI points or make a QPI score evidence of protection for a particular service.

### Prepare to change again

Cryptographic agility enables a bank to update cryptography in a controlled way as standards, threats and technologies evolve, while avoiding major disruption to services. [2, 5] PACT treats this as a continuing organisational capability. A bank needs to identify affected uses, coordinate decisions and providers, implement and verify change, and maintain acceptable protection and service conditions throughout.

That capability begins with today's inventory, architecture and procurement choices. It is demonstrated through further change, including the operating and recovery work that makes the result sustainable. Page 24 explains how to assess it.

**Reference Manual**: 1 and 6.4; Appendix B explains cryptographic functions and quantum exposure.

**2. GETTING STARTED**

# Begin with a useful piece of work

A bank can begin with a material service, information flow or shared platform. The initial scope should have sufficiently clear ownership, supporting information and decision-making authority to enable practical action. Broader discovery can proceed in parallel, provided that unresolved dependencies and information gaps remain visible in the overall transition plan.

### Choose a starting point people can own

A useful starting point is a service with an identifiable business owner and relevant technology and operations leads. It may involve information that must remain confidential for many years, a dependency shared by several important services, or an upcoming upgrade that creates a practical opportunity to prepare for PQC.

An early investigation needs a defined scope, named contributors and clarity about the access and time required. Security and architecture specialists, together with those managing suppliers or other counterparties, help establish whether the proposed work is feasible. Any testing or access that could affect operations should follow the bank's existing approval and control processes.

### Establish the protection and service needs

The assessment begins with what must remain confidential, authentic or trustworthy, for how long, and the consequences of failure. It also establishes the operating conditions that change must preserve, including processing accuracy and recovery. These needs give technical findings their business meaning.

Current application, configuration, certificate, supplier and recovery records provide initial evidence of the cryptographic uses supporting these needs. The assessment also covers connections and components controlled by others. Where a component cannot be examined, it remains a dependency to manage, with the evidence gap recorded as part of the assessment.

### Agree the next action

The findings may point to a supplier enquiry, clearer responsibilities, investigation of a shared dependency or a test of a design question. The record of this work identifies what is known, what remains uncertain, the owner of the next action and the decision its result will support. Wider coverage gaps belong in the institutional plan.

For an established programme, tracing one important service from its protection needs through the inventory, dependencies, approvals and delivery evidence provides a practical check of current arrangements. This can reveal whether the programme's records support the results it reports.

### The payment example

Throughout this Guide, a hypothetical bank sends corporate payment instructions to an external processor. It needs seven years of transmission confidentiality, mutual authentication and integrity, correct processing and reconciliation, and connection recovery within 30 minutes. The example follows a change to key establishment, the process by which communicating parties obtain a secret used to derive encryption keys. Authentication migration remains separately assigned. The different scopes matter when the bank reports what has been achieved.

**Reference Manual**: 2.2, 4.1, 4.7 and 8; the full hypothetical payment case is in Section 7.

## 2. GETTING STARTED

# Four pillars for quantum preparedness

PACT's four mutually supporting pillars provide a practical structure for advancing the QPI's four dimensions: Awareness, Planning, Pilots and Practical Preparedness. [2] Figure 1 shows how their contributions build on one another.

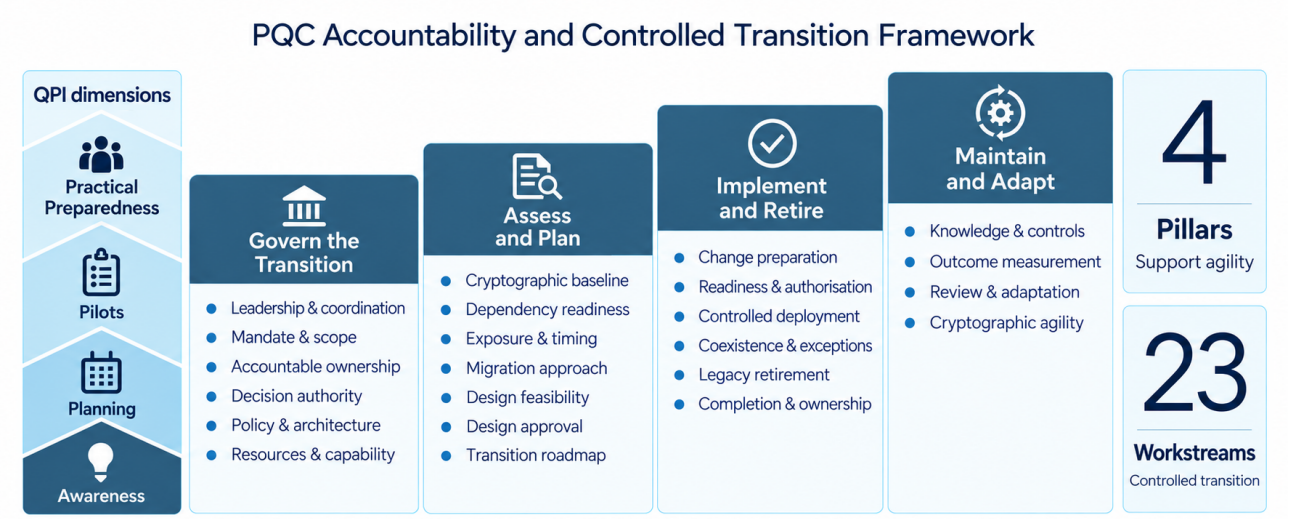



Figure 1. PACT at a glance.

**Govern the transition** provides a foundation for **Awareness**. Leadership, clear ownership, common requirements and relevant skills help people understand the implications of quantum change and organise the bank's response.

**Assess and plan** builds on that foundation to support **Planning**. It connects protection needs with the inventory, dependencies and priorities, develops suitable designs and a feasible roadmap and lays the groundwork for early pilots.

**Implement and retire** supports **Pilots** through controlled trials, drawing on design work and testing under Assess and plan. It also advances practical preparedness by introducing authorised changes, verifying operating results and withdrawing earlier arrangements where required.

**Maintain and adapt** sustains **Practical Preparedness**. Together with the other pillars, it keeps knowledge and controls current, responds to findings and demonstrates the ability to make further cryptographic changes while preserving protection and service continuity.

These contributions overlap. Governance and adaptation continue throughout, and design pilots can begin before wider implementation. Pillar reviews use the bank's existing arrangements.

### Decisions and findings stay connected

Management decisions guide the work, while findings from discovery, testing and operations inform subsequent decisions. The Manual calls these flows the **direction and decisions rail** and the **evidence and feedback rail**. Existing records can support both, provided an approval is distinguishable from the evidence on which it rests.

A supplier delay, for example, may change several delivery plans. The responsible owners establish its consequences; the transition manager brings the combined issue to the appropriate authority. The resulting decision returns to teams with clear actions, conditions and responsibilities.

**Reference Manual**: 2.3–2.5; pillar reviews support decisions about defined work through existing arrangements.

## 2. GETTING STARTED

# Connect services with accountable owners

PACT connects responsibility with the result the bank needs to preserve, known as a **protected outcome**. For the payment service, this includes the required confidentiality and trust, alongside correct processing and recovery. The business or information owner explains those needs and the consequences of failure.

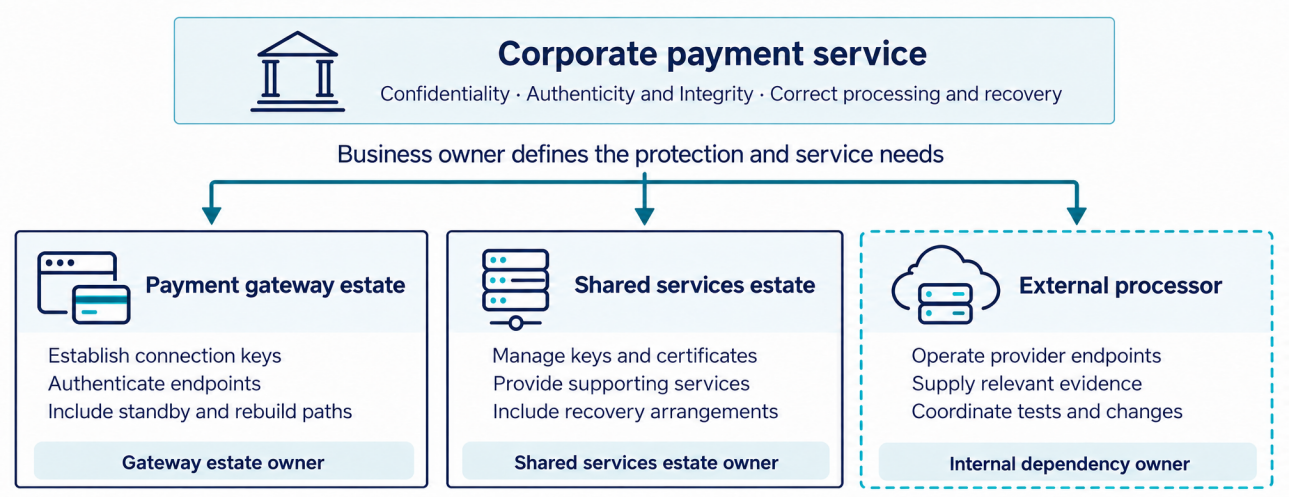



Figure 2. A service depends on several cryptographic uses and owners. The diagram simplifies the payment example; a change can involve work across both estates and the provider.

Technical teams identify the **cryptographic uses** supporting the outcome. Establishing a shared secret for encryption and authenticating the other endpoint are distinct uses, even when they occur within one connection. A use can support more than one outcome.

Each use belongs to one **cryptographic estate**: a manageable scope with an accountable owner for continuing management. An estate includes relevant standby, recovery and inactive capabilities. The payment gateways form one estate in the example; shared key and certificate services form another. Systems and organisational charts do not always align neatly with these boundaries, so the ownership map needs to make them explicit.

Where another party controls a required contribution, an internal **dependency owner** manages the bank's reliance, obtains evidence and escalates shortfalls. The provider or group service remains responsible for its contribution.

A **change package** brings a defined set of delivery work under an accountable package owner. It can cross estate boundaries. Completing the package leaves the business, estate and operations owners responsible for the resulting service and protection.

**Reference Manual**: 2.2 and 3.3; Section 2.4 connects institutional governance, estate management and engineering delivery.

### 3. GOVERN THE TRANSITION

# Give the work direction and authority

PQC transition requires decisions that individual delivery teams cannot settle alone. **Executive sponsors** secure resources, resolve competing priorities and provide a route for escalating issues. A **transition manager** connects contributors' plans and follows up agreed actions. These responsibilities can sit within existing positions and teams.

## Establish a usable mandate

The board or appropriate senior-management authority establishes sponsorship and the transition manager function through existing delegations. The board retains oversight, while senior management is responsible for implementation. The mandate defines the organisational scope, services, information and obligations covered, the protection sought and the operating conditions to preserve. It includes material shared services, external contributions and recovery arrangements. Retained information may still require protection after a service closes.

Sponsors secure support and resolve or escalate matters within their authority. Where sponsorship is shared, the remits collectively cover the programme and provide a clear route for decisions that cross boundaries. A group-led programme still needs identified local executive responsibility and access to evidence relevant to the local bank.

The transition manager maintains the integrated roadmap and responsibility map, reconciles contributions and brings unresolved issues to the appropriate decision-maker. Business, technology, operations and control functions remain accountable for their own assessments and commitments.

## Ownership, review and decision authority

The **responsibility map** identifies who prepares a proposal, who reviews the evidence, who approves the action and who carries it out. Owning delivery does not automatically confer authority to approve a design, deploy a release or accept remaining risk. Those decisions follow the bank's delegations and independent controls. Internal audit retains its independent assurance role.

A useful escalation gives the decision-maker a clear account of the affected service, evidence, uncertainty, available options and consequences of delay. It identifies the decision required and whether it falls within that person's authority.

## Payment case

The chief operating officer sponsors six weeks of investigation. The work needs a specialist and test facility already committed elsewhere. The transition manager brings the conflict to the sponsor, who secures two specialist days each week while preserving support for the other work. Relevant managers confirm the access and resources. This authorises the investigation; later design, production and risk decisions retain their respective approvers.

The governance review considers whether the work has a clear scope, accountable owners, decision routes and committed support. It identifies any gaps that prevent the proposed activity from proceeding.

**Reference Manual**: 3.1–3.4 and the Govern pillar review; payment case in 7.1.

**3. GOVERN THE TRANSITION**

# Equip teams for this change and the next

Common requirements help teams make compatible choices and avoid repeated investigation. They also create a basis for cryptographic agility, so that a later change can be planned and tested without rediscovering the whole environment.

### Set common technical requirements

**Specialist domain owners** maintain requirements for mechanisms, protocols, keys, certificates, implementation controls and recovery, working with the business, technology and operations owners who will apply them. An identifiable owner, scope, effective version, approver and review triggers make clear what applies and when it needs reconsideration.

Algorithm standards inform design choices alongside the protocol, implementation, configuration, interfaces and operating environment. The assessment distinguishes final standards from drafts and exploratory approaches. A reusable design also needs evidence that it applies to the bank's intended deployment.

A team proposing a departure explains its implications to the designated authority and seeks approval. When a requirement changes, its owner identifies the affected designs, purchases and approvals, allowing the transition manager to coordinate the consequences for plans.

### Build future change into current choices

Architecture and procurement decisions shape how easily cryptography can be replaced. Teams assessing these choices consider component boundaries, supported update paths, controlled configuration and interfaces. They also examine who controls changes, what supplier or certification constraints apply, and whether monitoring can confirm the mechanism actually used.

Recovery forms part of the same assessment: a rebuild that restores an obsolete or prohibited configuration leaves the upgrade path incomplete. Recovery images, key and certificate procedures, and provider-controlled components therefore form part of the design for further change.

### Commit the capability to deliver

Delivery depends on people with relevant skills, access, tools, test environments and continuing support. An indicative budget alone cannot establish whether a shared specialist or test facility will be available. Managers responsible for these contributions confirm the people, facilities and time they can commit to the plan.

Training reflects the different responsibilities involved. It helps business owners interpret protection needs and uncertainty, engineers apply discovery and testing methods, and operations teams carry out recovery procedures. Supplier managers need to recognise and obtain evidence that applies to the bank's deployment.

An exercise with a clearly defined scope can show whether this support works in practice. A discovery exercise, for example, may demonstrate that staff can obtain configuration evidence and connect it to a service. Reviewers record both the capability demonstrated and what remains unproven, with owners and response dates for any gaps.

**Reference Manual**: 3.5–3.6; design enablers and demonstrated agility are distinguished in 4.4 and 6.4.

**4. ASSESS AND PLAN**

# Build an inventory that supports sound decisions

A **cryptographic inventory** becomes useful when it connects technical findings to the service, deployment, owner and dependencies concerned. A list of algorithms alone cannot show which business needs are protected or where change is required.

Existing application inventories, configuration records, certificate and key systems, software records and supplier information provide a starting point. Their value depends on what they cover, who maintains them, how current they are and what they omit. Technical teams supplement them with inspection, observation and targeted enquiries, using discovery methods checked against known cases and collection arrangements that are safe for the environment.

### What the evidence can establish

| Evidence about | Question it can answer | Important limit |
|---|---|---|
| Product capability | What can this product or release support? | Support for a mechanism does not establish its use in the bank. |
| Installed capability | What is present in this deployment? | Installed code may be disabled or unused. |
| Permitted configuration | What can the deployment select or invoke? | A permitted choice may differ from the mechanism used for a particular exchange. |
| Observed use | What did the examined exchange or operation use? | An observation does not cover every connection, fallback or recovery path. |

A **cryptographic bill of materials**, or CBOM, can supply structured information about assets and dependencies. Whether it describes a product release, a particular deployment or another scope determines how it can contribute to the bank's inventory and ownership records. A PQC algorithm listed in a software library does not establish PQC protection for a live service.

### Keep gaps visible

Each finding is accompanied by its source, date, version, configuration and limitations. Stable identifiers link related records while keeping distinct deployments separate, and conflicting observations remain visible until reconciled. Records may refer to keys and certificates, while private keys, passwords and other secrets remain in protected systems.

Inventory coverage extends to relevant standby systems, recovery images and provider-controlled components. Where evidence is unavailable, the dependency remains in scope and a named owner manages the evidence gap. Work supported by the available evidence can proceed within its authority while further investigation expands coverage.

The resulting inventory explains the current cryptographic position, including what the bank knows and the boundaries of that knowledge.

**Reference Manual**: 4.1 and 2.5; the full inventory and evidence considerations remain in the Manual.

**4. ASSESS AND PLAN**

# Make dependencies part of the plan

A bank's migration may depend on software suppliers, cloud providers, counterparties, financial infrastructures or shared group services. Early engagement helps establish what they can deliver and gives the bank time to consider alternatives.

### The contribution required from each party

The estate owner works with business, security and operations colleagues to identify what is needed. The internal dependency owner then seeks agreement on what the controlling party will provide, including the product and version, interface, configuration, testing access, supporting evidence and delivery date. For hosted services, this discussion also clarifies control over algorithms, keys, trust settings and updates.

The bank's required date and the provider's offered date remain separate facts. A forecast estimates delivery, whereas a commitment identifies an agreed contribution and date. Neither replaces test evidence, which demonstrates capability only under the conditions examined. Laboratory access may therefore support design work while the production version remains unqualified.

Supplier and procurement arrangements can secure participation in testing, support, useful change notices and escalation. When several services depend on one contribution, the transition manager reflects that shared constraint across their plans. Any alternative route also needs assessment of lead time, compatibility, cost and service continuity.

### Apply group evidence to the local bank

A group programme may provide designs, specialists and shared test results. Their applicability depends on which local deployments they cover and whether the same assumptions, interfaces and recovery arrangements apply. The local institution establishes this fit and identifies any additional evidence or decisions needed for local obligations or operating needs.

Where head office controls delivery, an internal owner still manages the local reliance and records the required contribution, relevant dates, evidence and escalation route. These records connect the group commitment to the local plan, showing how it meets local needs and what a delay would affect.

### Payment case

The gateway change depends on the processor's endpoint and an inspection device on the connection. The bank needs to distinguish evidence from the provider's laboratory from evidence for the production configuration. The design test on page 15 shows why that distinction matters.

The review identifies unconfirmed contributions, evidence gaps and conflicting dates. Their effect on the available routes informs the next action and its assignment to an owner.

**Reference Manual**: 4.2, 4.7 and 8; payment dependency and pilot in 7.2.

**4. ASSESS AND PLAN**

# Work back from the protection need

Prioritisation brings together urgency, timing and delivery order. Exposure and the consequences of compromise determine how urgently protection is needed. Migration duration and contingency affect when work must start, while dependencies and capacity shape the order in which changes can be delivered. A difficult migration may therefore need earlier preparation.




Figure 3. Illustrative timing for new confidential transmissions. All dates and durations are assumptions in the hypothetical payment case, not predictions or supervisory deadlines.

For each new payment transmission, the example requires seven years of confidentiality. If the bank assumes, for planning purposes, that vulnerable encryption could be broken from 1 January 2035, it needs to stop new vulnerable transmissions by 1 January 2028 to preserve the seven-year protection period. Nine months of migration and two months of contingency give a required start of 1 February 2027. The bank plans to begin on 1 January 2027.

### Timing for different protection needs

The subtraction above concerns continuing confidential transmissions. Archives and backups require assessment of when information ceases to be sensitive and how ciphertext or keys could be exposed. Authentication and signatures require consideration of continued trust and retained records. Migration cannot undo exposure from ciphertext already captured under vulnerable protection.

The timing assessment starts with the earliest applicable completion limit for the defined target, together with its source and authority. The required start is calculated by subtracting the remaining migration duration and a separate contingency allowance, subject to any earlier binding start deadline. The duration includes supplier waiting, integration, testing, recovery preparation and required retirement.

The Manual recommends the earliest date in the bank's approved quantum-threat range as a conservative basis; a different basis needs a rationale and the appropriate decision. Scenarios show how uncertain assumptions affect the plan. A date not yet established differs from a known inability to meet a limit, although both need an owner and response. Revising the forecast does not remove the underlying exposure.

**Reference Manual**: 4.3 and 4.7; worked payment timing in 7.2.

**4. ASSESS AND PLAN**

# Choose a route and define success

The right transition route depends on the use, protection needs, delivery constraints and ability to sustain the result. Options may include a supported upgrade, component replacement, a shared service, a change to particular connections, restriction of a use or its retirement. Comparing these options involves the whole route, including withdrawal of earlier arrangements and future change.

### Specify the intended result

A clearly defined target identifies the uses and interfaces changing, mechanisms and parameters, products and versions, key and certificate arrangements, and permitted failure and recovery behaviour. This gives teams a basis for testing the design and later determining whether the agreed result has been achieved.

Different cryptographic functions can require separate migration decisions.

| Function | What it supports | Implication for the transition |
|---|---|---|
| Key establishment | Establishing a secret from which encryption keys can be derived. | Changing this function can address the risk of later decryption of newly transmitted traffic; authentication still needs its own assessment. |
| Authentication | Establishing the identity of an endpoint or other party. | Certificates, trust and identity checks need assessment separately from confidentiality. |
| Digital signatures | Verifying origin and integrity of signed information. | The assessment covers future reliance on signatures and retained records or evidence. |

Where a hybrid construction combines conventional and post-quantum mechanisms, they contribute jointly to the same cryptographic operation. The construction and its failure behaviour need assessment. Running different mechanisms alongside one another does not, by itself, establish that combined protection.

### Agree acceptance criteria

Business and operations owners translate the target into criteria for protection, compatibility, performance, correct service behaviour and recovery. These give technical teams a basis for deciding how achievement will be assessed. In a payment service, for example, successful cryptography is insufficient if reconnecting causes instructions to be lost, duplicated or reported with an incorrect status.

The same design decisions shape the bank's ability to change cryptography again. Relevant features include replaceable components, controlled settings and observation of actual use, considered alongside supplier, hardware and certification constraints. A protocol upgrade may enable later PQC adoption without itself providing PQC protection.

In the payment example, the bank selects a nine-month gateway upgrade over a fifteen-month replacement. The chosen package changes key establishment. Its target does not claim to complete authentication migration, which remains on a separate plan.

**Reference Manual**: 4.4; Appendix B explains functions, hybrid constructions and implementation considerations.

**4. ASSESS AND PLAN**

# Use testing to inform a decision

A useful pilot answers a question that could change the proposed design or the conditions for accepting it. Its scope follows an assessment of whether existing results apply to the intended versions, configuration, interfaces, environment and workload. The uncertainties that remain give a targeted trial its purpose.

### Set the question before running the test

A test plan sets out the acceptance criteria, evidence to collect, stopping conditions and recovery arrangements. Testing may examine interoperability, trust handling, performance, capacity, failure, fallback and recovery. Service behaviour forms part of this assessment, including the processing and reconciliation of payments where relevant.

Unsuccessful and inconclusive findings form part of the evidence alongside successful results. They may reveal a dependency, narrow the conditions in which the design is suitable or show that another route is needed. A material change to the design or its supporting conditions requires reassessment and affected retesting.

### Make the design decision clear

The estate owner brings the proposed design, results and unresolved matters together for a decision. Business and operations owners confirm whether their requirements are addressed, while reviewers assess the evidence and conformity with common requirements. The assigned approver identifies the design version and scope approved to proceed, together with any conditions.

For connected parties, the design agreement includes an interface profile setting out the protocols, mechanisms, parameters, certificates, trust settings and recovery behaviour for compatible operation. Dependency owners obtain the necessary agreements.

Design approval supports further preparation. The actual release still needs appropriate qualification and permission for the proposed action. A pilot that affects production also needs the controls and authority applicable to that production activity.

### Payment case

The design pilot fails because the provider's inspection device cannot handle the larger exchange. A correction to its laboratory setting resolves the problem, and retesting supports the proposed hybrid key-establishment design. The chief architect approves the profile for change preparation. The bank retains three important boundaries: the production correction must still be demonstrated; the final release must be qualified; and authentication migration remains separately assigned.

The design decision now gives delivery teams a usable basis for work. It also makes the remaining prerequisites explicit, so that a successful pilot cannot silently become permission for a wider deployment.

The design review considers what the tests establish, what remains untested and which decision the evidence can support.

**Reference Manual**: 4.5–4.6 and 5.2; payment design decision in 7.2.

**4. ASSESS AND PLAN**

# Build a deliverable roadmap

The **integrated roadmap** brings estate plans together so that the bank can assess whether shared dependencies and resource demands can be met. The transition manager coordinates this work, while contributing owners substantiate their plans and confirm their commitments.

### Dates, dependencies and capacity

Each roadmap item connects the protection need to the work, owner, prerequisites, resources, relevant dates and evidence of completion. Required dates, forecasts and agreed commitments remain distinguishable. Delivery order also reflects dependencies: an urgent application change may first require a shared-platform upgrade.

The transition manager compares demands across plans with the available specialists, funding, procurement capacity, testing facilities, change windows, stabilisation and retirement support. This includes the effort of operating earlier and replacement arrangements during coexistence. Individually plausible plans may still be undeliverable if they rely on the same unavailable team or provider.

Sponsors resolve priorities within their authority and obtain decisions beyond it. Where a dependency or resource is unconfirmed, the plan explains the impact and proposed response. When forecasts change, the original commitment remains visible, allowing management to see how delivery has moved against the agreed basis.

### Let useful work proceed

Investigation, enabling work and implementation can advance together. One service may need further discovery while another has a supported design and a third awaits a provider contribution. The roadmap keeps unknown and blocked work visible alongside other activity that can proceed with the relevant permission.

Experience of supplier delays, testing effort and recovery informs later estimates and revisions to the plan. The roadmap records delivery commitments, while design, production and risk decisions continue to require the evidence and authority appropriate to each action.

### Payment case

The funded plan starts on 1 January 2027 and aims to complete on 1 October. Two months of contingency extend through 1 December, ahead of the 1 January 2028 protection limit. The provider's production correction and final-release qualification remain prerequisites. Authentication follows its own plan and assessment.

This makes the plan's room for delay visible. If an estimate grows, the bank can assess whether it needs earlier work, more capacity, a different route or interim measures before the protection limit is threatened.

The roadmap review considers the proposed commitments and their supporting evidence, alongside unresolved dependencies and timing or capacity constraints. It identifies the decisions needed to resolve those constraints.

**Reference Manual**: 4.7 and the Assess and plan pillar review; payment roadmap in 7.2.

**5. IMPLEMENT AND RETIRE**

# Prepare and authorise the specific change

An approved design gives delivery teams a starting point. The next task is to establish whether the selected release can achieve the required protection and service conditions, and to obtain permission for the action proposed.

### Prepare the work and its operating support

The package owner defines the release and configuration, affected uses and interfaces, tasks, dependencies and completion criteria. This preparation brings together software, keys, certificates, trust settings and provider contributions. Versioned build instructions, change procedures and tested automation make the work reproducible and support later change.

Operations support covers monitoring, incident response and recovery, with the access, training and resources needed to use them. Recovery specifies the configuration returning to service and its protection. Procedures cover key generation, protection, permitted use and destruction, and certificate issuance, renewal and revocation. Backup or regeneration must suit the key's purpose and approved recovery design. Secrets remain outside ordinary change records; required retirement is planned from the outset.

### Match the evidence to the action

The evidence needed depends on whether a capability is being installed, activated for selected traffic or extended to a wider population. The proposed release, configuration, users, interfaces and operating conditions define the scope of that assessment. Earlier pilots and supplier tests remain useful where their supporting conditions apply.

Technical contributors test the actual candidate against relevant security, compatibility and service criteria under representative workloads, failures and recovery. Normal operation, standby operation and rebuilding after a major failure can reveal different weaknesses. Their assessment explains the findings and the limits of the conclusions supported.

Business, estate and operations owners assess the consequences within their responsibilities, while required reviewers challenge the evidence. The assigned approver then decides what may proceed under the bank's existing delegations. Material findings may require correction, a narrower supported scope or an authorised departure where permissible. An evidence gap is not an approved exception: a proposed departure must identify the requirement that would remain unmet.

### Make permission usable in operation

Permission identifies the action's boundaries, success criteria, observation period, stopping conditions and recovery response. It can cover several increments where the conditions for progression and authority to continue are clear. A material change that undermines the decision's basis requires reassessment.

For the payment service, the bank qualifies the gateway release and obtains permission for an attended first batch followed by a production pilot with defined limits. This permission is specific to that activity and its conditions. It does not establish completion of the package or of the bank's wider PQC transition.

**Reference Manual**: 5.1–5.2; decision authority in 3.4 and payment release preparation in 7.3.

**5. IMPLEMENT AND RETIRE**

# Check protection and service behaviour in operation

Live operation provides evidence that testing cannot fully supply. Operations teams monitor the mechanisms actually used alongside performance, errors and customer outcomes. Successful transactions alone cannot establish the cryptography used at every relevant point, while ordinary traffic may leave standby and recovery paths unexamined.

Where a provider controls part of the service, the dependency owner obtains evidence for its deployed release and settings, with inspection limits recorded. Rollout remains within approved conditions; if a stopping condition is reached, operations carries out the agreed response.

### Understand what recovery restores

Rollback reverses a change to an earlier release or configuration. Fallback uses another mechanism or path. Either may support recovery, but reintroducing vulnerable cryptography creates exposure that needs assessment and a record of its duration. Service restoration and the protection provided by the restored state must both be understood.

### Payment case

During the production pilot, a reconnect fault causes accepted payment instructions to appear as not submitted. Operations stops submissions, reconciles the instructions and follows the authorised procedure to restore the earlier release. Correct payment handling is part of the acceptance criteria, so the fault requires action even though the new key-establishment mechanism is working.

The corrected release resolves the payment problem. A complete rebuild then restores a prohibited cryptographic setting. The rebuilt instance remains isolated while the setting is corrected and verified, extending recovery to 38 minutes against the 30-minute tolerance.

Failover between the gateways works, but the earlier release remains the only demonstrated complete-rebuild route meeting both payment and recovery requirements. The assigned operations approver permits the corrected release with that restricted, temporary recovery arrangement. The relevant provider and supplier contributions, monitoring and conditions remain explicit.

The bank has made useful progress in normal operation. The unresolved rebuild path prevents the package from meeting its completion criteria.

### Keep temporary recovery under control

A temporary recovery route is an operating state with its own exposure, limits and exit requirements. Emergency restoration does not provide open-ended permission to retain it. The estate owner coordinates the remaining work and any required departure decision, with withdrawal dependent on evidence that the earlier arrangement can be retired safely.

**Reference Manual**: 5.3 and 5.4; full payment incident and recovery findings in 7.3.

**5. IMPLEMENT AND RETIRE**

# Control coexistence and departures from the plan

Predecessor and replacement arrangements may coexist while migration is under way. The bank needs to know which uses remain, why they remain and what will end that reliance. Keeping these reasons and exit conditions visible helps ensure that temporary arrangements remain subject to active oversight.

| Description | Meaning | What it does not establish |
|---|---|---|
| Remaining work | All work still needed to reach the approved target. | That the work is overdue or a departure has been approved. |
| Transition debt | Unfinished transition work carried beyond an agreed date or event, or outside approved conditions. | That the exposure has been accepted or the commitment erased. |
| Exception | An authorised, bounded departure from an identified requirement or operating condition. | That protection has improved or an unmet completion criterion has been satisfied. |

These descriptions can apply together. A missed retirement date may create transition debt while an exception permits a temporary operating arrangement. The records retain both the original commitment and the authorised departure.

### Make the exception specific

An exception request explains the need, affected use, exposure, alternatives and safeguards, together with the accountable owner, proposed duration and credible exit plan. Permission specifies the response to failed conditions or expiry. The decision rests with an approver authorised to permit the departure; acceptance of risk cannot waive a binding obligation.

Evidence for interim measures establishes what they can and cannot achieve. Extra monitoring may help detect misuse or control operation, but cannot supply confidentiality missing from the cryptographic mechanism or reverse earlier capture of ciphertext.

Renewal requires a fresh decision. Expiry is a trigger for action, not evidence that the departure has ended. Unresolved exposure and overdue work remain visible until resolution is verified.

### Payment case

The corrected recovery image will miss the agreed 30 September 2027 withdrawal date. The chief risk officer permits a departure for 1–20 October; technology operations separately confirms operating permission. The missed withdrawal becomes transition debt on 1 October. The original commitment and protection limit remain recorded.

The departure allows defined temporary operation. Completion still depends on correcting and testing recovery, authorising retirement and verifying that the prohibited earlier use is unavailable within the agreed scope.

**Reference Manual**: 5.4; completion criteria in 5.6 and payment exception in 7.3.

**5. IMPLEMENT AND RETIRE**

# Retire earlier arrangements safely

Installing a replacement does not establish that the earlier arrangement has been retired. The bank needs evidence that prohibited selection or invocation is prevented across the relevant operating and recovery paths. An observation period with no old traffic is insufficient on its own.

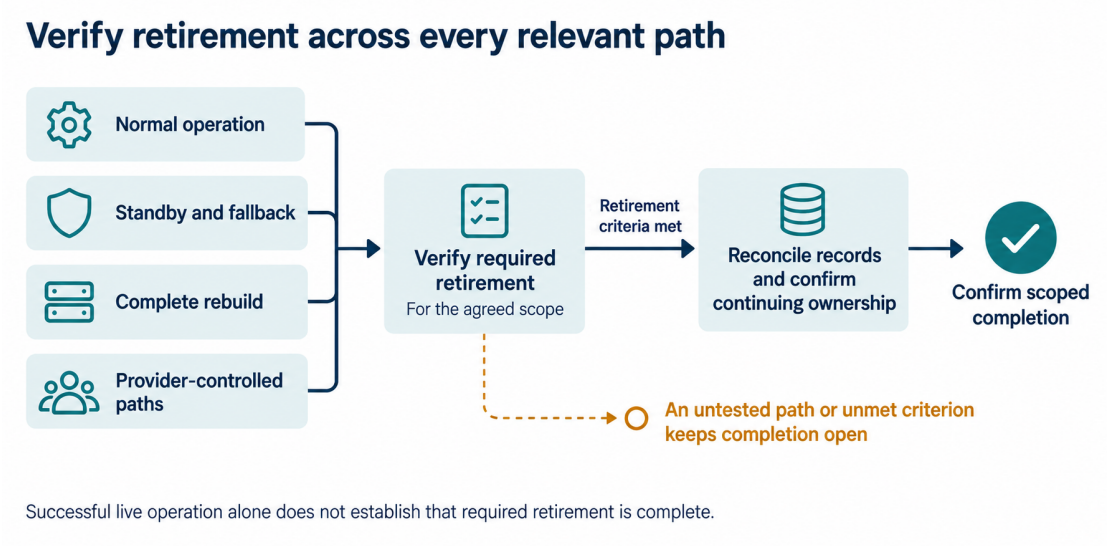



Figure 4. Completion draws on evidence across relevant paths. An unresolved required path keeps the package open, even where the replacement is working in normal operation.

## Establish the basis for withdrawal

Before retirement, responsible owners confirm that the replacement supports required service and recovery and that dependent parties are ready. Where the use itself is ending, continuing information and trust obligations still need coverage. The assigned approver authorises withdrawal. Deployment and retirement may share a record, but their permissions and evidence remain distinguishable.

Verification covers relevant standby settings, templates, inactive capabilities, fallback and recovery. A restored environment must reach the approved state before resuming the affected use. Provider-controlled paths also need evidence. A limitation that leaves a required path unverified prevents a retirement claim for that path.

## Preserve legitimate continuing uses

Retirement concerns the specified predecessor use. Historical decryption or signature verification may remain authorised under separate controls, although historical verification does not itself justify retaining private signing keys. Keys and material capable of regenerating them are destroyed when they have no remaining authorised purpose.

A conventional component retained within an approved hybrid construction is also distinct from the predecessor use being retired. A clearly defined target identifies what must become unavailable and what may legitimately remain, giving teams a consistent basis for withdrawal and verification.

**Reference Manual**: 5.5; completion and continuing ownership in 5.6.

**5. IMPLEMENT AND RETIRE**

# Confirm completion against the approved target

Completion is a decision about a defined scope and approved target. It brings together evidence of the protection and operating conditions achieved, including required retirement, and confirms that continuing owners can sustain the result.

The package owner assembles the results. Business and estate owners assess achievement against their requirements. Operations and dependency owners confirm the support arrangements. The assigned authority confirms completion through the bank's existing governance. A package may be complete while its estate remains in transition. A broader protection claim needs evidence across all relevant uses and dependencies.

### Reconcile the result with the records

The package owner coordinates reconciliation of the inventory, relevant CBOMs, dependencies, approvals and remaining-work records with the verified state. Continuing owners accept responsibility and confirm that the procedures, access, skills, resources and provider arrangements needed to manage it are in place. This handover preserves accountability after the delivery team closes its work.

An exception or administrative project closure cannot satisfy an unmet criterion. Where an authorised target revision is necessary, the record preserves the earlier target, reasons and decision so that the basis of the changed claim remains clear.

### Payment case

| Date in 2027 | Evidence or decision |
|---|---|
| 1 October | The missed withdrawal becomes debt; the time-limited departure begins. |
| 12 October | A corrected image has demonstrated a 26-minute rebuild. Retirement is separately authorised and verified across primary, standby, rebuild and provider paths. The debt and exception close. |
| 15 October | Records are reconciled and continuing ownership is accepted. The assigned authority confirms completion of the package. |

The package finishes later than its planned 1 October completion, but within the contingency and before the protection limit. Authentication migration remains open. Reporting therefore preserves each of these facts, making clear that completion of this package does not mean the whole payment service is fully migrated.

### The completion review

The completion review considers the target and uses in scope, current evidence for normal operation and recovery, and verification of required predecessor withdrawal. It also establishes what remains unresolved or separately assigned, and whether continuing owners have accepted responsibility with the support needed to fulfil it.

These considerations can be addressed within existing reviews. Together, they allow the bank to explain precisely what is complete and which obligations continue.

**Reference Manual**: 5.6 and the Implement and retire pillar review; payment completion in 7.3.

**6. MAINTAIN AND ADAPT**

# Keep knowledge and controls current

A completion decision reflects the scope and configuration assessed at that time. Software releases, provider changes, certificate events and recovery updates can alter the basis for that conclusion. Continuing owners need to recognise those changes and refresh the affected evidence.

### Keep the inventory connected to operation

The estate owner maintains the inventory and its links to outcomes, dependencies, decisions and outstanding work. This draws on business owners' information about changed protection or service needs and dependency owners' provider notices and evidence. Ownership transfers preserve access to the information and authority needed for ongoing control.

Configuration checks, operational observations and targeted discovery test whether records still match the deployed state, including fallback and recovery. Their depth and frequency reflect the consequences of error and pace of change. A changed collection method or inaccessible platform may itself create a blind spot that requires assessment.

Earlier results remain useful where their supporting conditions still apply. Changed conditions prompt the estate owner to identify conclusions requiring qualification or renewed testing. Missing evidence creates uncertainty; a test demonstrating prohibited behaviour establishes a failure. The response reflects this difference.

### Payment case

In November 2027, the processor replaces its standby endpoint. Normal operation continues to use the approved profile, but the earlier failover evidence does not cover the new endpoint. The bank records the gap, assesses continued operation and arranges a joint test within three working days. Retesting supports the changed endpoint.

The bank retains the October completion decision for the configuration assessed at that time and records the new conclusion for the replacement endpoint. This preserves the history of what was demonstrated while making the current evidence and operating state clear.

The review also finds that the maintenance notice did not clearly identify the changed endpoint or affected evidence. The dependency owner agrees more useful notices with the processor and later checks whether the improved handoff works.

### Follow correction through to a result

Each material gap or failure has an owner, response and due date. The responsible owners verify whether the response achieved its intended result and assess implications for other deployments, shared procedures or earlier approvals. The findings then inform management reporting and future designs.

**Reference Manual**: 6.1 and 6.3; payment endpoint change in 7.4.

### 6. MAINTAIN AND ADAPT

## Report what has been demonstrated

Management needs an account of protection achieved, remaining exposure, delivery progress and operating capability. These views answer different questions. Keeping them distinct helps decision-makers see where intervention is needed.

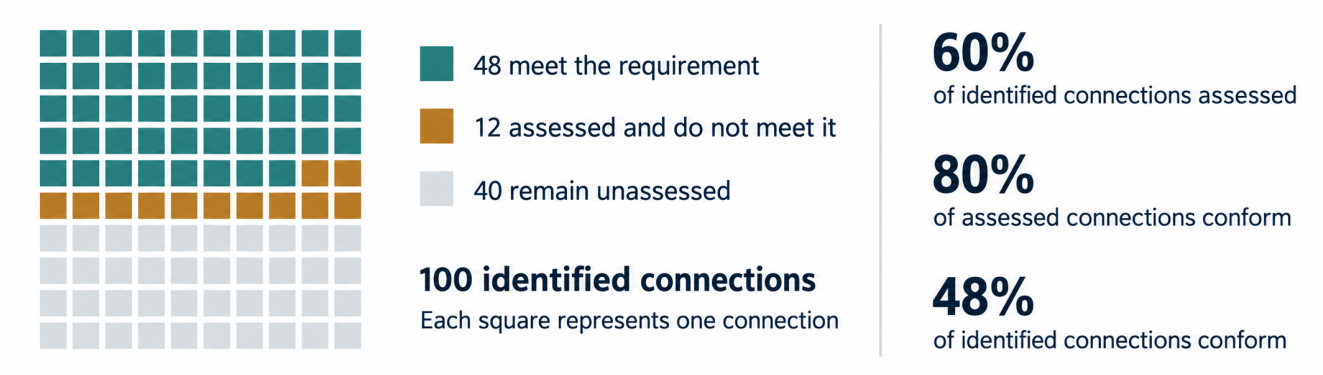



Figure 5. Illustrative reporting for 100 identified connections. Coverage and conformance use different denominators. These figures are neither QPI scores nor percentages of business risk removed.

In the example, 60 connections have sufficient current evidence. Of these, 48 meet the stated requirement and 12 do not. Forty remain unassessed. Reporting only "80% conformant" would conceal that just 48 of the 100 identified connections have been demonstrated to meet the requirement.

### Explain the population and its limits

Consistent counting units, dated populations and explicit definitions make the figures interpretable. Where the total population is unknown, reporting uses bounded counts or justified ranges and explains the blind spots. Newly discovered connections can change a percentage without showing deterioration in connections already assessed.

A useful report connects the figures to the services and dependencies they represent. Many completed minor changes cannot offset a shared dependency that prevents a critical service from meeting its target. Where intervention is needed, the report identifies the decision, its owner and the consequence of delay.

### Make capability claims specific

Reporting on cryptographic agility covers the further change assessed, its scope, elapsed time, staff effort, dependency delays, and protection, service and recovery results. It also identifies what remains unproven. A successful rehearsal in a replica environment supports a different conclusion from a completed production change.

The same underlying evidence may inform QPI responses. An approved plan, a demonstrated pilot and a controlled production result each support preparedness, but establish different things about protection. Reporting distinguishes these achievements so that each claim reflects the evidence available.

**Reference Manual**: 6.2 and 6.4; reporting definitions and the denominator example are in 6.2.

## 6. MAINTAIN AND ADAPT

# Demonstrate continuing cryptographic agility

Cryptographic agility means the demonstrated ability to organise and complete further cryptographic change within required protection, service and timing conditions. Replaceable components and flexible products help, but the capability also depends on decisions, people, providers, testing and recovery.

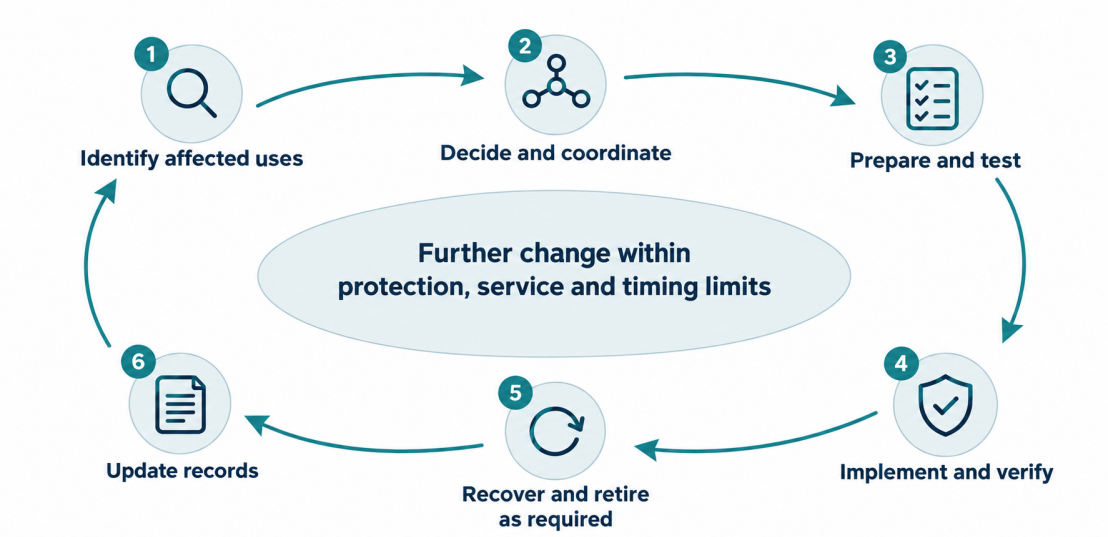



Figure 6. Agility covers the full change process. Elapsed time includes decisions and external waiting as well as technical work; staff effort is measured separately.

### Choose an exercise that tests a real need

Controlled exercises and suitable evidence from actual subsequent changes can demonstrate agility. Representative planned and urgent changes provide the basis for assessments with explicit scopes. Each assessment identifies the affected uses and intended result, with agreed permissions, stopping conditions, recovery and any required withdrawal of earlier arrangements. Discussion exercises test coordination; technical rehearsals establish behaviour under their tested conditions.

Elapsed time runs from the initiating event to the required result; staff effort, dependency waiting, and protection and service outcomes are measured alongside it. The record of the environment, mechanisms and scenarios covered defines the limits of the conclusion.

### Payment case

A controlled replica exercise changes the conventional component of the hybrid mechanism while retaining its post-quantum component. It covers both gateways, recovery, the shared hardware security module (HSM) interface and the provider test endpoint. The exercise finishes in nine working days against ten allowed, with correct payment reconciliation, a 27-minute rebuild and verified withdrawal of the former profile.

Production execution, replacement of the post-quantum component, authentication migration and an unplanned emergency change remain unproven. These limits help owners select the next exercise or improvement. The value lies in a repeatable, evidenced capability with a clear scope.

**Reference Manual**: 6.4 and the Maintain and adapt pillar review; full exercise and limitations in 7.4.

**7. APPLYING PACT ACROSS THE BANK**

# Adapt the approach and act on new findings

PACT can be applied in proportion to a bank's size, complexity, starting position and dependencies. Responsibilities may be combined where authority, capacity and required independence permit. The arrangement still needs identifiable owners, usable evidence and decisions made by the appropriate authority.

A smaller programme may use linked registers and existing change records. A larger institution may connect inventory, risk and portfolio systems. Both need to preserve the relationships between protection needs, uses, dependencies, commitments and results.

### Reassess when the basis changes

Review may be needed between scheduled assessments when material operating findings emerge or when supplier estimates, standards, threats, resources or protection needs change. Responsible owners identify the affected conclusions and decisions to revisit. The transition manager coordinates effects across estates, while the relevant teams implement and verify the response.

PACT recommends reviewing quantum-threat assumptions at least annually and earlier after credible material developments. Estate owners recalculate relevant completion limits and required start dates from approved assumptions and current migration estimates, retaining earlier assumptions and commitments.

In the payment case, a longer supplier estimate increases the estimated remaining duration of authentication migration from 18 to 21 months. With three months of contingency and the same 1 January 2030 completion target, the required start moves from 1 April to 1 January 2028. The earlier start is a planning consequence of the changed estimate; it does not alter the protection target.

### Make each review lead to action

Four questions give each review a common focus:

- What is being considered?
- What does the evidence establish?
- What remains unresolved?
- What action or decision follows?

Their application depends on the issue in scope, whether it concerns discovery, design, deployment, retirement or a further change.

Each resulting action has an owner, a clear purpose and a date or trigger for follow-up. Where a contribution is unavailable or timing is infeasible, the consequences remain visible in the plan as responsible owners pursue a response and other authorised work continues.

Across the bank, this discipline makes preparedness more sustainable. It maintains the knowledge and accountability needed to protect services today and to change cryptography again as conditions develop.

**Reference Manual**: 2.3, 6.3, 6.4 and 8; authentication timing reassessment in 7.4.

## 8. WORKING TERMINOLOGY

# Terms used in this Guide

These explanations support reading. The Reference Manual provides the complete definitions and qualifications.

| Term | Meaning |
|---|---|
| Protected outcome | The result to preserve for a service, information, critical operation or obligation, judged against protection and operating requirements. |
| Cryptographic use | A particular cryptographic function in an identifiable context, such as authenticating a gateway or establishing a connection secret. |
| Cryptographic estate | A defined scope of uses managed by one accountable owner, including relevant standby, recovery and inactive capabilities. |
| Cryptographic inventory | Records connecting uses and deployments with outcomes, owners, dependencies and supporting evidence. |
| CBOM | A cryptographic bill of materials describing assets and dependencies within a stated product, release or deployment scope. |
| Dependency | Reliance on a component, service or party for protection, operation or completion of a change. |
| Change package | A defined set of transition work with a delivery owner, including testing, implementation, recovery and required retirement. |
| Interface profile | The protocols, mechanisms, parameters, certificates, trust settings and operating rules agreed for compatible connections. |
| Hybrid cryptography | A construction in which conventional and post-quantum mechanisms contribute jointly to the same cryptographic operation. |
| Fallback and rollback | Fallback selects another mechanism or path. Rollback reverses a change to an earlier state. Both can alter exposure. |
| Transition debt | Unfinished transition work carried beyond an agreed date or event, or outside approved conditions, with the original commitment and consequences retained. |
| Exception | An authorised departure from a requirement or operating condition, limited by scope, duration and conditions. It cannot waive binding obligations. |
| Retirement | Verified withdrawal of a predecessor arrangement for the specified use, including relevant alternative and recovery paths. |
| Cryptographic agility | The demonstrated ability to organise and complete further cryptographic change within required protection, service and timing conditions. |

PQC means post-quantum cryptography. QPI means Quantum Preparedness Index. HSM means hardware security module. A digital certificate links a public key to an identity through an issuer's signature; its role is distinct from the use of the corresponding private key.

**Reference Manual**: Appendix A provides the full glossary; Appendix B provides the technical primer.

## 9. REFERENCE MANUAL NAVIGATION

# Governance and planning workstreams

The Guide follows the four pillars and groups its explanations around practical decisions. The following map links those decisions to all 23 workstreams in the Reference Manual, where the complete criteria, responsibilities and technical detail are set out.

| Pillar | Workstream | Manual | Guide pages |
|---|---|---|---|
| Govern the transition | Establish executive leadership and transition coordination | 3.1 | 9 |
| | Establish the mandate, scope and goals | 3.2 | 9 |
| | Assign accountable ownership | 3.3 | 9 |
| | Establish decision authority and independent control | 3.4 | 9 |
| | Set common policy and architecture requirements | 3.5 | 10 |
| | Secure resources and demonstrate capability | 3.6 | 10 |
| Assess and plan | Establish the current cryptographic position | 4.1 | 11 |
| | Establish dependency requirements and readiness | 4.2 | 12 |
| | Assess exposure, migration constraints and timing | 4.3 | 13 |
| | Select the migration approach and proposed target state | 4.4 | 14 |
| | Test design feasibility and suitability | 4.5 | 15 |
| | Approve the design and interface profiles | 4.6 | 15 |
| | Agree the integrated transition roadmap | 4.7 | 16 |

### Context and starting points

Manual Section 1 explains the purpose and banking context. Section 2 sets out the governing principles, core concepts, four pillars, operating levels and information flows. Sections 3 and 4 end with reviews that help interpret evidence and identify the next decision for the work being considered.

For a bank starting with limited visibility, Sections 4.1, 4.7 and 8 explain how investigation, prerequisite work and supported implementation can proceed in parallel. This allows useful progress while wider coverage gaps remain explicit.

## 9. REFERENCE MANUAL NAVIGATION

# Implementation and continuing capability

| Pillar | Workstream | Manual | Guide pages |
|---|---|---|---|
| Implement and retire | Prepare the change package | 5.1 | 17 |
| | Establish readiness and authorise the proposed action | 5.2 | 17 |
| | Deploy and establish controlled operation | 5.3 | 18 |
| | Control coexistence, remaining work and exceptions | 5.4 | 18-19 |
| | Retire predecessor arrangements | 5.5 | 20 |
| | Verify completion and establish continuing ownership | 5.6 | 19-21 |
| Maintain and adapt | Maintain current knowledge and effective controls | 6.1 | 22 |
| | Measure protection, exposure, progress and capability | 6.2 | 23 |
| | Review findings and adapt decisions and arrangements | 6.3 | 22 |
| | Demonstrate continuing cryptographic agility | 6.4 | 23-24 |

### Follow the full payment case

Manual Section 7 develops the hypothetical payment example across all four pillars. It provides the detailed configurations, test conditions, responsibilities, dates and decision limits behind the simplified narrative in this Guide. Its results illustrate the framework; they are not benchmarks for a bank's own recovery or migration performance.

### Tailoring and technical detail

Manual Section 8 explains adoption and proportionate application, including the use of existing arrangements and the limits of the framework. Appendix A contains terminology and abbreviations. Appendix B explains cryptographic functions, standards and implementation considerations. Appendix C compares selected jurisdictional approaches and milestones.

Current authoritative publications remain the basis for technical and jurisdictional decisions. The Manual specifies PACT, while external requirements retain their own scope and authority. Applying the framework does not itself establish regulatory compliance or cryptographic security.

**SOURCES**

# Framework and HKMA publications

[1] Huang, Allen H.; Fung, Terrance; Jin, Bruce; and Papadopoulos, Dimitrios. (November 2026). *PQC Accountability and Controlled Transition: A post-quantum cryptography transition framework for the banking industry. Reference Manual. HKUST Business School.*

[2] Hong Kong Monetary Authority. (July 2026). *Quantum Preparedness of Hong Kong's Banking Sector. Whitepaper.*

[3] Hong Kong Monetary Authority. (27 July 2026). *HKMA launches quantum preparedness whitepaper and index to support banking sector's readiness for quantum era. Press release.*

[4] Hong Kong Monetary Authority. (27 July 2026). *Results of Quantum Preparedness Index Survey. Circular B1/15C.*

[5] Chu, Carmen. (27 July 2026). *Opening Remarks at FiNETech8 on "Navigating Quantum Duality". Hong Kong Monetary Authority.*

[6] Hong Kong Monetary Authority. (31 May 2022). *Supervisory Policy Manual OR-2 Operational Resilience.*