2027 臺灣金融及關鍵產業 PQC 遷移實務白皮書

從 CBOM 盤點到加密敏捷性部署

2027 Taiwan PQC Migration White Paper

for the Financial and Critical Infrastructure Sectors

From CBOM Inventory to Crypto-Agility Deployment

發行單位

財團法人資訊工業策進會

編撰單位

財團法人資訊工業策進會

國立政治大學資訊安全科技研究中心

普鴻資訊股份有限公司

版次與日期：第 1.0 版，中華民國 115 年 11 月

版權頁

書名：2027 臺灣金融及關鍵產業 PQC 遷移實務白皮書：從 CBOM 盤點到加密敏捷性部署

英文書名：2027 Taiwan PQC Migration White Paper for the Financial and Critical Infrastructure Sectors: From CBOM Inventory to Crypto-Agility Deployment

發行單位：財團法人資訊工業策進會

編撰單位：

財團法人資訊工業策進會

國立政治大學資訊安全科技研究中心

普鴻資訊股份有限公司

審閱與指導委員（依姓氏筆畫排序）：

左瑞麟　國立政治大學資訊科學系特聘教授

李榮三　逢甲大學資訊工程學系特聘教授

林群國　普鴻資訊股份有限公司董事長

版次與日期：第 1.0 版，中華民國 115 年 11 月

資料基準日：本白皮書所引用之標準、法規、政策及產品資訊，資料查核截至中華民國 115 年 10 月 23 日。

著作權與免責聲明

一、參考用途說明

本白皮書係依編撰期間可取得之公開資料、相關標準、法規及產業實務資訊彙整而成，旨在提供金融及關鍵基礎設施相關機構推動後量子密碼（PQC）遷移之實務參考，並不構成任何法律、法規遵循、資訊安全、技術採購或投資之正式建議。

二、技術與政策時效性

後量子密碼相關技術、國際標準（如 NIST FIPS）、主管機關政策、法規要求及產品生態系仍持續快速發展與更新，本白皮書所載內容可能因時間及外部環境變化而有所調整。各機構於規劃及執行實際遷移作業時，應以主管機關最新公布之正式文件、適用標準及相關規範為依據，並考量自身業務特性、資訊系統架構及風險承受能力，進行適切之評估與決策。

三、免責條款

本白皮書之發行單位及編撰單位已盡力確保內容之正確性與完整性，惟不保證所有資訊均無錯誤、遺漏或已涵蓋最新發展，亦不對任何機構或個人因引用、解讀或使用本白皮書內容所採取之任何決策及其衍生之結果（包括但不限於營運中斷、系統變更風險或財務損失）負擔法律責任。

四、著作權與授權

本白皮書著作權為編撰單位共有。歡迎各界基於非商業目的引用或推廣，引用時請註明出處並保持內容完整性；未經書面授權，不得進行商業性重製、轉載、改作或銷售。

建議引用格式

財團法人資訊工業策進會、國立政治大學資訊安全科技研究中心、普鴻資訊股份有限公司（2026）。《2027 臺灣金融及關鍵產業 PQC 遷移實務白皮書：從 CBOM 盤點到加密敏捷性部署》（第 1.0 版）。財團法人資訊工業策進會。

Institute for Information Industry, Information Security Center of National Chengchi University, & Provision Information Co., Ltd. (2026). *2027 Taiwan PQC Migration White Paper for the Financial and Critical Infrastructure Sectors: From CBOM Inventory to Crypto-Agility Deployment* (Version 1.0). Institute for Information Industry.

序

過去數位簽章與密碼學演算法支撐著網路銀行、跨境支付、電子簽章與關鍵基礎設施通訊的安全，然而量子運算的發展，使得目前常用的金鑰與密碼在未來面臨被破解的挑戰，攻擊者現在就可以先攔截加密資料，待日後量子運算成熟再行解密（Harvest Now, Decrypt Later）。金融業與關鍵基礎設施的資料生命週期極長，將會首當其衝。

1991 年我開始投入資訊安全研究，過去談到後量子密碼演算法，常被認為言之過早。如今美國國家標準暨技術研究院（NIST）已於 2024 年發布首批後量子密碼演算法標準，國際與金融領域專家小組（如 G7、SWIFT、X9 等）陸續提出後量子密碼遷移藍圖，我國數位發展部與金融監督管理委員會也發布了相關政策與指引。後量子密碼遷移已經從研究議題，成為金融與關鍵基礎設施相關機構必須納入治理與營運規劃的實務工作。

過去企業多為當下專案功能需求而建置內部系統，未考量加密敏捷性，加密與簽章機制亦未釐清實質需求。因此，企業應把握此次後量子密碼遷移的契機，採用「精準遷移」策略，重新檢視現行加密及數位簽章機制的使用需求，評估既有的密碼技術是否適切運用於實際場景，避免不必要的技術部署與資源投入，才能有效降低大規模遷移的複雜度與成本。

本白皮書因此以 CBOM 盤點與風險評估作為起點，再說明雙軌過渡與加密敏捷性架構的設計。透過加密服務中台、金鑰與憑證集中管理，未來演算法更新可以盡量以調整組態完成，不必大幅修改應用系統。

後量子密碼遷移也無法由單一機構獨力完成。以金融領域為例，金融

機構需要與財金公司、聯卡中心、SWIFT 等共用平台，以及 HSM、CA 與系統供應商同步測試、協調時程，才能確保跨機構交易在過渡期間正常運作。白皮書最後一章即針對生態系協作，提出分層盤點與跨機構協調的做法。

資策會於 114 年即與後量子資安產業聯盟發布《後量子密碼遷移指引》，本白皮書在此基礎上，進一步聚焦金融業與關鍵產業的實務作法。本白皮書由資策會、國立政治大學資訊安全科技研究中心及普鴻資訊股份有限公司共同編撰，並承蒙國立政治大學左瑞麟特聘教授、逢甲大學李榮三特聘教授審閱指正，以及普鴻資訊股份有限公司林群國董事長提供指導，在此一併致謝。期盼本白皮書能為金融機構與關鍵基礎設施營運者提供實用的參考，共同為臺灣建立能因應量子威脅的數位信任環境。

財團法人資訊工業策進會

執行長　范俊逸　謹識

中華民國 115 年 11 月

目 錄

第一章 量子威脅與全球／臺灣 PQC 政策藍圖 1

一、HNDL 威脅與金融、關鍵基礎設施提早部署 PQC 的必要性 2

（一）量子運算發展帶來的密碼安全挑戰 2

（二）運用 Mosca 不等式評估遷移急迫性 3

（三）金融業與關鍵基礎設施為何需要提早部署 4

二、NIST 後量子密碼標準與 SWIFT 相關遷移規劃（2026–2029 年） .. 6

（一）NIST 已發布的三項 PQC 標準 6

（二）從密碼資產盤點到分階段遷移 7

（三）SWIFT 的 PQC 發展與 2026–2029 年規劃方式 9

三、臺灣數位發展部政策與金管會金融業指引 12

（一）數位發展部推動 PQC 遷移的政策方向 12

（二）金管會金融業後量子密碼遷移參考指引 13

（三）從政策指引走向組織落實 15

第二章 NIST PQC 演算法理論與加密敏捷性（Crypto-Agility）模型 17

一、新一代 PQC 標準演算法剖析：ML-KEM 與 ML-DSA 之數學原理與安全強度 18

（一）金鑰建立、資料保護與數位簽章 18

（二）晶格與帶誤差問題的直覺 19

（三）ML-KEM 如何建立共享秘密 21

（四）ML-DSA 如何簽署及驗證訊息 22

（五）安全類別與參數選擇 23

二、傳統密碼與 PQC 之效能與資源對比：RSA/ECC vs. PQC 長度、大小及延遲分析 25

（一）先對齊功能與資料表示 25
（二）公鑰、私鑰與簽章大小 25
（三）運算效能與工作負載 27
（四）記憶體、金鑰設備與網路成本 29
（五）金融場景與 PoC 驗收 31
三、加密敏捷性（Crypto-Agility）架構：不更換底層系統下的演算法動態抽換 33
（一）以可更新的密碼介面降低改造成本 33
（二）Hybrid 與雙軌共存 34
（三）金鑰與信任生命週期 35
（四）設備、軟體與合作方共同驗證 36
（五）受控切換與安全復原 37
（六）以可量測成果推進導入 38
第三章 PQC 遷移第一步：CBOM 盤點與風險評估方法論 41
一、密碼技術資產清冊（CBOM）的核心價值 42
（一）CBOM 是什麼 42
（二）CBOM 對金融業的重要性 42
（三）CBOM 的核心價值 43
二、密碼技術資產盤點流程與管理機制 45
（一）CBOM 加密清單的資產類型 45
（二）CBOM 的盤點原則 45
（三）盤點流程及步驟 46
（四）密碼技術資產盤點工具 51
三、風險評估與系統遷移優先順序規劃 56

（一）先做脆弱標記，再做評分 56
（二）量子風險評分（QR） 56
（三）遷移難度（MT）評分 58
（四）優先順序矩陣 60
四、CBOM 盤點工具及管理系統整合實務 62
（一）盤點工具與 CBOM 管理系統應具備功能 62
（二）CBOM 管理系統整合架構 63
（三）金融機構對 CBOM 整合實務需求 65
第四章 雙軌平滑遷移與加密敏捷性架構設計 67
一、雙軌模式（Hybrid Mode）設計理念與架構 68
（一）為什麼需要雙軌而非直接切換 68
（二）設計理念 69
（三）架構分層 69
（四）常見 Hybrid 組合方式 70
二、加密敏捷性平滑升級規劃與實務 73
（一）加密敏捷性的核心價值 73
（二）加密敏捷性的五大核心設計原則 74
（三）加密敏捷性架構設計及規劃 75
三、硬體安全模組（HSM）與作業系統強化（OS Hardening）實踐 79
（一）HSM 在 PQC 遷移中的角色 79
（二）PQC 遷移中 HSM 應具備的關鍵能力 82
（三）HSM 遷移實務注意事項 83
（四）作業系統強化（OS Hardening）實踐要點 84
第五章 實施部署與持續維運作業 87

一、實施與部署各階段流程及作業 88
（一）實施與部署整體流程 88
（二）實施與部署執行原則 88
二、軟體（演算法）、硬體（HSM）與基礎設施升級 90
（一）演算法升級（軟體層） 90
（二）硬體（HSM）與基礎設施升級 91
（三）系統整合與部署 92
（四）準備與 Pilot 測試 92
（五）驗證、監控與優化 93
（六）逐步移轉至 Pure PQC 93
三、全面轉型與持續維運 95
（一）從 Hybrid 逐步轉為 Pure PQC，完成全組織轉型 95
（二）建立持續監控儀表板，自動偵測新的脆弱演算法 95
（三）定期執行 re-inventory、訓練與演練 95
（四）設計模組化 Crypto API，讓未來演算法替換不需調整應用系統 96
（五）制定 Rollback 計畫與應急程序，確保業務連續性 96
（六）將 PDCA（Plan-Do-Check-Act）循環制度化 97
四、生態系成員協作與標準法規配合 98
（一）跨組織協作的必要性 98
（二）Hub-and-Spoke 與四階呈現 98
（三）跨機構協調與標準法規對齊 99
參考文獻 101

表目錄

表 2-1 NIST 安全類別 23
表 2-2 ML-KEM 物件大小 25
表 2-3 ML-DSA 物件大小 26
表 2-4 傳統簽章的大小基準 26
表 2-5 簽署與驗證時間 27
表 2-6 金鑰建立操作時間 28
表 2-7 金融 PoC 量測重點 31
表 2-8 架構中的可替換條件 34
表 2-9 金鑰與信任的遷移作業 35
表 2-10 端到端互通與故障測試 36
表 2-11 敏捷性驗收與觀測 39
表 3-1 金融業 CBOM 特性 42
表 3-2 CBOM 盤點原則-多來源蒐集 47
表 3-3 結構化建檔-基本欄位 48
表 3-4 結構化建檔-風險評估加值欄位 49
表 3-5 CBOM 管理機制 50
表 3-6 CBOM 管理權責 51
表 3-7 盤點工具涵蓋層面 52
表 3-8 盤點工具類型 54
表 3-9 盤點內容類型 54
表 3-10 脆弱標記 56
表 3-11 量子風險評級 57
表 3-12 量子風險評級 QR 值 57

表 3-13　遷移難度評分 59
表 3-14　遷移難度評分 MT 值 59
表 3-15　盤點工具與 CBOM 管理系統應具備功能 62
表 4-1　雙軌模式設計理念 69
表 4-2　軌模式架構分層 69
表 4-3　常見 Hybrid 組合方式 70
表 4-4　加密敏捷性的五大核心設計原則 74
表 4-5　開發與 DevOps 層 77
表 4-6　HSM 在密碼體系中的基本角色 79
表 4-7　HSM 對金融業的重要性 82
表 5-1　生態系盤點與遷移工作分層 98

圖目錄

圖 2-1 金融服務的密碼分工.....19
圖 2-2 誤差如何改變公開關係.....20
圖 2-3 ML-KEM 的公開交換與本地運算.....21
圖 2-4 ML-DSA 的簽署與驗證.....22
圖 2-5 金融服務的三種量測範圍.....30
圖 2-6 加密敏捷性的職責與相依.....33
圖 2-7 受控切換與安全復原.....38
圖 3-1 優先順序矩陣.....61
圖 3-2 CBOM 資產整合架構圖.....64
圖 4-1 混合式金鑰作業流程圖.....71
圖 4-2 加密敏捷性架構圖.....75
圖 5-1 全面轉型與持續維運.....97

第一章 量子威脅與全球／臺灣 PQC 政策藍圖

前言

公開金鑰密碼是當前數位信任的基石，從網路銀行、跨境支付、電子簽章到關鍵基礎設施的通訊防護，都仰賴 RSA 與 ECC 等演算法維繫安全。然而，量子運算的發展正逐步動搖這項基礎。一旦具備足夠規模且可容錯運作的量子電腦問世，現行公開金鑰機制將面臨遭到破解的風險。攻擊者若採取「先攔截、日後解密」（HNDL）模式，更可能使今日傳輸的機敏資料在多年後遭到揭露，因此量子威脅已是當下就必須面對的課題。

NIST 於 2024 年 8 月發布首批後量子密碼標準，並在 NIST IR 8547 草案中規劃量子脆弱演算法的退場時程。SWIFT、G7 Cyber Expert Group，以及我國數位發展部與金管會也陸續提出遷移時程與指引。後量子密碼（PQC）遷移已從技術研究議題，轉為組織治理與營運規劃的實務工作。

本章首先說明 HNDL 威脅的本質，並以 Mosca 不等式闡述金融業與關鍵基礎設施提早部署的必要性。其次整理 NIST 已發布的 PQC 標準，說明從密碼資產盤點到分階段遷移的方法，並探討 SWIFT 時程與金融機構 2026 至 2029 年的規劃窗口。最後介紹數位發展部的政策方向，以及金管會《金融業後量子密碼遷移參考指引》的重點與實務推動環節，期能為國內金融機構與關鍵基礎設施營運者，提供兼顧國際趨勢與本土需求的遷移參考。

一、HNDL 威脅與金融、關鍵基礎設施提早部署 PQC 的必要性

（一）量子運算發展帶來的密碼安全挑戰

隨著量子運算技術持續發展，現行密碼學所依賴的安全假設正面臨新的挑戰。當前網路通訊、數位身分驗證、電子簽章、金融交易與關鍵基礎設施的安全機制，大量仰賴 RSA、橢圓曲線密碼學（Elliptic Curve Cryptography, ECC）等公開金鑰密碼演算法。這些演算法在傳統運算環境下具有良好的安全性，但若未來具備足夠運算能力的量子電腦問世，Shor 演算法可能使特定整數分解與離散對數問題的求解效率大幅提升，進而威脅現行公開金鑰密碼機制的安全基礎。

量子運算的影響不只存在於未來，也可能透過「先攔截、日後解密」（Harvest Now, Decrypt Later, HNDL）模式提前形成風險。攻擊者可以在當下蒐集並保存經加密的網路通訊、商業文件、金融資料或其他敏感資訊，等待未來量子運算能力成熟後，再嘗試解密先前取得的資料。這代表即使組織目前尚未遭遇可實際破解現行密碼的量子攻擊，其長期機密性仍可能已受到威脅。

HNDL 對具有長期保密需求的資料尤其值得關注。例如，金融機構的客戶個資、交易紀錄、授信資料及企業併購資訊，政府與關鍵基礎設施所持有的機敏資訊，以及涉及國家安全、智慧財產或長期營運策略的文件，都可能具有多年甚至數十年的保護需求。若這些資料在今日遭到攔截並被長期保存，未來即使完成密碼系統升級，也不代表先前被蒐集的資料就能重新獲得保護。

因此，後量子密碼（Post-Quantum Cryptography, PQC）的推動不應僅被視為因應未來量子電腦的技術升級，而應納入組織整體資安治理、資訊資產管理、風險評估及營運持續規劃。NIST 已於 2024 年 8 月發布首批後量子密碼標準，並在 NIST IR 8547 草案中建議 112 位元安全強度的 RSA 與 ECC 參數自 2030 年起棄用，所有量子脆弱的公開金鑰演算法於 2035 年後禁用。標準與退場時程都已具體化，組織盤點及規劃轉型已有明確依據。

（二）運用 Mosca 不等式評估遷移急迫性

在規劃 PQC 遷移時，組織可參考 Mosca 不等式的概念，評估現行密碼系統是否可能在其保護需求結束之前遭遇量子威脅。其基本表示方式為：X + Y > Z。其中，X 代表目前仍需保密或維持安全的時間，Y 代表組織完成密碼系統遷移所需的時間，Z 則代表具備相關破解能力的量子電腦可能出現前的預估時間。

當 X + Y > Z 時，表示資料所需的保護期間與系統遷移時間合計，可能超過組織可安全等待的時間，應提高遷移優先順序。這項不等式並非用來精確預測量子電腦何時具備實際破解能力，而是協助組織將資料保密年限、系統改造週期與未來威脅的不確定性納入同一套風險評估架構。

例如，若某類金融資料必須保密十五年，而相關系統的盤點、採購、測試、驗證及全面部署可能需要數年，組織便不宜僅因目前尚未出現可實際破解 RSA 或 ECC 的量子電腦，就延後所有準備工作。相反地，應先辨識哪些資料具有長期保密需求、哪些系統依賴容易受到量子運算影響的密碼機制，再依風險與遷移成本安排工作順序。

（三）金融業與關鍵基礎設施為何需要提早部署

金融業高度仰賴數位信任機制。網路銀行、跨境支付、金融訊息交換、數位憑證、電子簽章、身分驗證及系統間的加密通訊，都可能涉及公開金鑰密碼技術。若相關密碼機制遭到破解，不僅可能影響資料機密性，也可能對身分驗證、交易完整性、數位簽章可信度及相關信任機制造成衝擊。

金融系統的遷移工作也具有高度複雜性。銀行、支付服務業者、金融基礎設施、軟體供應商及跨境金融網路彼此連結，單一機構即使完成自身系統升級，仍可能因交易對手或第三方服務尚未具備相容能力，而面臨互通性與營運持續風險。因此，金融業的 PQC 遷移不能僅以替換密碼演算法為目標，而應同時考量交易流程、系統介接、憑證管理、供應鏈依賴及服務不中斷等要求。

關鍵基礎設施則具有另一項特性：系統生命週期通常較長，部分工業控制系統、網路設備及專用設備不易頻繁更新，且升級時必須考量可用性、穩定性與安全性之間的平衡。若相關設備或系統使用難以替換的密碼元件，遷移可能需要經過採購、相容性測試、停機安排及重新驗證等程序。這使得提早建立密碼資產清冊、辨識高風險系統與規劃替換週期格外重要。

面對上述挑戰，金融業與關鍵基礎設施可優先採取四項措施：第一，盤點公開金鑰密碼、憑證、金鑰管理及相關協定的使用情形；第二，辨識具有長期保密需求或涉及重要營運功能的資訊資產；第三，評估設備、應用程式、雲端服務與外部供應商的遷移能力；第四，將 PQC 納入資安治理、採購規範、系統更新及營運持續計畫。這些工作可以降低未來集中遷

移的壓力，也能讓組織在標準與產品逐步成熟時，更有能力做出安全且可持續的技術選擇。

二、NIST 後量子密碼標準、SWIFT 時程與金融業遷移規劃（2026–2029 年）

（一）NIST 已發布的三項 PQC 標準

後量子密碼遷移的核心工作之一，是依據成熟、經過評估且具備標準依據的演算法，逐步調整現行密碼系統。美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）於 2024 年 8 月 13 日正式發布三項後量子密碼聯邦資訊處理標準（Federal Information Processing Standards, FIPS），分別涵蓋金鑰建立與數位簽章用途，為各界推動 PQC 遷移提供了重要基礎。三項標準的主要用途如下：

1.FIPS 203：ML-KEM（金鑰封裝機制）

ML-KEM 全名為 Module-Lattice-Based Key-Encapsulation Mechanism，源自 CRYSTALS-KYBER。其主要用途是讓通訊雙方透過公開通道建立共享的秘密金鑰，供後續加密通訊使用。它是傳統公開金鑰建立機制的重要後量子替代方案。

2.FIPS 204：ML-DSA（數位簽章）

ML-DSA 全名為 Module-Lattice-Based Digital Signature Algorithm，源自 CRYSTALS-Dilithium。數位簽章可用於驗證簽署者身分，以及偵測資料是否遭到未授權修改。未來在電子簽章、軟體更新驗證、憑證及其他需要數位信任的應用中，均可能涉及相關演算法的導入。

3.FIPS 205：SLH-DSA（無狀態雜湊式數位簽章）

SLH-DSA 全名為 Stateless Hash-Based Digital Signature Algorithm，源自 SPHINCS+。此標準採用雜湊函數為基礎的簽章設計，提供不同於晶格密碼的另一種技術路徑，有助於組織在規劃數位簽章遷移時，依實際需求評估演算法選擇。

除上述三項標準外，NIST 亦持續推進其他候選演算法的標準化工作。例如，NIST 於 2025 年 3 月選定 HQC 作為 ML-KEM 的備援金鑰封裝機制，預計 2027 年完成標準制定；源自 FALCON 的 FN-DSA（預定編號 FIPS 206）也在標準制定程序中。這些進展顯示，PQC 標準與產品生態系仍在演進，組織應持續關注正式標準、實作成熟度與相容性驗證結果，而不宜僅依據單一產品的宣稱就決定全面替換方案。

需要特別注意的是，PQC 並不是單純將舊演算法替換成新演算法。不同演算法在金鑰及簽章大小、運算負載、通訊封包、設備資源需求與協定相容性方面可能存在差異。因此，組織在選擇技術方案時，應同時評估安全需求、系統效能、既有通訊協定、憑證基礎設施及供應商支援能力，並透過測試環境驗證實際運作情境。

（二）從密碼資產盤點到分階段遷移

NIST 國家網路安全卓越中心（NCCoE）的 PQC 遷移計畫（NIST SP 1800-38 系列）強調，組織應先了解自身使用密碼技術的範圍，再規劃風險排序與遷移工作。若組織無法掌握哪些系統使用 RSA、ECC 或其他容易受到量子運算威脅的機制，就難以合理判斷遷移範圍、資源需求與執行順序。因此，遷移工作可依下列階段推進：

第一階段：建立密碼資產清冊

盤點應涵蓋應用系統、資料庫、網路設備、憑證與公私鑰、金鑰管理系統、加密協定、第三方服務及相關軟硬體產品。組織可進一步建立密碼技術資產清冊（Cryptography Bill of Materials, CBOM），記錄密碼演算法、用途、版本、部署位置、資料敏感程度及供應商資訊。CBOM 的價值不只是提供一份清單，更在於建立可持續更新的密碼資產可視性。

第二階段：進行風險分級

應綜合考量資料保密年限、系統重要性、外部曝露程度、密碼機制用途、設備更新難度及供應商遷移能力。對長期機密資料、重要身分驗證機制、核心金融交易與關鍵基礎設施系統，應優先評估遷移需求。

第三階段：進行概念驗證與互通性測試

在正式部署前，應於受控環境中驗證演算法實作、通訊協定、系統效能、憑證與金鑰管理、日誌監控及故障復原能力。對高度互聯的金融服務而言，還應確認不同廠牌、不同系統版本及外部交易對手之間的相容性。

第四階段：分階段部署並持續監控

優先從可控的測試環境或高風險系統開始，逐步擴大導入範圍；在遷移過程中，應保留必要的回復機制，並持續監控安全性、效能與

營運影響。

組織也應建立加密敏捷性（Cryptographic Agility），讓未來演算法、參數或標準發生變動時，可以在不大幅重建整體系統的情況下完成調整。

（三）SWIFT 的 PQC 發展與 2026–2029 年規劃方式

對金融機構而言，SWIFT 是跨境金融訊息交換與支付生態系的重要一環，其密碼安全時程會直接牽動銀行與相關服務提供者的遷移排程。SWIFT 已公布具體的 PQC 時程：Alliance Release 7.9 以技術更新及 SwiftNet Release 8.0 與 PQC 整備為重點；Release 8.0 為支援 PQC 的強制性主要版本，預定 2027 年 7 月底推出；Release 7.7 無法直接升級至 8.0，多數會員機構須先部署 7.9，而 7.9 的支援將於 8.0 推出後 15 個月終止。金管會指引另記載，SWIFT 規劃自 2025 年啟動 PQC 遷移準備，以 2030 年完成轉換並終止 RSA 架構支援為目標，策略上逐步導入混合式密碼機制。

必須區分的是 SWIFT 的訊息格式遷移與 PQC 遷移。SWIFT 公開的 CBPR+ 路線圖處理 ISO 20022 金融訊息標準及 MT 報文退場的實施安排，與 PQC 無關，不能作為 PQC 時程的依據。本章以 2026–2029 年作為金融機構的 PQC 規劃窗口，依據是金管會指引建議的「準備與規劃（2026–2027）」及「試辦與基礎升級（2027–2029）」兩個階段，並對應 SwiftNet Release 8.0（2027 年）及 SWIFT 的 2030 年目標；此窗口屬建議性工作框架，並非監理機關訂定的強制期限。在此原則下，金融機構可參考以下方式安排工作：

2026 年：盤點與治理準備

建立密碼資產清冊，辨識核心金融系統、跨境訊息交換、憑證與金鑰管理等環節的量子風險；確認內部治理權責、供應商依賴與高風險資料範圍，並將 PQC 遷移納入資安策略與中長期資訊系統規劃。

2027 年：概念驗證與互通性測試

針對高風險系統選擇適當的 PQC 標準與技術方案，進行效能、協定相容性、金鑰管理及故障復原測試；同時與系統供應商、金融服務合作夥伴及相關基礎設施業者確認支援時程。使用 SWIFT 的機構應在本年度完成 Alliance Release 7.9 部署，並配合 SwiftNet Release 8.0 於 2027 年 7 月底推出的時程安排介接測試。

2028 年：推動優先系統的分階段導入

在標準、產品及測試結果足以支持的前提下，優先處理高風險或可控範圍內的系統，建立可重複執行的遷移流程，並持續驗證服務品質、營運持續性及跨系統相容性。此階段對應金管會指引的試辦與基礎升級期，可測試混合模式（Hybrid Mode），評估對交易延遲與硬體效能的影響。

2029 年：檢視進度與擴大遷移

重新評估密碼資產清冊的完整性、優先系統的遷移成果、供應鏈支援狀況及剩餘風險，據此調整後續部署順序與資源配置。尚未完成遷移的系統，應具備明確的風險處理措施與預定改善時程。本年度同

時是金管會指引「優先遷移（2029–2032）」階段的起點，高風險與高關鍵系統應自此進入正式遷移。

上述規劃並非表示所有金融機構都應在 2029 年前完成全面 PQC 遷移。金管會指引以 2035 年前完成全面遷移為目標，2029–2032 年優先遷移高風險與高關鍵系統，2032–2035 年擴大至其餘系統；G7 Cyber Expert Group 2026 年 1 月的聲明亦指向 2035 年為整體目標年，並建議最關鍵的系統在 2030 至 2032 年間優先處理。實際時程仍須依系統風險、設備生命週期、法規要求、標準成熟度與供應商支援能力決定。國際金融業對 PQC 的共同方向，是及早辨識風險、建立協作機制並採取風險導向的遷移策略，而不是在缺乏相容性驗證的情況下，為追求時程而倉促更換密碼機制。

三、臺灣數位發展部政策與金管會金融業指引

（一）數位發展部推動 PQC 遷移的政策方向

面對量子運算可能帶來的密碼安全風險，臺灣的因應工作除了關注國際標準與技術發展，也需要建立符合國內產業環境的遷移指引、測試驗證能力及供應鏈協作機制。數位發展部數位產業署於 2025 年 4 月 16 日與後量子資安產業聯盟（PQC-CIA）共同發布我國首版《後量子密碼遷移指引》（1.00 版，由資策會編撰），說明後量子密碼的技術發展路徑，並提出涵蓋建立量子準備計畫、盤點密碼技術資產清單、與技術供應商討論量子準備計畫、確認供應鏈量子準備程度四個步驟的遷移路線圖，協助業者理解量子威脅、辨識受影響的密碼技術，並開始規劃相關系統的調整。資通安全署 2026 年 8 月發布的資通安全網路月報（115 年 7 月）亦說明美國及國際的 PQC 政策動態，並建議政府機關及早盤點機敏資料與密碼資產。從政策與產業推動的角度來看，PQC 遷移可從三個面向理解：

第一、密碼資產盤點與風險管理

組織應掌握現行系統所使用的密碼演算法、憑證、金鑰、通訊協定及相關設備，並確認哪些資料需要長期保護、哪些系統涉及重要服務，以及哪些設備或服務依賴外部供應商。這項工作有助於建立量子風險的基本視圖，避免遷移工作僅停留在技術研究而無法實際落實到資訊資產與營運流程。

第二、加密敏捷性與產品生命週期管理

PQC 標準、產品實作與安全驗證機制仍持續演進，組織應在新系

統設計、軟硬體採購及系統更新時，考量未來更換演算法、金鑰與憑證機制的能力。對難以更新的工業設備、網路設備與嵌入式系統而言，若能在採購與設計階段納入可更新性、供應商支援及長期維護要求，將有助於降低未來遷移成本。

第三、測試驗證與產業協作

PQC 遷移涉及演算法安全性、實作品質、系統效能及不同產品間的互通性，不能僅依據標準名稱或供應商聲明判定系統已具備量子安全能力。應透過適當的測試、驗證與實際情境評估，確認技術方案是否符合應用需求；同時促進政府、產業、研究機構及供應鏈業者之間的協作，降低各組織獨立摸索所產生的成本。

這些方向與 NIST 所強調的密碼資產可視性、風險管理、互通性測試及加密敏捷性具有一致性，可作為臺灣產業規劃 PQC 遷移時的參考架構。

（二）金管會金融業後量子密碼遷移參考指引

金融業的數位服務具有高度互聯、資料敏感度高及營運持續性要求嚴格等特性，因此，金融機構在推動 PQC 遷移時，除了參考國際標準，也需要將相關工作納入既有資安治理、風險管理及第三方服務管理機制。

金管會於 2026 年 6 月 18 日發布《金融業後量子密碼遷移參考指引》，提出七項策略建議：PQC 政策與治理、盤點密碼技術應用並建立密碼技術資產清單（CBOM）、提升加密敏捷性並優先清除密碼反模式、建立生態系協作機制與共通業務風險圖像、以風險導向建立遷移優先序、更新採購與供應鏈管理要求、建立測試切換與營運韌性機制；並建議分四階段推

動：準備與規劃（2026–2027）、試辦與基礎升級（2027–2029）、優先遷移（2029–2032）、全面遷移與收斂（2032–2035），以 2035 年前完成全面遷移為目標。在實務執行上，本章將遷移工作整理為四個相互連結的環節，說明如下：

第一、盤點密碼資產並評估風險

金融機構應辨識使用公開金鑰密碼的系統、應用程式、網路通訊、憑證及金鑰管理機制，並依據資料保密年限、系統重要性與外部依賴程度進行風險排序。盤點結果應能協助管理階層了解遷移範圍、優先順序及所需資源，而不只是由技術單位維護的設備清單。

第二、將供應鏈與第三方服務納入規劃

金融機構使用的核心系統、雲端服務、網路設備、金融訊息交換平台及安全產品，可能由不同供應商提供。若供應商尚未支援適當的 PQC 演算法或缺乏明確的產品更新計畫，即使金融機構內部已完成盤點，也可能無法依預期進度完成遷移。因此，應與供應商確認產品支援能力、預計更新時程、相容性測試安排及長期維護承諾，並在新採購與契約管理中逐步納入相關要求。

第三、透過概念驗證與測試確保安全及營運持續性

PQC 演算法導入可能影響金鑰與簽章資料大小、運算負載、通訊流程及既有協定的相容性。金融機構應先於適當的測試環境驗證方案，再依系統風險分階段部署，並設計監控、故障復原與必要的回復機制，以降低遷移對交易服務及營運流程的影響。

第四、建立治理機制並持續追蹤遷移進度

PQC 遷移涉及資訊、資安、風險管理、採購、法遵、營運及業務單位，不宜完全由單一技術團隊負責。金融機構應明確界定權責、訂定階段性目標、定期檢視風險與執行成果，並隨著國際標準、產品支援及監理要求的變化調整計畫。

以上四個環節是本章依 PQC 遷移實務需求整理的執行架構，對應指引七項策略中的治理、盤點、供應鏈與測試切換四項；風險優先序、加密敏捷性與生態系協作三項，分別於本白皮書第三章、第四章及第五章詳述。金融機構實際辦理時，仍應以金管會公布的正式文件、適用範圍及最新版本為準。

（三）從政策指引走向組織落實

臺灣推動 PQC 遷移，不能只依賴政策文件發布或單一演算法導入，應建立由政策指引、組織治理、技術驗證及供應鏈協作共構成的實施機制。

在政府與監理機關層面，可持續追蹤國際標準與遷移時程，提供產業可採用的實務指引，並促進測試驗證資源、技術知識與供應鏈資訊的交流。在金融機構及關鍵基礎設施營運者層面，則應將 PQC 遷移納入資安風險管理與中長期系統更新計畫，透過密碼資產盤點、風險分級、概念驗證及分階段部署，逐步降低量子威脅所帶來的風險。

此外，組織也應避免將「採用了 PQC 演算法」直接等同於「已完成量子安全轉型」。實際安全程度仍取決於演算法與實作是否適當、金鑰管理是否健全、系統是否完成相容性驗證，以及供應鏈與相關協定是否同步

調整。唯有將技術變更與治理制度結合，才能使 PQC 遷移成為可持續管理的資安工作。

對金融業而言，2026 至 2029 年對應金管會指引的準備與規劃、試辦與基礎升級兩個階段，可作為盤點、測試、優先系統導入及階段性檢視的規劃窗口；2035 年前完成全面遷移則是金管會指引與 G7 聲明共同指向的目標。各機構仍應依實際風險與正式監理要求制定自己的時程，指引屬參考性質，並非統一的強制期限。對關鍵基礎設施而言，則應更加重視設備生命週期、長期保密需求與系統更新限制，提早建立可執行的遷移路徑。

PQC 遷移的核心價值，在於讓組織不必等到量子威脅成為迫切危機時才開始行動，而能在標準與技術逐步成熟的過程中，持續掌握風險、調整系統並維持服務韌性。

第二章　NIST PQC 演算法理論與加密敏捷性（Crypto-Agility）模型

前言

金融機構導入後量子密碼，需要掌握演算法的用途、系統成本與持續更新能力。模組晶格金鑰封裝機制（ML-KEM）用來建立通訊秘密，模組晶格數位簽章演算法（ML-DSA）用來簽署及驗證訊息；兩者須配合既有協定、憑證與金鑰管理，才能支援安全的金融服務。本章先說明其原理與安全強度，再比較資料量及效能，最後提出可供導入與驗收的加密敏捷性架構。

本章以正式發布的聯邦資訊處理標準（FIPS）為依據，標準與產品狀態查核至 2026 年 10 月 23 日。公開效能數據用來說明取捨；正式容量規劃仍須以機構的設備、網路與業務負載驗證。

一、新一代 PQC 標準演算法剖析：ML-KEM 與 ML-DSA 之數學原理與安全強度

（一）金鑰建立、資料保護與數位簽章

以銀行間的應用程式介面（Application Programming Interface，API）為例，連線雙方先建立共享秘密，再用對稱式認證加密保護往來資料；若付款指令需要獨立驗證來源，則另加數位簽章。這三種功能使用不同的金鑰與驗證程序，選型時應先辨認用途。

金鑰封裝機制（Key-Encapsulation Mechanism，KEM）讓雙方透過公開通道建立共享秘密。ML-KEM 的封裝方使用接收方公鑰，產生共享秘密及封裝密文；接收方再以私鑰解封裝。封裝密文用來建立金鑰，交易資料則由 AES-GCM 等對稱式認證加密機制保護。實際金鑰衍生與用途分離依通訊協定辦理。

ML-DSA 提供訊息完整性與來源可驗證性的密碼學基礎。簽署者使用私鑰，接收者以可信公鑰驗章；公鑰與銀行、設備或授權角色的關係，由公開金鑰基礎設施（Public Key Infrastructure，PKI）或可信登錄建立。簽章保護的是訊息的可驗證性，敏感內容仍須加密。

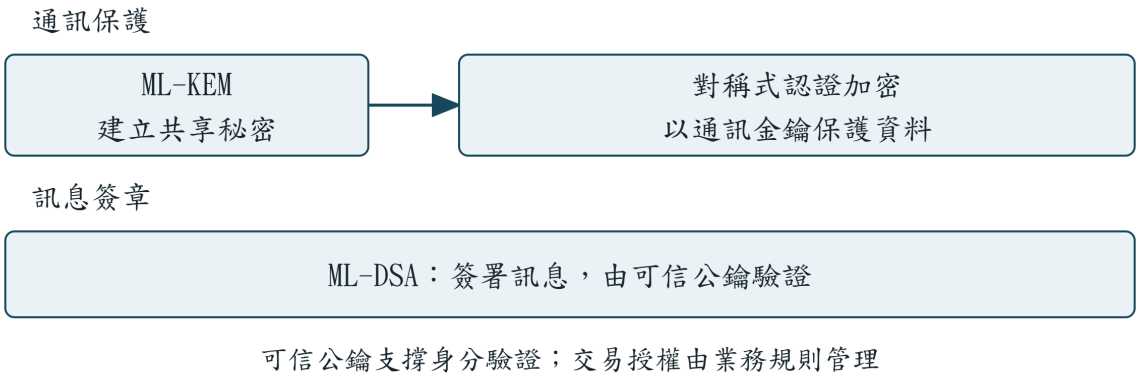

圖 2-1 金融服務的密碼分工

資料來源：依 NIST FIPS 203、FIPS 204、SP 800-227 繪製

對照傳統密碼時，橢圓曲線金鑰協議（ECDH）應與 ML-KEM 比較，橢圓曲線數位簽章（ECDSA）及 RSA-PSS 則與 ML-DSA 比較。傳輸層安全協定（Transport Layer Security，TLS）1.3 已移除靜態 RSA 金鑰傳送，仍可使用 RSA 簽章認證；因此遷移規劃應寫明替換的功能及協定版本。

美國國家標準暨技術研究院（NIST）於 2024 年 8 月 13 日發布 FIPS 203 與 FIPS 204，分別規範 ML-KEM 及 ML-DSA。兩者源自 CRYSTALS-Kyber 及 CRYSTALS-Dilithium，最終標準已調整部分雜湊、編碼及介面規則。採購與互通測試應以最終演算法、參數組、格式及實作版本識別，舊版名稱僅用於說明歷史或既有實驗。

（二）晶格與帶誤差問題的直覺

晶格可想成由基底向量的整數倍組合形成的規則點集合。二維方格容易辨認，高維晶格中的短向量與近點問題則可能非常困難。密碼設計利用特定問題及參數，使合法持有秘密的一方能有效運算，而攻擊者難以由公開資料還原秘密。

帶誤差學習問題（Learning With Errors，LWE）以公開結果隱藏秘密，其簡化關係為：

其中，A是公開矩陣，s是秘密向量，e是依規定分布產生的小誤差，b 是公開結果；mod q 表示運算結果依模數 q 取餘數。在足夠且獨立的方程式下，沒有誤差的關係可用線性代數求解。加入適當誤差後，公開結果不再直接給出無誤差的線性關係；配合高維結構及經分析的參數，便形成密碼設計所依賴的計算難題。

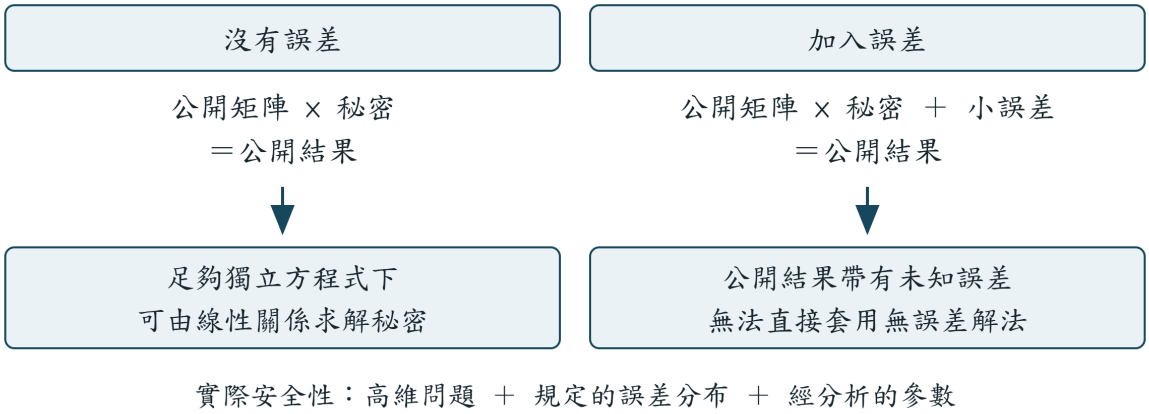

圖 2-2 誤差如何改變公開關係

資料來源：依 NIST FIPS 203 繪製。圖示說明誤差作用實際安全性來自高維問題、誤差分布與參數，不能由簡化示意推定

ML-KEM 與 ML-DSA 採用模組晶格結構，以多項式組織運算，兼顧安全性與計算效率。ML-KEM 的安全分析與模組帶誤差學習問題（Module Learning With Errors，MLWE）相關；ML-DSA 另涉及模組短整數解相關問題。金融機構應採用標準參數，並核對密碼函式庫或硬體模組的標準符合性與測試資料，將選型重點放在安全類別、資源成本與系統支援。

上述多項式運算使用下列多項式環，規定係數與高次項的處理方式，便於以固定大小的資料結構進行運算。兩項標準採用的模數與其他參數不同。

（三）ML-KEM 如何建立共享秘密

ML-KEM 包含金鑰產生、封裝與解封裝三個操作。接收方先產生公私鑰，將公鑰交給封裝方；封裝方產生共享秘密與封裝密文，並把密文送回。接收方以私鑰解封裝，取得相同的共享秘密。公鑰與封裝密文可傳送，私鑰與共享秘密則留在受保護的端點。

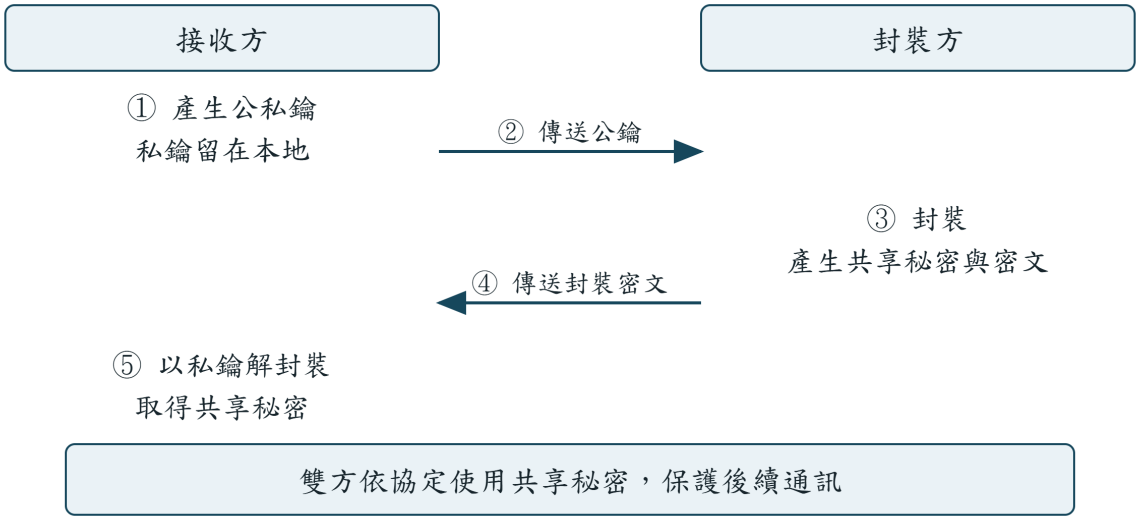

圖 2-3 ML-KEM 的公開交換與本地運算

資料來源：依 NIST FIPS 203、SP 800-227 繪製

公鑰與交換過程的真實性須由所選協定保障

封裝的內部運算延續「公開結構、秘密與誤差」的關係，使持有私鑰的一方能恢復用來建立共享秘密的資訊。完整標準還包含編碼、雜湊及輸入檢查；部署時應使用完整 ML-KEM 介面，不宜抽取內部組件自行拼接。

解封裝包含隱含拒絕機制，避免透過特定密文檢查結果洩漏秘密。系統仍須依協定完成身分驗證與金鑰確認，不能將「可執行解封裝」視為「已確認對方可信」。

銀行通訊的收送方向、用途與握手資料，應依協定綁定至所用金鑰。這使相同的密碼能力能支援不同服務，同時維持用途分離與互通性。

（四）ML-DSA 如何簽署及驗證訊息

以跨機構付款訊息為例，發送端以私鑰簽署格式明確的指令，接收端再以可信公鑰驗章。雙方必須使用一致的訊息內容、簽章模式及用途脈絡（context），例如將此簽章限定於指定應用。驗章成功表示密碼學檢查通過，交易是否獲授權仍由業務規則判斷。

ML-DSA 透過暫時隨機值遮蔽私鑰相關資訊，再把訊息納入雜湊挑戰，形成可由公鑰驗證的回應。驗證者能檢查訊息與簽章是否一致，而不需取得私鑰。

ML-DSA 使用拒絕抽樣：候選簽章不符合條件時，重新取樣，以避免洩漏私鑰資訊。這是正常程序，也使單次簽署時間有所變動。因此容量評估除了平均或中位數，還應觀察較慢請求的延遲，例如第 95 及 99 百分位（p95、p99），並在尖峰負載下測試。

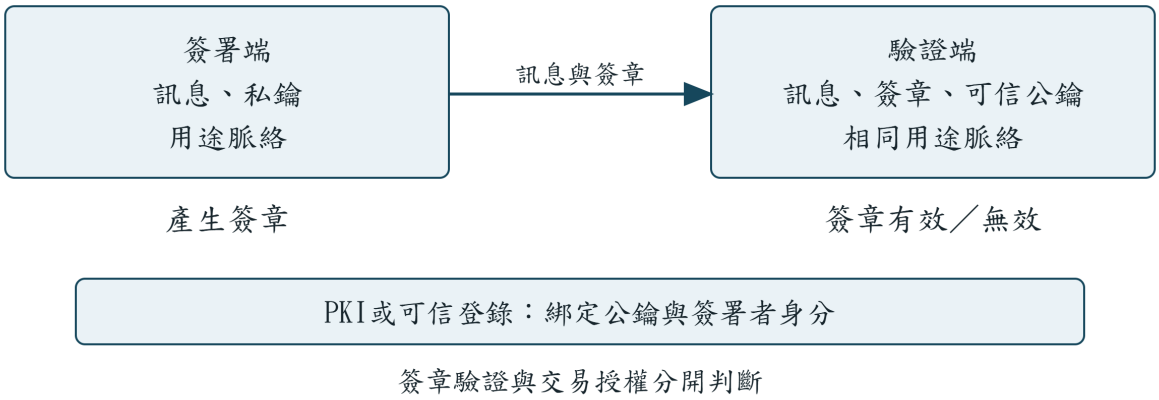

圖 2-4 ML-DSA 的簽署與驗證

資料來源：依 NIST FIPS 204、RFC 9881 繪製

標準提供結合新鮮亂數的簽署方式，也允許決定性變體。選型時應一併確認亂數品質及對時間、功耗等側通道洩漏的防護，不宜僅以速度選擇實作。

簽署與驗證必須使用相同的訊息模式。付款欄位、幣別及版本應採用一致的格式與排列順序，確保雙方驗證的是同一份授權內容。其中，pure ML-DSA 直接接受訊息，HashML-DSA 則使用標準定義的預雜湊流程，兩者不能任意混用；RFC 9881 的 X.509 憑證配置採用 pure ML-DSA。

（五）安全類別與參數選擇

NIST 以五個安全類別，將攻擊所需資源與區塊密碼金鑰搜尋或雜湊碰撞搜尋比較。這是選型的安全目標，與傳統密碼的安全位元估計採不同評估方式。

表 2-1　NIST 安全類別

類別	參照問題	本章參數組
1	AES-128 金鑰搜尋	ML-KEM-512
2	SHA-256 碰撞搜尋	ML-DSA-44
3	AES-192 金鑰搜尋	ML-KEM-768、ML-DSA-65
4	SHA-384 碰撞搜尋	—
5	AES-256 金鑰搜尋	ML-KEM-1024、ML-DSA-87

資料來源：依 NIST FIPS 203、FIPS 204 等繪製

SHA3-256／384 亦為對應碰撞搜尋參照；「—」表示本章六組參數無此分類

ML-DSA-44 屬類別 2；ML-KEM-768 中的 768 及 ML-DSA-65 中的 65 都是參數名稱，不能讀成安全位元數。選型應查閱正式安全類別，再評估用途與相容能力。

FIPS 203 建議以 ML-KEM-768 作為預設選擇，兼顧安全餘裕與效能；實際仍可依需求採其他參數。ML-DSA 的選擇則應依簽署用途、安全政策、保存期限及對端能力評估。參數提高時，物件大小與處理成本也會變動，下一節將分別量化。

正式部署還須確認亂數品質，保護私鑰等秘密資料，並落實側通道防護、輸入檢查及金鑰生命週期管理。銀行驗收宜依序確認演算法符合性、模組驗證範圍、協定互通與服務能力，並保留各項測試或認證資料。

二、傳統密碼與 PQC 之效能與資源對比：RSA/ECC vs. PQC 長度、大小及延遲分析

（一）先對齊功能與資料表示

效能比較分為三層：標準物件大小、特定實作的運算時間，以及完整金融服務的表現。前者用於估算資料量，中間層說明運算取捨，最後一層才能回答容量與客戶等待時間。銀行應沿著資料實際流經的協定、閘道及金鑰設備，逐層建立基準。

RSA-2048 約對應 112-bit 傳統安全強度；RSA-3072、P-256 約為 128-bit，P-384 約為 192-bit，X25519 的設計目標約為 128-bit。這些傳統強度無法抵抗足夠規模的量子攻擊，與 PQC 安全類別分欄解讀。

本節以 B 表示位元組，bit 表示位元。原始公鑰、DER 二進位編碼、PEM 文字表示、X.509 憑證與完整憑證鏈是不同物件。容量估算應先確認資料的表示層次，再計入格式、複寫與備份成本。

（二）公鑰、私鑰與簽章大小

表 2-2　ML-KEM 物件大小

參數組	類別	公鑰	展開私鑰	密文
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

資料來源：依 NIST FIPS 203 繪製，表 3。單位 B；三組共享秘密均為 32 B。

表 2-3　ML-DSA 物件大小

參數組	類別	公鑰	展開私鑰	簽章
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

資料來源：依 NIST FIPS 204 繪製，表 2。單位 B；以上均為演算法編碼物件。

部分實作可保存短種子，再重建完整私鑰；種子須比照私鑰保護。這能減少長期儲存，卻不代表執行時只需要同樣大小的記憶體。實際匯入、備份與還原格式仍取決於設備支援。

主體公鑰資訊（Subject Public Key Info，SPKI）是把公鑰與演算法識別放在一起的標準結構，適用時也包含演算法參數。它是公鑰的包裝，並非完整憑證。下表以 DER 編碼的 SPKI 列出傳統公鑰大小。

表 2-4　傳統簽章的大小基準

演算法	SPKI 公鑰	簽章格式	簽章大小
RSA-2048	294	固定長度	256
RSA-3072	422	固定長度	384
ECDSA P-256	91	DER	≤72
ECDSA P-384	120	DER	≤104

資料來源：依 IETF 文獻編碼規則推導

單位 B，RSA 採常用公開指數 65537 與標準演算法識別；ECC 公鑰採未壓縮點

ECDSA 若以兩個整數的固定長度串接表示，P-256／P-384 簽章分別為 64／96 B

表 2-4 的 SPKI 與表 2-3 的 FIPS 演算法物件位於不同編碼層次，不能直接作為同格式大小排名。將 PQC 導入 PKI 時，還須計入演算法識別及憑證包裝。精確容量應以實際匯出的物件計算。

憑證還包含主體、簽發者、有效期、擴充欄位與演算法識別，完整鏈可能含多張憑證。估算網路資料量時，應按實際鏈及雙向認證配置計算。RFC 9881 已規範 ML-DSA 的 X.509 識別與公鑰表示。

金鑰建立方面，X25519 分享為 32 B，P-256／P-384 未壓縮點為 65／97 B。RFC 10024 的 X25519MLKEM768 將 X25519 與 ML-KEM-768 組合：客戶端 key_exchange 為 1,216 B，伺服器為 1,120 B。這是特定交換欄位的長度；完整握手另含標頭、憑證與其他訊息。導入此群組改善的是金鑰建立，身分認證仍須依所用簽章及憑證另行評估。

（三）運算效能與工作負載

以下兩表使用 PQShield／Thom Wiggers 公布的測試資料，各表均取自同一次測試的原始紀錄。CPU 型號皆為 Intel Xeon Platinum 8488C，但主機、日期與系統核心版本不同，應各自解讀。這些是特定實作的公開量測，並非本章的銀行環境實測。

表 2-5　簽署與驗證時間

演算法	簽署	驗證	樣本數
RSA-2048	524.9	20.2	200
RSA-3072	1,177.9	39.5	50

演算法	簽署	驗證	樣本數
ECDSA P-256	22.3	63.7	1,000
ECDSA P-384	161.7	366.1	1,000
ML-DSA-44	46.7	21.6	1,000
ML-DSA-65	76.1	34.7	1,000
ML-DSA-87	96.7	54.1	1,000

資料來源：NIST PQC Signature Zoo: Signature benchmark, September 18, 2026

2026 年 9 月 18 日原始執行。單位 µs，列中位數；樣本數為每種操作次數

測試使用 32 B 訊息與單執行緒；傳統簽章透過 OpenSSL 3.5.5，ML-DSA 採支援 AVX2 指令集加速的實作。計時包含各實作的訊息雜湊與簽署／驗證處理，不含金鑰檔案載入或 HSM 呼叫。不同演算法的軟體處理與最佳化方式有所差異，表中結果不代表同安全強度或所有平台的速度排名。

此例中，ECDSA P-256 簽署較 ML-DSA-44 快，驗證則較慢。若一份交易訊息由多個節點驗章，驗證成本的權重便提高；大量產生簽章的平台則更在意簽署容量。金融機構應依實際簽署／驗證比例評估，而非以單一速度排名選型。

表 2-6　金鑰建立操作時間

演算法	產生金鑰	發送端操作	接收端操作
X25519	35.8	67.9	34.6

演算法	產生金鑰	發送端操作	接收端操作
ECDH P-256	17.1	79.6	65.5
ECDH P-384	136.3	472.4	326.4
ML-KEM-512	7.7	8.6	10.1
ML-KEM-768	11.5	12.4	14.6
ML-KEM-1024	16.4	17.6	20.8

資料來源：NIST PQC Signature Zoo: Key establishment benchmark, October 6, 2026

2026 年 10 月 6 日原始執行。單位 µs，列中位數；每操作 1,000 次

ML-KEM 三欄依序為金鑰產生、封裝與解封裝。ECDH 的發送端操作包含臨時金鑰產生、公鑰匯出及共享秘密計算；接收端包含對端公鑰匯入及共享秘密計算。因此，表中比較的是測試所定義的金鑰建立操作，不是相同的底層數學運算。ML-KEM 採 mlkem-native 的 AVX2 最佳化實作，ECDH 採 OpenSSL。

此例顯示，公鑰較大不一定代表運算較慢，資料量與 CPU 成本應分別評估。來源未完整披露頻率與建置條件，也未提供 p99；以上數據可用來比較各操作的時間差異，正式容量規劃仍需完整服務的負載測試。

（四）記憶體、金鑰設備與網路成本

長期儲存包含金鑰、憑證、簽章與備份；執行記憶體還包括運算工作區、程式物件與收發緩衝。兩者應分開估計，並在預期併發量下量測記憶體峰值。前述速度資料沒有提供可直接比較的記憶體數據，不能以金鑰

長度推算執行需求。

硬體安全模組（Hardware Security Module，HSM）與金鑰管理服務（Key Management Service，KMS）的延遲，除了密碼運算，還包含安全通道、呼叫往返及裝置佇列。應依應用程式實際呼叫 HSM 或 KMS 的流程量測持續吞吐與尖峰延遲；設備支援、驗證範圍及備援條件則於本章三、（四）說明。

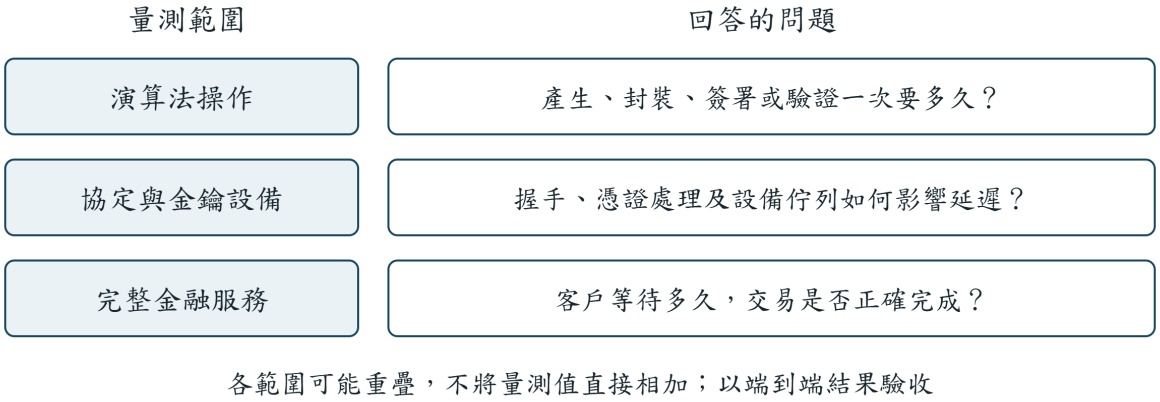

圖 2-5 金融服務的三種量測範圍

資料來源：自行整理。以端到端時間為主，再分層追蹤瓶頸。

握手資料增加後，影響取決於網路往返時間（Round-Trip Time，RTT）、頻寬、丟包與憑證鏈。短連線反覆建立時，握手成本較突出；長連線可將成本分攤至多次請求。測試應區分完整握手與會話恢復，並明確界定起訖，最後以 API 回應或交易完成時間判斷服務影響。

Kampanakis 的受控 TLS 研究顯示，較大的後續傳輸可降低握手成本所占的比例。該研究以增加認證資料量模擬影響，未實測最終 ML-DSA 完整憑證鏈、雙向 TLS 或 HSM；可借鏡的是固定網路條件與量測範圍的方法。

（五）金融場景與 PoC 驗收

概念驗證（Proof of Concept，PoC）應從能協調雙方系統與測試條件的服務開始。銀行間 API 若採雙向 TLS（mTLS），應分別測試金鑰建立、伺服器認證與客戶端認證，再組合完整流程。每輪記錄實際協商結果，並涵蓋閘道、代理與後端，確認保護延伸至需要保護的接收端。

交易簽署的量測終點應涵蓋驗章、授權及交易處理。國際清算銀行（BIS）的 Project Leap Phase 2 在 T2 測試環境驗證 PQC 訊息，但採標準前的 Dilithium 與軟體金鑰檔，尚未納入完整 PKI。由於參考資料管理系統缺少對應憑證，PQC 路徑未完成最終結算。這說明密碼操作可行之後，仍須完成可信公鑰註冊與業務整合。

保存期長的交易訊息，還須留存演算法、參數、簽章、憑證及當時的驗證條件，使未來仍能查明簽署與驗證條件。這類需求應在試點時一併設計。

表 2-7　金融 PoC 量測重點

層次	主要指標	關鍵條件
物件與傳輸	大小、鏈長、線上資料量	編碼、雙向認證、標頭
演算法	各操作延遲、操作率	實作、硬體、訊息、亂數
記憶體	運行峰值、併發增量	基準、暖機、負載
TLS／mTLS	握手、恢復、成功率	RTT、頻寬、丟包、鏈

層次	主要指標	關鍵條件
API 與交易	p50／p95／p99、吞吐、失敗率	負載、起訖、交易完成條件
HSM／KMS	往返、佇列、持續吞吐	韌體、連線、備援

資料來源：自行整理。p50 為延遲中位數，p95／p99 用於觀察較慢請求門檻依機構服務需求與風險政策設定

PoC 先確認功能與互通，再測正常、尖峰、長時間及故障負載。報告保留樣本數、分布與失敗率，並標明未測項目。非法簽章、未知或撤銷憑證、逾時與復原須有對應結果，才能判斷效能改善是否伴隨完整驗證與正確交易狀態。

三、加密敏捷性（Crypto-Agility）架構：不更換底層系統下的演算法動態抽換

（一）以可更新的密碼介面降低改造成本

加密敏捷性是組織能依風險與政策，有控制地新增、替換及停用密碼機制的能力。它涵蓋業務流程、協定、格式、金鑰、設備與維運。NIST 將其視為跨系統與治理的持續能力，應以實際變更所需時間、改動範圍與測試結果評估。

「不更換底層系統」成立的前提，是既有介面、欄位容量、更新路徑與對端已容納新演算法。預先將密碼功能集中在可更新的服務介面，可減少業務程式改寫；遇到固定欄長、舊協定、韌體限制或不支援的憑證格式，仍須升級相關元件。演算法切換應使用經核准的設定，並分階段部署。

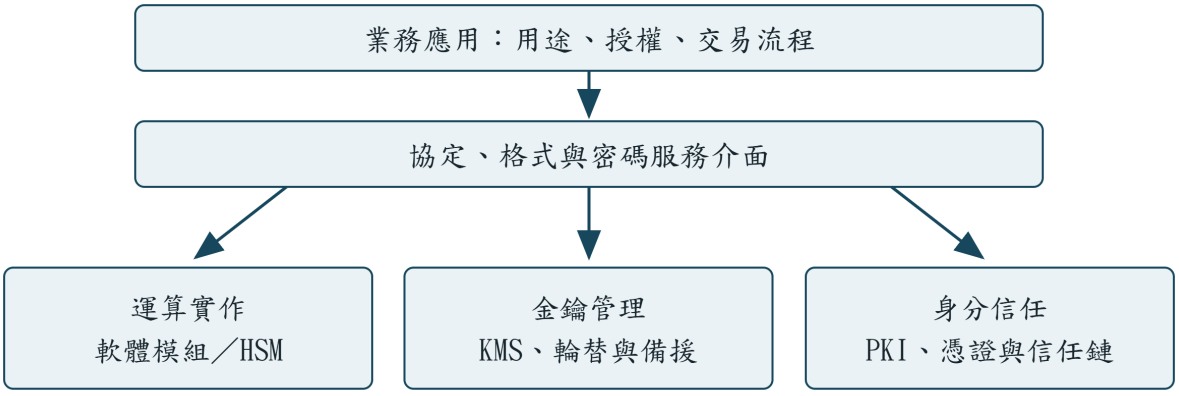

圖 2-6 加密敏捷性的職責與相依

資料來源：依 NIST 及 IETF 文獻整理

業務應用宜透過簽署、驗章、通訊保護等服務介面表達需求，由密碼實作模組或 HSM 執行運算。KMS 管理金鑰生命週期，PKI 管理憑證與身分信任；各自的更新與相容條件須一起確認。各層都應核對實際使用的演算法與參數是否符合核准設定。

表 2-8　架構中的可替換條件

層次	預留能力	驗證重點
業務應用	介面用途、錯誤處理	欄位容量、交易處理規則
協定與格式	識別、協商、編碼	對端及中介互通
密碼介面	型別、參數、能力查詢	用途檢查、錯誤拒絕
實作與設備	版本更新、實作模組更換	韌體、API、驗證範圍
金鑰與信任	產生、發布、輪替、撤銷	PKI、備援、歷史查驗
治理與觀測	政策、核准、例外到期處理	實際配置、失敗原因

資料來源：依 NIST 相關文獻整理

（二）Hybrid 與雙軌共存

傳統／後量子混合式（PQ/T hybrid）金鑰建立，在指定協定中組合兩類元件。其安全性取決於組合方式、輸入檢查與協商保護，應採用已定義的群組及規範。混合金鑰建立、複合簽章與不同端點的雙軌共存，是不同過渡安排；各自需要獨立的政策與驗證條件。

截至查核日，RFC 10024 已定義 TLS 1.3 的傳統／PQC 混合金鑰建立

機制，RFC 9881 則規範 ML-DSA 的 X.509 配置。金鑰建立與簽章各有自己的協定及格式要求，不能因其中一項已支援，就視為整條服務路徑完成遷移。

複合簽章須明定簽署格式與接受規則，例如是否要求兩種簽章皆通過。雙軌共存則讓不同端點暫用不同配置，傳統通路仍承擔其原有風險。例外應綁定用途、對端與到期日，配合退出計畫管理。

（三）金鑰與信任生命週期

演算法更換通常需要新型別金鑰、憑證與信任資料。機構宜沿服務的實際執行路徑建立密碼資產清冊（Cryptography Bill of Materials，CBOM），連結用途、演算法、實作、金鑰位置、對端及負責人。再依保護期限、更新條件及相依關係安排遷移順序。

表 2-9　金鑰與信任的遷移作業

階段	必要作業
產生與註冊	核准位置、用途、金鑰 ID
發布與啟用	憑證鏈、信任資料、依政策啟用
輪替	重疊期、接收端更新、佇列處理
停用與撤銷	停止新用途、發布撤銷資訊
保存與復原	歷史驗證、備援還原、權限
銷毀與退出	處置私鑰等秘密資料及備份

資料來源：依 NIST 相關文獻整理

新簽章的產生與歷史證據的查驗應分開管理。停用某演算法的新簽署，不必然取消所有歷史查驗需求；應保留足以重建當時驗證條件的資料，再依保存與風險政策決定處置。私鑰備援則依用途、不可匯出限制及權限分工設計，並實際演練還原。

（四）設備、軟體與合作方共同驗證

共用 API 能減少業務程式對特定演算法的依賴，但實際支援仍取決於軟體模組、韌體、格式與對端。導入時應從實際服務呼叫確認運算位置與協商結果，不能只憑函式庫的功能清單判定相容。

向供應商確認 HSM 支援能力時，應核對型號、韌體、支援參數、金鑰格式及備援能力。若涉及密碼模組驗證計畫（Cryptographic Module Validation Program，CMVP），須核對證書涵蓋的模組版本、操作環境與批准模式。機構還應實測金鑰不可匯出、權限隔離、還原及故障時的替代路徑。

表 2-10　端到端互通與故障測試

路徑	正向驗證	反向／故障驗證
用戶端—TLS 終止點	完整握手、恢復	無共同群組、竄改、逾時
終止點—後端	每段符合政策	內段配置偏差、舊端點
憑證機構—驗證端	鏈、用途、輪替	過期、撤銷、未知識別
應用—HSM／KMS	正確金鑰與運算位置	離線、錯型別、權限不足

路徑	正向驗證	反向／故障驗證
訊息—接收與處理	驗章至交易處理完成	錯簽、重試、輪替中斷
主站—備援	還原、歷史查驗	備份不相容、禁用配置

資料來源：依 NIST 等相關文獻整理

每條路徑應留存實際演算法、版本、金鑰識別與失敗階段，並能連回交易結果。表中的 TLS 終止點是解開 TLS 連線的閘道或服務；若其後還有內部連線，也須逐段驗證。BIS 案例中的憑證註冊與結算相依，應轉成本地試點的驗收項目。

（五）受控切換與安全復原

每個用途應建立允許配置，記錄政策版本、端點、參數、所需的最低軟體與韌體版本、金鑰用途、啟停條件及例外期限。TLS 群組、伺服器／用戶端認證及交易簽章分別管理，並透過協商完整性與實際配置監測，防止未核准降級。

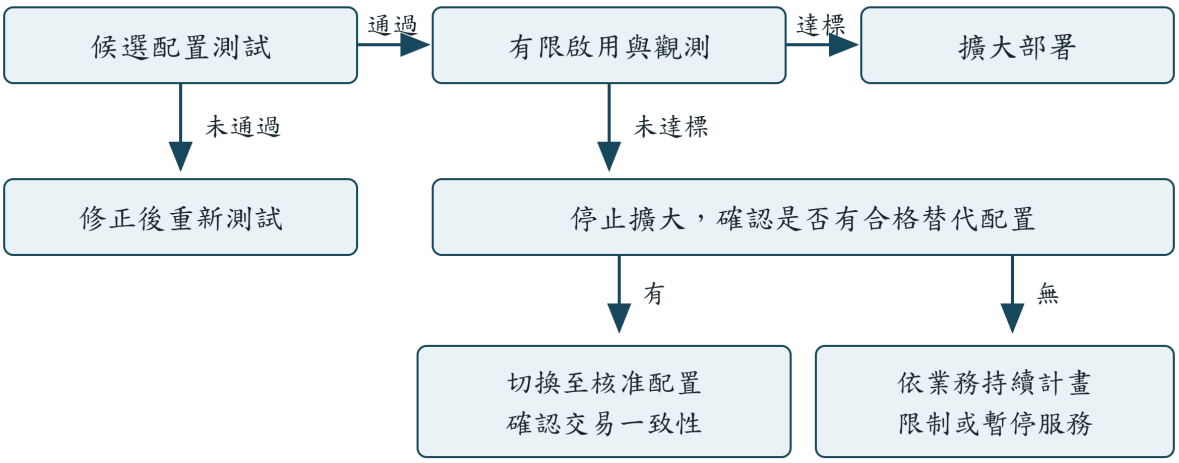

圖 2-7 受控切換與安全復原

資料來源：依 NIST CSWP 39 繪製

替代配置須同時符合安全底線及服務條件

候選配置通過互通、負載、失敗處理及復原演練後，先有限啟用，再依觀測擴大。若安全或服務未達標，停止擴大並切換至事先通過上述測試、並獲核准的替代設定；沒有符合安全與服務要求的替代設定時，依業務持續計畫限制服務或暫停通路。已禁用的機制不得以復原名義重新啟用。

支付與簽章流程的復原，還須處理重試、待處理訊息與輪替中的金鑰。驗收應確認交易不遺失、不重複入帳，也不錯誤接受訊息，並可追溯當時使用的配置。

（六）以可量測成果推進導入

試點宜選範圍明確、雙方可控制且有現況基準的流程，例如一組銀行合作 API 或交易簽署服務。除了本章第二節的效能與資源指標，還應觀察變更是否可控、復原是否安全，以及舊配置能否按計畫退出。

表 2-11　敏捷性驗收與觀測

面向	保留的證據
相依項目盤點	已確認範圍、未知項、負責人
變更效率	核准至啟用時間、等待與改動元件
互通與配置	必測通過率、失敗項、實際協商結果
安全復原	復原時間、配置、交易一致性
舊配置退出	移除範圍、剩餘例外及期限

資料來源：依 NIST 相關文獻及本章 PoC 設計整理

驗收紀錄應明列測試範圍與未通過項目，不能讓整體通過率掩蓋關鍵合作方的失敗。日誌保留追溯所需的演算法名稱、金鑰編號與錯誤原因，避免記錄私鑰、共享秘密或不必要的交易明文。

PoC 交付應包含依賴清單、核准配置、互通與負載結果，以及復原、擴展和退出安排，由服務擁有者、資安、維運及合作方共同確認。再逐步納入正式候選設備、完整 PKI 與真實網路，形成可持續更新的金融服務能力。

第三章 PQC 遷移第一步：CBOM 盤點與風險評估方法論

前言

前兩章說明了量子威脅的背景、金管會指引的精神與整體遷移方法論，本章進入實務的第一步。金融業的加密技術廣泛分布在對外交易、跨機構介接、憑證、金鑰、HSM、應用程式與供應商元件中，且多數處於隱性狀態。若未掌握現況就直接替換演算法或更換設備，容易遺漏真正高風險的資產，也可能因不清楚影響範圍而導致服務中斷。因此，遷移的第一步不是替換演算法，而是透過密碼技術資產清冊（CBOM）的盤點與風險評估，掌握「哪些密碼技術資產在哪裡、保護什麼資料、量子風險有多高、遷移難度有多大」，作為後續架構規劃與實施部署的依據。

本章首先說明 CBOM 的定義及其在可見性、可追溯性、風險量化與加密敏捷性上的核心價值。其次介紹盤點的原則、流程、結構化欄位與管理機制，以及網路、憑證金鑰、程式碼與主機等不同層面的盤點工具。接著說明如何以量子風險（QR）與遷移難度（MT）雙維度評分，建立遷移優先順序矩陣。最後說明盤點工具與 CBOM 管理系統如何與 CLM、EKM 及 CaaS 整合，使 CBOM 從一次性的盤點成果，成為可持續維運、可向監理說明的治理基礎。

一、密碼技術資產清冊（CBOM）的核心價值

（一）CBOM 是什麼

CBOM（Cryptographic Bill of Materials，密碼技術資產清冊）是一份結構化清冊，記錄機構內（或指定範圍內）實際使用的密碼技術資產，至少包含：

1. 資產／系統／服務是什麼
2. 用什麼協定與演算法
3. 金鑰與憑證怎麼用、放在哪
4. 保護的是什麼資料、保存多久
5. 是否量子脆弱、資料從哪裡來

它不是單純的「憑證清單」或「TLS 掃描結果」，而是把密碼學使用現況轉成可治理、可評分、可維護的資產資料。

（二）CBOM 對金融業的重要性

依金融業特性說明 CBOM 的重要性，如下：

表 3-1　金融業 CBOM 特性

金融業特性	CBOM 的重要性	CBOM 帶來的價值
高可用性、零容忍中斷	遷移時不知道影響面，容易停機或誤切	先標出可先改、不可先改的系統

金融業特性	CBOM 的重要性	CBOM 帶來的價值
長效資料（帳戶、契約、交易、保單）	無法判斷 HNDL／TNFL 真正暴露在哪些資產	把「保存期限」納入優先順序
嚴格合規與金檢	無法證明已盤點、已評估、已排序	可對監理說明治理與決策依據
高度依賴第三方（同業、共用中心、雲、HSM、CA）	只看自家系統，漏掉生態系瓶頸	把供應商與共用平台一併入帳
加密散落各處（應用、LB、VPN、HSM、憑證、SSH）	各單位各做各的，重複或遺漏	建立全機構共同語言

資料來源：自行整理

（三）CBOM 的核心價值

對金融業而言，CBOM 的核心價值可歸納為五點：

1. 可見性（Visibility）

把「加密」從隱性技術債變成可盤點的資產。沒有清冊，就無法談遷移範圍、預算與時程。

2. 可追溯性（Traceability）

每一筆加密使用都能對應到系統、負責單位、資料來源與評分依

據，後續稽核與金檢可說明「為何先遷 A、後遷 B」。

3. 風險可量化（Quantifiability）

把演算法脆弱性、資料保存期限、敏感度、曝露面轉成 QR（量子風險）與優先級，避免只憑「感覺 RSA 很危險」做決策。

4. 加密敏捷性的基礎（Foundation of Crypto-Agility）

CLM、EKM、CaaS、模組化 Crypto API 都需要先知道「現在有哪些金鑰、憑證、演算法」。沒有 CBOM，平台升級會變成盲目替換。

5. 可延續、可擴充（Repeatability）

第一次可先做對外交易網路或核心通道；同一欄位與流程可擴到全行、子公司、保險核心、共用平台。CBOM 不是一次性專案產出，而是持續維運的資產帳。

重點不是一次做完全部資產盤點，而是欄位一致、來源可追溯、可分期遷移。

二、密碼技術資產盤點流程與管理機制

（一）CBOM 加密清單的資產類型

金融業 CBOM 應涵蓋的資產類型包括：

1. 傳輸層：TLS／HTTPS、VPN、專線加密、API Gateway
2. 遠端與檔案：SSH、SFTP、程式碼簽章
3. 身分與憑證：伺服器憑證、客戶端憑證、電子簽章、CA／RA
4. 金鑰與硬體：HSM、金鑰庫、資料庫欄位加密金鑰、金鑰封裝（KEM／Wrapping）
5. 應用與函式庫：自行開發或第三方密碼函式庫、固定寫死的演算法
6. 生態系：同業介接、共用中心、雲端服務、供應商元件

（二）CBOM 的盤點原則

1. 先鎖定小範圍、再擴展到全面：先對外服務／核心交易通道，再內網、再長尾系統至全面盤點。
2. 資料最小化：盤點加密技術中繼資料（協定、套件、憑證、金鑰類型），不擷取業務內容。
3. 工具＋人工：掃描找得到的先掃；掃不到的（硬編碼、HSM 內、

舊系統）用設定檔與訪談補。

4. 來源必記：每筆資產註明資料來自掃描、設定、訪談或文件，避免「帳上有、現場無」。

5. 治理先行：指定 Owner、更新頻率、變更觸發條件，否則清冊會在三個月後失效。

（三）盤點流程及步驟

盤點流程建議採下列五步驟：

1. 治理與範圍對齊

(1) 指定專案窗口與資產 Owner（資訊安全、系統、網路、憑證、應用）。

(2) 確認本期範圍：例如「對外交易主機網路與 TLS／VPN／API」，以及排除清單。

(3) 確認工具使用、掃描時段、資料保存與銷毀原則（金融業通常需事前資安同意）。

(4) 對齊金管會指引：風險導向、分期分流、生態系協作。

2. 多來源蒐集

表 3-2 CBOM 盤點原則-多來源蒐集

層次	做法	適用對象
主動掃描	TLS／SSH／VPN／API 端點探測	對外服務、網路負載平衡設備、公開入口
設定與架構	LB、防火牆、憑證庫、HSM 設定、應用組態	掃不到內部細節時
主機與函式庫	套件、OpenSSL／JSSE 版本、硬編碼演算法	應用與長尾系統
訪談與文件	系統負責人、供應商、共用中心介接規格	第三方與無法掃描環境
流量中繼（若允許）	僅協定、憑證、Cipher Suite、連線指標	需嚴格限制，禁止解密業務資料

資料來源：自行整理

金融業特別要注意：高可用性環境不可無預警全網掃描；應採同意時段、指定網段、最小權限，避免影響正常營運。

3. 結構化建檔

CBOM 欄位建議採結構化建檔，依不同屬性可區分以下欄位內容：

(1) 基本欄位

表 3-3 結構化建檔-基本欄位

欄位	說明
資產編號	唯一識別 ID
資產／服務名稱	系統或服務
資產類型	server／service／certificate／key／library／hsm
通訊協定	TLS、SSH、VPN、CMS 等
演算法／Cipher Suite	RSA、ECDSA、AES、套件名稱
金鑰長度／參數	2048、P-256、AES-256
憑證或金鑰資訊	主體、簽發者、有效期、存放位置
量子脆弱	Y／N／Partial
資料來源	掃描、設定、訪談
盤點日期	蒐集日

資料來源：自行整理

(2) 風險評估加值欄位

表 3-4 結構化建檔-風險評估加值欄位

欄位	說明
用途	簽章、傳輸加密、資料加密、金鑰交換
業務情境	核心交易、客戶通道、跨機構、內部管理
Shelf Life	資料／憑證相關保存或有效期間
Severity	敏感度 L1／L2／L3
Exposure	曝露 L1／L2／L3
QR	量子風險 1～3
遷移難度 MT	低／中／高
優先級	P0～P3
Owner／供應商	負責單位、CA、系統商、HSM 廠商
反模式／Hybrid 就緒	硬編碼、弱 Cipher、無法輪替等

資料來源：自行整理

4. 驗證與補漏

(1) 掃描結果與設定檔交叉比對（常見：負載平衡設備 對外一套、後端又一套）。

(2) 高風險項目（RSA／ECDSA 簽章、長期資料加密、對外 TLS）人工覆核及確認。

(3) 標註限制與假設：例如「僅網路層、未含應用內金鑰庫」。

(4) 補上掃不到的資產，避免 CBOM 只有「工具掃的資料」。

5. 管理機制與持續維運

(1) CBOM 建完不是結束，要建立後續管理機制，包括：

表 3-5 CBOM 管理機制

機制	建議做法
權責	每筆資產有 Owner；資訊安全負責方法論與品質
更新頻率	至少每年 re-inventory；憑證展期、系統上線、供應商變更時觸發更新
變更觸發	新系統上線、演算法變更、HSM／CLM／EKM 異動必更新 CBOM
品質門檻	必填欄位完整率、來源可追溯率、高風險項人工覆核率

機制	建議做法
與平台整合	逐步對接 CLM（憑證）、EKM（金鑰）、CaaS（加密政策），減少人工抄寫
版本管理	CBOM 版本、基準日、與報告／金檢資料一致

資料來源：自行整理

(2) 管理權責：

表 3-6 CBOM 管理權責

角色	職責
專案／PQC 治理小組	範圍、優先級政策、向高層與監理說明
資安／密碼治理	方法論、評分尺度、反模式清單、抽核
系統／網路 Owner	提供現況、確認業務情境與遷移可行性
憑證／金鑰管理（CLM／EKM）	憑證與金鑰生命週期資料回寫 CBOM
供應商管理	要求第三方提供演算法與 PQC 路徑

資料來源：自行整理

（四）密碼技術資產盤點工具

CBOM 密碼技術資產產不僅存在於原始碼儲存庫與第三方函式庫中，憑證或網路封包、韌體（Firmware）與硬體安全模組（HSM）及應用系

統等均會存有密碼技術資產。在 TLS 組態、API gateway、HSM、晶片卡、備份加密、CI 套件、供應商 SDK、設定檔中也使用各種金鑰、憑證或演算法。且這些金鑰或憑證經常在變動，因此若僅以人工方式盤點，不但耗費人力且無法取得完整及即時的資料。

1. 盤點工具涵蓋層面

真正的密碼技術資產盤點工具必須能覆蓋演算法、金鑰、憑證、協定、實作函式庫五個層面，並產出可機器讀取的 CBOM（目前主流標準為 CycloneDX CBOM，自 v1.6 起正式支援）。沒有單一工具能覆蓋全部，成熟做法是多層組合：

表 3-7 盤點工具涵蓋層面

發現層	方法	能找到什麼
1. 網路層（Network）	主動 Handshaking / 被動流量分析	實際協商的 TLS/SSH 版本、Cipher Suite、金鑰交換、憑證
2.憑證與金鑰層	憑證發現、Log、PKI 查詢	憑證演算法、金鑰長度、到期日、CA 鏈、存放位置
3.程式碼/二進位層	靜態分析、容器掃描	硬編碼金鑰、使用的加密函式庫、演算法呼叫
4.設定檔/主機層	設定檔解析、有限權限掃描	Keystore、HSM 設定、應用程式加密參數

資料來源：自行整理

銀行實務重點：對外服務與跨機構介接優先用網路層；核心系統

與金鑰管理再用設定檔/程式碼層補強。

2. 盤點工具類型

盤點工具可區分為靜態掃描、動態/運行時掃描及網路掃描（被動）。

(1) 靜態掃描工具（Static Analysis）主要掃描原始碼、二進位檔、容器映像或檔案系統，適合 CI/CD 整合，能及早發現硬編碼的加密演算法。

(2) 動態/運行時掃描工具（Dynamic / Runtime Analysis）則在應用程式運行時監控加密函式呼叫，適合發現運行中的加密使用情形。

(3) 網路掃描工具（Network Scanning，通常為被動）：監控網路流量，適合發現傳輸中的加密協議與演算法，而不影響系統效能。

金融業因高度監管（FSC、PCI DSS、SWIFT CSCF）、零容忍中斷、Hub 系統複雜性，以及 HNDL（先攔截、日後解密）風險，需採用多層次、互補的掃描策略，才能產生完整、持續更新的 CBOM。可採以下「靜態（開發階段）+動態（運行階段）+網路（流量可視化）」的全覆蓋架構：

表 3-8 盤點工具類型

層級	掃描類型	主要優勢（金融業適用）	CBOM 支援
靜態掃描	原始碼、二進位、容器、檔案系統	早期發現硬編碼演算法、CI/CD 整合容易、支援 Java/.NET 等金融核心系統語言	佳（CycloneDX 原生）
動態/運行時掃描	運行時函式呼叫、記憶體、端點代理	發現實際使用中的加密情境、HSM 與 Keystore 可視化、風險分數	良好
網路掃描（被動）	被動流量監聽（TLS、IPsec 等）	不影響效能、發現傳輸中弱演算法與憑證、適合 Hub 系統	中等（可匯入 CBOM）

資料來源：自行整理

3. 盤點內容型態

以盤點的內容型態說明掃描方式及相關內容資料，如下表：

表 3-9 盤點內容類型

類型	掃描方式	可掃到資料	無法掃到資料
主動掃描	對 IP／網域發探測，讀 Handshaking 與憑證	對外與可連到的服務、實際套件、憑證鏈	沒開埠的系統、掃描當下沒出現的連線
被動封包	掃描 Handshaking 內容，不解密應用層	線上真正連線完成的版本與金鑰交換	已加密的內容、沒流過鏡像埠的流量

類型	掃描方式	可掃到資料	無法掃到資料
主機／代理	在作業系統、設定、金鑰庫就地讀	本機憑證、JKS、OpenSSL 組態、部分函式庫	未安裝代理的設備、網路設備內部
程式與套件	掃原始碼、映像、SBOM	硬編碼演算法、依賴的 crypto 函式庫	執行時才載入、或只在供應商二進位裡的實作
憑證與金鑰平台	從 CA、CLM、HSM、EKM 匯出	憑證生命週期、金鑰長度、保管位置	沒進金鑰系統的自簽與硬編碼金鑰
雲端組態	讀雲上負載平衡、EKM、API gateway 設定	雲端代管的 TLS 與金鑰政策	地端與專線另一側

資料來源：自行整理

三、風險評估與系統遷移優先順序規劃

盤點完成後，需針對 CBOM 資產評估其量子風險，據以規劃其遷移優先順序。評估方式如下：

（一）先做脆弱標記，再做評分

表 3-10　脆弱標記

類型	標記	金融業意涵
RSA、ECDSA、ECDH、DH、DSA	量子脆弱=Y	金鑰交換與簽章直接受 Shor 威脅
以 RSA／ECC 包裝的 AES 金鑰	整體偏高風險	資料本身可能還在，金鑰可被解
AES-256、SHA-2 以上	Partial／視金鑰來源	對稱與雜湊相對抗量子，但金鑰來源若脆弱仍高風險
TLS 1.0／1.1、3DES、RC4、SHA-1	反模式，優先清除	屬「無悔作為」，不必等 PQC

資料來源：自行整理

「無悔作為」應與 PQC 遷移分開：弱協定、過期憑證、硬編碼金鑰、無法輪替，即使量子電腦尚未到來也該先處理。

（二）量子風險評分（QR）

量子風險量化指標建議採三個維度，即資料保存時間（Shelf Life）、資料敏感度（Severity）及曝露程度（Exposure），可依下列範例公式計算

QR 值：

$$QR = \text{ROUND}\left(\frac{\text{Shelf Life} + \text{Severity} + \text{Exposure}}{3}\right)$$

1. 評級

表 3-11　量子風險評級

維度	L1（1 分）	L2（2 分）	L3（3 分）
Shelf Life	≤5 年	5～10 年	> 10 年或需長期驗證
Severity	一般內部資料	客戶資料、一般交易	資金／契約效力、高敏感個資、核心清算
Exposure	資料僅限於自有基礎設施存取	資料存取僅限於特定的第三方	資料為公開可存取，或極易外洩

資料來源：自行整理

2. 依上述公式計算後取得 QR 值，其代表的意義如下表

表 3-12　量子風險評級 QR 值

QR	等級	意義
1	低	短期、低敏感、低曝露
2	中	中等保存或中等曝露／敏感
3	高	長效、高敏感或高曝露（HNDL／TNFL 關注對象）

資料來源：自行整理

可依下列建議，進行評分：

(1) 核心交易、清算、跨行／跨市場介接：Severity 至少 L2，多數為 L3。

(2) 公開 Internet 的交易入口、行動 App API：Exposure 多為 L3（與 TNFL／被動收集有關）。

(3) 電子契約、長期憑證、保險保單、貸款契約：Shelf Life 常為 L3。

(4) 內部測試或即將汰換系統：即使演算法脆弱，QR 可能中等，可併入汰換時程。

（三）遷移難度（MT）評分

QR 只針對風險進行評分，必須將遷移時間及難度納入考量，獨立評分，方可取得系統遷移的優先順序。

遷移難度量化指標建議亦採三個維度，包括解決方案可用性（Solution Availability）、執行成本與時間（Execution Cost and Time）及外部依賴程度（External Dependencies），可依下列範例公式計算 MT 值：

$$MT = \text{ROUND}\left(\frac{\text{Solution Availability} + \text{Execution Cost and Time} + \text{External Dependencies}}{3}\right)$$

1. 評級

表 3-13 遷移難度評分

維度	L1（1 分）	L2（2 分）	L3（3 分）
Solution Availability	目前已可用，或預計於 1 年內推出	預計於 1 至 3 年內推出	不確定，或需 3 年以上
Execution Cost and Time	屬於日常營運（BAU）的一部分，僅需進行微調	需要中度的架構變更	需要重大、具不確定性或高昂成本的升級
External Dependencies	依賴極低，或解決方案已被廣泛採用	依賴第三方，且其轉型路線圖（Roadmap）明確為 1 至 3 年	依賴第三方，但其轉型路線圖不確定或需 3 年以上

資料來源：自行整理

2. 依上述公式計算後取得 MT 值，其代表的意義如下表

表 3-14 遷移難度評分 MT 值

MT	等級	定義	金融業例子
1	低	設定或憑證／演算法調整，影響面可控	關閉弱演算法、升級 TLS 1.3
2	中	需設備／中介層改版或供應商支援	負載平衡設備、VPN、憑證鏈、應用組態

MT	等級	定義	金融業例子
3	高	多方互通、核心系統改造、長驗證與高可用性限制	跨機構協定、核心帳務、舊 HSM、無 PQC 路徑的長尾系統

資料來源：自行整理

（四）優先順序矩陣

透過遷移難度（MT）及量子風險（QR）雙重面向的考量，決定後量子遷移優先順序。優先順序評估原則如下：

1. 高優先：高風險且已有現成方案者，立即進行；高風險但須事前準備者，列入近期規劃；具長期依賴關係的高風險與中風險項目，列入長期規劃。

2. 中優先：遷移路徑較短的中風險項目，可納入日常營運的升級計畫一併處理；需規劃的中風險項目，應持續追蹤，以確定最佳的準備時程。

3. 低優先：低風險項目，可配合標準的系統現代化計畫，適時一併處理。

遷移優先順序矩陣如下：

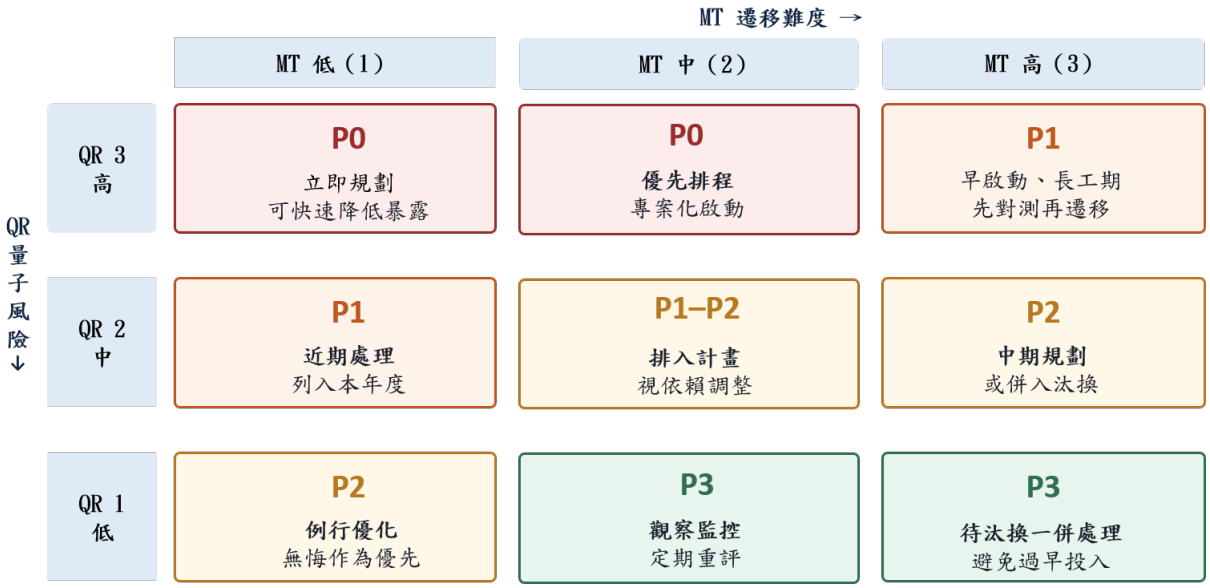

圖 3-1　優先順序矩陣

資料來源：自行整理

四、CBOM 盤點工具及管理系統整合實務

依金管會《金融業後量子密碼遷移參考指引》，建議評估運用 AI 等自動化工具輔助密碼技術資產盤點與 CBOM 維護，以降低人工盤點成本、提升覆蓋率並強化持續治理。因此建置一套完善的盤點工具及管理系統，實為金融機構於 PQC 遷移作業首要工作。

（一）盤點工具與 CBOM 管理系統應具備功能

盤點工具與 CBOM 管理系統為 PQC 遷移初期重要的協助工具，主要功能及其效益如下：

表 3-15　盤點工具與 CBOM 管理系統應具備功能

功能	盤點工具（掃描／發現）	CBOM 管理系統（持續治理）
主要功能	自動或半自動發現 TLS、SSH、憑證、金鑰、演算法使用	結構化儲存、版本管理、Owner 指派、與其他系統對帳
解決的問題	人工清冊不完整、容易漏掉長尾與設定檔	清冊做完就過期、無法追蹤異動
金融業價值	快速建立基線，覆蓋伺服器、應用、網路設備	成為持續維運資產，支援定期 re-inventory 與風險重評
與遷移的關係	產出第一版 CBOM 與風險清單	支撐優先矩陣、變更追蹤、遷移進度與合規報告

資料來源：自行整理

另在 PQC 遷移各階段的具體作用包括：

1. 盤點與風險評估階段：建立 CBOM，標記量子脆弱演算法，計算 QR／MT，產出優先矩陣。
2. 規劃與試辦階段：依 CBOM 選定 Pilot 系統，確認相依關係與 Hybrid 可行性。
3. 實施與部署階段：追蹤及管理哪些資產已切換、哪些仍為雙軌或待處理項目。
4. 全面轉型與持續維運：定期 re-inventory、偵測新出現的弱演算法、更新優先序，形成 PDCA 循環。

（二）CBOM 管理系統整合架構

CBOM 為 PQC 遷移的核心管理資料，需持續盤點、蒐集、維護及運用，以 CBOM 密碼技術資產盤點作業為核心之產品關聯圖如下：

以 OWASP CycloneDX CBOM 為基礎，以 JSON 格式整合網路通訊、單點 IP、程式碼及檔案、憑證、金鑰及演算法等 CBOM 資料至 CBOM 管理系統，可加速盤點作業及資料正確性。

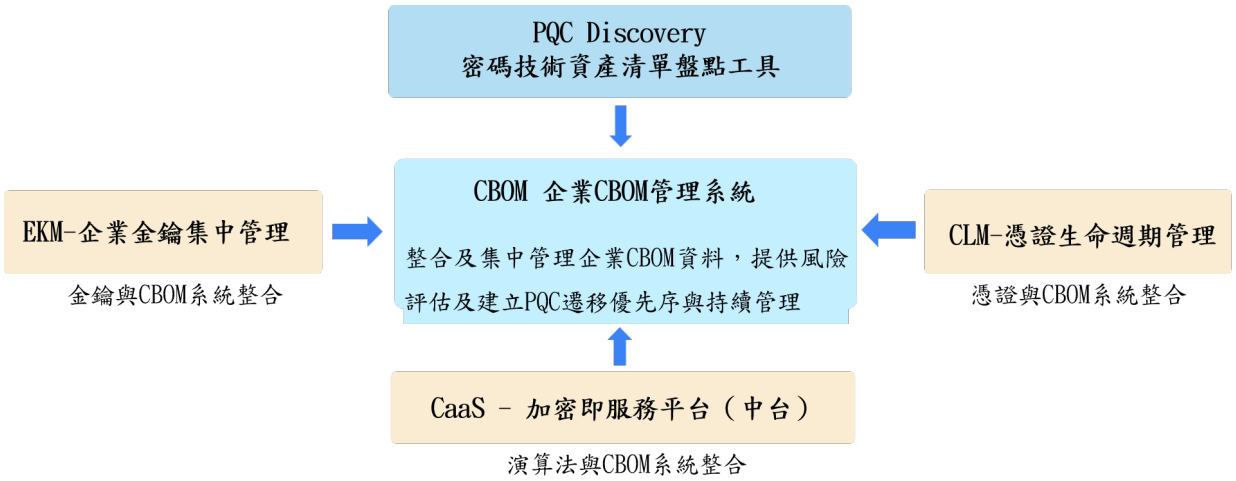

圖 3-2 CBOM 資產整合架構圖

資料來源：自行整理

1. PQC Discovery 密碼技術資產盤點工具：可針對企業網路通訊、單點 IP、程式碼及檔案進行掃描，產出 CBOM 分析其安全性並加以評等。

2. CBOM 企業 CBOM 清單管理系統：整合及集中管理企業 CBOM 資料，提供風險評估及建立 PQC 遷移優先序與各類管理報表。

3. CLM（Certificate Lifecycle Management）憑證生命週期管理：自動化憑證申請、部署、輪替、撤銷與 CaaS 整合，提供憑證生命週期管理。

4. EKM（Enterprise Key Management）企業金鑰集中管理：集中金鑰產生、儲存、輪替、存取控管與 CaaS 整合，提供金鑰生命週期管理。

5. CaaS（Crypto as a Service）加密即服務中台：統一加密介面、演算法組態化、Hybrid 支援及政策控管等。

（三）金融機構對 CBOM 整合實務需求

1. 合規與可稽核

金管會《金融業後量子密碼遷移參考指引》強調密碼技術資產治理與風險評估。CBOM 是證明「已盤點、已評估、已排優先」的核心證據，金檢或內部稽核時可直接對應。

2. 高可用性與零容忍中斷

核心帳務、跨行、支付、保險契約等系統不能停機。盤點結果用來判斷哪些可以先做 Hybrid 試辦、哪些必須雙軌運行、哪些只能併入汰換，降低遷移中斷風險。

3. 第三方與生態系依賴

同業、共用中心（Hub）、雲端、外包廠商、憑證機構都在範圍內。CBOM 可記錄供應商、介接協定與演算法，作為要求對方提供 PQC／Hybrid 路徑的依據。

4. 長期資料與高價值資產

電子保單、契約、交易紀錄、個資等需長期保密或驗證。盤點可標記這些資產的量子脆弱性，避免只改「看起來重要」的系統而遺漏真正高風險項目。

5. 加密敏捷性落地

要實現 Policy·Key·Payload 分離、模組化 Crypto API、CLM／EKM／CaaS 整合，必須先知道現況。CBOM 是這些平台的「資產主檔」，否則中控平台無法對帳、也無法強制政策。

第四章 雙軌平滑遷移與加密敏捷性架構設計

前言

隨著量子運算技術快速發展，現行金融體系廣泛使用的 RSA、ECC 等公開金鑰密碼演算法，未來可能被量子電腦破解。「先攔截、日後解密」（HNDL）與「現在信任、未來偽造」（TNFL）等攻擊模式，更使需要長期保密或長期驗證的金融資料已經暴露於風險之中。NIST 已發布 FIPS 203、204、205 等後量子密碼標準，金管會亦發布《金融業後量子密碼遷移參考指引》，促請金融機構及早規劃遷移。然而，金融業不容許服務中斷、合規要求嚴格且跨機構高度互通，加上 PQC 標準與實作仍在演進，一次全面切換恐導致交易中斷、互通失敗或無法回退。因此，如何在不影響業務的前提下安全、平穩且可控地完成遷移，是金融機構必須面對的核心課題。

本章承接前一章 CBOM 盤點與風險評估的成果，聚焦於遷移的架構設計與技術落實。首先介紹雙軌（Hybrid）模式的設計理念與常見組合，作為傳統演算法過渡至後量子演算法的橋梁。其次闡述加密敏捷性的設計原則，透過 CaaS、CLM、EKM 與模組化設計，使未來演算法變更只需調整組態，不必大幅改寫應用程式。最後說明 HSM 作為金鑰信任基點應具備的能力，以及作業系統強化（OS Hardening）如何提供穩固的底層防護。期能協助金融機構建構兼具安全性、互通性與敏捷性的密碼架構，為後續實施部署奠定基礎。

一、雙軌模式（Hybrid Mode）設計理念與架構

（一）為什麼需要雙軌而非直接切換

1. Hybrid Mode（雙軌／混合模式）是指在同一通訊或簽章流程中，同時使用傳統演算法（RSA、ECDSA）與後量子演算法（ML-KEM、ML-DSA 等），金鑰建立時由兩者的共享秘密共同導出會談金鑰，簽章驗證則依政策決定是否要求兩種簽章皆通過。這不是終態，而是過渡手段。

2. 直接切換純 PQC 的風險包括：對方尚未支援、效能與延遲尚未量測、標準或實作仍在演進、無法快速回退。金管會指引強調加密敏捷與生態系對齊，Hybrid 正是讓機構能在不中斷營運的前提下，逐步驗證與擴大。

3. 在 PQC 遷移過程中，Hybrid 模式是 NIST CSWP 39 列出的過渡路徑之一，也是金管會指引建議於試辦階段測試的作法。

4. Hybrid 模式的優點：

   (1) 提升安全性：即使傳統或 PQC 其中一種被破解，整體仍安全

   (2) 確保互通性：新舊系統可平滑過渡，避免一次性全面替換

   (3) 加密敏捷性：未來可快速切換或移除單一演算法

（二）設計理念

表 4-1　雙軌模式設計理念

設計理念	說明
雙方都必須成功	傳統與 PQC 任一失敗即拒絕，避免單邊弱點
可組態切換	演算法組合由政策／組態決定，不寫死在程式
可監控（Monitor）與可回復（Rollback）	能量測延遲、失敗率；能在不重編譯下關閉 PQC 功能
用途導向	應用呼叫「用途」（如 TLS 金鑰交換），不指定具體演算法
預留第二次切換	設計時即規劃未來拿掉傳統演算法的行程與條件

資料來源：自行整理

（三）架構分層

表 4-2　雙軌模式架構分層

層次	職責	關鍵設計點
政策層（Policy Layer）	定義核准演算法清單、Hybrid 組合、例外期限	動態維護，版本化發布
抽象層（Crypto Agility Layer）	依用途選擇演算法、組合 Hybrid、處理協商	PKCS#11 或自有介面；不暴露私鑰

層次	職責	關鍵設計點
運作層（Operator Layer）	HSM、軟體庫、雲端 KMS 實作具體演算法	可熱插拔；支援 ML-KEM／ML-DSA
監測層（Monitor Layer）	延遲、失敗率、協商結果、回退次數	接入監控與告警

資料來源：自行整理

（四）常見 Hybrid 組合方式

Hybrid 分為兩大類，Hybrid Key Establishment / KEM（金鑰建立／封裝）及 Hybrid Signature（數位簽章）：

表 4-3　常見 Hybrid 組合方式

場景	傳統	PQC	備註
TLS 金鑰交換	X25519 或 ECDHE	ML-KEM-768	雙方都必須完成；失敗即降級或拒絕（依政策）
數位簽章	ECDSA P-256	ML-DSA-65	簽章與驗證皆雙軌；注意大小與效能
金鑰包裹	RSA-OAEP	ML-KEM	適用長期保存資料的金鑰保護

資料來源：自行整理

1. 混合式加密方案-Hybrid Key Establishment / KEM（金鑰建立／封裝）

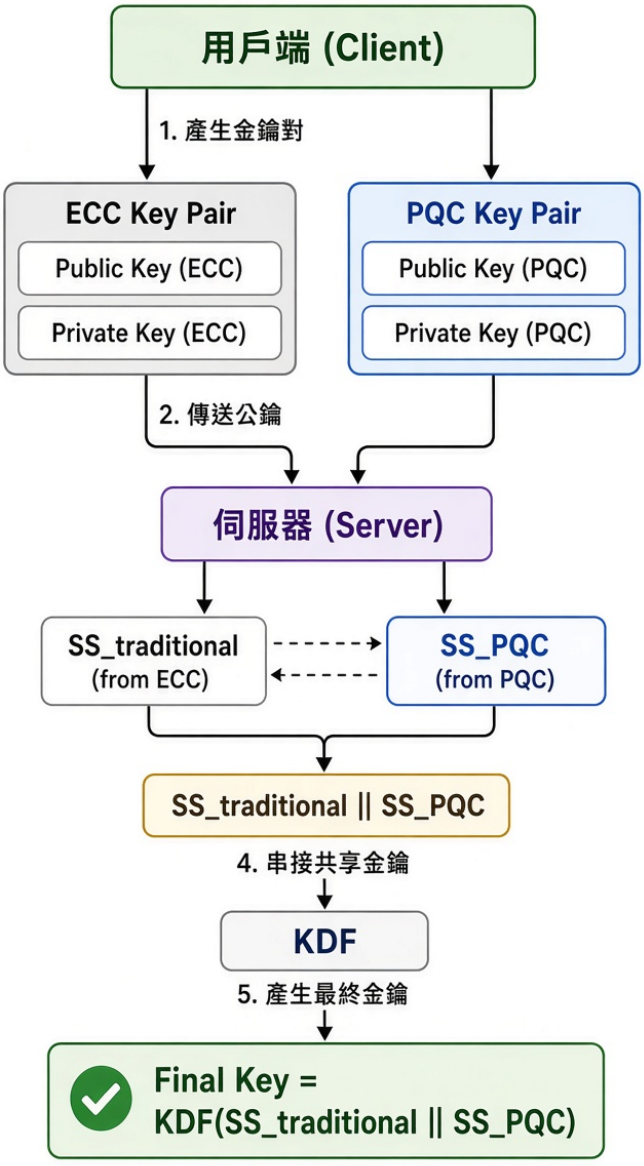

圖 4-1 混合式金鑰作業流程圖

資料來源：自行整理

說明如下：

(1) 雙方同時執行兩個獨立的金鑰建立：傳統 ECC Key Pair：ECDH（例如 X25519 或 secp256r1）。PQC Key Pair：ML-KEM（例如 ML-KEM-768）。

(2) 傳送公鑰：將各自公鑰傳送至伺服器端。

(3) 伺服器產生共享金鑰：各自產生兩個「共享秘密」（Shared Secret），SS_classical（傳統）及 SS_pqc（後量子）

(4) 串接共享金鑰：SS_classical 合併 SS_pqc。

(5) 產生最終金鑰：使用 KDF（Key Derivation Function） 合併兩個秘密，常見方式：Concatenate（SS_classical || SS_pqc） → Hash（SHA-384 或 HKDF） → 最終 Session Key。實際組合應依 NIST FIPS 203、SP 800-227、供應商支援與互通測試結果決定，並納入核准演算法清單動態維護。

2. 混合式加密方案- Hybrid Signature（數位簽章）

可以兩種實現方式：

(1) Dual / Parallel Signature：同時產生兩個獨立簽章（ECDSA 簽章 + ML-DSA 簽章），接收端驗證兩個。

(2) Composite Signature：將兩個公鑰／簽章封裝成單一結構（IETF 正在標準化）

二、加密敏捷性平滑升級規劃與實務

完成 CBOM 盤點與風險評估後，機構已知道哪些系統優先處理。本節進一步說明如何建立能支撐遷移的架構，透過 CaaS、CLM、EKM 與模組化設計，讓演算法替換不必大幅修改應用，並為後續 HSM 與實施部署奠定基礎。

（一）加密敏捷性的核心價值

加密敏捷性是指系統能夠快速、有效率、低風險地替換或更新密碼演算法、參數、金鑰、協定與憑證，而不需要大幅修改應用程式架構或造成營運中斷的能力。

在後量子密碼（PQC）遷移背景下，加密敏捷性特別重要，因為：

1. NIST 標準仍在演進（後續可能有更多演算法或參數更新）
2. 過渡期需要支援混合模式（Hybrid Cryptography）
3. 未來可能出現演算法被棄用或參數調整的情況

金管會指引明確指出：加密敏捷性的終極目標是將加密技術設計為「獨立模組」，讓未來演算法變更對應用開發者來說僅是「組態調整」，而非大型程式重構。

（二）加密敏捷性的五大核心設計原則

表 4-4　加密敏捷性的五大核心設計原則

原則	說明	實作重點
模組化（Modularity）	將加密邏輯與業務邏輯完全隔離	建立 Crypto Service/Crypto Abstraction Layer
組態化（Configurability）	演算法、參數、金鑰大小可透過組態變更	使用外部設定檔+驗證機制，避免硬編碼
抽象化（Abstraction）	透過標準介面存取密碼功能	PKCS#11、JCA Provider、雲端 KMS 抽象層、OpenSSL Provider
集中化（Centralization）	盡量將金鑰/憑證及密碼運算集中管理	EKM/CLM/HSM+Crypto Gateway /Crypto-as-a-Service
可觀測性與可測試性	能輕鬆測試新演算法並監控使用情況	加密使用日誌、CBOM 自動更新、A/B 測試能力

資料來源：自行整理

（三）加密敏捷性架構設計及規劃

1. 加密敏捷性架構

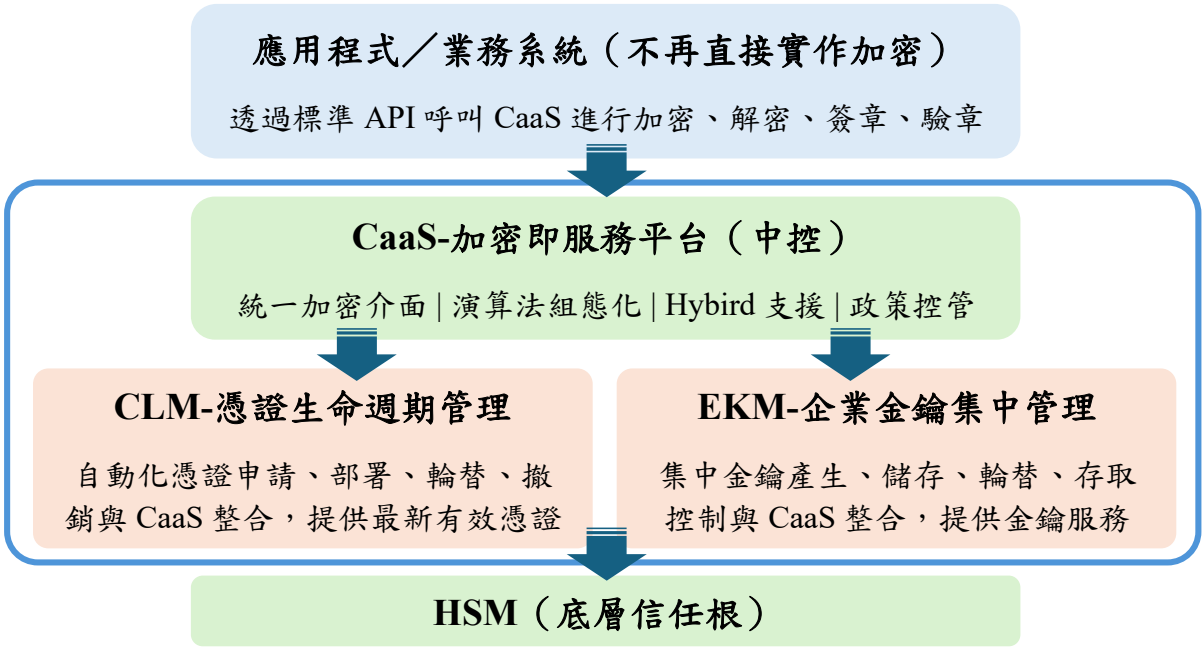

圖 4-2 加密敏捷性架構圖

資料來源：自行整理

- CaaS：統一加密介面、演算法組態化、Hybrid 支援及政策控管等
- CLM：自動化憑證申請、部署、輪替、撤銷與 CaaS 整合，提供憑證生命週期管理
- EKM：集中金鑰產生、儲存、輪替、存取控管與 CaaS 整合，提供金鑰生命週期管理
- HSM：硬體安全模組

2. 加密敏捷性架構規劃

加密敏捷性架構可以下列幾個層面說明：

(1) 架構層（Architecture Level）

以獨立的 Crypto Service（可為微服務、函式庫或 API Gateway）建立 CaaS 加密服務中台，所有應用程式透過此服務進行加密、解密、簽章及驗章等服務，可達到：

- PQC 遷移只需調整 CaaS 內部設定，應用程式不用大幅修改，可大幅降低 PQC 遷移成本
- CaaS 可同時呼叫傳統與 PQC 演算法，可快速支援 Hybrid Cryptography

(2) 應用程式層（Application Level）

應用程式層透過標準 API 執行 Crypto Service，可達到：

- 消除密碼反模式：禁止硬編碼演算法或將金鑰或憑證寫在程式碼或設定檔中
- 使用 Configuration-driven Crypto（YAML/JSON + Schema 驗證）
- 建立允許的演算法白名單（Policy-as-Code）
- 支援 Composite / Hybrid Signature 設定

(3) 金鑰與憑證管理層

- 導入 Certificate Lifecycle Management（CLM）：自動化憑證申請、部署、輪替、撤銷

- 集中式 KMS/HSM：支援多種演算法（包含 PQC 混合模式）
- 金鑰用途隔離：不同業務使用不同金鑰，避免單一金鑰被多處共用
- 金鑰輪替自動化：設定輪替政策與自動觸發機制

(4) 開發與 DevOps 層

表 4-5 開發與 DevOps 層

實作項目	說明	備註
加密掃描	在 CI/CD 中掃描硬編碼金鑰與不安全演算法	
政策阻擋	掃描到禁止項目直接阻擋 Merge/Deploy	Policy-as-Code
加密單元測試	針對不同演算法與參數組合進行自動化測試	
CBOM 自動生成	在建置流程中自動產生或更新 CBOM	CycloneDX+自訂外掛
金鑰輪替演練	定期執行金鑰輪替與回退演練	定期演練計畫

資料來源：自行整理

(5) 混合密碼學（Hybrid Cryptography）支援

PQC 遷移過渡期最重要的作業需求。

- TLS 層：優先支援 TLS 1.3+hybrid key exchange（classical +ML-

KEM）

- 應用層簽章：採用 Composite Signature（例如 RSA + ML-DSA）或 Parallel Signature
- 協定支援：JSON Web Signature（JWS）、CMS、PDF 簽章等需支援 hybrid 模式
- 協商機制：讓客戶端與伺服器能協商使用哪種演算法組合

三、硬體安全模組（HSM）與作業系統強化（OS Hardening）實踐

架構規劃完成後，必須確保金鑰保護與底層環境能夠支撐實際切換。本節說明 HSM 在遷移中的角色與應具備的能力，以及作業系統強化如何成為安全、穩定遷移的基礎，避免上層演算法切換被底層弱點抵消。

（一）HSM 在 PQC 遷移中的角色

HSM（Hardware Security Module，硬體安全模組）是金融業保護金鑰的核心設備。在後量子密碼（PQC）遷移中，它不只是「金鑰保險箱」，更是能否安全、可稽核、可控制地完成遷移的關鍵基礎。金管會《金融業後量子密碼遷移參考指引》強調密碼技術資產治理與加密敏捷性，HSM 正是落實這兩項的實務載體。

1. HSM 在密碼體系中的基本角色

表 4-6　HSM 在密碼體系中的基本角色

功能	說明	金融業常見用途
金鑰保護	金鑰在硬體邊界內產生、儲存、使用，不以明文離開	核心帳務、交易簽章、資料庫加密、憑證私鑰
密碼運算	在模組內執行加密、解密、簽章、金鑰封裝	高價值交易、電子憑證、跨機構介接
存取控制與稽核	雙人控管、角色權限、完整操作日誌	符合內控、金檢與合規要求

功能	說明	金融業常見用途
認證基準	需符合 FIPS 140-3 或等同標準	監理與第三方評估的信任基礎

資料來源：自行整理

若未使用 HSM，高價值金鑰容易散落在應用、設定檔或一般伺服器，遷移時風險與稽核難度都會大幅上升。

2. HSM 在 PQC 遷移中的具體角色

(1) 金鑰與演算法的「安全切換點」

- 依現行安控規範，現有電子銀行RSA／ECDSA 金鑰均需由HSM保護。
- 遷移到 ML-KEM、ML-DSA、SLH-DSA（或 Hybrid）時，新金鑰也應在 HSM 內產生與使用。
- HSM 成為「舊演算法退役、新演算法上線」的受控介面，避免應用直接處理長期金鑰。

(2) 支援 Hybrid 與逐步過渡

- 實務上多採 Hybrid（傳統＋PQC）先上線，再逐步轉純 PQC。
- PQC-ready 的 HSM 應能同時處理傳統與後量子演算法，並支援金鑰封裝（KEM）與簽章的混合模式。
- 這讓金融業能在不中斷業務的前提下驗證互通性與效能。

(3) 加密敏捷性的硬體基礎

- 與 CLM（憑證生命週期）、EKM（企業金鑰管理）、CaaS（加密即服務）整合時，HSM 提供可信任的金鑰來源。
- 應用透過 Policy 呼叫加密服務，而不是直接綁定特定演算法；HSM 則負責實際運算與金鑰保護。
- 未來演算法再替換時，只要 HSM 與中控平台支援，應用端改動可降至最低。

(4) 長期資料與高風險場景的保護

- 電子保單、契約簽章、長期交易紀錄、跨機構清算等，常需長期驗證（LTV）或長期保密。
- 這些高 QR（量子風險）項目的金鑰若放在一般系統，HNDL／TNFL 風險較高；放在 HSM 可降低金鑰被竊取後再被量子破解的整體暴露。

(5) 合規與稽核證據

- 金檢或內部稽核常要求證明「高價值金鑰有適當保護」。
- HSM 的認證等級、操作日誌、雙人控管，可作為遷移過程中「金鑰安全轉移」的證據。

3. HSM 對金融業的重要性

表 4-7　HSM 對金融業的重要性

金融業特性	沒有妥善處理 HSM 的後果	HSM 的價值
零容忍中斷	金鑰切換失敗可能導致交易中斷	受控的金鑰遷移與回復
嚴格合規	難以向監理說明金鑰保護與遷移軌跡	認證模組＋完整日誌
高價值與長效資料	金鑰外洩後，量子威脅可回溯解密或偽造	金鑰不出硬體邊界
第三方與共用平台依賴	與同業、共用中心、雲端互通時缺乏信任基點	標準化 HSM 介面與演算法支援
加密敏捷性要求	應用硬編碼演算法，遷移時大量改程式	金鑰與演算法由 HSM＋中控平台管理

資料來源：自行整理

HSM 是金融業 PQC 遷移的「金鑰信任基點」：它決定高價值金鑰能否安全地從 RSA／ECC 過渡到 PQC 或 Hybrid，同時維持可稽核、可控制、不中斷業務的能力。沒有妥善規劃 HSM，遷移容易變成應用端大量改寫，且難以向監理證明金鑰安全。

（二）PQC 遷移中 HSM 應具備的關鍵能力

根據金融業的運用與國際實務要求（NIST、FIPS 規範），PQC-ready 或可升級的 HSM 通常需涵蓋：

1. 支援 NIST 後量子演算法：包含 FIPS 203（ML-KEM）、FIPS 204（ML-DSA），視需求含 FIPS 205（SLH-DSA）及後續公布的演算法。

2. 支援 Hybrid 模式（傳統＋PQC 金鑰交換或簽章）。

3. 認證等級應為 FIPS 140-3 Level 3 或以上。

4. 金鑰產生、儲存、使用、備份及銷毀全生命週期皆在受控範圍內。

5. 與現有 CLM／EKM／應用的介面可升級，避免受廠商系統升級限制影響。

6. 效能與容量評估：PQC 金鑰與簽章通常較大，需確認交易延遲與吞吐量影響。

7. 供應商有明確的 PQC 路線圖與韌體／模組升級計畫。

（三）HSM 遷移實務注意事項

1. 先盤點再升級：在 CBOM 中標記哪些金鑰／憑證依賴哪台 HSM，哪些系統直接呼叫 HSM。

2. 分階段：先讓 HSM 支援 Hybrid 與新演算法，再讓高優先（P0／P1）系統切換，最後處理長尾。

3. 互通測試：與同業、共用中心、雲端服務及 CA 進行對測，確認

Hybrid 或純 PQC 可互通。

4. 備援與回復：HSM 叢集、備份金鑰、切換失敗時的回復程序必須事先演練。

5. 避免成為瓶頸：確認 HSM 效能足以支撐尖峰交易，必要時擴充或分區。

6. 供應商鎖定風險：評估是否可支援多廠商或標準介面，降低 HSM 供應商風險。

（四）作業系統強化（OS Hardening）實踐要點

在現行複雜且嚴峻的資安環境中，作業系統的角色至關重要，不僅是系統調度資源的中樞，更是最關鍵的安全防線，肩負身分驗證、權限管控、程式隔離與資訊保護的資訊安全重責，如果作業系統有漏洞，運作在其上的服務、資料庫等都暴露在巨大的風險之下。

在後量子密碼（PQC）遷移過程中，OS Hardening（作業系統強化）並非核心演算法替換本身，而是遷移得以安全、穩定、可稽核進行的基礎防護層。金融業在金管會指引下強調「最小業務中斷」與「加密敏捷性」，若底層作業系統仍存在弱設定、過時元件或未受控的密碼函式庫，即使上層已切換到 Hybrid 或 PQC，整體風險仍可能被放大。

建議在 PQC 遷移專案中納入以下 OS Hardening 檢查：

1. 密碼相關基線

(1) 更新並鎖定密碼函式庫版本。

(2) 停用已知弱演算法與 Cipher Suite（SHA-1、3DES、過舊 TLS 等）。

(3) 設定系統層級的加密政策（例如 crypto policy）。

2. 金鑰與憑證存放

(1) 避免金鑰以明文或弱保護存放在一般目錄。

(2) 優先導向 HSM 或受控 Keystore。

3. 服務與協定最小化

(1) 關閉不必要的遠端管理、過期服務。

(2) SSH、RDP 等管理通道使用強演算法並限制來源。

4. 變更與監控

(1) 加密相關變更納入變更管理。

(2) 監控異常的演算法使用或函式庫載入。

5. 長尾與老舊系統

(1) 無法 Hardening 或升級的 OS 應在 CBOM 中標記，並納入隔離、補償控制或汰換計畫。

第五章 實施部署與持續維運作業

前言

前幾章已完成密碼技術資產盤點、量子風險評估、架構規劃與基礎設施準備，本章進入實際執行與長期維運階段。金融業不容許服務中斷，合規要求嚴格，且高度依賴同業、供應商與共用中心，因此遷移不能一次全面切換，而應在最小業務中斷的前提下，先以 Pilot 小規模驗證互通性、效能與安全性，再以 Hybrid 模式確保與尚未升級系統的相容並保留回退能力，最後依風險高低分階段 Rollout，逐步移轉至 Pure PQC。

本章首先說明實施與部署的整體流程與執行原則，以及演算法、HSM 與基礎設施的升級作業、系統整合方式與 Pilot 測試重點。其次說明如何將監控、re-inventory、Rollback 與 PDCA 循環制度化，使遷移成果得以持續維持，並能因應未來標準更新或新威脅。最後說明如何透過 Hub-and-Spoke 與「四階呈現」概念，與同業、共用中心及供應商協作，並對齊國內外標準與法規，確保遷移不僅在機構內部可行，也能在整體金融生態系中穩定運作。

一、實施與部署各階段流程及作業

實施與部署階段位於盤點、風險評估與規劃之後，是實際執行遷移的主要階段。重點是最小業務中斷、Hybrid 過渡與加密敏捷性。另金融業因高可用性要求（零容忍 downtime）、嚴格合規與第三方（同業、廠商及共用中心）依賴，因此需特別注重 Pilot 測試與逐步 Rollout。

（一）實施與部署整體流程

1. 演算法升級（軟體層）
2. 硬體與基礎設施（HSM 升級）
3. 系統整合部署（加密敏捷性）
4. Pilot 測試（小規模驗證）
5. 驗證、監控與優化（持續改善）
6. 逐步 Rollout（Pure PQC）

（二）實施與部署執行原則

1. 高風險/高關鍵系統優先：本階段聚焦對業務影響大、量子風險高的系統（如交易系統、跨機構介接等）
2. Hybrid 模式為主要過渡策略：大部分系統先導入 Hybrid，確保與尚未升級系統的互通性，並保留快速回退能力

3. 加密敏捷性設計為強制要求：所有新部署或重大升級系統，必須透過模組化 Crypto API 實作

4. Pilot + 逐步 Rollout：選定具代表性的系統先行 Pilot，驗證流程與工具後，再分批擴大 Rollout，降低整體風險

5. 第三方與生態系協作：與同業、廠商、共用中心（財金、卡組織等）同步測試窗口與時程，確保跨機構互通

二、軟體（演算法）、硬體（HSM）與基礎設施升級

（一）演算法升級（軟體層）

1. 更新或替換加密函式庫

(1) 對稱式加密由 3DES 升級至 AES（GCM）。

(2) 非對稱式加密（RSA/ECC）簽章/加密支援 PQC 演算法。

2. 調整應用程式程式碼

(1) 使用模組化設計，讓演算法選擇可透過配置檔或政策決定。

(2) 實作 Hybrid 模式（同時計算傳統 + PQC，合併結果）。

3. 更新安全協議

(1) TLS 1.3：啟用 混合金鑰交換群組（例如 X25519MLKEM768），並搭配 TLS_AES_256_GCM_SHA384 等密碼套件。

(2) IPsec、S/MIME 等協議的演算法協商機制。

4. 憑證與 PKI 升級

(1) 發行 Hybrid 或 Pure PQC 憑證（ML-DSA 簽章 + ML-KEM 公鑰）。

(2) 建立雙 CA 架構（Classical Issuing CA + PQC Issuing CA）。

5. 實作自動化部署管線（CI/CD），執行加密敏捷檢查

（二）硬體（HSM）與基礎設施升級

1. HSM（Hardware Security Module）升級

   (1) 評估現有 HSM 是否支援 PQC 韌體更新。

   (2) 若支援，則進行 HSM 韌體升級作業。

   (3) 若不支援則採購/替換新一代 PQC-ready HSM（支援 ML-KEM/ML-DSA）。

   (4) 遷移金鑰或重建：從舊 HSM 安全匯出、新 HSM 匯入（使用量子安全通道）。

2. 加密作業平台升級（加密敏捷性）

   (1) 優先處理 Cryptographic Antipatterns（密碼反模式）。

   (2) 建置 CaaS（Crypto as a Service）加密即服務中台。

   (3) 建置 EKM 企業金鑰集中管理。

   (4) 建置 CLM 憑證生命週期管理。

3. 其他硬體升級

   (1) TPM、Smart Card、Crypto Accelerator、網路設備（路由器、負載平衡器等）。

   (2) 嵌入式系統或舊硬體：使用 Crypto Gateway（將舊系統流量導向外部 PQC 代理裝置）或 FPGA 重組方案。

（三）系統整合與部署

1. 採用階段式部署，以降低風險，可區分為下列幾個階段部署：

   - Phase 1：非生產 / 低風險系統（第二/三類系統）
   - Phase 2：面向客戶的系統（網銀、行動 App）（第一類系統）
   - Phase 3：核心系統（支付、核心銀行、資料庫加密）
   - Phase 4：供應鏈與外部介接系統

   Phase 1 以部署非生產/低風險系統為主，而非高 QR／MT 系統，主要基於風險控制與學習曲線考量。第一次上線 Hybrid 或新演算法時，常會遇到函式庫相容、效能、對端協商、日誌不足等問題。在非生產或低風險環境先暴露並修正，可有效控管風險。

2. 採混合演算法（Hybrid Cryptography） 模式，確保與尚未升級的外部系統相容。

3. 建立自動化金鑰輪替與憑證更新機制。

4. 與供應商/合作夥伴/共用中心同步。

（四）準備與 Pilot 測試

1. 選擇 1~3 個代表性系統進行 Pilot（例如網銀 TLS、支付 API、非核心內部系統）。

2. 建立測試環境（開發/測試/ staging），模擬正式環境流量。

3. 檢視及驗證結果：互通性（interoperability）、效能影響（latency、throughput）、安全性驗證（無 downgrade）。

4. 測試混合演算法（Hybrid Cryptography）組合：

(1) 金鑰交換：ECDH + ML-KEM（FIPS 203）。

(2) 數位簽章：ECDSA + ML-DSA（FIPS 204）。

(3) 混合憑證鏈（Dual-certificate 或 Composite Certificate）。

5. 執行負載測試與壓力測試，評估 PQC 較大參數帶來的效能衝擊。

6. 記錄追蹤及處理所有問題（相容性、函式庫 bug、HSM 支援度）。

（五）驗證、監控與優化

1. 進行完整安全驗證：

(1) 互通性測試（與傳統系統共存）。

(2) 效能與穩定性驗證。

2. 部署監控儀表板（Monitor 工具），持續追蹤加密使用情況與異常。

3. 準備 Rollback 計畫（可快速切回傳統演算法）。

4. 執行使用者與運維團隊訓練。

（六）逐步移轉至 Pure PQC

1. 當 Hybrid 穩定運行一段時間（通常 1~2 年）後，逐步移除傳統演

算法。

2. 定期重新評估（每 6~12 個月），因應新 PQC 標準或攻擊進展。

三、全面轉型與持續維運

（一）從 Hybrid 逐步轉為 Pure PQC，完成全組織轉型

當 Hybrid（混合式）模式於生產環境穩定運作一段時間（建議觀察 1 至 2 年）且生態系合作夥伴（如 SWIFT、財金公司、央行及核心金鑰供應商）均已具備 PQC 能力後，機構應擬定過渡退場計畫。透過階段性停用傳統加密演算法（如 RSA/ECC），將交易通道與簽章機制完全移轉至 Pure PQC（純後量子密碼）。此階段需配合金管會及國際標準的最新退場時程，完成全組織資訊資產的終極轉型，徹底消除「先攔截、日後解密」（HNDL）與「現在信任、未來偽造」（TNFL）的長期殘留風險。

（二）建立持續監控儀表板，自動偵測新的脆弱演算法

將 CBOM（密碼技術資產清冊）管理系統與資安監控儀表板深度整合，建立自動化密碼健康度稽核機制。儀表板應具備即時掃描與告警功能，能自動偵測網路流量、 API 介面、伺服器組態及原始碼中是否不慎引入未核准的傳統演算法、過期憑證、弱 Cipher Suite 或硬編碼金鑰（Hardcoded Keys）。透過視覺化儀表板，管理層與資安團隊能隨時掌握全行密碼資產的合規率與量子風險曝露程度。

（三）定期執行 re-inventory、訓練與演練

後量子密碼遷移並非一次性的專案，而是一項長期維運的資安治理機制。機構應建立定期盤點（re-inventory）制度，至少每年或於重大系統上線/改版時更新 CBOM 清冊。同時，針對開發人員、系統維運團隊

及資安人員辦理 PQC 與加密敏捷性（Crypto-Agility）專業培訓。每年應至少舉辦一次「密碼緊急應變與金鑰輪替演練」，模擬當現行演算法突發密碼學漏洞或遭破解時的快速切換與金鑰復原程序，確保團隊具備實際作戰能力。

（四）設計模組化 Crypto API，讓未來演算法替換不需調整應用系統

遵循「Policy-Key-Payload」分離與加密敏捷性原則，將加密、解密、簽章及驗章等功能封裝為標準化的中台加密服務（Crypto as a Service, CaaS）或模組化 Crypto API。業務應用系統僅需透過統一介面呼叫服務，而不直接呼叫特定演算法函式庫或硬體指令。當未來 NIST 發布新一代演算法、參數調整或演算法被棄用時，資訊團隊僅需於 CaaS 中台或 HSM 側調整設定檔與政策，即可無縫完成演算法抽換，大幅降低應用系統二次重構的開發成本與營運風險。

（五）制定 Rollback 計畫與應急程序，確保業務連續性

在任何系統切換或升級過程中，高可用性與金融服務不中斷（Zero-Downtime）為最高原則。機構必須針對每個遷移系統制定詳細的 Rollback（回退）計畫與應急標準作業程序（SOP）。當新升級的 PQC 或 Hybrid 設定於生產環境引發非預期的交易延遲、效能瓶頸、協商失敗或跨機構互通中斷時，應能於指定的安全窗口（SLA）內，自動或人工受控地回退至事先核准的備用安全配置（但不包含已宣布禁用的極度脆弱配置），並立即啟動問題排查，確保金融服務的連續性與穩定性。

（六）將 PDCA（Plan-Do-Check-Act）循環制度化

1. Plan：定期風險評估、演算法迭代規劃、供應鏈準備度檢討

2. Do：執行演算法替換、系統升級、訓練與演練

3. Check：監控數據分析、CBOM 審核、相容性驗證

4. Act：調整優先序、更新政策、持續改善機制回饋到 Plan

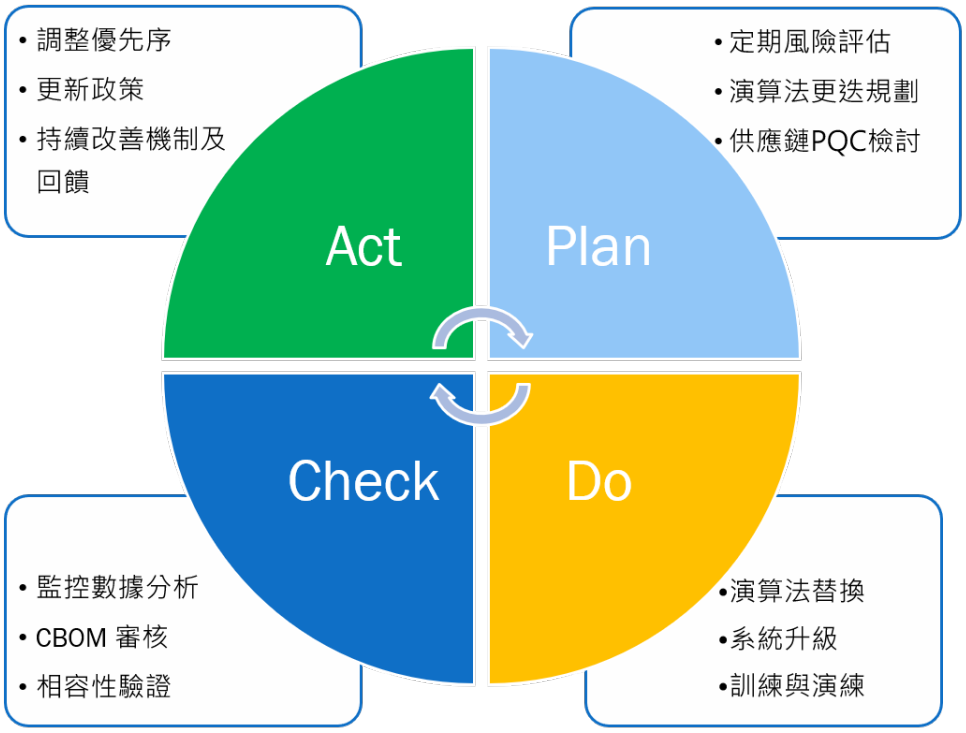

圖 5-1 全面轉型與持續維運

資料來源：自行整理

四、生態系成員協作與標準法規配合

即使單一機構完成內部遷移，跨機構互通與外部依賴仍可能成為瓶頸。本節說明如何透過 Hub-and-Spoke 模式與同業、共用中心、供應商協調，並對齊國內外標準與法規，確保遷移不僅在內部可行，也能在生態系中持續運作。

（一）跨組織協作的必要性

PQC 標準與配套規範仍在演進（FIPS 203／204／205 已定稿，FN-DSA、HQC 與 IETF 協定規範仍在制定中），單一組織無法獨力完成遷移，需跨供應商、標準組織與監管單位協作，才能確保互通性與合規。

（二）Hub-and-Spoke 與四階呈現

依金管會指引建議，可採 Hub-and-Spoke 與「四階呈現」概念，將生態系盤點與遷移工作分層如下：

表 5-1　生態系盤點與遷移工作分層

階層	名稱	負責主體	主要工作內容
第一階	Hub 型業務	樞紐機構（共通基礎設施或同業平台）	界定跨機構互通/共用平台的範疇、角色分工、關鍵相依性
第二階	對接單位延伸盤點	各金融機構	針對「對接 Hub」的業務/系統/介接點進行延伸盤點

階層	名稱	負責主體	主要工作內容
第三階	自主盤點遷移	各金融機構	非前兩階涵蓋的系統，由各機構自行盤點與規劃遷移
第四階	共通性基礎設施與供應商資訊	生態系共同	將關鍵供應商與共通元件/服務納入共同盤點語言

資料來源：自行整理

（三）跨機構協調與標準法規對齊

1. Hub 系統（財金、聯卡、SWIFT）跨機構協調：與軟體供應商、硬體廠商、共用中心（財金公司、票交所、央行及聯徵中心等）及金融同業建立合作關係，建立過渡期互通與共同測試的版本基準。

2. 追蹤國內外金融及 PQC 相關標準與規範（如 SWIFT CSCF、PCI DSS、ISO 20022 等），對齊 PQC 遷移規劃與時程

3. 建立聯合測試環境及平台，驗證混合演算法的互通性

參考文獻

1. 金融監督管理委員會。(2026 年 6 月)。金融業後量子密碼遷移參考指引。https://www.fsc.gov.tw/uploaddowndoc?file=news%2F202606181420231.pdf&filedisplay=%E9%87%91%E8%9E%8D%E6%A5%AD%E5%BE%8C%E9%87%8F%E5%AD%90%E5%AF%86%E7%A2%BC%E9%81%B7%E7%A7%BB%E5%8F%83%E8%80%83%E6%8C%87%E5%BC%95.pdf&flag=doc
2. 金融監督管理委員會。(2026 年 6 月 18 日)。金管會發布「金融業後量子密碼遷移參考指引」引導金融機構強化量子風險整備〔新聞稿〕。https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202606180001&dtable=News
3. 後量子資安產業聯盟、財團法人資訊工業策進會。(2025 年 4 月 16 日)。後量子密碼遷移指引(1.00 版)。https://www-api.moda.gov.tw/File/Get/adi/zh-tw/3m7h6KvGXJUUWmU
4. 數位發展部資通安全署。(2026 年 8 月 17 日)。資通安全網路月報(115 年 7 月)。https://moda.gov.tw/ACS/press/report/20430
5. 數位發展部數位產業署。(2025 年 4 月 16 日)。數產署攜手後量子資安產業聯盟發布「後量子密碼遷移指引」，協助產業提升資安保障、建構更安全的資安環境〔新聞稿〕。https://moda.gov.tw/ADI/news/latest-news/16090
6. BIS Innovation Hub. (2025). Project Leap phase 2: Quantum-proofing payment systems. https://www.bis.org/publications/project-leap-phase-2-

quantum-proofing-payment-systems.pdf

7. Cooper, D., et al. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280), §4.1.2.7. https://www.rfc-editor.org/rfc/rfc5280#section-4.1.2.7
8. G7 Cyber Expert Group. (2026, January 13). G7 Cyber Expert Group statement on advancing a coordinated roadmap for the transition to post-quantum cryptography in the financial sector. HM Treasury. https://www.gov.uk/government/publications/advancing-a-coordinated-roadmap-for-the-transition-to-post-quantum-cryptography-in-the-financial-sector
9. IETF. (2002). Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile (RFC 3279). https://www.rfc-editor.org/rfc/rfc3279.html
10. IETF. (2009). Elliptic Curve Cryptography Subject Public Key Information (RFC 5480). https://www.rfc-editor.org/rfc/rfc5480.html
11. IETF. (2015). JSON Web Algorithms (RFC 7518). https://www.rfc-editor.org/rfc/rfc7518.html
12. IETF. (2016). Elliptic Curves for Security (RFC 7748). https://www.rfc-editor.org/rfc/rfc7748.html
13. IETF. (2016). PKCS #1: RSA Cryptography Specifications Version 2.2 (RFC 8017). https://www.rfc-editor.org/rfc/rfc8017.html
14. IETF. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). https://www.rfc-editor.org/rfc/rfc8446.html
15. IETF. (2025). Internet X.509 Public Key Infrastructure—Algorithm Identifiers for ML-DSA (RFC 9881). https://www.rfc-editor.org/rfc/rfc9881.html
16. IETF. (2026). Hybrid Key Exchange in TLS 1.3 (RFC 9954). https://www.rfc-

editor.org/info/rfc9954/

17. IETF. (2026). Post-Quantum Traditional Hybrid Key Agreement Mechanisms for TLS 1.3 (RFC 10024). https://www.rfc-editor.org/rfc/rfc10024.html
18. International Organization for Standardization (ISO). (n.d.). ISO 20022: Universal financial industry message scheme. https://www.iso20022.org/
19. Kampanakis. (2024). The impact of data-heavy, post-quantum TLS 1.3 on the Time-To-Last-Byte of real-world connections. https://doi.org/10.14722/madweb.2024.23010
20. Menezes, A. (2026, September 16). A Gentle Introduction to Lattice-Based Cryptography (Version 3.3). https://cryptography101.ca/wp-content/uploads/lattice-based-cryptography.pdf
21. National Institute of Standards and Technology (NIST). (n.d.). Cryptographic Module Validation Program. https://csrc.nist.gov/projects/cryptographic-module-validation-program
22. National Institute of Standards and Technology (NIST). (n.d.). Post-Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
23. National Institute of Standards and Technology (NIST). (n.d.). Post-Quantum Cryptography Standardization. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post_Quantum_Cryptography-Standardization
24. National Institute of Standards and Technology (NIST). (n.d.). Post-Quantum Cryptography Standardization: Security evaluation criteria. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)
25. National Institute of Standards and Technology (NIST). (2019). FIPS 140-3: Security Requirements for Cryptographic Modules. https://doi.org/10.6028/NIST.FIPS.140-3

26. National Institute of Standards and Technology (NIST). (2020). Recommendation for Key Management: Part 1—General (SP 800-57 Part 1 Rev. 5). https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
27. National Institute of Standards and Technology (NIST). (2024). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://doi.org/10.6028/NIST.FIPS.203
28. National Institute of Standards and Technology (NIST). (2024). FIPS 204: Module-Lattice-Based Digital Signature Standard. https://doi.org/10.6028/NIST.FIPS.204
29. National Institute of Standards and Technology (NIST). (2024). FIPS 205: Stateless Hash-Based Digital Signature Standard. https://doi.org/10.6028/NIST.FIPS.205
30. National Institute of Standards and Technology (NIST). (2024, November 12). Transition to post-quantum cryptography standards (NIST IR 8547, initial public draft). https://doi.org/10.6028/NIST.IR.8547.ipd
31. National Institute of Standards and Technology (NIST). (2025). Recommendations for Key-Encapsulation Mechanisms (SP 800-227). https://csrc.nist.gov/pubs/sp/800/227/final
32. National Institute of Standards and Technology (NIST). (2025, March 11). NIST selects HQC as fifth algorithm for post-quantum encryption [News release]. https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption
33. National Institute of Standards and Technology (NIST). (2026). Considerations for Achieving Crypto Agility: Strategies and Practices (CSWP 39-upd1). https://csrc.nist.gov/pubs/cswp/39/upd1/considerations-for-achieving-crypto-agility/final

34. National Institute of Standards and Technology (NIST). (2026). Post-Quantum Cryptography FAQs: Seed formats (updated June 16, 2026). https://csrc.nist.gov/projects/post-quantum-cryptography/faqs
35. National Institute of Standards and Technology, National Cybersecurity Center of Excellence (NIST NCCoE). (n.d.). Migration to Post-Quantum Cryptography [Project page]. https://pages.nist.gov/nccoe-migration-post-quantum-cryptography/
36. National Institute of Standards and Technology, National Cybersecurity Center of Excellence (NIST NCCoE). (2023). Migration to Post-Quantum Cryptography (SP 1800-38C, preliminary draft). https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf
37. OWASP Foundation. (2024). CycloneDX specification (Version 1.6), including Cryptography Bill of Materials (CBOM). https://cyclonedx.org/specification/overview/
38. PCI Security Standards Council. (2024). Payment Card Industry Data Security Standard: Requirements and testing procedures (Version 4.0.1). https://www.pcisecuritystandards.org/document_library/
39. PQShield / Wiggers. (2026). NIST PQC Signature Zoo: Key establishment benchmark, October 6, 2026. https://github.com/PQShield/nist-sigs-zoo/blob/b55c4d81e46f84dc2240d1a9d0c1ebbd49daac51/bench-kem/results/20261006T140640Z_intel_r_xeon_r_platinum_8488c.txt
40. PQShield / Wiggers. (2026). NIST PQC Signature Zoo: Signature benchmark, September 18, 2026. https://github.com/PQShield/nist-sigs-zoo/blob/b55c4d81e46f84dc2240d1a9d0c1ebbd49daac51/bench/results/20260918T175855Z_intel_r_xeon_r_platinum_8488c.txt

41. Swift. (n.d.). Release 7.9. https://www.swift.com/interfaces-and-integration/release-79
42. Swift. (n.d.). Swift Operations Forum. https://www.swift.com/news-events/events/swift-operations-forum
43. Swift. (2025). CBPR+ roadmap beyond November 2025. https://www.swift.com/swift-resource/252463/download
44. Swift. (2026). Customer Security Controls Framework (CSCF v2027). https://www.swift.com/myswift/customer-security-programme-csp/security-controls
45. Swift. (2026, October 1). From AI to quantum: Trust, resilience and the technologies ahead [Newsletter]. https://www.swift.com/insights/newsletters/ai-quantum-trust-resilience-and-technologies-ahead