後量子密碼學（PQC）於金融支付與交易系統之遷移策略與風險管理

曾健全

中華民國 115 年 7 月

作者任職於中央銀行資訊處，本文內容純屬個人意見，與服務單位無關，如有錯誤概由作者負責。

摘　要

隨著量子運算技術的快速發展，現行金融體系高度仰賴的非對稱密碼學（如 RSA、ECC）面臨被破解的風險，衍生出「先攔截、日後解密（HNDL）」與「現在信任、稍後偽造（TNFL）」等實質威脅。為因應此一系統性風險，本研究參考美國 NIST、我國金管會等國內外最新監理指引與政策方針，探討金融業邁向後量子密碼學（PQC）之遷移策略、方法與實務注意事項。

本研究首先探討金融支付與交易系統之密碼應用現況，從「非對稱密碼（Shor 演算法威脅）」、「對稱密碼與雜湊強度（Grover 演算法威脅）」及「遷移效能與互通性」等三個面向，分析現有金融四大核心交易場景所面臨之技術挑戰；其次，匯集國內外監理合規藍圖，包含金管會於 2026 年 6 月正式頒布之《金融業後量子密碼遷移參考指引》，並彙整該指引中關於 PQC 遷移的策略方向及推動時程建議。

在內部資產盤點與優先順序評估方面，本研究說明密碼技術資產清單（CBOM）之實務建置框架，並整合 Mosca 定理之動態量化邏輯，探討如何透過風險熱力圖協助金融機構排定漸進式之系統遷移優先序。

針對內部 IT 落地與敏捷設計，本研究分析如何透過加解密中台化架構、混合加密模式（Hybrid Mode）、硬體安全模組（HSM）的過渡防禦策略，以及採購合約管理與遺留系統例外控管，來穩健落實加密敏捷性（Crypto-Agility）。

隨後，本研究探討外部生態系與國家級金融市場基礎設施（FMI）之聯防，歸納由樞紐機構（Hubs）領頭之共同遷移治理機制，包含制定共通 PQC 版本基準、推動互通性沙盒、關鍵供應商共用查核機制，以及全局灰度切換與實戰演練等跨機構協作框架。

最後，本研究彙總 PQC 遷移面臨之實務挑戰與「風險導向、循序漸進」等因應原則，並歸納網路銀行、ATM 跨行清算、線上證券及跨境電匯等四大核心交易場景之遷移建議，以及通訊安全、加密保護、數位簽章、憑證體系、載具與硬體等五大核心面向之因應策略，期能提供金融機構實務推動 PQC 遷移與風險管理之參考方向。

目　次

一、緒論 1

二、金融支付與交易系統之密碼應用現況與量子曝險 4

(一) 四大核心交易場景之技術風險與曝險剖析 4

(二) 生態系與供應鏈依賴之管理現況 7

三、國內外監理合規藍圖 8

(一) 國際標準化與跨國監理政策路線圖 8

(二) 我國金融資安藍圖與 PQC 政策發展方向 10

四、資產盤點與動態風險量化機制 12

(一) 密碼技術資產清單（CBOM）之實務建置與生態系盤點框架 12

(二) 雙軸動態量化評估與遷移優先序熱力圖 15

(三) 實務量化評估範例 18

五、遷移策略與加密敏捷設計 19

(一) 加解密中台化架構 20

(二) 混合加密模式（Hybrid Mode） 21

(三) 硬體安全模組過渡防禦策略 21

(四) 供應鏈風險管理 21

(五) 遺留系統例外管理 21

六、金融生態系共同遷移治理機制 22

(一) 歸納共通之「金融 PQC 版本基準 (Profile)」 22

(二) 整合「關鍵供應商共用查核機制」 22

(三) 落實「跨機構共同測試與互通沙盒」 23

(四) 建立「灰度切換與回退（Rollback）」標準程序 23

(五) 將量子斷鏈風險納入「跨機構實戰演練」 23

七、結論與建議 24
(一) PQC 遷移挑戰與因應原則 24
(二) 四大核心支付與交易場域之遷移建議 25
(三) 金融機構後量子五大核心面向因應策略 26
(四) 結語 26
參考文獻 27

一、緒論

近年來，量子運算技術取得突破性進展，其利用量子力學的「疊加」（Superposition）與「纏結」（Entanglement）特性，賦予了量子架構在處理特定數學問題時，具備傳統電腦無法比擬的指數級平行處理能力。然而，這種運算模式的根本轉變，亦對當代金融業廣泛賴以維繫的傳統非對稱式密碼體系（如 RSA 或 ECC）帶來了前所未有的系統性威脅。

現階段 IBM、Google 等科技巨擘所展示的量子電腦硬體系統，多屬於容易受到環境干擾、雜訊偏高的物理量子位元（Physical Qubits）階段；若要達到真正具備破密能力的「密碼學實用量子電腦」（Cryptanalytically Useful Quantum Computer, CRQC），必須透過高度複雜的錯誤修正（Error Correction）機制，將數千個物理量子位元轉化為一個能穩定運算的邏輯量子位元（Logical Qubits）。根據推算，若要徹底攻破目前金融業核心所採用的非對稱式密碼體系，量子運算架構預計需要擁有大約 2,000 個穩定無誤的邏輯量子位元，這在實體硬體製造上，往往對應著高達數千萬個物理量子位元的龐大除錯工程。

因硬體層面仍面臨工程瓶頸，傳統密碼防線被徹底攻破的技術臨界點（資安界通稱為「Q-Day」），在學術與產業界仍具高度不確定性。雖然部分科技巨擘與顧問機構（如 Gartner 或 Google）曾提出 2029 年至 2030 年代的特定時程預測與內部遷移目標，但國際清算銀行（BIS）與全球金融監理機構普遍強調，面對量子威脅不應陷入「精確預言破密日期」的迷思，而應將其視為一項重大的「情境風險（Scenario Risk）」。特別是考量到金融業對資料長期保存的嚴格法遵需求，以及系統全面遷移所需的漫長前置時間，金融機構絕不能被動等待 Q-Day 逼近才啟動防禦；相反地，金融機構應秉持營運韌性與風險治理的原則，現在就必須啟動量子風險認知（Awareness）、進行密碼資產盤點（Cryptographic Inventory）與擬定過渡遷移規劃（Transition Planning）。

基於上述前瞻性的風險治理思維，國際專業機構已主動訂定防禦性的遷移時程框架，美國國家安全局（NSA）發布的 CNSA 2.0 政策，明令關鍵

基礎設施須於 2030 年前開始過渡，並於 2035 年全面淘汰舊有傳統密碼；G7 網路專家小組（CEG）亦發布聲明，建議全球金融機構應以 2035 年前完成全面遷移為共同目標。

對於金融機構而言，量子破密威脅已是不容忽視的現實挑戰，更是當前必須嚴陣以待的兩大即時營運風險：

- **現在竊取，稍後解密（HNDL, Harvest Now, Decrypt Later）**
  外部威脅組織目前正大量側錄並儲存金融機構的加密通訊封包，待 Q-Day 到來，這些具備長年保存價值與法規要求的歷史資料（如客戶個資、長期授信合約）將被輕易解密，引發嚴重的機密外洩與商譽損失。

- **現在信任，稍後偽造（TNFL, Trust Now, Forge Later）**
  數位簽章是金融電子合約與交易不可否認性的基礎，若攻擊者未來能利用量子運算反推私鑰，將可竄改歷史交易軌跡或偽造憑證授權，嚴重衝擊金融信任基礎，並衍生重大營運與法遵風險。

面對上述威脅，全面遷移至抗量子加密架構已成為金融業不可迴避的戰略必要性。然而，PQC 遷移工程在實務層面極具複雜度，絕非依循常規資安更新（如單純安裝修補程式）即可一夕達成，相較於一般資安修補僅針對特定漏洞進行局部更新，PQC 遷移牽涉到底層基礎設施的全面重構，以及整體金融生態系的高度相依性，使其實務落地面臨多重嚴峻的技術與營運壁壘：

- **內部技術包袱與硬編碼限制（Legacy Dependency）**
  早期金融系統設計普遍缺乏模組化，密碼演算法與業務邏輯存在深度的「硬編碼 （Hardcoding）」，抽換演算法需要漫長的開發與迴歸測試。

- **硬體支援度與網路傳輸效能限制**
  新一代 PQC 演算法（如 ML-KEM 或 ML-DSA）的金鑰體積與數位簽章長度遠大於傳統密碼，這將帶來了兩大直接限制：首先，在硬體

設備方面，現有的硬體安全模組（HSM）、資安防護設備與終端晶片，往往受限於既有規格，不一定已經能夠支援 PQC 的龐大運算與儲存需求；其次，在網路傳輸方面，金鑰尺寸的增加會導致通訊封包變大，不僅容易引發封包分段（Fragmentation）與傳輸延遲，更可能影響整體網路的傳輸效能與服務高可用性。

- **生態系高度相依的斷鏈危機（Ecosystem Dependency）**

  金融產業並非封閉的資訊孤島，而是由核心清算中樞、信用資訊交換平台、財金資訊公司、聯合信用卡中心、外匯指定銀行及無數會員機構共同交織而成的生命共同體。單一銀行內部系統縱使完成 PQC 改造，若對接的清算節點或外部生態圈未能同步支援，將直接導致通訊封包無法解析，進而提高金融服務中斷與互通失效之風險。

基於上述複雜挑戰，PQC 遷移必須透過縝密的資源分配，採取與整體金融生態系步調一致的「漸進式遷移」策略。因此，面對不斷逼近的 Q-Day，金融機構在實務上已無充裕時間等待技術全面成熟才啟動轉型，而是必須立即著手進行「有效且有序的資源分配」，即管理階層應將有限的資安預算與技術資源優先投入於最危急的節點，藉此排定漸進式的遷移優先順序矩陣，落實有效且有序的風險治理理念。

本研究將聚焦金融支付與交易系統面臨量子威脅之遷移策略與注意事項，並針對以下核心面向進行探討，供作金融機構佈局 PQC 遷移與風險管理之實務參考方向：

(一)監理合規與現況識別

彙整國內外主管機關最新頒布之政策方針與監理要求，確立金融業由「合規導向」邁向「營運韌性」的戰略藍圖。

(二)資產盤點與風險動態量化

探討專屬於金融情境的「密碼技術資產清單（CBOM）」建置，並結合量子風險量化模型，供金融機構在有限資源下排定系統汰換的優先順序矩陣。

(三)遷移策略與技術落地架構

分析應用程式與密碼解耦之「加密敏捷性（Crypto-Agility）」中台化設計，以及兼顧現有合規與向下相容的「混合加密模式（Hybrid Mode）」過渡方案。

(四)例外管理與供應鏈風險管控

針對第三方軟體依存性、供應鏈盡職調查，以及無法即時升級之遺留系統（Legacy Systems），探討合約規範更新與例外補償性控管之注意事項。

(五)金融生態系共同遷移治理機制

探討由國家級金融市場基礎設施（FMI）與樞紐機構（Hubs）領頭之跨機構聯防架構，歸納制定共通 PQC 版本基準、互通性沙盒、供應商共用查核與全局灰度切換等生態系協作機制。

二、金融支付與交易系統之密碼應用現況與量子曝險

量子運算技術的快速發展，正對全球金融支付與交易生態系的底層架構構成系統性風險，一旦支撐現代金融信任基石的傳統非對稱式密碼學防線遭攻破，將對核心清算與交易體系的互通性與信任鏈造成重大衝擊，進而影響跨國資金調度、客戶資產安全與整體市場的公信力。面對此一技術發展趨勢，金融機構採風險導向啟動 PQC 遷移與落實加密敏捷性，已是確保營運連續性與金融韌性的重要核心戰略。

為釐清遷移 PQC 面臨之真實風險邊界與基礎設施挑戰，以下針對金融交易系統中四大核心交易場景的「非對稱密碼風險」、「對稱密碼與雜湊強度風險」與「遷移效能與互通性風險」進行分析與說明：

（一）四大核心交易場景之技術風險與曝險剖析

1. 網路銀行與行動支付系統

- 非對稱密碼風險

  網路銀行與行動支付高度依賴 TLS 通道之 ECDHE 或 RSA-2048 進行金鑰交換，此機制面臨「先竊取，稍後解密（HNDL）」側錄風

險，將嚴重影響歷史通訊的機密性，待 Q-Day 到來，駭客能解密歷史封包導致客戶個資外洩。

- 對稱密碼與雜湊強度風險

  通道建立後的資料傳輸依賴對稱密碼（如 AES-GCM）與雜湊（SHA-256），受 Grover 演算法削弱影響，其安全強度將面臨折損。依據 NIST 安全強度分類原則，對具長期保密需求、高價值資料或核心信任根相關場景，應優先採用 AES-256 或相當安全強度之配置；對一般短期交易通訊，則可依資料保存年限、威脅模型與效能需求，採風險導向方式逐步調整，以維持通訊安全性。

- 遷移效能與互通性風險

  PQC 憑證與金鑰體積龐大，極易超過網路設備之最大傳輸單元（MTU），導致 TCP 封包分段與傳輸延遲，引發網路銀行交易逾時（Timeout）斷鏈。

2. ATM 跨行清算與卡片交易系統

- 非對稱密碼風險

  系統之遠端管理、主機間通訊信任鏈與 HSM 韌體簽章高度依賴 X.509 等憑證體系，若設備憑證、遠端維運通道或韌體簽章仍依賴傳統 RSA/ECC，一旦遭 Shor 演算法破譯，未來可能面臨設備身分偽冒、韌體更新驗證失效、主機間通訊信任鏈被破壞，或設備管理權限遭濫用等系統性風險。

- 對稱密碼與雜湊強度風險

  晶片卡與 ATM 間的 PIN Block 及 MAC 訊息鑑別碼，多採用 3DES 或 AES-128，受 Grover 演算法削弱影響，應另以提升金鑰長度（如升級至 AES-256）、確保安全餘裕、強化 HSM 控管與設備汰換週期來進行風險評估與防護。

- 遷移效能與互通性風險

  現行維運中的舊款 HSM 設備與終端晶片卡，受限於晶片實體記憶體配額與運算暫存區，導入 PQC 演算法極易引發記憶體溢位（Buffer Overflow）或因運算過久導致清算逾時。

3. 線上證券與期貨下單系統

- 非對稱密碼風險

  電子下單高度依賴商用 PKI 憑證與金融 FIDO 進行數位簽章，該機制面臨「現在信任、稍後偽造（TNFL）」的完整性危機，駭客未來可跨越時間偽造歷史交易軌跡或電子契約。

- 對稱密碼與雜湊強度風險

  數位簽章底層依賴之雜湊函數（如 SHA-256）必須同步檢視其抗碰撞（Collision Resistance）強度，避免因雜湊碰撞導致簽章防護力下降。

- 遷移效能與互通性風險

  雙軌憑證過渡期間，需確保客戶端載具（如手機 App、硬體憑證）同步支援新舊演算法，維持向下相容性，避免投資人無法下單引發客訴與市場波動。

4. 跨境大額電匯與外匯業務

- 非對稱密碼風險

  跨境業務高度依賴 SWIFT 等國際金融市場基礎設施（FMI）骨幹網路的 PKI 簽章體系，若遭破譯將衝擊跨國結算的不可否認性，並對整體生態系的信任鏈與互通性形成重大營運風險。

- 對稱密碼與雜湊強度風險

  跨國大額押碼機制所使用之對稱金鑰與雜湊檢驗碼，必須配合國際組織規範，全面盤點並升級至高強度標準。

- 遷移效能與互通性風險

  跨境核決涉及複雜之多元演算法相依性，高度依賴跨國第三方 IT 供應鏈，若內部升級排程未能與 SWIFT 切換期限對齊，將導致通訊電文遭拒與清算斷鏈。

為清晰勾勒具體之風險輪廓，四大核心交易場景之 PQC 技術風險與遷移挑戰，彙整分析如表 1：

表 1：四大核心交易場景之 PQC 技術風險與遷移挑戰分析表

核心交易場景	非對稱密碼風險 (Shor 演算法威脅)	對稱密碼與雜湊強度風險 (Grover 演算法威脅)	遷移效能與互通性風險 (架構與生態系衝擊)
網路銀行與行動支付	**HNDL 機密性風險：**TLS 憑證與金鑰交換遭破譯，歷史側錄封包遭解密外洩	**對稱密碼強度面臨折損：**AES 通道加密與 SHA 雜湊應採風險導向調整；高機敏場景優先採 AES-256，一般短效通訊則依效能逐步加固	**封包膨脹與傳輸延遲：**PQC 憑證與金鑰體積龐大，極易超過設備最大傳輸單元（MTU）導致封包分段，引發網銀交易逾時斷鏈
ATM 跨行清算與卡片交易	**設備偽冒與信任鏈破壞：**設備憑證、遠端維運通道或 HSM 韌體簽章遭反推私鑰後，將面臨身分偽冒、韌體驗證失效或管理權限遭濫用等風險	**PIN/MAC 強度管理：**面臨金鑰強度不足風險，應依安全餘裕與 HSM 設備汰換週期進行評估與防護	**端點記憶體溢位：**現行維運中之舊型 HSM 與終端晶片卡，極易因 PQC 龐大運算量引發實體記憶體溢位（Buffer Overflow）與清算逾時
線上證券與期貨下單	**TNFL 完整性與法律風險：**PKI 與 FIDO 簽章遭偽造，駭客可跨越時間竄改歷史交易軌跡	**雜湊抗碰撞風險：**數位簽章底層之雜湊長度若不足，將直接影響簽章有效性	**用戶端相容性：**雙軌憑證過渡期需維持舊載具互通性，避免引發下單中斷
跨境大額電匯與外匯業務	**國際信任鏈受衝擊：**SWIFT 等國際金融訊息網路之 PKI 或簽章機制若遭破譯，將衝擊跨境訊息驗證、不可否認性與互通性	**押碼機制強度風險：**跨國押碼對稱金鑰需配合國際規範全面加固升級	**生態系斷鏈危機：**高度依賴國際 FMI，若未對齊 SWIFT 遷移時程將導致電文遭拒

資料來源：本研究整理

（二）生態系與供應鏈依賴之管理現況

在檢視完上述四大核心交易場景後，金融機構在推動 PQC 遷移前，尚需客觀檢視以下兩大系統性現況與管理議題：

1. 共通基礎設施的樞紐連動限制 （Hub-and-Spoke Dependency）

   全球金融產業具備高度互聯的生態系特性，跨機構資料交換與清算多仰賴樞紐機構（Hub）建立共通基礎設施與信任鏈，個別商業銀行在評估 PQC 遷移時，無法單獨變更跨行 API 或專線的加密規格。實務上，必須由生態系中的樞紐機構（以國內為例，如財金資訊公司、聯合徵信中心等關鍵資訊基礎設施）先行確立共同測試基準與過渡期互

通方案，因此，金融業的 PQC 轉換時程具備高度連動性，必須配合共通基礎設施的聯防升級節奏，方能避免單一節點延遲導致整體互通失效之風險。

2. 第三方軟體黑箱（Black-box）與相依性限制
金融機構內部運行大量委外開發的套裝軟體（COTS），其密碼學模組多深埋於編譯後的檔案中，形成「黑箱（Black-box）」限制。由於過往普遍缺乏軟體材料表（SBOM）的管理，導致資安團隊在進行加密現況盤點時，往往無法精準識別委外系統中涵蓋的傳統演算法，這使得遷移進度易受制於原廠升級規劃，成為現階段供應鏈管理需克服的挑戰。

三、國內外監理合規藍圖

PQC 的遷移並非金融機構單一實體的技術升級，而是一場高度依賴全球生態系互操作性的集體行動，若缺乏統一的技術標準與明確監管時程，將導致密碼體系碎片化，進而引發營運中斷風險。為因應此一系統性威脅，全球關鍵主管機關與標準化組織已紛紛提出具體的遷移藍圖、遷移時程與方法論，甚至將 PQC 準備度升格為金融資安的法遵合規要求與規範指引，期望透過確立統一的技術標準與明確的監管時程，讓全球金融生態系能有所依循，落實步調一致的集體行動。奠基於此一全球監理趨勢，以下將探討國內外監理合規藍圖與治理框架：

（一）國際標準化與跨國監理政策路線圖

面對量子破密威脅，國際標準化組織、各國金融監理機構以及跨國金融基礎設施，已加速從理論風險評估邁向實質合規要求的頒布與技術落地：

1. 美國國家標準暨技術研究院（NIST）：於 2024 年 8 月正式發布全球首批 PQC 聯邦資訊處理標準（FIPS），包含 FIPS 203（ML-KEM，用於金鑰封裝）、FIPS 204（ML-DSA，用於數位簽章）以及 FIPS 205（SLH-DSA，用於無狀態雜湊數位簽章），此舉意味著後量子密碼技術已跨越純學術理論的探討，正式進入可供企業與金融機構實際導入、建置於商用資訊系統的落地階段。

2. 美國國家安全局（NSA）：於 2024 年 12 月更新《商用國家安全演算法套件 2.0》（CNSA 2.0）強制令，要求各類關鍵通訊作業與網路傳輸協定於 2030 年前完成 PQC 配置，並於 2035 年全面汰除 RSA 與 ECC 等傳統加密技術。

3. 歐盟數位營運韌性法案（DORA）：於 2025 年 1 月正式適用，明確要求董事會必須對資通訊科技（ICT）風險管理負最終責任，並強制金融機構將供應商之「量子準備程度」納入第三方風險管理與供應鏈合規查核中。

4. 國際清算銀行（BIS）：於 2025 年 7 月發布《金融體系的量子就緒度：路線圖》，強調各國央行與商業金融機構必須將量子風險納入總體審慎監理框架與企業全面營運韌性治理框架中。

5. G7 網路專家小組（CEG）：於 2026 年 1 月發布「金融領域後量子密碼遷移協調路線圖」聲明，建議全球金融機構應以 2035 年前完成全面遷移為共同目標，並於 2030 至 2032 年間優先推動高風險系統之遷移，以避免單一機構或節點因密碼遭破譯，進而引發整體金融網路的連鎖性危機。

6. 日本金融廳（FSA）：於 2024 年 11 月發布報告書，強調金融機構除了掌握自身系統外，更必須盤點委託第三方維運之重要系統與訊號傳輸加密方式，落實供應鏈盤查。

7. 新加坡金融管理局（MAS）：於 2024 年 2 月發布「量子風險資安諮詢」，明令金融機構須盤點密碼資產並逐步過渡至 PQC；後續於 2024 年 11 月與法國央行聯合發布實驗報告，推動跨境通訊驗證。

8. 全球銀行間金融電訊網路（SWIFT）：公開資訊顯示 SWIFT 已將 SwiftNet 8.0 與 PQC 支援納入後續升級路線，金融機構內部排程應預留足夠時間配合外部網路之共同測試、分階段切換與回退演練。

9. 支付卡產業安全標準委員會（PCI SSC）：於 2024 年 3 月生效之 PCI DSS v4.0 規範中，要求企業維護客製化及第三方軟體之元件清單，並建立加密敏捷性以防範未來威脅。

10. 世界經濟論壇（WEF）：於 2024 年 1 月發布白皮書，提出四階段路線圖，包含：準備（盤點加密資產）、釐清（分析遷移成本）、指導（促進標準化與跨境一致性）以及轉型與監測，以協調全球金融生態系的步調。

（二）我國金融資安藍圖與 PQC 政策發展方向

對接國際監理趨勢，我國資安政策與金融監理體系亦積極展開前瞻部署，整體政策方針透過跨部會協作與資安藍圖的推動，引導金融業將 PQC 遷移視為提升營運韌性的核心戰略，具體推動主軸可歸納如下：

1. 金融資安韌性發展藍圖的前瞻部署

   金融監督管理委員會（FSC）於 2025 年 12 月發布《金融資安韌性發展藍圖》，強調金融資安防護應從傳統的「合規導向」轉型為以「營運韌性」為核心的成果導向。該藍圖中明確將 PQC 遷移列為推動重點，並要求金融機構推動「資安左移（Secure by Design）」，在軟體開發生命週期（SDLC）中導入軟體物料清單（SBOM）與加密敏捷性（Crypto-Agility），從根本強化防護體質。

2. 跨部會指引與金融業先導計畫之推動

   在國家層級，數位發展部（MODA）於 2025 年 4 月發布《後量子密碼遷移指引》，提出「建立量子準備計畫、盤點加密資產清單、與技術供應商討論、確認供應鏈準備程度」之四階段基礎框架。為使政策精準貼合金融實務，金管會於 2025 年 6 月訂定「金融業後量子密碼遷移先導計畫」，邀集財金公司、集保結算所、銀行、證券、保險等代表性機構籌組「金融業後量子密碼遷移先導小組」，透過金融資安資訊分享與分析中心（F-ISAC）建立溝通討論平台，先行啟動加密技術盤點與業務衝擊評估，以凝聚推動共識。

3. 發布專屬遷移指引與七大策略框架

   基於先導計畫的實務回饋，金管會於 2026 年 6 月正式頒布《金融業後量子密碼遷移參考指引》。該指引明確提出因應 PQC 遷移的七大策略方向（彙整如表 2），並勾勒出至 2035 年的推動時程建議（彙

整如表 3），希望能透過此一涵蓋方法、策略與時程的綜合性參考指引，供金融機構能有系統地調度跨部門與供應鏈資源，穩健落實轉型任務。

表 2：金融業因應 PQC 遷移的七大策略

策略編號	策略方向	具體實務重點
策略一	PQC 政策與治理	將密碼技術風險納入企業風險管理。將量子風險提升至董事會層級，並成立由資安長 （CISO） 或資訊長（CIO）召集之跨部門「後量子遷移工作小組」，明確權責與資源配置
策略二	盤點密碼技術應用，建立密碼技術資產清單 （CBOM）	依「先風險、後全面」原則，建立可連結業務情境與外部依賴的動態資產清單，並評估導入自動化工具輔助維護
策略三	提升加密敏捷性，優先清除密碼反模式	採模組化加密設計與憑證自動化管理 （CLM），優先改善手動憑證管理、弱加密套件與金鑰硬編碼等技術負債，以因應未來演算法的靈活抽換
策略四	建立生態系協作機制與共通業務風險圖像	透過「四階呈現」概念推動跨機構對齊，由樞紐機構（如財金公司、證交所等）統籌推進並制定共通標準，協助同業以一致脈絡展開自體盤點
策略五	以風險導向建立遷移優先序	採「量子風險評分」與「遷移時間評分」雙軸交叉評估，將系統分群排序，結合外部約束條件，產出可執行的分期推進路線圖
策略六	更新採購與供應鏈管理要求	將 PQC 準備度納入採購與委外合約管理，啟動關鍵供應商調查與共同驗證機制，降低因「卡關元件」未升級而導致的遷移延宕風險
策略七	建立測試、切換與營運韌性機制	在系統上線時應採取「分段逐步切換」以控制影響範圍，並確實演練「異常時的復原倒退（Rollback）機制」；同時需建立系統監控與留存完整測試紀錄，形成可稽核的證據鏈，以將遷移期間發生服務中斷或連線失敗的營運風險降至最低

資料來源：本研究參考金管會指引整理

表 3：金融業後量子密碼遷移推動時程建議

推動階段	預計時程	建議重點
短期	2026-2027 年	聚焦建立治理架構與 CBOM 清冊
中期	2027-2029 年	著重推動試辦驗證與基礎升級
中長期	2029-2035 年	優先完成高風險系統遷移並逐步擴大場景

資料來源：本研究參考金管會指引整理

四、資產盤點與動態風險量化機制

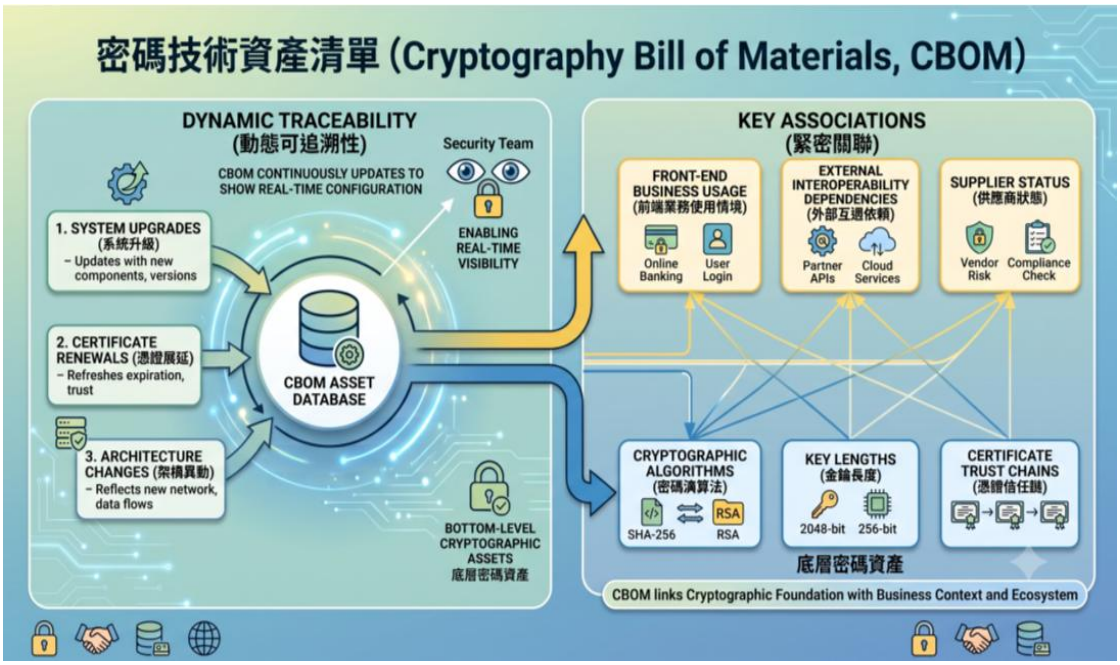
（一）密碼技術資產清單（CBOM）之實務建置與生態系盤點框架

在資訊安全管理領域，「資產可視性（Visibility）」是風險防禦的基石，這點在面對量子破密威脅時尤為關鍵，依據國內外主管機關之指引，金融機構推動 PQC 遷移的首要任務，即是全面清查並建立專屬的密碼技術資產清單（Cryptography Bill of Materials, CBOM），相關說明如下：

1. 密碼技術資產清單之定義與產出價值

CBOM 並非一份單純的靜態 IT 硬體或軟體設備清冊，而是一份具備動態可追溯性（即清單內容需隨系統升級、憑證展延或架構異動而持續更新，使資安團隊能隨時掌握加密資產的真實配置），且能將「底層密碼演算法、金鑰長度、憑證信任鏈」與「前端業務使用情境、外部互通依賴及供應商狀態」緊密關聯的密碼技術資產清單（如圖 1 所示）。

圖 1：密碼技術資產清單關聯示意圖



資料來源：本研究整理 AI 繪製

產出 CBOM 的核心價值在於透過盤查消除系統深處的加密盲區（例如深埋於系統底層的硬編碼金鑰或第三方套件中未被察覺的傳統弱密碼演算法）。透過此清單，管理階層得以量化評估量子曝險程度，精

準識別缺乏加密敏捷性（Crypto-Agility，即系統能快速且無痛抽換底層密碼演算法的彈性）的技術負債，據以排定系統汰換的優先序，並將其作為檢視供應商合規狀態與擬定長期採購預算的具體依據。

2. 盤點範圍與執行順序策略

面對金融機構內部成千上萬的異質資訊系統，若初始即要求全面性普查，極易因耗時過長而延宕實質遷移進度，實務上應採取「風險導向（Risk-based）、漸進擴張（Phased）」的策略。在執行順序上，第一階段應優先鎖定高曝險（如對外網銀 TLS 端點、跨機構 API 閘道、VPN 連線）與高價值（如保存期限長達 10 年以上的客戶個資、電子保單、核心帳務資料庫）之應用場景；第二階段再逐步擴展至內部一般行政系統、封閉環境網路與非敏感日誌儲存系統。

3. 盤點方法論、工具與相關理論框架

為確保 CBOM 的精確性與覆蓋率，業界最佳實務提倡結合「Top-Down（由上而下之業務視角）」與「Bottom-Up（由下而上之工具探測）」的雙軌盤點方法論及清單最小可用欄位：

- Top-Down 業務視角盤點與理論框架

依據數位發展部指引，組織可引入標準化風險框架協助盤點與分類，例如導入 PASTA（攻擊模擬與威脅分析流程），由核心業務目標（如跨行轉帳、證券下單）出發，向下拆解應用程式與資料流，識別出外部網路或限定設備中可能遭受攔截的關鍵加密控制點；同時可搭配 CARAF（加密敏捷性風險評估框架），評估所盤點出之演算法是否應用於關鍵業務、是否有適用的新演算法可替換，以及系統轉換的技術可行性。

- Bottom-Up 自動化工具探測

單靠人工填報易產生漏網之魚，必須導入自動化探測工具。實務上可利用網路流量側錄與探測工具（掃描 Cipher Suites、TLS 版本與憑證效期），並結合軟體成分分析（SCA），深入剖析遺留系統（Legacy

System）或第三方套裝軟體（COTS），找出以硬編碼（Hard-coded）形式深埋的傳統弱密碼函式庫。

- 清單最小可用欄位

  產出的 CBOM 應強制包含最小可用欄位：業務情境、密碼演算法與參數（如 RSA-2048）、憑證信任鏈、金鑰來源部署（自建 CA、KMS、HSM），以及供應商版本支援狀態等。

4. 統一生態系盤點標準的「四階呈現」概念

   金融系統具備高度互連性，跨行轉帳、證券交割等業務皆需要多家機構的系統對接，如果各銀行使用自己的標準和術語來盤點系統，在未來切換新加密演算法時，極易因 API 規格不一致而導致連線中斷（斷鏈），為解決此問題，金管會最新指引建議使用「四階呈現」的盤點概念。該概念從資訊工程與系統介接的角度而言，其核心邏輯是釐清「誰先開規格、誰跟著盤點」，讓整個金融圈能在同一個基準上對齊規格，彙整「四階呈現」概念如表 4：

表 4：統一生態系盤點標準的「四階呈現」概念

呈現階層	概念與具體作法
第一階 （樞紐定義規格）	由生態系的中心樞紐（Hub，例如財金公司、證交所、聯徵中心等）先行啟動，明確定義跨機構共用平台的 API 介接規格、密碼標準與預計切換時程
第二階 （對接端點盤點）	各商業銀行（對接端）收到樞紐機構開出的標準後，再回頭檢視自身負責對接該 Hub 的閘道器或系統，盤點其金鑰來源與相依供應商是否能支援新規格
第三階 （內部自主盤點）	對於完全不涉及跨機構連線的銀行內部核心系統，由各機構依自身業務需求與系統架構，自主進行風險盤點與遷移規劃
第四階 （共通基礎設施統整）	將整個金融圈共同依賴的底層技術（如特定廠牌的硬體安全模組 HSM、憑證機構 CA 等）獨立納入盤點，集中追蹤這些關鍵供應商的升級進度

資料來源：本研究參考金管會指引整理

（二）雙軸動態量化評估與遷移優先序熱力圖

當金融機構完成 CBOM 建置後，面對龐大的資訊系統，必須在有限的資安預算與營運人力下，客觀排定系統的汰換順序，實務上，金融機構應導入科學化的動態量化模型，並結合金管會指引中建議的雙軸評估指標，建構具備實質執行力的「遷移優先序熱力圖」，相關評估方法論如下：

1. 整合 Mosca 定理評估量子破密風險

為了協助金融機構具體評估遷移至 PQC 的急迫性，實務上常導入密碼學權威提出的「莫斯卡定理（Mosca's Theorem）」，該定理以不等式 D + T > Q 作為核心治理邏輯，各項變數定義如下：

•D（Data Shelf-life / 資料保密年限）

金融數據需要保持絕對機密的法定或業務年限（如 10 年）。

•T（Transition Time / 系統遷移時間）

組織將現有基礎設施全面升級至 PQC 並完成測試所需的時間（保守估計需 3 至 5 年）。

•Q（Quantum Timeline / Q-Day 倒數）

距離實用化量子電腦（CRQC）問世、具備實質破密能力的時間（儘管目前的具體年限仍有高度不確定性，但實務上常以 10 年作為風險評估的情境基準）。

從上述公式可知，若某核心系統的 D（10 年）+ T（5 年）> Q（10 年），即代表該系統已處於「量子破密危險期」，對於駭客採取「先攔截、日後解密（HNDL）」攻擊的高價值資料而言，金融機構必須立即啟動遷移專案，以防範資料在未來遭回溯解密的實質風險。

2. 建構雙軸交叉評估模型

Mosca 定理確立了時間上的急迫性，但在決定企業資源配置的優先順序時，還需整合「雙軸交叉評估模型」進行綜合量化，此雙軸指標（如圖 2 所示）將協助管理階層客觀衡量系統的風險與轉換難度：

- Y 軸：量子風險評分（急迫性）

衡量該系統遭破密後的損害程度，主要考量因子包含：

A. 資料敏感保密年限：呼應 Mosca 定理中防範 HNDL 攻擊的需求。

B. 系統曝露程度：對外網路通路、跨機構 API 介接等外部攻擊面。

C. 衝擊嚴重性：營運中斷、法遵罰鍰與聲譽損失。

- X 軸：遷移時間評分（難易度）

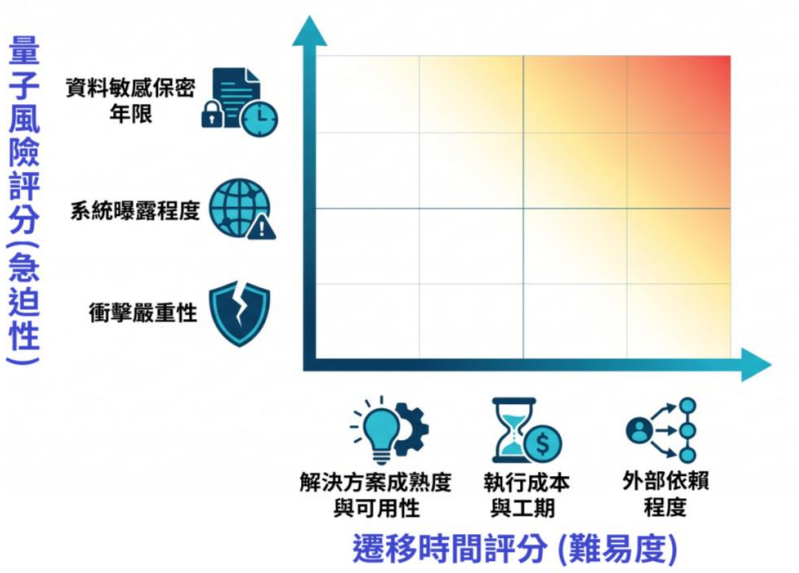
衡量該系統轉換至 PQC 的執行難度與工期，主要考量因子包含：

A. 解決方案成熟度與可用性：市場上是否有成熟的 PQC 替代方案。

B. 執行成本與工期：是否牽涉龐大的硬體（如 HSM）汰換或底層架構重構。

C. 外部依賴程度：供應商的 PQC 準備度與國際標準對齊狀況。

圖 2：雙軸交叉評估模型指標



資料來源：本研究整理 AI 繪製

3. 遷移優先序熱力圖與實務處置

將上述兩軸的評分結果進行高低分群後，即可繪製出「遷移優先序熱力圖」(如圖 3 所示)。透過此矩陣，管理階層即可將資源配置於四大對應區塊中，其具體實務處置說明如下：

- 優先處理（高風險、低複雜度）— 現代化計畫／近期改版處置

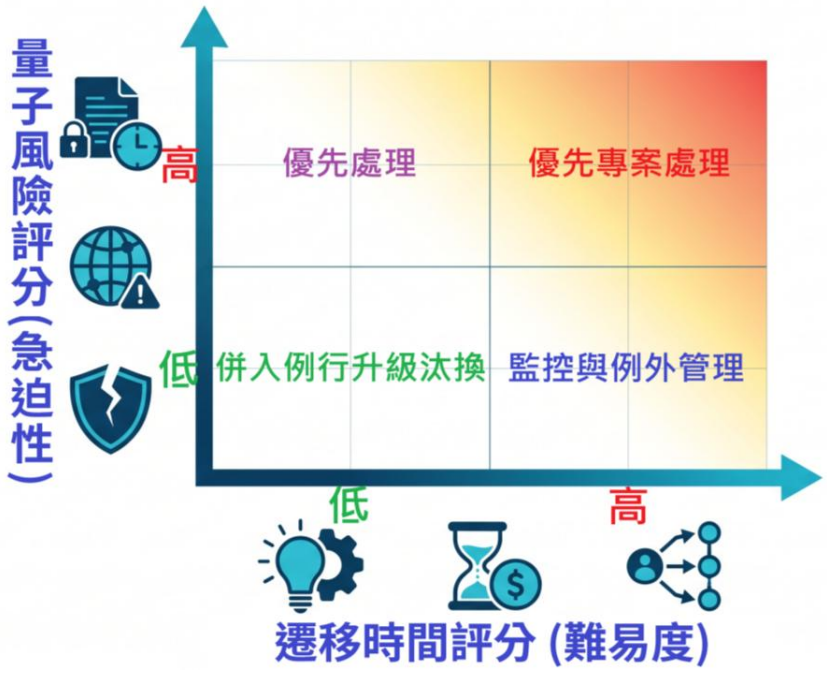
涵蓋高曝險但易於調整的系統（如：對外網銀 / 行動銀行之 TLS 端點），可優先納入近期改版，透過「無悔作為」快速清理密碼技術負債。

- 優先專案處理（高風險、高複雜度）— 跨部門專案／及早啟動
  涵蓋威脅極高且牽連廣泛的核心系統（如：核心帳務系統、外匯交易撮合系統及憑證基礎建設 CA），必須立即啟動供應鏈對話與共同測試。

- 併入例行升級汰換（低風險、低複雜度）— 例行維運自然滾動
  涵蓋低曝險且易於轉換的系統(如：內部行政、非敏感日誌儲存系統)，隨系統日常維運與生命週期自然滾動更新即可。

- 監控與例外管理（低風險、高複雜度）— 併入長期設備汰換
  涵蓋低風險但牽涉底層硬體的系統(如：內部資料庫備份)，可與長期設備汰換節奏整合，在日常改版中自然消化，並加強周邊防護監控。

圖 3：金融系統 PQC 遷移優先序熱力圖



資料來源：本研究整理 AI 繪製

4. 外部關鍵機構與規範之優先遵循（重要約束條件）
   在運用熱力圖評估系統汰換優先序時，金融機構不應僅依賴內部評分結果，更應將外部金融市場基礎設施與主管機關之遷移藍圖，列為資源配置與專案排程之重要約束條件。實務上，若系統涉及跨機構連線

（如 SWIFT 網路），或其存證資料具備長期驗證（LTV）需求，且外部機構或法規已建立明確轉換里程碑，金融機構即應主動對齊外部切換窗口。此類外部規範的時程指標應優先於內部排程，金融機構應據此重新檢視專案優先級，並預留充分時間配合共同測試與升級，以確保內部排程與外部生態系無縫接軌，防範互通失效與營運中斷風險。

（三）實務量化評估範例

依據上述「量子風險評分」與「遷移時間評分」雙軸交叉評估模型，結合 Mosca 定理中 Q=10 年（情境基準）之不等式邏輯，針對六大常見金融關鍵資訊資產進行模擬量化評估（如表 5 所示），透過界定各系統資產之資料保密年限（D）、內部遷移工期（T）與外部供應鏈限制，精準推導其於熱力圖之落點與執行優先序，進而作為管理階層優化資源配置、排定中長期專案時程與制定遷移藍圖之關鍵依據。

表 5：金融支付與交易系統 PQC 遷移優先序量化評估範例表

系統資產與應用場景	量子風險評分 (Quantum Risk)			遷移時間評分 (Migration Time)			Mosca 風險判定	熱力圖落點	遷移優先序
	資料保密年限 (D)	曝露程度	衝擊嚴重性	內部工期 (T)	外部依賴程度	解決方案成熟度			
1.根憑證基礎建設(Root CA 系統)	15 年 (長效憑證)	中 (封閉維運)	極高 (信任根)	4 年	高 (跨機構)	中 (PQC 標準剛落地)	15+4>10 (信任根基已具 TNFL 偽造風險)	**【優先專案處理】** (高風險/高需時)	跨部門專案／及早啟動 (納入核心打底範圍，優先排入預算)
2.跨境電匯閘道 (SWIFT Gateway)	10 年 (法規存證)	中 (專線/封閉)	高 (斷鏈風險)	3 年	極高 (國際組織)	中 (配合升級)	10+3>10 (資料保密已具 HNDL 風險)	**【優先專案處理】** (高風險/高需時)	強約束條件／限期專案 (內部排程須緊貼 SWIFT 升級切換時程)
3.網銀/行動 App TLS Gateway	3 年 (短效通訊)	極高 (網際網路)	高 (資料外洩)	1 年	低 (自控端點)	高 (軟體成熟)	3+1<10 (風險雖急，但可速解)	**【優先處理】** (高風險/低需時)	近期改版／無悔作為 (因應網際網路曝險較高，應優先處置以收斂風險)

4.ATM 硬體安全模組(HSM)	5 年(PIN/MAC 效期)	低(實體隔離網路)	高(設備信任鏈與交易驗證風險)	3 年	高(PCI/FMI 認證)	低(原廠韌體發展中)	5+3<10(對稱機制風險較低；設備憑證與韌體簽章須納入汰換週期)	**【監控與例外管理】**(低風險/高需時)	併入例行升級／設備汰換(PIN/MAC 對稱加密受 Grover 威脅為主，應加固金鑰長度並等待 HSM 原廠成熟)
5.內部核心資料庫備份 (DB Backup)	10 年(客戶核心個資)	極低(內部深層網路)	高(大量歷史資料外洩)	3 年(巨量歷史數據轉置)	低(內部系統)	中(既有加密套件)	10+3>10(資料保密已有 HNDL 風險)	**【監控與例外管理】**(低風險/高需時)	併入長期維運／自然滾動 (因內部網路隔離使當前風險受控，後續採加密敏捷逐步汰換)
6.次要內部應用系統 (如行政系統)	3 年(行政資料)	極低(內部深層網路)	低(無機敏資料)	1 年	低(內部系統)	高(軟體成熟)	3+1<10(資料保密尚在 HNDL 威脅安全期)	**【併入例行升級汰換】**(低風險/低需時)	例行維運／延後處理(排於最後階段處理)

資料來源：本研究整理

上述量化評估範例表為情境模擬（設定情境 Q=10 年），實際評分與工期應依各金融機構之 CBOM 盤點現況為準。由該量化評估範例表可知，「1.根憑證基礎建設(Root CA 系統)」與「2.跨境電匯閘道(SWIFT Gateway)」不僅資料保密年限長，且高度受制於國際組織時程與第三方機構(高遷移時間），故熱力圖落於「優先專案處理」（高風險/高需時），應由董事會層級優先核定為跨部門中長期專案，以避免在未來的生態系切換中引發互通失效與營運中斷風險；而「3.網銀/行動 App TLS Gateway」雖然面臨外部駭客高度的 HNDL 側錄曝險（高量子風險），但因其軟體升級技術已相對成熟且外部依賴低（低遷移時間），故熱力圖落於「優先處理」（高風險/低需時），可由 IT 單位透過年度預算快速升級以達成「無悔作為」。

五、遷移策略與加密敏捷設計

面對 PQC 帶來的底層技術衝擊，金融機構無法、也不可能採取全面性且一次性的系統抽換。此次面臨由傳統密碼學遷移至 PQC 的過程，是一個持續精進的轉型，正是金融機構重新思考底層架構設計與落地防禦實作的

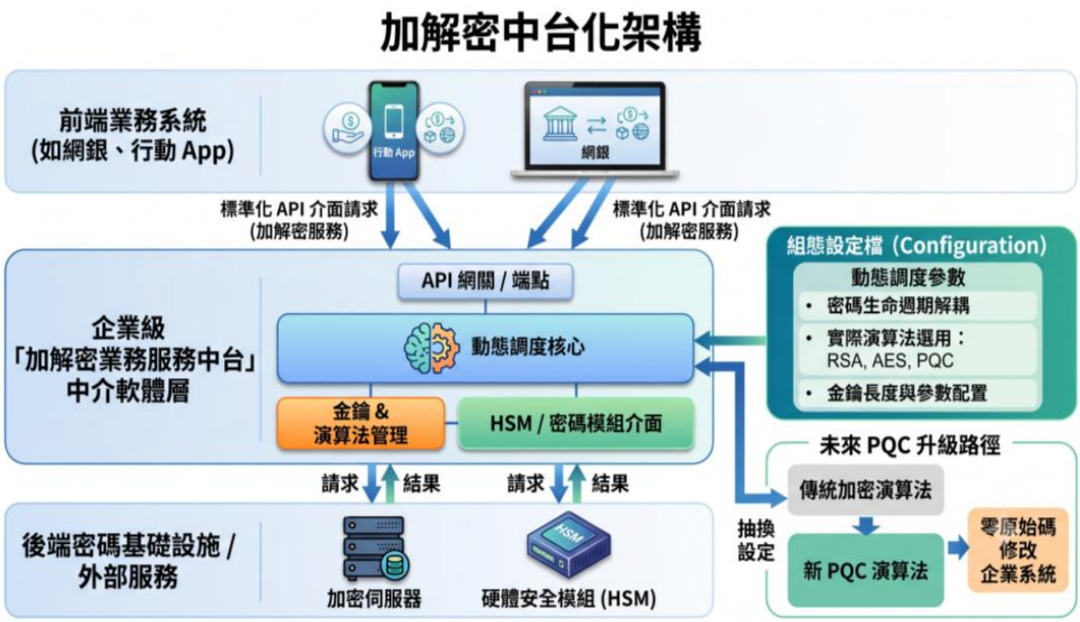
絕佳機會；更可藉由架構改造，因應未來潛在的密碼學更迭與系統相容替換等需求。因此，以下將探討如何透過加解密中台化架構、混合加密模式、硬體安全模組（HSM）的過渡防禦策略，以及供應鏈風險管理，來穩健落實加密敏捷性策略：

（一）加解密中台化架構

為避免重蹈傳統系統開發將特定加密演算法或金鑰直接硬編碼於原始碼之錯誤技術負債，金融機構應優先啟動「無悔作為」，清除不安全、過時的「密碼反模式（Cryptographic Antipatterns）」（如加密演算法硬編碼、手動管理憑證、使用弱加密套件等）。

實務上，應落實應用程式與密碼生命週期解耦，透過建構企業級的「加解密業務服務中台」或中介軟體層，讓前端業務系統（如網銀、行動App）只需呼叫標準化的 API 介面請求加解密服務；而實際的演算法選用、金鑰長度與參數配置，則由後端中台統一透過組態設定檔（Configuration）進行動態調度。如此一來，未來面對 PQC 演算法的迭代或實作漏洞修補時，資安團隊僅需在中台抽換設定，即可達成加密機制的無痛升級，實現零原始碼修改的敏捷防禦（加解密中台化架構示意如圖 4 所示）。

圖 4：加解密中台化架構



資料來源：本研究整理 AI 繪製

此外，為提升整體的加密敏捷性，針對龐大且繁雜的憑證，應導入自動化憑證生命週期管理（Automated CLM）系統，透過支援 ACME（自動憑證管理環境）、EST（憑證註冊與輪替標準）等標準協定與 CI/CD 流程整合。

（二）混合加密模式（Hybrid Mode）

當新一代 PQC 演算法尚未在全球硬體與瀏覽器生態系中得到全面優化與實戰驗證的過渡期，單獨部署純 PQC 演算法仍存在未知的實作漏洞或旁道攻擊風險。為了同時抵禦傳統駭客與未來量子電腦的雙重威脅，業界建議可採取混合加密模式作為安全強化的過渡手段，即在同一個通訊協定中，同時結合傳統密碼（如 ECC/RSA）與後量子密碼（如 ML-KEM/ML-DSA），只要其中一種演算法未被破解，通訊與資料即屬安全。

（三）硬體安全模組過渡防禦策略

面對既有硬體安全模組設備可能尚未支援 PQC 或短期內無法更動的前提下，金融機構可優先採用「軟體先行、硬體跟進」的過渡策略，於關鍵傳輸資料的外層，先透過軟體方案疊加一層 PQC 混合加密隧道進行保護作為因應，用以抵禦「先攔截、日後解密」的資料側錄風險，同時應將 HSM 硬體升級優先排入例行設備汰換與改版週期中。

（四）供應鏈風險管理

金融機構在新購軟硬體或重大系統改版時，應將前述資產盤點結果作為向供應商要求技術升級路線圖（Roadmap）的依據，防堵不合規之軟硬體設備進入企業環境。建議應於 RFP（需求建議書）與技術規格中明確列入「PQC 準備度」與「加密敏捷性」查核項目，同時在委外合約中，應要求廠商提供軟體物料清單（SBOM），揭露其套裝軟體內部的開源密碼函式庫版本，並將 PQC 升級承諾與退場替代方案明訂於服務水準協議（SLA）中，以確保供應商具備持續合規的升級能力。

（五）遺留系統例外管理

針對建置年代久遠、架構封閉且原廠已停止維護的老舊遺留系統

（Legacy Systems），往往存在無法升級至 PQC 演算法之技術限制，金融機構應對此類遺留系統進行補償性控管措施，具體作法包含：建構實體隔離的專屬受控網路環境，或在敏感數據進入老舊系統前，於外圍先行實施代碼化（Tokenization）或去識別化脫敏技術。如此一來，即使底層古典密碼在未來遭量子電腦攻破，駭客能回溯收割的資料亦將大幅降低其商業機敏價值，進而從源頭有效阻斷並收斂資料外洩之量子曝險。

六、金融生態系共同遷移治理機制

後量子密碼遷移絕非單一金融機構內部之 IT 升級專案，而是一場牽動全局的系統性工程，依據 G7 網路專家小組（CEG）與世界經濟論壇（WEF）之報告指出，缺乏協調的孤島式遷移將引發碎片化風險，導致國家和地區間的金融機構信任鏈與跨境互通斷裂。此外，我國金管會於近期發布之《金融業後量子密碼遷移參考指引》與《金融資安韌性發展藍圖》中，亦高度強調「生態系協作」與「建構跨域共防」之重要性。

為具體落實上述國內外監理指引之精神，彙整並歸納出由生態系樞紐機構（Hubs）領頭的五大共同遷移治理實務機制及治理分工表（如表 6 所示），供金融機構與周邊單位作為跨機構聯防之參考框架：

（一）歸納共通之「金融 PQC 版本基準（Profile）」

呼應《金融業後量子密碼遷移參考指引》中關於「建立過渡期互通與共同測試的版本基準」之要求，應由核心樞紐機構（如財金公司、證交所等）協同主管機關，彙整出金融生態系專屬之版本基準。該基準宜明確規範過渡期所需之強制混合金鑰交換組合（如 X25519 結合 ML-KEM-768）、雙軌憑證之標準格式，以及為因應封包膨脹而統一律定之最大傳輸單元（MTU）與連線逾時（Timeout）參數底線，以消弭各機構各自為政所造成的技術分歧與重工。

（二）整合「關鍵供應商共用查核機制」

依循《金融業後量子密碼遷移參考指引》中「建置（或整合）共通供應鏈調查與追蹤機制」以「降低重複詢查成本」之建議，考量金融生

態系高度共用少數關鍵之 HSM 供應商、CA 機構與核心系統商，業界可藉由金融資安資訊分享與分析中心（F-ISAC）統籌，建立共用之供應商準備度查核平台。透過統一的問卷與查核標準，要求供應商提供可驗證之軟體材料表（SBOM）、版本支援時程與測試證據，作為全體金融機構採購與驗收之共通準據。

（三）落實「跨機構共同測試與互通沙盒」

配合《金融業後量子密碼遷移參考指引》中「推動先導試辦與經驗分享」與建立「共同測試與驗證機制」之方向，核心清算網路與交易平台應提供 PQC 互通性沙盒測試環境。周邊對接之金融機構必須於沙盒中完成端到端之測試案例（包含測試憑證鏈與交易腳本），驗證新舊加密協定之相容性與系統處理延遲。唯有通過測試並取得互通性驗證之機構，方能排入正式生產環境之切換梯次。

（四）建立「灰度切換與回退（Rollback）」標準程序

依據《金融業後量子密碼遷移參考指引》對營運韌性之要求，跨行清算與跨境大額電匯之遷移不應採取一次性全面替換，而必須設計「分段切換、灰度（逐步）上線與平行運行」策略。跨機構間應共同協定切換之維護窗口與回退條件，一旦上線過程中觸發異常（如大量封包因 PQC 體積過大而遭網路節點拋棄或交易逾時），必須具備在極短時間內觸發「跨機構全局回退（Global Rollback）」之應變能力，將退版視為必備能力而非例外，防堵單點故障演變為系統性阻斷。

（五）將量子斷鏈風險納入「跨機構實戰演練」

對接《金融資安韌性發展藍圖》中「因應複合災難情境，建立關鍵服務多層次備援機制」之方針，主管機關與 F-ISAC 宜將「量子密碼遷移失敗導致之清算斷鏈」或「根憑證遭偽造」等極端情境，正式納入國家級之重大資安事件應變情境演練中。透過跨機構之實兵演訓，驗證各節點在面臨複合式量子災難時之跨區資源調度、替代通道切換與營運持續計畫（BCP）量能，從根本鑄造具備量子抵抗力之金融營運韌性。

表 6：金融生態系 PQC 共同遷移治理分工表

治理項目	主責單位	參與單位	具體產出物	建議時程
1.制定金融 PQC 版本基準 (Profile)	主管機關／FMI Hub	銀行、證券、CA 機構、HSM 廠商	共通演算法基準、憑證標準格式、MTU 與 Timeout 基準	短期 (準備與規劃期)
2.推動供應商共用查核機制	F-ISAC 或指定共用平台	HSM、CA、核心系統商等關鍵供應商	標準化共用問卷、軟體材料表 (SBOM)、供應商支援 Roadmap	短期 (準備與規劃期)
3.建置跨機構互通性沙盒	FMI Hub	對接之金融機構、第三方支付業者	端到端測試案例、交易腳本、互通性驗證通過報告	中期 (試辦與基礎升級期)
4.制定灰度切換與回退程序	FMI Hub／參與機構	全體清算網路與交易對接節點	跨機構共同切換窗口、全局回退 (Rollback)觸發標準與 SOP	中期 (優先遷移期)
5.將量子斷鏈納入跨機構演練	主管機關／F-ISAC	金融機構、FMI、關鍵技術供應商	重大資安事件演練報告、營運持續(BCP)檢討與改善清單	持續 (常態化辦理)

資料來源：本研究整理

七、結論與建議

面對量子運算技術對現行非對稱密碼體系帶來的潛在威脅，金融機構之 PQC 遷移是一項跨越技術、營運與供應鏈的長期系統性工程，本研究綜合國內外監理政策與主管機關發布之相關指引，於此彙總出 PQC 遷移面臨之實務挑戰與因應原則，並歸納四大核心交易場景及五大核心面向之因應策略，供金融機構實務推動之參考：

（一）PQC 遷移挑戰與因應原則

金融系統高度依賴密碼技術以確保交易安全與資產信任，在推動 PQC 遷移時，金融機構面臨加密技術應用分散、供應鏈高度相依、以及營運中斷容忍度低等實務挑戰，因此，金融機構應跳脫一次性演算法替換的思維，採取「風險導向、循序漸進」的原則，透過「提升加密敏捷性」，並落實「軟體先行、硬體跟進」與「混合加密模式」等過渡策略，在不衝擊交易連續性的前提下，穩健推進密碼體系之升級。

（二）四大核心支付與交易場域之遷移建議

針對先前四大核心交易場景之 PQC 技術風險與遷移挑戰，提出相對應之風險管理、實務作為與遷移順序等建議，彙整如表 7 所示：

表 7：四大金融核心場景之密碼應用與 PQC 遷移策略對照矩陣

金融功能業務	現行主要加密機制	量子曝險與技術挑戰	風險管理與實務建議作為	遷移權重建議
網路銀行與行動支付	•TLS 1.2/1.3 通道加密 •ECDHE 金鑰交換 •RSA-2048 伺服器憑證	1.非對稱：HNDL 側錄影響歷史通訊機密性 2.對稱：AES/SHA 強度面臨降級風險 3.效能：PQC 憑證過大導致 MTU 分段與傳輸延遲	•全面清查通訊設備升級路徑，並調整 MTU 緩衝區與連線逾時參數 •對稱密碼採風險導向升級，高價值資料優先配置 AES-256，短效期通訊則依效能逐步加固 •通道外層利用軟體疊加 PQC 混合隧道 •推動自動化憑證生命週期管理(CLM)	**【高】** 優先處理／立即規劃
ATM 跨行清算與卡片交易	•非對稱：X.509 憑證、HSM 韌體簽章 •對稱：MAC 訊息鑑別碼、3DES/AES-128 PIN Block	1.非對稱：信任鏈遭破壞引發身分偽冒與韌體驗證失效 2.對稱：PIN/MAC 需依安全餘裕與 HSM 汰換週期評估 3.效能：舊型 HSM 易引發 Buffer Overflow 與逾時	•針對憑證與簽章採取「軟體先行、硬體跟進」過渡策略 •針對 PIN/MAC，另行強化對稱金鑰長度與 HSM 汰換週期管理 •於採購需求(RFP)中強制加入 PQC-Ready 條款逐步汰換舊機	**【中】** 高度關注／短期推動
線上證券與期貨下單	•PKI 數位簽章 (RSA/ECC) •商用 CA 下單憑證 •金融 FIDO 身分認證	1.非對稱：TNFL 偽造影響歷史交易不可否認性 2.對稱：底層雜湊抗碰撞強度面臨考驗 3.效能：雙軌過渡期舊載具相容性維持困難	•引進雙軌憑證或複合式簽章，確保過渡期互通性 •針對高曝險內部客戶端認證憑證解耦並改用專屬 AP 憑證	**【高】** 優先處理／立即規劃
跨境大額電匯與外匯業務	•SWIFT 骨幹網路 PKI 簽章 •跨國大額押碼機制 •傳統多元演算法核決	1.非對稱：國際骨幹簽章破解引發信任危機 2.對稱：跨國押碼強度需配合國際標準升級 3.效能：未對齊國際 FMI 切換時程將引發斷鏈	•密切追蹤 SWIFT 及主要國際 FMI 的 PQC 遷移計畫，內部排程不得晚於外部切換期限 •依循 G7 CEG 路線圖，強化跨司法管轄區與第三方 IT 供應鏈協調	**【中長】** 中長程規劃／配合生態系

資料來源：本研究整理

（三）金融機構後量子五大核心面向因應策略

針對金融機構多元的加解密應用情境，實務上可將 PQC 因應策略歸納為五大核心面向，並採計美國國家安全局 CNSA 2.0 政策明定 2030 年前開始過渡、2035 年完成遷移之時間表，分別列示過渡階段（預計至 2030 年止）及實施遷移階段（預計至 2035 年止）之因應策略（彙整如表 8 所示），作為整體資源配置與架構檢視之參考框架：

表 8：金融機構後量子五大核心面向因應策略

因應面向	過渡策略	遷移策略	關鍵應用場景
通訊安全	導入 TLS 1.3，採用混合式金鑰交換（如 X25519 結合 ML-KEM）	全面汰換舊版傳輸協定，落實 PQC 端到端安全	網路銀行、跨機構 API 對接、內部系統串接
加密保護	依資料保存年限與機敏程度採風險導向調整；高機敏或長期保存資料優先採 AES-256，並推行自動化密碼管理	全面落實資料庫與檔案存儲的防護	核心帳務資料庫、客戶個資儲存
數位簽章	升級至 SHA-2 以上，強化雜湊函數長度並捨棄 SHA-1	導入 PQC 簽章演算法，部署 ML-DSA 與 SLH-DSA	數位身分識別、電子合約簽署
憑證體系	維持傳統 RSA-2048 / ECC，調高金鑰長度並縮短憑證效期	建立全面支援 PQC 的 PKI 體系，發行原生 PQC 憑證	股票下單、跨行轉帳、TLS 網站憑證
載具與硬體	盤點並主動詢問硬體供應商的 PQC 升級方案，分階段汰換	採購並更換支援 PQC 標準之底層硬體設備	硬體安全模組（HSM）、網路通訊設備、終端 IC 卡

資料來源：本研究參考相關指引整理

（四）結語

PQC 遷移是一項跨越技術、網路架構、委外供應鏈與日常維運的系統性管理工程，期望本研究參考相關指引所歸納之方法與對策，能協助讀者加速釐清 PQC 遷移所涉及之挑戰與實務重點；並期盼能為金融業提供彙整之參考方向，進而應用於未來的遷移實務中，以務實、有序的步伐，建構出具備量子抵抗力的現代化金融資安韌性。

參考文獻

1. 李依珊、左瑞麟（2025）。〈金融業後量子密碼 (PQC) 遷移指引〉,《中華民國資訊安全學會通訊 (Communications of the CCISA)》，第 31 卷第 1 期，頁 45-55。
2. 金融監督管理委員會（2025）。《金融資安韌性發展藍圖》。
3. 金融監督管理委員會（2026）。《金融業後量子密碼遷移參考指引》。
4. 數位發展部、後量子資安產業聯盟（2025）。《後量子密碼遷移指引》。
5. 臺灣網路認證公司 (TWCA)（2026）。〈金融業的量子挑戰與後量子密碼 (PQC) 因應策略〉,取自證交所證券商後量子密碼學 (PQC) 遷移作業研討會之專題演講後量子因應對策。
6. Bank for International Settlements (BIS). (2025). Quantum-readiness for the financial system: A roadmap (BIS Papers No. 158).
7. Bank for International Settlements (BIS). (2023). Project Leap: Quantum-proofing the financial system. BIS Innovation Hub Eurosystem Centre.
8. Cybersecurity and Infrastructure Security Agency (CISA). (2023). Quantum-readiness: Migration to post-quantum cryptography.
9. Costa, D. B. C. (2025). Post-quantum financial infrastructure framework (PQFIF): A roadmap for the quantum-safe transition of global financial infrastructure. Written input prepared for the U.S. SEC Crypto Assets Task Force.
10. Financial Services Information Sharing and Analysis Center (FS-ISAC). (2023). Preparing for a post-quantum world by managing cryptographic risk.
11. G7 Cyber Expert Group (CEG). (2026). Statement on planning for the opportunities and risks of quantum computing & coordinating roadmap for post-quantum cryptography migration in the financial sector.
12. Monetary Authority of Singapore (MAS). (2024). Advisory on addressing the cybersecurity risks associated with quantum.
13. Mosca, M., & Mulholland, J. (2017). A methodology for quantum risk assessment. Global Risk Institute.
14. National Institute of Standards and Technology (NIST). (2024). FIPS PUB 203: Module-lattice-based key-encapsulation mechanism standard. U.S. Department of Commerce.
15. National Institute of Standards and Technology (NIST). (2024). FIPS PUB 204: Module-lattice-based digital signature standard. U.S. Department of Commerce.
16. National Institute of Standards and Technology (NIST). (2024). FIPS PUB 205: Stateless hash-based digital signature standard. U.S. Department of Commerce.
17. National Institute of Standards and Technology (NIST). (2024). NIST IR 8547: Transition to post-quantum cryptography standards (Initial Public Draft). U.S. Department of Commerce.
18. National Security Agency (NSA). (2024). The Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) and quantum computing FAQ.
19. World Economic Forum (WEF) & Financial Conduct Authority (FCA). (2024). Quantum security for the financial sector: Informing global regulatory approaches.