金融業後量子密碼遷移參考指引

金融監督管理委員會

中華民國 115 年 6 月

目錄

本參考指引旨在協助金融機構因應後量子密碼（PQC）轉換趨勢，採風險導向、分期分流方式推動遷移準備，降低「先攔截、日後解密」(HNDL）與「現在信任、稍後偽造」(TNFL）等量子威脅對機密性、完整性與不可否認性之衝擊。文件重點包含：建立治理與跨部門協作機制；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（Crypto-Agility）並優先清理常見密碼反模式；以生態系協作與「四階呈現」方法對齊跨機構互通依賴；以及將供應鏈管理、測試驗證、切換與回退演練制度化，形成可稽核的證據鏈。附錄提供生態系協作案例與關鍵供應商／共通元件盤點示例，供各金融機構於實務盤點、溝通對齊與遷移規劃時參考。

一、緣起

量子電腦之演算法已證實較傳統電腦處理質因數分解的速度有指數性成長優勢，這使得建立在質因數分解問題上的「非對稱式加密技術」受到被破解的威脅，影響網路交易、電子簽章及身分驗證等加密安全性。雖現行量子電腦的位元數及容錯率尚不足以破解廣泛使用中的非對稱式加密演算法（RSA-2048），但隨量子運算技術的逐年發展，雲端安全聯盟（Cloud Security Alliance, CSA）於 2022 年啟動「Y2Q 倒數」倡議[1]，並以 2030 年 4 月 14 日作為風險里程碑的推估日期，用以提醒業界加速遷移（屬風險推估，非確定時間點），估計在這個日期，量子電腦將能夠破解現今的網路安全基礎設施，以提醒威脅的迫近以及尋找和實施新解決方案的必要性。

除前述「未來破密」威脅外，需特別留意「先攔截、日後解密」(Harvest Now, Decrypt Later, HNDL）風險：攻擊者可在現階段先行攔截並長期保存加密通訊或交換資料，待未來具破密能力之量子電腦成熟後再回溯解密。另亦須關注利用量子計算破解數位簽章算法，偽造合法的數位憑證與身分證明的「現在信任，稍後偽造」(Trust Now, Forge Later, TNFL）風險，一旦核心 PKI 體系被破解，攻擊者可偽造金融交易簽署指令、竄改代碼簽署(Code Signing）以植入惡意軟體，從根本上瓦解不可否認性。

美國國家標準暨技術研究院（NIST）於 2024 年 8 月 13 日發布首批 PQC 標準：FIPS 203（ML-KEM)、FIPS 204（ML-DSA）與 FIPS 205（SLH-DSA）[2]，並於隔日公告生效；後續仍將持續推進其他演算法與配套文件。資訊工業策進

[1] https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/
[2] https://csrc.nist.gov/projects/post-quantum-cryptography

會受數位發展部數位產業署與後量子資安產業聯盟(PQC-CIA) 委託，於 2025 年 4 月 16 日發表我國首版「後量子密碼遷移指引」[3]，以推動臺灣產業達成「PQC Ready」為目標。指引內容大致說明當前後量子密碼的技術發展路徑，並透過解析 NIST 及相關國際組織陸續發布的後量子密碼遷移研究報告，提出後量子密碼遷移路線圖。

二、國際金融領域因應 PQC 議題現況

NIST 與摩根大通(JPMorgan Chase & Co.)早於 2020 年即聯合發布全球金融機構後量子遷移報告[4]，建議金融機構因應 PQC 議題採以資料為中心，風險導向進行，在推動後量子密碼學過渡的過程中，應先確保系統具備加密敏捷性（能夠快速靈活地替換現有的加密算法及協議)，並提出 PQC 遷移時間表，建議金融機構於 2024 年開始著手進行。美國 FS-ISAC 亦已設置 PQC 工作小組，自 2023 年起陸續發布有關盤點基礎設施加密技術、因應後量子密碼準備路線圖、建構加密敏捷性、對支付卡產業衝擊等報告[5]。

世界經濟論壇(WEF)於 2024 年 1 月發佈「金融部門量子安全：全球監管方法」報告[6]，該白皮書是與英國金融行為監管局（Financial Conduct Authority）聯合編寫，指出因應 PQC 風險的方法可能因國家和地區而異，但金融機構的系統是相互關聯的並遍佈全球的，部分金融機構延遲回應的影響可能會影響其他國家和地區的金融機構，量子技術帶來的共同威脅需要產業和監理機構之間的密切合作，協調一致的方法。報告中並就 PQC 遷移提出四階段路線圖，包含：

（一）準備（Prepare)：提高量子認知、盤點加密資產、建立內部能力（技能與人才)。
（二）釐清（Clarify)：啟動監管者與業界的合作、盤點現有法規、分析遷移成本。
（三）指導（Guide)：解決監管漏洞、將技術標準落地應用，促進標準化與跨境一致性。
（四）轉型與監測（Transition and Monitor)：實施量子安全措施、持續監控威脅變化、推動加密技術現代化。

[3] https://moda.gov.tw/ADI/news/latest-news/16090
[4] https://www.nccoe.nist.gov/sites/default/files/2021-10/6-Yassir-NIST-%2020200819-8.pdf
[5] https://www.fsisac.com/knowledge/pqc
[6] https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf

另 G7 網路專家小組（G7 Cyber Expert Group, CEG）亦就量子運算風險提出跨境協調倡議：該小組於 2024 年 9 月發布聲明，提醒金融體系需因應量子電腦對既有公鑰密碼之威脅與「現在攔截、日後解密」（Harvest Now, Decrypt Later）風險；並於 2026 年 1 月發布「金融領域後量子密碼遷移協調路線圖」聲明[7]，提出以風險為導向、分階段推動之整體規劃方向，並建議金融機構宜以 2035 年前完成全面遷移為共同目標，於 2025–2027 年間完成盤點與規劃，並視系統重要性與曝露程度，於 2030–2032 間優先推動高風險／高關鍵系統之遷移，以降低體系性風險外溢；路線圖亦特別強調跨境互通與共同基礎設施的同步性、供應鏈與第三方依賴管理、以及建立加密敏捷性（crypto agility）以支撐後續演算法與標準演進之持續調整需求。

在亞洲，新加坡金融管理局（MAS）於 2024 年 2 月發布「量子風險資安諮詢」要求金融機構強化加密敏捷性與盤點[8]；並於 2024 年 8 月與多家銀行及業者簽署 MoU 展開 QKD 量子安全試驗[9]。同年，新加坡 IMDA 亦推動 NQSN+國家量子安全網路以支援量子安全通訊落地，支持金融機構與生態系統利益相關者合作，在新加坡發展量子能力，包含：後量子密碼學和量子密鑰分發，以保護關鍵資料。日本金融廳召開了存款機構因應後量子密碼學研究小組會議，與相關方深入討論在金融領域推動向後量子密碼學（PQC）轉型時的建議、課題及應注意事項，2024 年 11 月發布研究報告[10]，指出金融領域對後量子密碼的需求，包含財務數據的機密性與完整性等，以及可能面臨威脅場景，如支付系統身分驗證變弱、銀行間介面受損、偽造金融交易紀錄等，並提出遷移建議，包含以風險導向選擇優先遷移標的、盤點加密技術清單、更新加密架構、與資通訊供應商合作等。

除政府政策外，國際金融基礎設施亦陸續啟動後量子轉型，SWIFT 已規劃自 2025 年啟動 PQC 遷移準備，並以 2030 年完成轉換並終止 RSA 架構支援為目標，其策略包含逐步導入混合式密碼機制，確保全球金融訊息服務之互通性與穩定性，同時降低轉換期間對基礎設施之衝擊[11]。PCI 安全標準委員會（PCI Security Standards Council，PCI SSC）正透過 PCI DSS v4.0（Requirement

[7] https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf
[8] https://www.itnews.asia/news/singapore-issues-advisory-for-fis-to-mitigate-quantum-computing-risks-605273
[9] https://speqtralquantum.com/newsroom/mas-collaborates-with-banks-and-technology-partners-on-quantum-security-trials-to-address-quantum-computing-threats
[10] https://www.fsa.go.jp/news/r6/singi/20241126.html
[11] https://www.swift.com/news-events/events/swift-operations-forum

12.3.3） 強制企業進行加密資產清查，並協同 NIST 演算法標準化進程，呼籲支付產業建立「加密敏捷性」以防範未來量子電腦的解密威脅[12]。

另就產業界動向，Google 於 2026 年 3 月發布其 PQC 遷移時間表[13]，將完成遷移之目標提早至 2029 年（相較多數公部門與國際倡議所採期程更為積極），並說明其判斷係基於量子運算硬體發展、量子錯誤校正進展，以及量子分解資源估計更新等因素，認為量子風險可能「比預期更近」。該文並區分兩類主要威脅：（一）加密之「先攔截後解密」（Store/Harvest Now, Decrypt Later）屬於現時風險；（二）數位簽章與身分驗證等屬於需在具破密能力量子電腦（CRQC）出現前完成遷移之前置風險，並指出其已調整威脅模型，優先推動認證服務之 PQC 遷移，並呼籲產業加速規劃與導入。就金融業意涵而言，瀏覽器、行動作業系統與雲端平台等關鍵生態系若提早導入 PQC/混合模式，留給金融機構把對外連線（例如網銀／行銀的 TLS）與憑證相關設定完成升級、測試與切換的時間可能會變少；金融機構宜及早完成端點盤點、相容性與壓力測試，並建立回退機制與供應鏈協調安排，以降低服務中斷風險。

三、金融業 PQC 遷移的挑戰

前揭國際監理機關、同業組織與主要科技／雲端供應商已陸續提出量子風險警示與 PQC 遷移方向，顯示金融體系必須及早啟動盤點與規劃；惟現有文件多著重技術面分析、方法論及通用遷移框架，仍不足以涵蓋金融業多元加解密應用情境、跨機構互通依賴與高可用營運限制等特性。本參考指引旨在提供金融業具體可落地之參考，協助規劃辦理 PQC 遷移準備事宜。以下先就金融業特性出發，彙整因應 PQC 遷移時常見之挑戰：

（一）對密碼技術倚賴深，無處不在

金融業的核心業務（存放款、投資交易、支付清算、保單服務與理賠等）普遍依賴密碼學機制以確保「身分可驗證、交易不可否認、資料不可竄改、傳輸不可窺視」。因此，一旦公鑰密碼（如 RSA/ECC）在可預期期間內可能失去安全性，影響將同時擴及前台通路、後台核心系統、跨機構介接與第三方委外服務。常見受影響情境與資產範圍例舉如下：

[12] https://www.pcisecuritystandards.org/document_library/

[13] https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/

1. **【身分鑑別／授權（含對外通路）】**網銀／行動銀行登入、客戶身分驗證與裝置綁定、憑證式身分驗證、交易或敏感操作之授權指令簽章、憑證／金鑰保護。

2. **【內部身分與存取管理（IAM）】**內部身分基礎建設（如 AD/LDAP、單一登入、特權帳號與管理端存取、裝置憑證與機器身分）亦高度依賴憑證／金鑰與簽章驗證，若未納入遷移範圍，易形成內部長尾風險。

3. **【交易簽章／完整性／不可否認（含存證）】**電子簽章、交易簽章驗證、指令授權（含多因子／多方簽核）、時間戳記與長期驗證需求（含交易存證）。

4. **【傳輸通道與互通】**網銀／行銀之 TLS 端點、VPN、API 閘道與對外/對內介接通道；跨行／跨境訊息與電文（如 SWIFT、ISO 20022）之安全機制與介接協定。

5. **【金鑰／憑證基礎設施】**根 CA/中繼 CA、憑證生命週期管理（CLM）、KMS/HSM 與金鑰輪替機制。

6. **【應用／程式碼與第三方元件】**硬編碼演算法/金鑰、加密函式庫版本、第三方 SDK/套件（SCA 範圍）。

7. **【通路／終端／設備】**主機／中介軟體／批次作業中的舊簽章格式、長尾介接模組與客戶端元件（常受版本差異與供應商支援限制），以及已進入 EOL/EOS 之設備與載具所造成的升級瓶頸；另亦應納入金融交易生態系之終端與驗章鏈，例如支付卡 POS/ATM 終端、收單/卡組織相關介接，以及卡片／終端簽章驗證鏈之相依元件。

8. **【批次／檔案交換與報送】**批次檔案傳輸（如 SFTP）、PGP 檔案加解密、檔案簽章與對帳／報送流程（常屬長尾流程，且易隱藏於排程與中介系統）。

9. **【資料儲存與稽核軌跡保護】**資料庫加密、備份／歸檔加密、金鑰封存與取用權限控管，以及稽核軌跡（Audit Trail）與營運紀錄之完整性保護（避免被竄改或偽造）。

（二）加密技術應用分散，盤點耗工

加密資產往往散落於多層技術堆疊（應用程式、API 介接、中介軟體、網路設備、金鑰管理與 HSM、憑證管理、雲端服務、終端載具等），且多數加密行

為由既有框架或第三方元件「隱性」完成，導致盤點與風險分級難度高、成本高、且容易遺漏。常見盤點盲點（造成耗工的根因）例舉如下：

1. 多源頭憑證與金鑰：自建 CA、第三方 CA（如銀行 FXML 憑證、證券下單憑證）、網站 TLS 憑證、雲端 KMS、HSM 與各式應用內建金鑰庫並存，資訊分散且欄位／命名／生命週期事件定義不一，缺乏一致且可持續維護的權威清冊（如加密資產清單／系統紀錄來源），致盤點、風險分級與稽核追溯不易。
2. 遺留系統與長尾介接：舊型主機/中介軟體/批次作業、老舊協定（如 TLS 1.2 以下、舊版 SSH 或安全性較低的簽章格式（如：SHA-1））仍在關鍵流程中運行。
3. 第三方 SDK 與委外平台：支付/身分驗證/風控/簡訊/簽章服務等供應商元件可能含硬編碼演算法或受限於版本更新節奏。
4. 影子 IT 與臨時環境：測試環境、PoC 與部門自行採購之 SaaS 可能繞過既有治理，形成盤點死角。

（三）生態系相互關聯且須國際接軌

金融服務具有高度互通性與跨境性，PQC 遷移涉及共同基礎設施、跨機構訊息標準與憑證信任鏈；任何單一節點延遲，均可能在過渡期造成互通失效、驗證失敗或風險外溢。相較一般產業，金融業需同時兼顧國內監理要求與國際同業／同業公會／跨境網路之標準節奏，例如跨境金融訊息網路之 PKI 與資安要求（如 SWIFT 相關規範）、ISO 20022 電文與安全機制的測試／平行運行窗口，以及瀏覽器與 WebPKI 根信任政策的調整節奏等。涉及之關鍵依賴例舉如下：

1. 共同基礎設施依賴：跨行清算/支付網路、集中式平台與憑證機構的升級時程，將直接影響全體參與機構之可用性。
2. 跨境與國際訊息標準：SWIFT、ISO 20022 等電文格式與安全機制一旦調整，需配合測試期、平行運行與上線窗口。
3. 支付卡網路與卡組織規範：PCI 等規範、卡組織技術公告與終端供應鏈汰換時程，將影響收單／卡組織介接、以及 POS/ATM 等終端之簽章驗證鏈切換窗口與過渡期安排。

4. 通路生態系：瀏覽器、作業系統、CDN、WAF、負載平衡器等對 TLS/PQC 的支援進程不同，易造成客戶端相容性問題。

（四）需與供應鏈體系協作，無法獨力完成

PQC 遷移牽涉眾多商用產品與委外服務（如 HSM、憑證管理系統、核心中介軟體、ATM/刷卡設備、行動裝置安全模組、雲端 KMS、資安設備與第三方 SDK 等）。金融機構多半無法單方面決定演算法、協定或產品版本/認證升級時程，需透過採購、委外與合約管理機制，要求供應商提出可驗證的路線圖與相容性測試計畫；否則可能面臨「關鍵元件卡關」導致整體遷移延宕的風險。涉及之關鍵供應鏈風險面向例舉如下：

1. 版本與支援落差:供應商可能僅在新版本支援 PQC,舊版本進入 EOL/EOS,迫使金融機構同時面對升級與遷移的雙重專案；若供應商無法提供明確承諾或時程,亦需及早評估替代產品／替代架構與退出策略(Exit Plan),避免被單一供應商綁定而影響整體路線圖。
2. 相容性與驗證:PQC/混合模式可能改變憑證格式、握手流程與封包大小,需供應商提供測試工具、設定指引與已驗證的部署範本。
3. 硬體/載具限制：晶片卡、USB Token、特定終端或舊型 HSM 可能無法負荷 PQC 運算與金鑰大小，需提前規劃汰換與客戶移轉。
4. 合約與 SLA 約束：委外契約宜納入 PQC 準備度要求（路線圖、測試、升級窗口、資安通報與弱點修補承諾），並明確責任歸屬。
5. 分包商／下游供應商依賴(第三方):關鍵服務常由合約供應商再分包(例如雲端代管、簽章服務、支付或身分元件),金融機構若僅掌握合約供應商，仍可能因分包商未支援 PQC 而形成隱性瓶頸；宜要求揭露關鍵分包鏈、相依產品與其升級時程，並於契約與委外管理機制中明確責任與交付。
6. 供應鏈透明度與 SBOM/CBOM 串接：即使已建立內部 CBOM，供應商未必能提供機器可讀且可更新的 SBOM 或加密使用資訊(例如所用加密函式庫版本與啟用模式),使得「實際相依」難以驗證與持續追蹤，易形成遷移盲點。

7. 證據與可查核要求：除供應商宣告外，宜要求提供可驗證佐證（例如支援版本清單、相容性測試報告、已知限制與回退方案、以及必要之合規/認證狀態），以降低「口頭承諾」與實際可用性落差。

（五）衝擊評估範圍跨技術／營運／法遵，且需可查核證據鏈

就金融業而言，PQC 的影響往往跨越「技術可行」與「營運可用」兩個層面：一方面需面對演算法替換、效能與相容性議題，另一方面又必須回應法遵、存證、營運持續與外部互通時程等要求。若未能以風險為導向完成衝擊評估，將「量子風險」具體化為可管理的資產清單、差距分析與遷移里程碑，常會導致決策層無法掌握優先序、專案資源難以核定，且在監理溝通或稽核查核時缺乏一致且可追溯的證據鏈；因此，衝擊評估除聚焦演算法替換外，亦宜同時涵蓋效能、相容性、營運連續與法遵等面向：

1. **機密性**（Confidentiality）：長效期機敏資料是否可能遭 HNDL 影響（如客戶個資、交易明細、保單/理賠資料、授信資料）。
2. **完整性與不可否認**（Integrity/Non-repudiation）：交易簽章、電子文件簽署與存證機制一旦弱化，可能引發交易爭議與法律風險。
3. **既有資料回溯保護與歷史包袱**（Legacy Data）：除新產生資料外，既有備份/歸檔、交易存證、稽核留存資料與長期保存文件，是否需要重加密、重新封存金鑰或重新簽章/時間戳記，常涉及龐大成本、作業窗口與法遵可接受性，亦是衝擊評估不可忽略的範圍。
4. **可用性與效能**（Availability/Performance）：PQC 造成的封包增大、延遲上升、設備負載增加，是否影響尖峰交易量與服務等級。
5. **合規與外部要求**（Compliance）：國內監理期待、國際標準（NIST/FIPS 等）與跨境網路/合作夥伴之要求是否存在時程壓力；另因標準與實作生態系仍在演進，亦宜預留演算法更新、參數調整與版本迭代之空間。

（六）遷移期間之營運切換與組織能力挑戰

除技術遷移本身外，金融機構在推動 PQC 時亦常面臨「做得到」與「切得上線」之落差：一方面需要跨域人才與既有流程整合，另一方面又受制於高可用營運要求、變更窗口稀缺、端到端測試環境不足與回退演練成本等因素，導致遷移推進速度不易與外部期程對齊。常見挑戰如下：

1. 跨域人才與能力缺口：針對 PQC 所涉 PKI、網路協定、應用改版、資安測試、法遵與稽核佐證等領域，組織內可能尚未形成共同語言與訓練／知識傳承機制，導致需求定義易反覆、交付進度不易控管。

2. 切換策略與變更協調機制可能不足：考量金融交易高峰明確、停機容忍度低，且多數變更需跨通路、跨系統與跨機構協作，若未能預先建立分段切換、灰度(逐步)上線與回復機制，遷移上線時程可能不易對齊外部期程。

3. 端到端測試環境不完備：測試憑證鏈、測試資料與交易腳本未必可完整重現關鍵情境，且與外部夥伴協調之測試窗口可能受限，使相容性、效能與例外情境之驗證週期可能拉長。

4. 加密敏捷性（Crypto-Agility）可能不足：若演算法、參數或憑證／簽章格式仍寫死於程式碼或固定於架構，面對標準更新、演算法淘汰或參數調整時，可能需要以大型改版處理，亦不易與例行變更節奏整合，使測試與切換負擔增加。

5. 資料分級與保存年限不清：若資料分類與保存年限未能制度化，且資料流追蹤不足，則 HNDL 風險較難量化並轉化為可執行的優先序，亦可能影響稽核查核之一致性。

6. 跨單位協作與權責切分不易：面對業務、資訊、資安、風險、法遵、採購／委外與外部機構等多方利害關係人，若權責、決策節點與升級機制未能事前定義，里程碑達成可能受等待與協調成本影響。

四、金融業因應 PQC 的策略建議

（一）PQC 政策與治理：將密碼技術風險納入企業風險管理

PQC 遷移是一項跨年度、跨部門的長期工程，絕非單一部門可獨立完成。金融機構必須將量子風險提升至董事會層級，視為企業風險管理的戰略議題。金融機構應成立跨部門「後量子遷移工作小組」，建議由資安長(CISO)、資訊長(CIO)或相當層級主管擔任召集人，並明確訂定義權責：

1. 由董事會或高階管理層指定權責主管，核定 PQC 遷移之治理架構、風險胃納、資源投入原則與跨年度路線圖。

2. 成立跨部門 PQC 遷移工作小組（含資訊、資安、風險、法遵、業務、採購/委外管理等），明確界定決策層級、例外核准與升級通報機制，明確盤點、測試、試辦與切換等權責。

3. 將 PQC 遷移納入資訊安全管理制度與重大專案管理：訂定里程碑、KPI/KRI（如盤點覆蓋率、高風險資產比例、供應商回覆率、測試通過率等）並定期追蹤。

具有母子公司或跨境集團架構之金融機構，建議將 PQC 治理提升至集團層級，建立集團與子公司間之協調治理與分工機制，以推動整體遷移策略、風險管理及資源配置。

（二）盤點密碼技術應用，建立密碼技術資產清單（CBOM）

密碼技術盤點的目的不僅是列出系統清單，而是要形成可持續維護、可連結到「業務使用情境」與「外部互通依賴」的密碼技術資產清單，作為後續風險分級、遷移優先序、供應鏈管理與監理溝通之共同依據。

就盤點策略而言，在加密治理尚未成熟、且加密資產分散於各系統之情境下，若一開始即要求全系統全面盤點，可能導致盤點作業耗時過長而延宕實質遷移；因此宜採「先依風險與優先度限定盤點範圍、逐步擴張覆蓋」之策略，例如先以已知高曝露或高關鍵之使用情境作為第一輪範圍(如對外通路 TLS 端點、跨機構介接、身分鑑別、交易簽章、以及需長期保存之敏感資料)，並以清單品質（可追溯、可維護）優先於一次性追求全面盤點。

為使盤點作業可快速落地並兼顧清單品質（可追溯、可維護），建議可依下列實務作法逐步推進：

1. 建立基礎清冊：優先盤點對外 TLS 端點，以及 PKI/CLM/KMS/HSM 等關鍵基礎設施，並以「可追溯、可維護」為最低要求，明確標示系統／介接點責任人與對應證據來源（如設定檔、憑證清單、CLM/KMS 報表）。

2. 使用情境（Use Case）導向：以「使用情境」(身分鑑別、交易簽章、對外 TLS、跨機構介接、需長期保存之敏感資料等）關聯到系統、介接點、憑證鏈與金鑰來源，並將關聯結果作為後續 CBOM 欄位填列之依據。

3. 建立可維護的密碼技術資產清單（CBOM）：定義最小欄位（如用途、演算法/參數、憑證鏈/金鑰來源、部署位置、供應商版本與支援狀態、可替

換性/預估工期等），並可依成熟度分階段逐步補齊，納入版本控管與審核流程。

4. 分層導入盤點方法：先在業務/系統面彙整初版清冊（搭配使用情境對齊範圍與優先序），再延伸既有工具（如弱掃、資產探索、SSL/TLS 掃描、CLM/KMS 報表等），最後評估導入專用盤點工具提升覆蓋與持續性。

5. 盤點「制度化」：將 CBOM 更新納入系統上線、憑證輪替、供應商版本更新與重大變更流程；以覆蓋率、缺漏率、例外到期率等 KPI/KRI 定期稽核清單品質。

另建議評估運用 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；惟導入前應先界定可用資料來源、權限與稽核要求，並將模型風險與資料外洩風險納入控管。

（三）提升加密敏捷性(Crypto-Agility)，優先清除「密碼反模式」

由於後量子標準與產品生態系仍在演進，不宜僅以一次性「替換演算法」為目標，而應同步提升加密敏捷性。加密敏捷性是「能快速有效率地調整演算法（含參數與金鑰），在不大改架構、最小營運干擾、短切換時間下完成更新/替換」的能力：透過模組化、組態化與標準化介面，使未來演算法/參數迭代、憑證格式調整或供應商版本更替時，能以例行變更方式納入測試、切換與回復演練，避免每次更新都演變為大型改版專案。

加密敏捷性的終極目標是將加密技術設計為「獨立模組」：將加密邏輯與上層應用程式完全隔離，使未來的演算法變更對應用開發者來說僅是「組態調整」，而非大規模的程式重構。另建議搭配憑證自動化管理（CLM），評估導入自動化憑證生命週期管理（部署、輪替、撤銷），減少手動操作並為未來縮短憑證效期做準備。

於實務上，建議優先參考歐洲刑警組織(Europol)與 FS-ISAC 等聯合報告[14]所列之「密碼反模式」(Cryptographic Antipatterns)改善方向，先以「可快速落地且能降低後續遷移風險」為原則，推動 TLS、憑證及金鑰等組態與治理之「無悔作為」(No-regret actions)。此類作為不僅可直接降低既有弱點與誤用風險，亦可在 PQC 與混合模式尚未全面成熟前，先行清理密碼技術負債、

[14] https://www.europol.europa.eu/publications-events/publications/prioritising-post-quantum-cryptography-migration-activities-in-financial-services

提升加密敏捷性，避免未來演算法／憑證格式或供應商版本更新時被「寫死的配置」與「長尾相依」綁住。具體而言，宜包含：建立一致且可稽核的 TLS 組態基準（含版本與套件淘汰策略）、提升 TLS 1.3 覆蓋率並以監測數據收斂向下相容；導入憑證生命週期管理(CLM)與自動化輪替／撤銷機制，將信任例外與臨時措施納入核准、到期與稽核追蹤；強化金鑰集中治理（KMS/HSM）、最小權限、輪替節奏與用途隔離，並清理硬編碼金鑰／密碼；同時把協商版本、憑證鏈驗證錯誤與握手失敗率等可觀測性指標納入監控與告警。（參考**附錄 A：常見密碼反模式與建議作法**）

上述作為宜與 CBOM 相互勾稽，納入變更管理與例外管理流程，形成可追溯且可滾動更新的治理證據，作為後續遷移分期排序與跨機構對齊之基礎。

（四）建立生態系協作機制與共通業務風險圖像

鑑於金融業生態系高度互聯，PQC 遷移宜採「生態系協作」及「自體盤點」並行：由共通基礎設施或主要參與者先行定義共同盤點語言（範圍、欄位、版本基準與測試方法），再由各金融機構依自身系統與通路落實盤點與維護，並將對齊後之結果回寫至 CBOM 與遷移路線圖，以降低互通落差與重工。

1. 生態系協作(Hub-and-Spoke)，建立共同盤點語言

針對跨行清算、憑證信任鏈、跨機構介接與支付網路等共通基礎設施，宜由樞紐機構先行定義盤點範圍與欄位（如：介接業務、系統介接介面（如 API／電文／通道）、密碼技術應用（如簽章、加密及存證）以及相關法規要求等），並建立過渡期互通與共同測試的版本基準，其輸出物可作為各參與機構對接業務、系統介接及密碼技術盤點之對齊基準，降低各自為政造成的欄位不一致與重工。

為確保跨機構互通與期程對齊，樞紐機構應擔任統籌推進角色，負責擬訂生態系遷移路線圖並運作跨機構協作機制，主導下列事項：

（1）關注國際金融相關組織 PQC 遷移政策（如 SWIFT、PCI SSC、ISO 等），對齊 PQC 遷移規劃與時程。

（2）盤點並滾動檢討現行法規、監理規範／自律規範、以及跨機構作業規章與契約條款中涉及加密、憑證、簽章、留存與不可否認性等要求，辨識

量子風險下可能之不足或衝突，提出修正／增訂建議，並偕同公會或及主管機關辦理法規修正。

(3) 就跨行交易、憑證信任鏈、跨機構介接等共通基礎設施，擬定生態系遷移計畫，並建立跨機構協調窗口、期程與程序（治理、時程、測試、變更公告、例外處理）。

(4) 規劃過渡期互通方案（雙模／混合模式閘道、相容性矩陣、灰度切換策略），並訂定平行運行與回復條件。

(5) 建立共同測試與驗證機制（測試憑證鏈、測試環境、端到端交易測試案例）。

在建立生態系協作機制與共同盤點語言時，可參考附錄 B 支付卡產業案例，作為規劃跨角色盤點欄位、測試窗口與分階段切換安排之實務範本。

2. 建立共通業務框架與風險圖像

為降低各機構自行盤點所造成的落差，收斂盤點成果並形成可溝通的「風險圖像」，建議採「四階呈現」概念：

(1) **第一階（Hub 型業務）**：以生態系的樞紐機構為主軸，界定跨機構互通/共用平台之範疇與邊界，建立「影響範圍、參與者主導及配合之角色分工、關鍵相依性與協作流程」的整體視圖。（參考**附錄 C：生態系協作的樞紐機構與負責業務**）。

(2) **第二階（對接單位延伸盤點）**：由各金融機構（或生態系參加單位）針對其「對接 Hub 之業務/系統/介接點」進行延伸，盤點本機構內部受影響之系統、通道、憑證/金鑰來源、加密/簽章/存證使用情境與相依供應商。

(3) **第三階（自主盤點遷移）**：針對「非第一、二階」所涵蓋之情境（亦即不屬 Hub 型共通平台、且非屬對接 Hub 之延伸介接範圍者），由各金融機構依自身系統與業務特性自主盤點加密資產與使用情境，進行風險分級並規劃遷移路線圖。

(4) **第四階（共通性基礎設施與供應商資訊）**：在完成上述盤點後，彙整跨生態系共通依賴（例如憑證信任鏈、金鑰管理、介接中介設備與終端/

載具等），將「關鍵供應商」與「共通元件/服務」納入共同盤點語言。（參考**附錄 D 與附錄 E 示例**）

於實務作業，另可由具代表性之金融機構先行提出「共通業務盤點框架」與「風險圖像」作為參考底稿，協助同業以一致脈絡展開自體盤點，並對齊高風險情境之優先序與必要欄位，以降低重工並提升遷移一致性與效率。（參考**附錄 F**）

（五）以風險導向建立遷移優先序

同樣參考前揭 Europol 與 FS-ISAC 聯合報告，採「量子風險評分(Quantum Risk Score)」與「遷移時間評分（Migration Time Score)」兩軸交叉評估，建立 PQC 遷移優先序與分期路線圖。各評分由三項因子構成：

1. **量子風險評分（Quantum Risk Score)**：由（1）資料敏感年限（Shelf-life；對 HNDL 之急迫性核心)、(2）曝露程度（Exposure；對外通路、跨機構傳輸、第三方可攔截或實體可取得程度)、(3）衝擊嚴重性（Severity；法遵、詐欺、財務損失、聲譽與營運中斷）三因子構成。
2. **遷移時間評分（Migration Time Score)**：由（1）解決方案可用性（Solution availability；標準、產品與部署模式成熟度)、(2）執行成本與工期（Execution cost & time；含軟體改版、測試、切換窗口、效能影響與必要硬體汰換)、(3）外部依賴（External dependencies；供應商版本、共同基礎設施、標準組織、監理要求與合作夥伴互通窗口）三因子構成。

為使評分結果可直接支援分期推動，建議將上述兩軸評分轉化為「風險高低」與「遷移難易」之分群，並以相對排序方式決定優先序與資源投入（重點在於可執行的分期與對齊節奏，而非追求精準量化)。例如：

1. 量子風險評分高且遷移時間評分高者，宜列為跨部門專案並及早啟動供應鏈對話、共同測試與切換規劃。
2. 量子風險評分高但遷移時間評分較低者，可優先納入近期改版與現代化計畫快速處置。
3. 量子風險評分較低者，則可併入例行升級（BAU upgrades）或與設備汰換節奏整合。

4. 另針對存在明確外部互通窗口（共同基礎設施、跨機構介接、供應商版本）或需長期驗證（LTV）之存證資料者，宜作為調整優先序與分期里程碑之約束條件（如提前或設定必達期限），使排序不僅停留於分數計算，而能落到可執行的路線圖與資源配置。

綜上，遷移優先序不只在於「評分」，更在於把評分結果轉為可執行的分期分工與驗收節奏，並納入外部互通窗口、供應鏈版本可得性及既有資料處置等約束條件，形成可滾動更新的遷移路線圖；爰整理實務建議如下：

1. 就 HNDL 風險，於規劃演算法遷移外，應先強化多層次防護（例如資料最小化與保存年限管理、敏感欄位／分段加密或代碼化／去識別、金鑰分離與最小權限存取控管、以及異常存取監測），以降低「現在攔截、日後解密」情境下，被攔截資料於未來遭回溯解密之價值與影響。

2. 金融業須以生態系為單位對齊（共同基礎設施、跨機構互通窗口、供應商版本與信任鏈政策），將外部依賴視為遷移時間的關鍵約束，避免單一機構孤島式推進而造成互通失效或驗證斷鏈。

3. 就機構自主辦理部分：

   （1） 優先推動「簡單且能先做」的無悔作為（如提升 TLS 1.3 覆蓋率、淘汰弱套件、導入 CLM 與自動化輪替、清理硬編碼演算法／金鑰），以降低後續作業範圍並壓縮遷移時間。

   （2） 在不影響外部互通窗口之前提下，若相關調整可於既有升級／汰換生命週期內控管（量子風險評分較低或遷移路徑短者），建議優先依例行升級（BAU）原則推進，併入既有改版與標準現代化計畫執行，以降低專案化成本。

   （3） 若涉及多系統／多通路調整，且測試與切換工期較長者，建議專案化推進：先完成端到端測試、切換與回退演練規劃，再分批上線以降低營運風險。

4. 就 TNFL 風險，訂定「既有資料」處置策略：釐清哪些備份／歸檔／存證需重加密、重新封存金鑰或重新簽章／時間戳記，並就可行窗口、成本與法遵可接受性提出分期計畫與例外管理。

另於規劃遷移路徑與分期推動時，除前述風險評分與分群結果外，亦應將下列事項視為落地之關鍵約束條件與作業重點（涉及架構衝擊、過渡策略、

資源量能、測試切換與人才），以確保路線圖可執行且可驗證：

1. **評估架構衝擊而非簡單替換**：PQC 演算法並非 RSA 或 ECC 的 1:1 等效替代品。遷移需考慮其在金鑰大小、封包長度及運算效能上的差異，並針對硬體（如 HSM）的限制進行提前規劃。
2. **採用混合模式過渡 (Hybrid Mode)**：在過渡期結合使用後量子演算法與傳統演算法，以在確保量子安全的同時維持現有的合規性與韌性。混合模式應視為過渡策略而非最終狀態。
3. **分流推進(專案 vs. 例行升級)**:把「可併入例行升級(BAU upgrades)」與「需跨機構協作/高風險而需專案管理」明確分流，前者納入年度改版與現代化計畫，後者設里程碑、驗收條件與回退演練機制。
4. **量能與資源**：將專案資源集中投入於高風險或外部依賴高、且需跨機構協作之優先標的，以避免分散投入而影響整體遷移成效。另應把端到端測試能力（測試憑證鏈、交易腳本、壓測指標）、回退/回復演練、與外部夥伴協調共同測試環境與窗口等列為必備資源。
5. **上線策略**:採分段切換、灰度上線與平行運行，並把回退機制納入演練；對高可用系統預先規劃變更窗口與例外處置。
6. **人才培訓**：針對 PKI、TLS、PQC 演算法、效能測試、法遵存證與稽核佐證，規劃訓練與內部知識庫。
7. **以戰代訓**：先擇非核心系統中實施 PQC 遷移測試，在低風險環境下掌握效能衝擊與運維難題，避免直接在關鍵系統出錯，同步養成 PQC 專業人才實作技能。

（六）更新採購與供應鏈管理要求

PQC 遷移高度依賴供應商產品與委外服務的支援時程，金融機構宜將「PQC 準備度」與「加密敏捷性（Crypto-Agility)」明確納入採購、委外與合約管理機制。參考美國 NSA 等機關倡議，對於新採購或重大改版之系統，宜優先要求具備量子安全（抗量子）能力，或至少具備可導入 PQC／混合模式之設計；並於供應鏈治理上，對關鍵供應商（例如 HSM、憑證／金鑰管理、雲端服務、資安設備、簽章／加解密 SDK 等）進行準備度調查與持續追蹤，確保可取得可驗證之路線圖、測試方法與交付物，降低遷移「卡關元件」風險。

為將前述要求落實至採購、驗收與合約治理，並使供應商承諾可被查核與持續追蹤，建議可依下列實務作法分階段導入：

1. **啟動關鍵供應商 PQC 準備度調查**：進行供應商盤點，優先針對高依賴供應商對話及進行準備度調查，要求提供可查核佐證與交付物（如支援版本與參數、升級路徑與時程、EOL/EOS、相容性／效能測試結果、已知限制、回退方案、合規／認證狀態等）。將結果彙整為可追蹤清冊（含風險評等、缺口、承諾日期與到期提醒），作為內部風險判讀與優先序調整依據，並納入定期檢視與續約／變更決策。

2. **更新採購文件要求（招標／規格／驗收）**：在 RFI／RFP／技術規格書與評選表中，明確列入「PQC 準備度」與「加密敏捷性」之功能性需求與查核項目，例如：支援之 PQC／混合模式範圍、可組態化切換演算法與參數、相容性矩陣、測試計畫與測試報告樣本、效能影響評估、以及預計交付之技術文件等；並把驗收所需證據（文件、測試結果、設定檔與版本資訊）寫入驗收條件。

3. **增修採購與委外合約（責任／SLA）**：於新購或續約時，將供應商在 PQC 遷移期間之責任與可執行承諾契約化，例如：配合升級與維運之責任分工、分包鏈與第三方依賴揭露、稽核/查核配合與資料提供義務、未達支援時程或無法支援之違約處理、以及退出與替代方案（Exit Plan）等；以確保後續能依契約要求落實交付與治理。

4. **建立「卡關元件」提早處置機制**：針對舊型 HSM、終端載具（USB Token／IC 卡）、ATM／POS、第三方 SDK 等高依賴且升級不確定之元件，列入優先汰換／替代清單，並對齊資產生命週期、年度預算與專案里程碑，降低供應商版本落差造成之延宕。針對無法升級 PQC 的老舊設備，若短期內無法汰換，應提出補償性控制措施（如 PQC 能力的 VPN 閘道、代理伺服器等，或強化多層次防護）。

5. **建立「供應鏈共同驗證」機制**：針對關鍵元件（如 HSM、TLS 終端設備、簽章 SDK、憑證管理平台等），要求供應商提供可重複之相容性／效能測試方法與交付物（支援模式、建議參數、限制與已知問題清單、回退方案）；必要時可由樞紐機構或同業協作建立共同測試平台與版本基準，以降低各機構重工並避免過渡期互通失效。

6. **以供應鏈資訊回饋遷移排序**：將供應商成熟度、版本可得性與外部依賴程度回饋至使用情境之遷移工期評估與路線圖，並持續更新風險與時程假設，避免因「技術可行但版本不可得」造成計畫失真。

（七）建立測試、切換與營運韌性機制

除選定演算法與完成供應鏈協調外，PQC／混合模式的導入能否「安全上線、穩定營運」，關鍵在於測試治理、切換策略、回退演練與可觀測性。金融機構宜將相關活動制度化，形成可重複、可稽核的證據鏈，以降低遷移期間之服務中斷、互通失效與例外處置風險。

為確保 PQC／混合模式在測試、上線切換與事件應變上可被制度化執行，並能留下可稽核之證據鏈，建議可依下列實務作法逐步導入：

1. **測試治理（Test Governance）**：建立 PQC／混合模式測試案例庫與版本基準（協定版本、憑證鏈、演算法／參數），涵蓋互通性、效能／壓力、例外情境（降級、防呆、逾時、封包大小／MTU）與相容性矩陣；並明確測試環境、測試窗口與外部夥伴共同測試安排。
2. **切換與回退（Cutover & Rollback）**：設計分段切換、灰度上線、平行運行與回退條件；針對關鍵對外通路（如 TLS 端點）、關鍵驗章服務與跨機構介接，訂定回復 SOP 與演練頻率，並將退版視為必備能力而非例外。
3. **監控與可觀測性（Observability）**：將協商結果（如版本／套件／金鑰交換）、握手失敗率、延遲、憑證鏈驗證錯誤與異常流量等指標納入監控與告警；對新舊模式並行期間，建立可快速定位問題的追蹤與回應流程。
4. **證據留存與稽核對應**：將測試報告、變更單、核准紀錄、演練紀錄、例外核准與到期追蹤、以及上線後監控報表納入證據管理，確保可回溯至 CBOM 與遷移路線圖，以支援稽核查核。

五、後續推動重點

後量子密碼遷移屬跨年度、跨機構之系統性工程，後續推動將優先聚焦於「生態系對齊、供應鏈治理、試辦驗證」三條主線，逐步形成可複製的範本與共同基準，以降低各機構重工並提升互通一致性：

（一）**擬訂金融生態系遷移計畫**：由樞紐機構（如共通基礎設施或同業協作平台）參依國際標準時程，訂定跨機構的共同里程碑、測試窗口、平行運行安排與變更公告機制，並提出「共同版本基準／相容性矩陣」以供各機構對齊自體路線圖。

（二）**建置（或整合）共通供應鏈調查與追蹤機制**：供應鏈 PQC 準備度係全球且跨業之共通議題，針對高依賴供應商建立標準化準備度問卷與證據要求（版本、時程、EOL/EOS、測試、回退等），評估跨機關及跨業合作彙整為可追蹤清冊與風險評等，作為採購、續約與遷移排序之共同依據，並降低重複詢查成本。

（三）**推動先導試辦與經驗分享**：優先選擇「可控範圍、可驗證」之使用情境（如對外 TLS 端點、驗章服務、特定跨機構介接）進行 PoC/試辦，沉澱測試案例、切換/回退 SOP、監控指標與證據模板，並透過工作坊或報告定期分享，形成可擴散的落地方法。

除本參考指引外， F-ISAC 將持續擔任交流平台，偕同金融機構彙整作業參考範本與實務案例，彙編「實務作業參考手冊」，包含共通業務框架及風險圖像（以使用情境分類，如身分鑑別、交易簽章、對外 TLS、跨機構介接、長期保存資料等；並對應 HNDL/TNFL 風險、資料敏感年限、曝露程度與衝擊嚴重性等評估）、實作參考範本（如 CBOM 最小欄位範本、供應鏈準備度問卷與證據清單、TLS 基準與弱套件淘汰策略、憑證生命週期管理與金鑰治理檢核表、測試案例庫/版本基準與切換/回退 SOP 範本）及經驗分享（如先導試辦之測試數據、相容性矩陣、常見卡關元件與補償性控制做法、以及跨機構共同測試窗口之運作經驗），並以工作坊或定期交流機制持續更新。

六、推動時程建議

以下時程係參考 NIST、G7、FS-ISAC 等遷移路線圖為推動建議，實際期程仍應視國際標準演進、產品生態系支援、共同基礎設施及金融生態系互通要求，採滾動檢討方式調整。

階段	建議時程	重點工作
準備與規劃	2026－2027	● 建立治理架構與盤點方法。 ● 優先盤點對外 TLS 端點與關鍵 PKI/CLM/KMS/HSM。

		● 建立 CBOM 黃金資料來源。 ● 啟動供應鏈準備度治理與採購文件更新。 ● 建立測試案例與版本基準雛形。 ● 逐步提升既有演算法至安全性較高的演算法(如 3DES 升級為 AES 256、SHA 1 升級為 SHA 2)。
試辦與基礎升級	2027－2029	● 選定可控情境進行 PoC／試辦。 ● 測試混合模式（Hybrid Mode)，評估對交易延遲與硬體效能的衝擊。 ● 提升 TLS 1.3 覆蓋率並清理反密碼模式。 ● 導入或強化憑證自動化與金鑰治理。 ● 建立切換與回退演練。 ● 開始建立跨機構共同測試窗口。
優先遷移（高風險/高關鍵）	2029－2032	● 依量子風險評分與外部互通窗口，優先推動對外通路、跨機構介接、關鍵驗章/簽章與高敏感長效期資料之遷移。 ● 導入 PQC 或混合模式並完成端到端測試；同步處置「卡關元件」汰換。
全面遷移與收斂	2032－2035	● 擴大至剩餘中低風險情境與長尾系統。 ● 完成跨體系 PKI 與信任鏈一致化。 ● 針對需 LTV 之既有存證/歸檔資料完成分期處置。 ● 建立常態化的演算法迭代與例行升級流程。

七、結語

後量子密碼遷移的核心不在於單一演算法替換，而在於以風險導向、分期分流的方式，系統性地提升金融體系對量子風險的韌性。由於標準與產品生態系仍在演進，且金融服務高度互通、供應鏈依賴深，金融機構宜及早完成治理與盤點、強化加密敏捷性與測試切換能力，並透過跨機構協作與供應鏈治理對齊時程與基準。本參考指引後續亦將持續關注量子技術發展趨勢，採「滾動檢討、持續修正」原則適時更新，金融機構於實務推動亦應秉此原則，以確保在監理溝通、遷移作業、稽核查核與實際營運上線時，均能維持安全、可用與可驗證。

附錄 A：常見密碼反模式及建議作法

本附錄彙整「常見密碼反模式」(Cryptographic Antipatterns) 及其對應之「無悔作為」(No-regret actions)，內容係摘錄自 Europol 與 FS-ISAC 聯合報告[15]之建議重點，供各金融機構於提升加密敏捷性、清理密碼技術負債與規劃 PQC／混合模式前置工作時，作為快速對照與落地推動之參考清單。

常見反模式（Antipatterns）	**建議作法**（No-regret actions）
手動管理 TLS 憑證	評估導入憑證生命週期自動化管理（部署、更新、輪替、撤銷）並保留稽核紀錄，以降低憑證改版與後續遷移的作業複雜度。
TLS 組態不一致（各環境／系統各自設定）	建立 TLS 組態基準（Baseline），並以自動化方式套用與稽核，提升一致性與可查核性；同時提高 TLS 1.3 覆蓋率，作為後續導入 PQC/混合模式的重要前置工作，以降低相容性與切換風險。
過度向下相容（仍允許 TLS 1.0/1.1 或弱加密套件）	監測 TLS 交握實際協商到的版本／套件／金鑰交換，並以使用量、來源、失敗率等決定淘汰順序，逐步收斂長尾依賴以降低切換風險。
把憑證／公鑰「寫死」或以信任例外繞過驗證（未受控；Pinning / Trust exceptions）	建立憑證簽發監測與防誤簽控管（例如：透過 CT 掌握是否出現未授權憑證，並以 CAA 限制可簽發的 CA），同時將各項信任例外納入申請核准、到期日與稽核追蹤，避免例外被長期保留。
使用萬用字元憑證（Wildcard）	改用主機名專屬憑證，縮小單一憑證外洩或誤用時的影響面，並降低後續切換與撤換成本。
金鑰治理分散（缺乏集中管控與權限控管）	將金鑰集中至 KMS/HSM 或受控金鑰庫，落實最小權限、金鑰清冊、輪替節奏與稽核紀錄，並避免同一把金鑰跨多用途／多系統共用。

[15] https://www.europol.europa.eu/publications-events/publications/prioritising-post-quantum-cryptography-migration-activities-in-financial-services

硬編碼金鑰／密碼（Hard-coded secrets）	導入秘密管理（Secrets Management），並在 CI/CD 設「掃描關卡」（policy gating）：只要掃到硬編碼就直接擋下來不讓合併/發布；必要例外須走核准並設定到期追蹤，確保可輪替與可撤銷。
不可替換加密（演算法／參數／格式被寫死）	採用標準化加密介面與組態化設定（可切換演算法與參數），並推動模組化／集中化加密元件，降低每次標準更新都需大改版的風險。
弱隨機數來源（Weak RNG）或不當金鑰生成	使用可信的安全亂數來源，並透過經審核的密碼庫/金鑰生成機制產生金鑰；同時在開發／測試流程加入檢核，避免自行實作亂數或採用不安全來源。
自行實作加密（Home-grown crypto）或不安全封裝	建立開發規範：禁止自行設計加密流程；統一使用經核准之標準函式庫與服務（含簽章／加解密／金鑰管理），並以程式碼審查與自動掃描落實。
缺乏 SBOM/CBOM（相依不可追溯）	建立並版本化 CBOM，並要求供應商提供可機器讀且可更新的 SBOM 或加密使用資訊；將其納入變更管理與例外追蹤，以支撐風險分級與遷移排序。

附錄 B：生態系協作示例—支付卡產業

支付卡生態系具備跨境互通、角色分工明確、標準與終端供應鏈高度相依等特性，可用來類比金融業多數「跨機構互通」場景（如跨行清算、收單／發卡、共同基礎設施、終端與中介設備），爰參考美國 FS-ISAC 就量子運算對支付卡產業衝擊報告[16]，摘要「支付卡產業」在 PQC 遷移時之跨角色協作案例，作為規劃 PQC 遷移生態系協作之參考。本案例用以說明，在高度互通的支付卡生態系中，各關鍵節點必須依共同節奏推進；否則可能影響整體安全與互通性，爰須以共同語言、共同測試與分階段時程進行協調。

一、案例背景與範圍

（一）支付卡生態系為多層次、跨組織的全球網絡，各角色（標準制定、卡組織、交換中心、銀行、終端與關鍵供應商）共同完成一筆支付交易；PQC 遷移需全鏈路協同，任何單一節點的遺漏都可能導致被破密的風險提高。

（二）量子運算對現行廣泛使用之公開金鑰密碼（如 RSA、ECC）構成長期破密威脅，將影響支付卡交易、發卡、授權、清算等核心流程。

（三）本案例整理重點聚焦於：角色分工、互動流程、關鍵相依性與分階段遷移策略；不涵蓋一般 IT 後勤（如帳單寄送、一般交易紀錄儲存）等非核心支付流程。

二、角色分工與協作任務

角色	主要職責	PQC 遷移中的協作任務（示例）
標準制定機構（NIST、PCI SSC、EMVCo、ISO）	制定加密與支付標準（如 AES、PQC 演算法、EMV、PIN 格式、RKL 等）。	選定/發布 PQC 與相關規格；制定遷移時程與測試規範；推動由 3DES 遷移至 AES（含 DUKPT 等標準修訂）；提供相容性與安全需求基準。
卡組織／卡網處理端（Card Brands Processing）	全球交易網絡運作與互通性管理；提供交換路由、授權支援與處理端服務（含備援處理 STIP）。	協調發卡/收單同步推進互通窗口；推動交換路由金鑰（Interchange Key）與相關 ZMK 等遷移至 AES；規劃並遷移備援授權服務（STIP）涵蓋 EMV／磁

[16] https://www.fsisac.com/knowledge/pqc

		條／CNP／PIN 驗證等流程。亦可透過責任轉移（Liability Shift）機制訂定轉換時程期限，規定收單/發卡於期限內完成轉換。
轉接中心／清算網路	跨機構交易路由、清算；管理 ATM/POS 相關網路互聯。	規劃共同測試與平行運行；驗證新版加密規格；提供跨機構切換窗口、回退條件與公告機制。另應訂定連線單位規格，並需支援新舊驗證方式。
發卡銀行（Issuer）	發卡、授權與風控；管理卡片與持卡人相關金鑰/憑證。	更新卡片製作/發行流程；推動 PIN 產製與儲存遷移至 AES；配合卡組織調整發卡相關系統以支援新舊驗證機制（如連線授權系統、卡片錢包 APP 等），完成互通測試與切換（含交換路由與 STIP 相關測試），並訂定卡片換發計畫。
收單銀行／PSP	商戶與 POS/ATM 接入；管理交易上傳與授權鏈路。	升級 POS/ATM 與後端介接；配合交換路由金鑰與 ZMK 等遷移至 AES（與卡組織協作）；確保端到端交易鏈路可用；調整收單相關系統支援新舊驗證機制（如收單授權、網路收單系統等），並配合卡組織規範訂定 POS/ATM 設備更版或汰換計畫，使 POS/ATM 可支援新舊驗證機制。
HSM 製造商	提供金鑰管理與密碼運算之高保證硬體平台。	支援 AES 金鑰與依新標準導入之 PQC（含混合模式）；提供相容性矩陣、效能數據與測試證據；針對韌體實作需考量側信道攻擊防護。

EPP／PED 製造商	提供 PIN 輸入與保護等安全模組（高保證終端）。	依 PCI PTS 要求支援 AES 與 PQC（含 RKL 規格更新）；提供側信道防護與驗證證據；規劃在 PQC 硬體可用前的 AES 金鑰分發過渡策略。
晶片／卡片製造商	生產支援 EMV 規格之晶片與卡片載具。	依新 EMV 規格導入 AES 與 PQC（含混合模式）；提供效能、儲存空間與側信道防護設計說明，支援驗證與認證。
行動裝置／POI 終端製造商	提供行動支付載具與 POS/ATM 等終端設備與韌體。	依新 EMV 規格導入 AES 與 PQC（含混合模式）；配合終端韌體升級、相容性測試與部署指引，並揭露封包大小、效能與維運限制。
網路、掃碼商戶	提供網路交易或掃碼支付之商戶服務。	依收單機構規格配合進行系統調整。

三、跨角色互動流程（交易安全生命週期）

（一）卡片製作與發行

1. 標準制定機構：定義 EMV 與 PQC 相關要求（演算法、金鑰/簽章格式、測試規範）。
2. 晶片/卡片供應商：依規格生產支援新要求之晶片與個人化（Personalization）流程。
3. 發卡銀行：透過 HSM 生成金鑰並寫入晶片，完成發卡與後續授權所需之金鑰與資料設定。
4. 卡組織：審核並登錄卡片，使其可於全球交易網絡互通。

協作要點：若卡片端與發卡端金鑰/簽章機制未依同一版本基準同步升級，將導致離線驗證、授權或後續清算流程發生驗證失敗；因此需由標準與卡組織先行定義版本基準與測試窗口。

（二）POS／ATM 交易與授權路由

1. 持卡人於 POS/ATM 發起交易。

2. POS/ATM（含 EPP/PED 等安全模組）進行 EMV 流程處理及對交易資料進行加密處理後，送往收單銀行／PSP。

3. 收單銀行／PSP 使用 HSM 等元件驗證 PIN 與交易資訊，並依路由規則送往卡組織／轉接中心。

4. 卡組織／轉接中心轉送至發卡銀行。

5. 發卡銀行進行授權與風控判斷後回覆結果，沿原路返回 POS/ATM 完成交易。

協作要點：交易鏈路同時涉及終端金鑰管理（例如 DUKPT）、傳輸層協定（TLS、IPsec/VPN）與後端 HSM 能力。過渡期常見作法為優先推動以 AES 強化對稱機制（例如推動 DUKPT 標準修訂與導入支援 AES 之模式），並規劃在非對稱加密相關場景導入 PQC／混合模式（視標準與產品可得性分批推進）；若終端韌體或中介設備（WAF/負載平衡器/VPN Gateway）等軟硬體支援度落後，將成為整體切換瓶頸。

（三）清算與結算

1. 卡組織／轉接中心彙整交易並執行跨機構清算與結算；訂定批次檔案連線標準。

2. 發卡銀行與收單銀行依結算規範交換與保護清算資料（含加密、簽章、完整性驗證）。

3. 標準制定機構／產業組織視需要更新規格與介接標準（例如 ISO 20022 相關規範）。

註：依 FS-ISAC 報告之範圍界定，「Settlement of accounts」多屬大量資料傳輸、更新與彙整等一般標準基礎設施活動，非其文件聚焦之「支付卡特有」密碼實作範疇；本附件保留此段落，主要用於提醒跨機構遷移時仍需考量端到端時程對齊與互通協調。

四、關鍵相依性與協作風險

相依方向	可能影響	協作控管建議
銀行 → 標準制定機構	若標準/測試規範未明確或版本頻繁變動，機構難以規劃路線圖與驗收依據，導致各自為政與	建立「共同版本基準」與「共同測試規格」；設定過渡期政策（混合模式、例外與到期管理）。

	互通風險。	
銀行 → 關鍵供應商（HSM、晶片、終端、中介設備）	供應商僅在新版本支援 PQC，或效能/封包/韌體限制導致無法部署，形成卡關元件與時程延宕。	要求路線圖與可驗證證據（相容性矩陣、測試報告、限制清單、回退方案）。
供應商（POI/HSM/EPP/PED）→ 銀行／卡組織	在高保證韌體環境導入 PQC 的實作經驗仍有限，且需滿足側信道攻擊防護與 PCI PTS、EMV 等認證要求；若驗證不足，可能導致終端設備無法通過認證或上線後暴露新的攻擊面。	在採購/驗收與共同測試中納入：側信道防護聲明與測試證據、PCI PTS/EMV 適用性與認證計畫、韌體升級與回退策略；並預留認證與量產交付時程。
卡組織／轉接中心 → 銀行（發卡/收單）	互通網路需雙方同步升級；任一側延遲可能造成交易拒絕、驗證失敗或服務中斷。	規劃共同上線窗口、平行運行與灰度切換；建立跨機構例外處理與通報機制。
商戶 → 收單銀行／PSP	若 POS/後端介接未更新，商戶可能無法完成交易或暴露於弱加密機制。	以分批汰換/韌體升級配合；提供商戶側切換指引與必要的相容性測試。

五、分階段遷移建議

階段	**時間區間**	**主要行動（跨角色協作重點）**
準備期	2025–2027	• 標準與卡組織：發布/更新 PQC 與測試規格、版本基準；啟動共同測試規劃。 • 銀行與交換中心：建立互通盤點語言（介接點、協定、憑證/金鑰、依賴供應商）；形成共同相容性矩陣初稿。 • 供應商：提出 PQC/混合模式路線圖、限制清單與驗證證據。

過渡期	2027－2030	• 採混合模式/雙軌策略以兼顧互通與風險控管（視場景分批導入）。 • 推動終端與中介設備升級（POS/ATM、Gateway、VPN/WAF/負載平衡器），並完成端到端壓測。 • 建立平行運行、灰度切換、回退條件與跨機構事件通報流程。
完成期	2030 以後	• 逐步淘汰不再適用之傳統公開金鑰機制，完成全鏈路一致性。 • 將演算法迭代納入例行變更與稽核證據鏈，持續更新相容性矩陣與供應鏈證據。

附錄 C：生態系協作的樞紐機構與負責業務

本附錄彙整金融生態系中具「樞紐(Hub)」角色之機關／單位，及其所主導(或維運)之跨機構共通平台與對接業務生態系，供各機構進行跨機構盤點、協作分工與遷移時程對齊之參考。

下表所列「樞紐機構／負責業務生態系」之範圍，係以需進行跨機構互通、共同平台運作或共通信任鏈／共同基礎設施對齊等「生態系協同」情境為主；若僅屬單純使用者（例如一般網站 Web TLS、單純檔案傳輸 SFTP 等未涉及跨機構協作之使用情境)，原則毋須納入金融生態系協作範圍。

樞紐機構(HUB)	負責之業務生態系（範疇）	主要對接對象／外部利害關係人
銀行公會	● 產業共通規範與介接技術規格（包含金融 XML 憑證共通性技術規範等） ● 跨機構協作之共通技術基準	● 財金公司及參加金融機構 ● 其他需依公會規格對齊之跨機構
財金資訊公司(跨行金流與共同平台)	● 清算／轉帳與提領（跨行 ATM、通匯等） ● 資料交換／電文服務（FEDI/FXML 等） ● 公用金流服務（繳費、繳稅等） ● 共通數位服務（電子支付共用平台、Open API、身分查驗等）	● 參加金融機構 ● 合作業者（如電支／第三方服務業者） ● 主管機關與相關公部門（視業務介接） ● 一般民眾與企業用戶
聯合信用卡中心(信用卡與支付卡交換／授權轉接)	● 交易授權／路由服務（POS/ATM 收單、發卡授權等） ● 交易安全／驗證服務（3DS/ACS、OTP、代碼化等） ● 批次／檔案作業（檔案收送、請款、對帳等） ● 風險控管／加值介接（風險警示/控管、信託資訊交換、數位身分等）	● 參加機構（發卡機構、收單連線機構） ● 商店／特店 ● 國際卡組織（VISA、Mastercard、JCB、銀聯） ● 持卡人

金融聯合徵信中心 (信用資料查詢與公務／監理查核)	● 信用資訊查詢（會員查詢、API查詢等） ● 檔案報送與交換（報送/回傳、傳輸加解密器等） ● 公務／監理介接（公務機關查詢/同意書驗證、監理平台申報等）	● 會員金融機構 ● 主管機關／監理機關/公務機關 ● 查詢對象（自然人／企業）
證券交易所 (證券市場交易與資訊服務)	● 交易／競價服務（交易平台、競價/備援等） ● 申報／資訊揭露（申報單一窗口、公開資訊觀測站、證券商網際網路傳輸系統等） ● 資訊服務／資料交換／連線設施（行情/資訊服務、ETMP、主機共置等） ● 結算交割／款項介接（結算交割相關介接等）	● 參加機構（證券商、投信、保管銀行、交割銀行等） ● 資訊服務業者／訂閱戶 ● 發行公司（上市、上櫃、興櫃、公開發行公司） ● 一般投資人 ● 主管機關與相關公部門（視款項/介接情境） ● 證券期貨周邊單位
證券櫃檯買賣中心 (店頭市場交易、申報與資訊服務)	● 交易服務（興櫃、債券、店頭衍生性商品等） ● 申報／監理資料（TR申報、證券商申報等） ● 資訊揭露／資料服務（公開資訊、交易資訊服務等） ● 新興業務資料庫（VASP申報/資料庫等）	● 參加機構（證券商、投信、保管銀行等） ● 發行公司與相關業者 ● 資訊服務業者／訂閱戶 ● 一般投資人 ● 主管機關（視申報/監理情境） ● 證券期貨周邊單位
期貨交易所 (期貨市場交易、結算與申報服務)	● 交易／結算服務（交易、集中結算等） ● 會員／交易人服務（期貨商管理、交易人查詢等） ● 備援交易 ● 線路管理與入金等周邊作業（線路管理、入金作業等）	● 參加機構（期貨商、結算會員等） ● 交易人 ● 主管機關與相關公會 ● 結算銀行（入金等介接情境） ● 證交所、櫃檯買賣中心、集保結算所

集保結算所（證券／期貨／票券／基金服務）	● 集中保管與結算交割（證券/債券/票券保管、登錄發行、帳簿劃撥、結算交割、股務作業等） ● 資料交換／對外介接（與證交/櫃買/期交資料交換、央行相關介接等） ● 投資人／股東服務（股東ｅ服務、第三方金融服務平台等） ● 申報／查詢與合規支援（申報、AML/CFT 相關查詢等）	● 參加機構（證券商、期貨商、票券商等參加人） ● 證交所、櫃買中心、期交所 ● 合作銀行與財金公司（視業務介接） ● 投資人／股東 ● 主管機關與相關公部門
壽險公會（保險科技運用共享平台）	● 保單／文件服務（電子保單存證等） ● 理賠協作服務（理賠/保經理賠、醫起通等） ● 保全與資料協作（保全聯盟鏈等） ● 身分驗證與授權（身分驗證中心等）	● 會員保險公司 ● 合作機構（保經代、醫療院所等，視服務情境） ● 保戶／一般民眾
產險公會（產險共通平台與聯盟鏈）	● 車險共用與同業協作（車險共用平台、同業分攤/聯盟鏈等） ● 共通作業支援（業務員管理、通報平台等）	● 會員機構（承做車險之產險公司、保經代公司等） ● 業務員 ● 主管機關（視申報/監理情境） ● 一般民眾（通報與服務使用者）
保險事業發展中心（保險資料交換與查詢）	● 強制險相關查詢／驗證（強制車險資訊、電子式保險證等） ● 電子保單與文件存證（認存證平台等） ● 業務統計與資料報送（各險種統計報送等） ● 保單／住宅火險等資料交換	● 會員保險公司 ● 合作機構（監理站、債權銀行等，視業務介接） ● 保戶／一般民眾

	（住宅火險電子化、保單存摺等）	
地震基金	住宅火險複保險查詢	● 參加機構（產險公司等） ● 主管機關（視作業/查核情境）
中央銀行	● 大額／零售支付清算與金融市場基礎設施（FMI）（如跨行清算、支付系統、跨行資金移轉、以及與金融監理／公共基礎設施之對接） ● 金融資料收集與查詢（如外匯資料與金融資料申報與查詢等） ● 公開市場操作與公債投開標	● 財金公司與參加金融機構 ● 主管機關／監理機關與相關公部門 ● 跨境／國際組織或合作方（視具體系統與介接情境）
票據交換所	票據交換與代收代付作業（包含支票／票據交換、媒體交換檔案／代收代付交易收送、結算結果通知與對帳、參加機構介接與作業協調等）	● 參加機構（銀行、信用合作社等） ● 合作業者（如電子支付業者、收費業者） ● 主管機關與相關公部門（視業務介接） ● 企業與一般民眾

附錄 D：關鍵供應商（例示）

除樞紐機構主導之跨機構平台外，金融生態系亦高度依賴少數「底層共通元件／服務」供應商（例如憑證信任鏈、註冊/驗證服務、資料交換介接平台等）。此類供應商雖未必是特定業務生態系之『主導機關』，但其服務一旦變更（例如憑證格式、金鑰長度、介接協定或加密套件支援度），將對多個 Hub 與大量參加機構造成同步影響，爰於本附錄一併列示。

關鍵供應商	提供之共通元件／服務	主要使用／依賴之金融生態系
臺灣網路認證股份有限公司	• TPKI/PKI 相關服務與安控元件（例：RA 註冊系統、VA 驗證系統、客戶端安控元件） • 金融 XML（FXML）憑證等產業共用憑證/信任鏈服務 • 身分識別/憑證相關服務（例：TWID 等） • TLS 站台憑證	• 財金公司 FEDI／FXML 等跨行資料交換（盤點表多處將 TWCA 列為外部利害關係人） • 證券期貨市場對外身分驗證與憑證應用（例：證券業 EC+ 憑證等） • 各金融機構對外 TLS 站台憑證、伺服器/裝置身分憑證等（屬跨域共同依賴）
臺灣行動支付股份有限公司	• 行動支付相關共通服務與業務協作角色（於部分財金公司繳費/支付相關流程中作為外部利害關係人）	• 財金公司全國繳費（ebill）等相關對接情境 • 行動支付/錢包等跨機構支付生態系之參與機構與使用者

附錄 E：共通元件／服務（例示）

本附錄以「第四階：共通性基礎設施與供應商資訊」角度進行延伸盤點，彙整常見之共通元件／服務作為盤點時的檢核清單參考：凡系統使用到該類元件，建議應向供應商確認PQC／混合模式支援版本、效能影響、相容性矩陣、EOL/EOS與回退方案。

共通元件／服務	盤點／驗證重點	影響之使用情境／生態系
HSM（硬體安全模組）/PQC module 韌體安全模組	• 是否支援 NIST PQC（或 PQC／混合模式）相關演算法／介面；是否需韌體更新或設備汰換 • 效能與併發能力（PQC 封包/金鑰變大、簽章驗證成本上升） • 密碼模組認證/驗證（如 FIPS 140-3）與版本相容性	• 金鑰/憑證基礎設施（KMS/HSM） • 交易簽章、電文簽章、PIN/支付相關金鑰作業 • 跨機構介接（財金、聯卡、聯徵等）涉及之簽章/驗證
KMS（含雲端 KMS/代管金鑰服務）	• 支援之金鑰型別、KEM/簽章、API 版本與相容性 • 金鑰輪替、封存與存取權限（最小權限/稽核軌跡） • 跨區/備援架構對效能與可用性影響	• 資料加密（儲存/傳輸）與服務端憑證/金鑰管理 • 雲端應用、SaaS 串接、API Gateway 等
PKI／CA／RA／VA（含外部憑證與信任鏈服務）	• 憑證格式與演算法政策（PQC/混合模式）、簽發/撤銷/OCSP 流程 • 憑證效期縮短與自動化輪替（作業量暴增） • 信任鏈一致性（Root/Intermediate、相容性政策）	• 身分驗證（對外 TLS、裝置/伺服器身分憑證） • 跨機構資料交換（如 FXML 憑證） • 交易簽章/驗章鏈（含長期驗證需求）
CLM（憑證生命週期管理／自動化發佈輪替）	• 是否支援新憑證類型/演算法與自動化佈署 • 憑證輪替、撤銷、稽核報表與回復機制	• 對外通路 TLS 端點大規模輪替 • 內部 IAM/設備憑證治理

WAF／ADC／負載平衡器（LB）	• TLS 1.3 與 PQC／混合模式支援度、封包大小／握手延遲影響 • 與既有規則/策略（WAF 規則、TLS Baseline）相容性 • 版本支援與 EOL/EOS 造成之升級壓力	• 對外網站/網銀/行銀、API 對外服務 • 生態系互通入口（如 Hub 對接之閘道）
CDN／DDoS 防護／網路邊界代管服務	• TLS 終端點所在位置（自有／代管）與 PQC／混合支援時程 • 封包放大對連線品質與攻擊面（誤判/丟包/限流）之影響	• 對外通路（網站/APP API） • 尖峰交易量與可用性需求高之服務
Proxy／API Gateway	• 對外／對內介接協定（TLS、JWS、JWE 等）之支援版本 • 電文/簽章尺寸變大對欄位長度、訊息處理與紀錄存證之影響	• 外部串接（跨行傳輸、第三方 API、SaaS 串接） • Hub-and-Spoke 對接閘道
VPN／IPsec／遠端存取閘道	• 協定堆疊對 PQC／混合模式之支援、韌體升級／授權限制 • 效能、MTU/封包增大、握手延遲對遠距維運與營運之影響	• 遠距辦公/維運管理通道 • 機房/資料中心跨區連線
防火牆／IPS／IDS	• 對新握手與封包特徵之檢測/誤判風險 • 升級版本是否影響既有策略與高可用	• 對外通路與跨區連線邊界 • 跨機構介接專線/通道
端點載具（USB Token／智慧卡／行動安全元件）	• 運算/記憶體限制是否可支援 PQC（常需汰換） • 發放、更新、回收與客戶端相容性風險	• 企業金融憑證載具（如特定業務憑證） • 高不可否認性場景之簽章載具

身分鑑別與驗證機制（SSO/MFA/FIDO 等；含機器身分驗證）	• 驗證流程所依賴之加密通道與信任鏈（TLS、憑證鏈、伺服器／用戶／裝置憑證）及其演算法政策 • 若涉及挑戰回應、簽章或驗證器（如 FIDO 私鑰、裝置金鑰、交易授權簽章），需盤點金鑰保護位置（TEE/SE、Token）與供應商支援之演算法／版本（含 PQC／混合模式）	• 客戶／員工身分鑑別、特權登入、交易授權（含多因子與裝置驗證） • 跨機構身分驗證（依生態系服務而定）
DNS／憑證名稱解析（含 DNSSEC）	• 若採 DNSSEC 或憑證自動化（ACME/DNS-01），需確認簽章演算法/金鑰長度、區域簽署與輪替策略 • 變更期間需確保名稱解析與服務可用性（避免大規模失效）	• 對外網站/API、行動 App 後端、跨機構互通入口
NTP／時間同步、時間戳記（TSA）服務	• 長期驗證（LTV）與存證需求常依賴時間戳記之簽章/驗證鏈，需確認演算法政策與可長期驗證策略 • 時間同步異常將造成驗章、日誌關聯與稽核可信度下降	• 交易存證、電子文件簽署、保單/理賠等需長期保存之簽章資料
SFTP／檔案交換平台（含批次傳輸、檔案加解密/簽章）	• 確認 SSH/SFTP 版本、金鑰交換/簽章支援路線圖（含混合模式可能性） • 批次檔案簽章/加解密（例如 PGP）之演算法與金鑰管理（輪替、封存、回溯驗證）	• 跨機構檔案報送/對帳（例：期交所交易系統 SFTP、批次報送與資料交換）

MQ／ESB／企業整合中介（訊息佇列、介接匯流排）	• 若中介層負責 TLS 終止、訊息簽章、或加解密封裝，需確認其加密套件、憑證/金鑰來源與版本支援 • 訊息尺寸放大與延遲上升對吞吐量與尖峰壓力之影響（需壓測）	• 跨系統整合、跨機構介接閘道、批次與即時混合流程之中介層
郵件安全閘道（加密郵件、簽章、S/MIME）	• 確認郵件簽章/加密機制（S/MIME）與憑證鏈之演算法政策、輪替與相容性（含外部對象） • 若為雲端郵件或代管服務，需釐清金鑰管理模式（BYOK、代管）與可驗證證據	• 對外公務/商務往來、對外通知與具不可否認性需求之郵件流程
SSH Bastion／跳板機（特權維運通道）	• 確認 SSH 版本、金鑰交換/簽章演算法支援，與既有主機端相容性矩陣 • 與 PAM/IAM 整合之認證機制（憑證、短效金鑰、MFA）及稽核軌跡	• 重要主機與核心系統之維運管理、委外廠商遠端維運通道
資料庫／儲存加密與代碼化（TDE、欄位層加密、Tokenization）	• 金鑰來源（KMS/HSM、內建金鑰庫）、輪替與稽核；加密模式是否可調適/可替換 • 對長期保存資料之 HNDL 風險控管（欄位最小化、代碼化、金鑰分離）	• 核心帳務、交易/理賠/授信等高敏感資料庫；跨系統資料交換落地儲存
備份／歸檔加密（含離線媒體、雲端備份）	• 備份加密演算法/金鑰管理、封存與可回復性（包含金鑰遺失風險） • 長期保存資料若以傳統公開金鑰保護（加密金鑰封裝/簽章），需評估未來回溯解密風險與處置策略	• 全域備份/復原、法遵留存、營運持續（BCP/DR）

為利將本附錄盤點清單轉化為可執行之盤點與供應商調查作業，建議參考以下使用方式：

1. 若系統對接附錄 C 所列 Hub 平台，除依 Hub 規格調整外，亦應檢核本表所涉之共通元件（例如：對外通路之 WAF/LB/CDN、介接閘道、HSM/PKI）是否已具備可支援之版本與測試證據。

2. 參考本表「盤點／驗證重點」欄位轉為供應商問卷題目（版本、支援模式、相容性矩陣、效能數據、EOL/EOS、回退方案）。

附錄 F：共通業務盤點參考框架（示例）

本附錄提供「共通業務參考框架」之示例，協助各金融機構以一致脈絡整理自身業務線與關鍵使用情境，作為盤點加密資產（CBOM）、辨識跨機構互通依賴與規劃遷移優先序之導引。各機構可依自身業務範圍與系統架構選用或調整本示例之分類方式，並可搭配附錄 C（Hub 生態系）、附錄 D（關鍵供應商）與附錄 E（共通元件／服務）進行延伸對照；本附錄為參考示例，建議依自身業務範圍與系統架構增刪調整。

一、銀行業

法規	業務	應用
金融機構提供自動櫃員機系統安全作業規範	ATM	訊息驗證、身分驗證
金融機構辦理電子銀行業務安全控管作業基準	企業網路銀行	網站憑證、加密傳輸、身分驗證、資料隱蔽
金融機構辦理電子銀行業務安全控管作業基準	個人網路銀行	網站憑證、加密傳輸、金鑰憑證、身分驗證、資料隱蔽
金融機構辦理電子銀行業務安全控管作業基準 金融機構提供行動裝置應用程式作業規範 金融機構提供 QR Code 掃描支付應用安全控管規範	行動銀行 APP	網站憑證、加密儲存、加密傳輸、金鑰憑證、身分驗證、裝置驗證、交易存證、資料隱蔽
金融機構辦理電子銀行業務安全控管作業基準	線上申請服務(如開戶、申貸…)	網站憑證、加密傳輸、身分驗證、資料隱蔽

金融機構辦理電子銀行業務安全控管作業基準	線上理財服務(如理財試算、智能理財…)	網站憑證、加密傳輸、身分驗證
金融機構辦理電子銀行業務安全控管作業基準	線上代收服務(如學雜費、帳單代收….)	網站憑證、加密傳輸、資料隱蔽
金融機構辦理電子銀行業務安全控管作業基準	網路收單(如信用卡/晶片金融卡網路收單….)	網站憑證、加密傳輸、身分驗證、交易存證、金鑰憑證、資料隱蔽
金融機構辦理電子銀行業務安全控管作業基準	對外提供服務資訊查詢(如匯利率/牌價查詢…)	網站憑證、加密傳輸
金融機構辦理電子銀行業務安全控管作業基準	官方網站	網站憑證、加密傳輸
金融機構提供 QR Code 掃描支付應用安全控管規範	行動支付後台管理	網站憑證、加密傳輸、雙向憑證、數位簽章、專線
無	分行臨櫃業務	網站憑證、加密傳輸、身分驗證

二、證券業

類別	業務	應用
交易類	提供下單、委託處理等交易	身分驗證、加密傳輸、交易存證
行情報價類	提供市場即時行情資訊	身分驗證、加密傳輸
帳務類	提供帳務結算	身分驗證、加密傳輸
複委託類	提供海外股票複委託交易	身分驗證、加密傳輸、交易存證

三、期貨業

類別	業務	應用
交易類	提供期貨下單與委託處理	身分驗證、加密傳輸、交易存證
行情與報價	提供市場即時行情資訊	身分驗證、加密傳輸
帳務與結算	客戶資金與保證金計算處理	身分驗證、加密傳輸

四、壽險業

類別	業務	應用
底層基礎服務	認證、登入、授權控管、金鑰、憑證、稽核、加解密	加密傳輸、身分驗證、數位簽章、加密儲存
財務系統	FTP/SFTP、電文、與銀行/政府串接	加密傳輸、身分驗證、加密儲存
保險營運系統	保單、單據、表單、理賠作業	數位簽章、加密儲存、身分驗證、加密傳輸
通路管理	保戶使用的所有數位服務	身分驗證、加密傳輸、加密儲存、數位簽章

客戶管理	外勤工具、投保、查詢	身分驗證、數位簽章、加密傳輸
內部營運	行政、法遵、活動	身分驗證、加密傳輸、加密儲存
投資交易系統	投資交易相關	身分驗證、加密儲存、加密傳輸

五、產險業

類別	**業務**	**應用**
資訊基礎服務	底層資訊營運及管理系統	加密傳輸、身分驗證、加密儲存
客戶服務	保戶使用的所有數位服務	身分驗證、加密傳輸、交易存證
通路服務	業務員或合作通路使用的數位工具	加密傳輸、身分驗證、加密儲存
保險營運系統	報價、出單(印單)、批改(保全)、理賠、再保、客服	身分驗證、加密儲存、加密傳輸、交易存證、數位簽章
業務支援	資料倉儲、行銷分析	身分驗證、加密傳輸、加密儲存
財務系統	財務收付相關資料處理及交換作業	身分驗證、數位簽章、加密傳輸
內部營運管理	行政、法遵、稽核	身分驗證、加密傳輸
投資交易系統	投資交易相關	身分驗證、加密儲存、加密傳輸

附錄 G：名詞解釋

名詞／縮寫	說明
AES	對稱式加密標準（Advanced Encryption Standard），常用於資料儲存加密、通道加密的資料加密階段與金鑰封裝後的內容保護。量子風險下通常以提高金鑰長度（如 AES-256）作為強化方向。
API Gateway / Proxy	用於 API 流量之入口控管與轉送元件，常負責 TLS 終止、身分驗證、授權、流量控管與日誌；因此其支援之協定版本、加密套件與憑證/金鑰管理能力會直接影響 PQC 導入與互通性。
BYOK	Bring Your Own Key，客戶自帶金鑰模式：將自有金鑰（常在自有 HSM/KMS 產生）匯入雲端/代管服務使用，以提升金鑰主控性。盤點時需釐清金鑰邊界、輪替/撤銷流程與供應商對 PQC 之支援。
CA/RA/VA	憑證機構角色：CA（簽發憑證）、RA（註冊/身分審核）、VA（驗證服務，如憑證狀態查詢）。
CBOM	密碼技術資產清單，彙整系統/流程中使用之加密資產（演算法、參數、憑證鏈、金鑰來源、部署位置、供應商版本、可替換性等）的清單，用於風險分級與遷移規劃。
CDN	內容傳遞網路（Content Delivery Network），常用於加速對外網站/服務與吸收流量；若 TLS 終止點在 CDN 側，其對 PQC／混合模式支援與封包限制會直接影響用戶端相容性。
Certificate Transparency (CT)	憑證透明度機制：公開記錄已簽發之 TLS 憑證，協助發現誤簽或未授權憑證。盤點時可用來強化對外服務之信任鏈治理與風險偵測。
CLM	憑證生命週期管理，用於憑證申請、部署、輪替、撤銷與稽核之自動化/管理能力，支撐縮短憑證效期與大量端點輪替。
CRL	憑證撤銷清單（Certificate Revocation List），以檔案形式提供被撤銷憑證清單。遷移時需檢視 CRL 發布頻率、分發方式與簽章演算法，並評估下載量與延遲對驗證流程之影響。

CRQC	Cryptographically Relevant Quantum Computer，具備足以破解現行主流公鑰密碼（如 RSA/ECC）之量子電腦能力門檻（概念性門檻，非單一固定規格）。
Crypto-Agility	加密敏捷性，指系統能以可控方式快速替換/調整加密演算法、參數、憑證格式與協定版本之能力，並能納入測試、切換與回退機制。
DDoS	分散式阻斷服務攻擊（Distributed Denial of Service）。在 PQC／混合模式下，握手封包與運算成本可能上升，需納入邊界設備/代管防護之容量與誤判風險評估。
DNSSEC	Domain Name System Security Extensions，以數位簽章保護 DNS 解析結果之完整性與可驗證性。遷移時需關注區域簽署金鑰（KSK/ZSK）輪替、演算法政策與相容性。
ECC	橢圓曲線密碼學（Elliptic Curve Cryptography），常用於 TLS 金鑰交換與數位簽章（如 ECDHE/ECDSA）。在量子威脅下同樣屬主要替換標的。
EOL/EOS	產品生命週期狀態：EOL（停止銷售/更新）與 EOS（停止支援），常造成升級或汰換時程壓力。
FIDO / FIDO2	身分鑑別標準（以公私鑰與挑戰回應進行驗證），常用於免密碼或多因子驗證。盤點時需關注驗證器（硬體/軟體）金鑰保護位置（TEE/SE）與供應商對演算法/版本之支援。
FIPS	美國聯邦資訊處理標準（Federal Information Processing Standards），由 NIST 發布，常用於規範政府與受規範產業採用之密碼演算法、模組與安全要求（例如 FIPS 140-3）。
FIPS 203/204/205	首批後量子密碼標準（2024 年發布）：FIPS 203 為 ML-KEM（金鑰封裝機制），FIPS 204 為 ML-DSA（數位簽章），FIPS 205 為 SLH-DSA（雜湊式數位簽章）。
FMI	Financial Market Infrastructure，金融市場基礎設施（例如支付系統、清算結算系統、中央證券保管等）。其互通與可用性要求高，且通常涉及跨機構信任鏈與加密通道。

HNDL	先攔截、日後解密，攻擊者於現階段攔截並保存加密通訊/資料，待未來量子電腦成熟後回溯解密，影響長效期機敏資料之機密性。
HSM	硬體安全模組，用於產生、封存與使用金鑰之專用硬體，提供防竄改與強化存取控制，常用於交易簽章、金鑰管理、支付金鑰作業與 PKI 等關鍵場景。
Hub-and-Spoke	生態系協作模式：由樞紐（Hub）機構/平台制定共通介接規格、測試窗口與遷移節奏，各參與者（Spokes）依共同基準完成對接與切換，以維持互通性與降低重工。
Hybrid Mode	混合模式，指過渡期同時使用傳統演算法與 PQC 演算法（例如同時進行兩種金鑰交換/簽章），以兼顧互通性與風險控管。
IAM / PAM	身分與存取管理（Identity and Access Management）與特權存取管理（Privileged Access Management）。在本文件脈絡中，重點在於其所依賴之加密機制（憑證、簽章、MFA、管理通道）與機器身分互信。
IPsec	網際網路協定安全套件，常用於站點對站點 VPN 與跨區加密連線。遷移時需關注協商用的金鑰交換與認證機制、設備韌體版本，以及與既有專線/路由架構的相容性。
JWS / JWE	JOSE 標準中的兩種封裝：JWS（JSON Web Signature）用於電文簽章；JWE（JSON Web Encryption）用於電文加密。常用於 API 與跨機構資料交換（例如以 JWT 承載）。
KMS	金鑰管理服務，集中化管理金鑰之產生、封存、輪替、存取控制與稽核之服務/平台（含雲端 KMS）。
LTV	長期保存/可驗證之簽章與存證需求，通常涉及時間戳記、憑證撤銷資訊與驗章策略，以確保存證在多年後仍可被驗證。
ML-KEM / ML-DSA / SLH-DSA	三項 NIST 標準化後量子演算法：ML-KEM 用於金鑰交換/封裝（常見於 TLS 與通道建立），ML-DSA 與 SLH-DSA 用於數位簽章（常見於身分驗證、程式碼簽章與不可否認性需求）。

MQ / ESB	訊息佇列（Message Queue）與企業服務匯流排（Enterprise Service Bus）。若中介層負責 TLS 終止、訊息簽章或加解密封裝，其加密套件、憑證/金鑰來源與版本支援將影響端到端互通與效能。
MTU	Maximum Transmission Unit，單一封包可承載的最大大小。導入 PQC／混合模式後握手封包可能變大，易觸發分段、丟包或設備限制，因此需納入壓測與邊界設備檢核。
OCSP	線上憑證狀態查詢協定（Online Certificate Status Protocol），用於確認憑證是否已撤銷。盤點時需確認 OCSP 端點、回應簽章演算法與可用性，避免在遷移或縮短憑證效期時造成驗證瓶頸。
PKI	公鑰基礎建設，以憑證與信任鏈支撐身分驗證、加密通道與數位簽章之體系，含憑證簽發、撤銷、驗證與信任鏈管理。
PQC	後量子密碼，指能抵抗具規模量子電腦攻擊之密碼演算法與相關標準/實作，主要用於取代現行易受量子攻擊之公開金鑰演算法（如 RSA/ECC）場景。
PQC Module	實作 NIST 標準化後量子演算法之模組且通過 NIST CAVP 韌體驗證。
Root CA / Intermediate CA	憑證信任鏈中的根憑證與中繼憑證。遷移至 PQC／混合模式時，通常需同步考量信任錨點、交叉簽署、相容性矩陣與部署順序，以避免互通失效。
RSA	常用之公開金鑰演算法（加密/簽章）。在具規模量子電腦下可能被 Shor 演算法破解，為 PQC 遷移的主要替換標的之一。
SFTP	SSH File Transfer Protocol，以 SSH 通道提供檔案傳輸與身分驗證；常用於批次報送/對帳。盤點時需關注 SSH 金鑰交換、主機金鑰/簽章演算法、以及外加檔案加解密/簽章（如 PGP）之相依。
Secrets Management	秘密資訊管理：集中管理密碼、API 金鑰、憑證私鑰等機敏資訊，支援最小權限、稽核與自動輪替，避免硬編碼或散落於設定檔造成長尾風險。

SHA-2 / SHA-3	雜湊函數家族（用於完整性保護、簽章摘要、金鑰衍生等）。量子情境下通常以提升摘要長度或改採更強參數作為強化方向（例如避免弱雜湊如 SHA-1）。
SNI	Server Name Indication，TLS 擴充，用於在同一 IP/端點上提供多站台憑證。盤點對外端點時需留意是否經由 LB/CDN/WAF 終止及其相容性。
SSH	安全遠端登入/通道協定（含金鑰交換、加密與主機金鑰簽章）。盤點批次檔案交換（SFTP）與維運跳板機時，需特別關注主機金鑰/簽章演算法與升級相容性。
TSA	Time Stamping Authority，時間戳記服務提供者；用以對資料/簽章加上可信時間，使其在多年後仍可驗證（LTV）。需關注其簽章演算法政策與長期驗證策略（含 PQC／混合模式）。
TLS	傳輸層安全協定，用於保護通訊傳輸之機密性與完整性，常搭配伺服器/用戶憑證與金鑰交換機制。
TNFL	現在信任、稍後偽造，攻擊者於未來可偽造數位簽章、憑證或身分驗證結果，回溯影響不可否認性、完整性與信任鏈（例如偽造交易指令簽署）。
WAF	網頁應用防火牆（Web Application Firewall），常部署於對外通路前端，可能同時負責 TLS 終止或檢視流量；其版本/效能限制會影響 TLS 1.3 與 PQC／混合模式之導入。
WebPKI	瀏覽器與作業系統所信任的公開 PKI 信任體系（根憑證、憑證政策、撤銷機制等）。金融機構對外 TLS 服務需受其政策變更與憑證存活期調整影響。

註：本附錄名詞解釋係供本文討論與盤點作業之工作定義；如相關規範或國際標準文件另有明確定義，應以其定義為準。