金融業後量子密碼(PQC)遷移參考指引

金融監督管理委員會

2026年6月

什麼是後量子時代的資安挑戰？

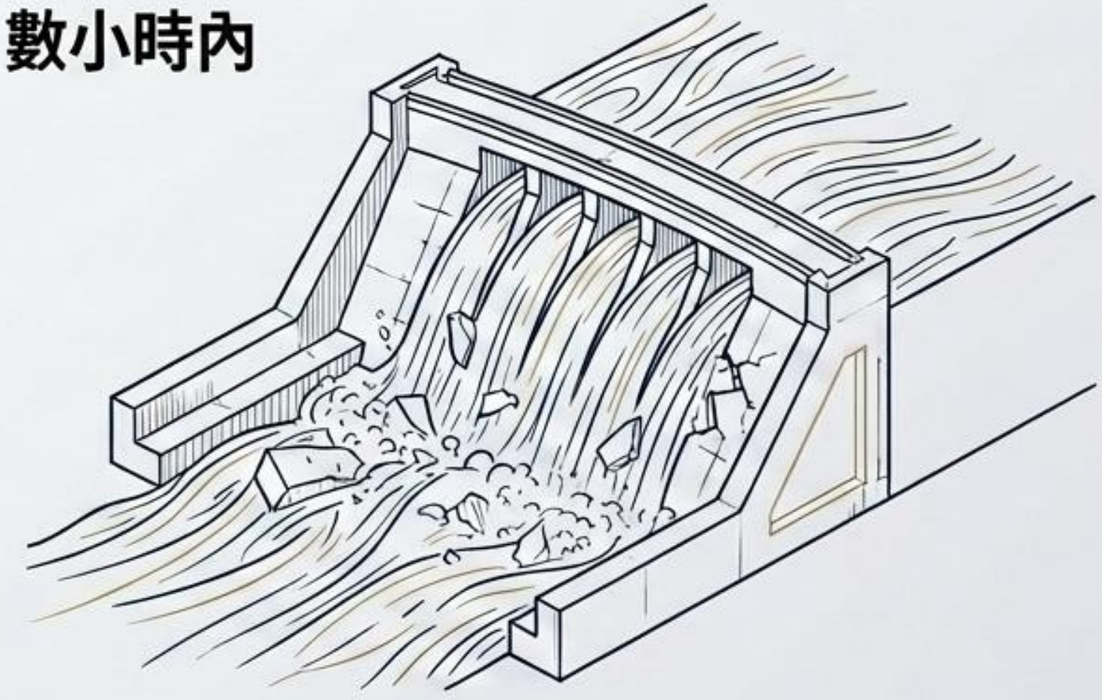
現行傳統加密技術 (RSA-2048)

耗時數百年

現況：金融服務高度仰賴公鑰密碼機制（身分驗證、交易簽章、資料保護）。這是金融信任的基石。

具破密能力之量子電腦 (CRQC)

數小時內



危機：量子運算技術具備指數性成長的算力，現有安全鎖將在未來面臨失效的風險 (Y2Q)。

雙重量子威脅：今日的竊取與明日的偽造

HNDL (Harvest Now, Decrypt Later)

威脅機制：攻擊者現階段攔截並儲存加密通訊，待未來量子運算成熟後回溯解密。

時間發酵點：現在立即發生 (現時風險)。

受衝擊資產：具備長期敏感生命週期 (Shelf-life) 的機密資料 (如客戶個資、交易明細、授信資料、保單紀錄)。

緩解優先序：需優先實施多層次防護、資料最小化與端點加密升級。

TNFL (Trust Now, Forge Later)

威脅機制：利用量子計算破解數位簽章演算法，偽造合法憑證與身分證明。

時間發酵點：具備破密能力之量子電腦 (CRQC) 出現時。

受衝擊資產：核心 PKI 體系、金融交易簽署指令、代碼簽署、長期驗證 (LTV) 之電子存證。

緩解優先序：需於 CRQC 出現前完成系統認證與簽章機制之 PQC 遷移。

國際監理與生態系脈動：全球已進入加速過渡期

Global Pulse Dashboard

NIST (美國國家標準暨技術研究院)

- 2024年8月正式發布首批 PQC 標準並立即生效。
- 涵蓋 FIPS 203, 204, 205。
- 技術標準底定，全球正式進入落地階段。

G7 與 WEF (世界經濟論壇)

- G7 倡議：2025-2027 完成盤點，2030-2032 高風險遷移，2035 全面完成。
- WEF 提出四階段路線：準備、釐清、指導、轉型與監測。

2030 (Y2Q)

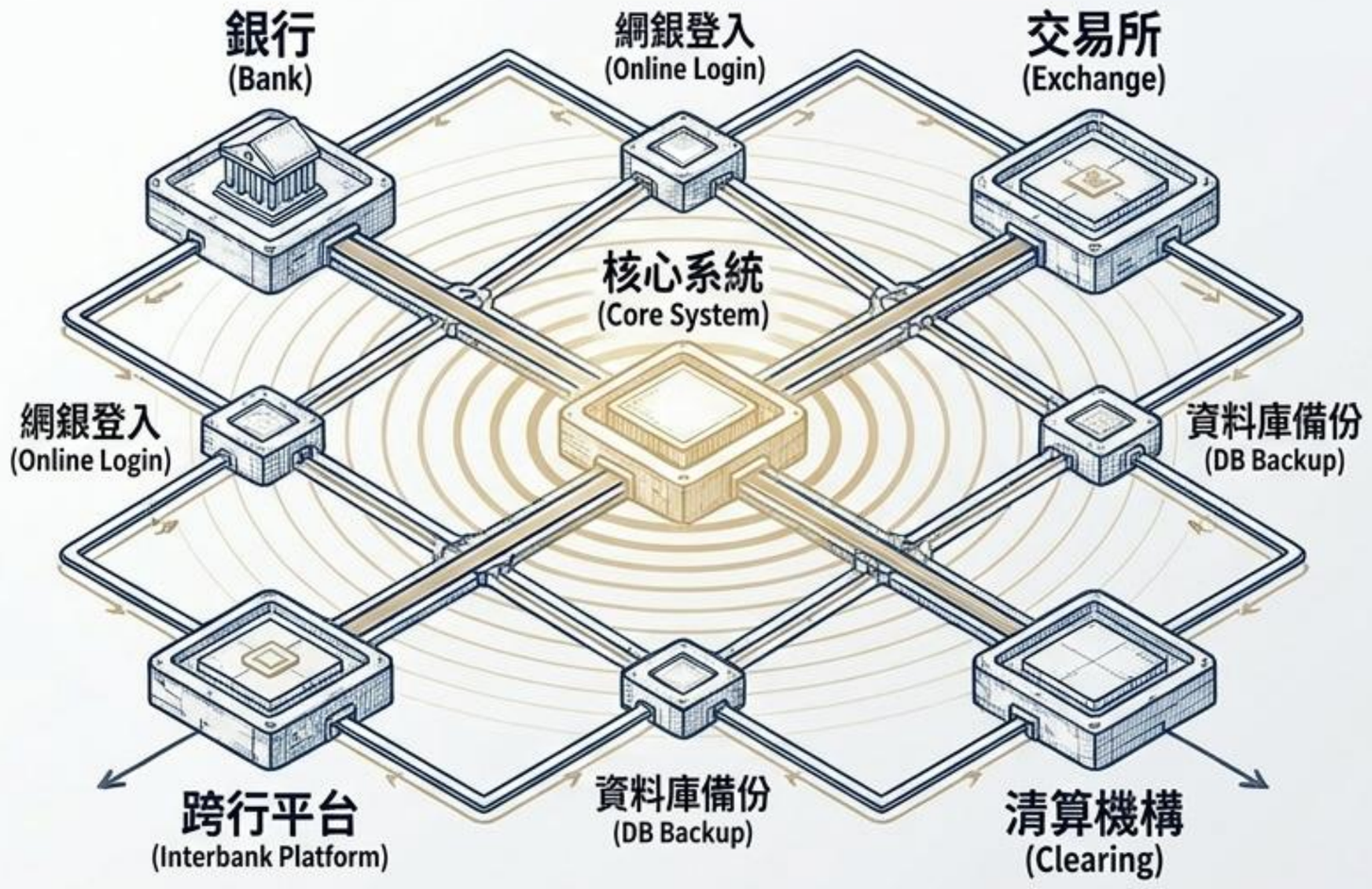
亞洲監理動態 (新加坡 MAS & 日本金融廳)

- 新加坡：發布量子風險資安諮詢，要求強化加密敏捷性並啟動 QKD 試驗。
- 日本：發布高風險衝擊報告，針對支付系統與銀行介面提出警告與盤點要求。

科技生態系 (Google 的極進步調)

- 將 PQC 遷移目標大幅提前至 2029 年。
- 瀏覽器與雲端平台的提早切換，將嚴重壓縮金融業對外連線 (TLS) 的準備時間。

金融業面對 PQC 遷移的兩大獨特挑戰



痛點一：密碼無所不在，盤點如大海撈針

從網銀登入、ATM 連線、跨行交易到資料庫備份，加密技術散落於技術堆疊的各個暗角。

痛點二：生態系緊密互聯，無法單打獨鬥

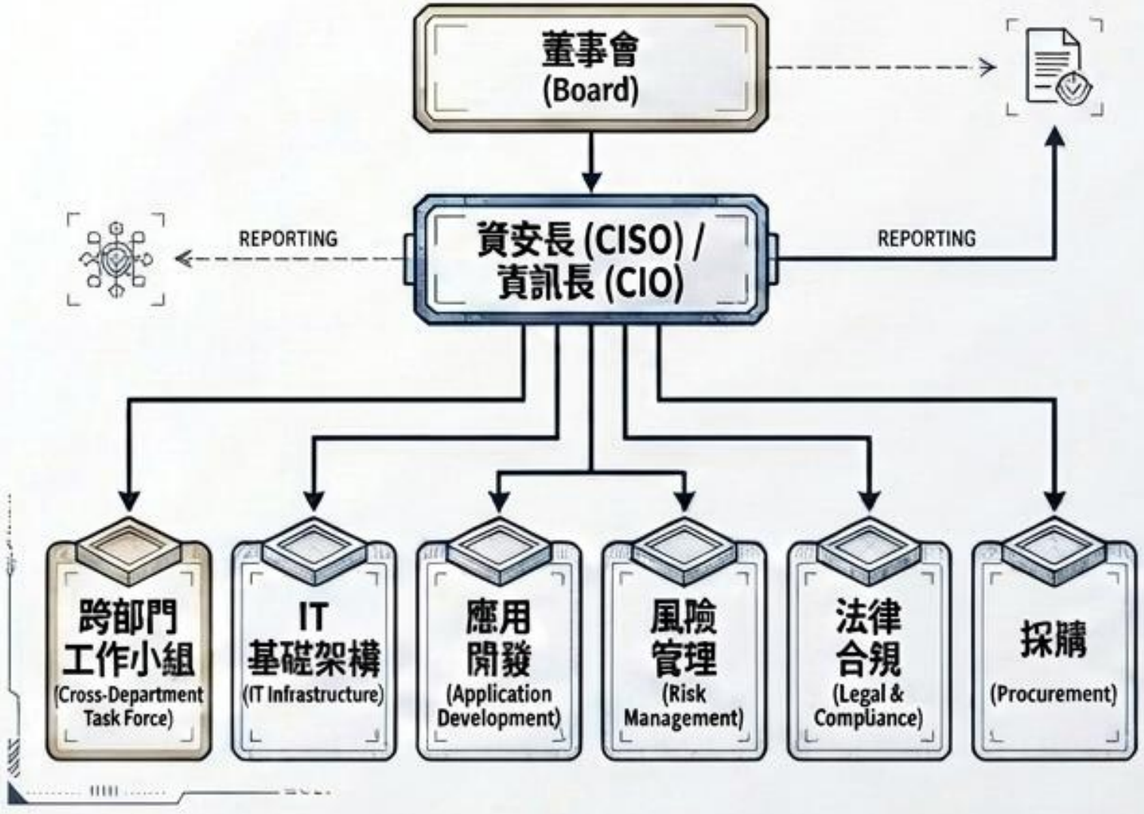
金融體系是相互扣連的艦隊。單一機構升級，若跨行平台或供應商未跟上，將導致交易中斷與互通失效。

因此，金管會提出「七大策略」，引導金融業循序漸進、穩健轉型。

打底：提升至董事會層級，建立「密碼技術清單」

策略 1：PQC 政策與治理

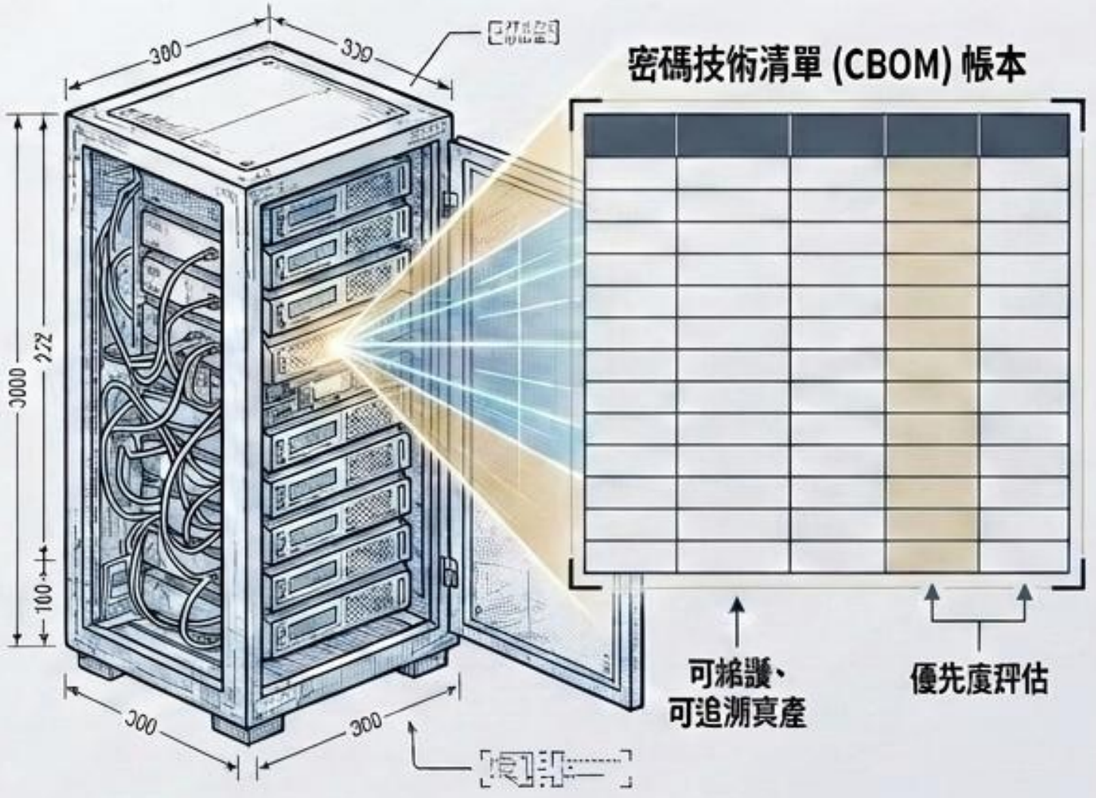
將量子風險視為企業戰略議題。由資安長 (CISO) 或資訊長 (CIO) 領軍，成立跨部門工作小組。



TIME FLOW

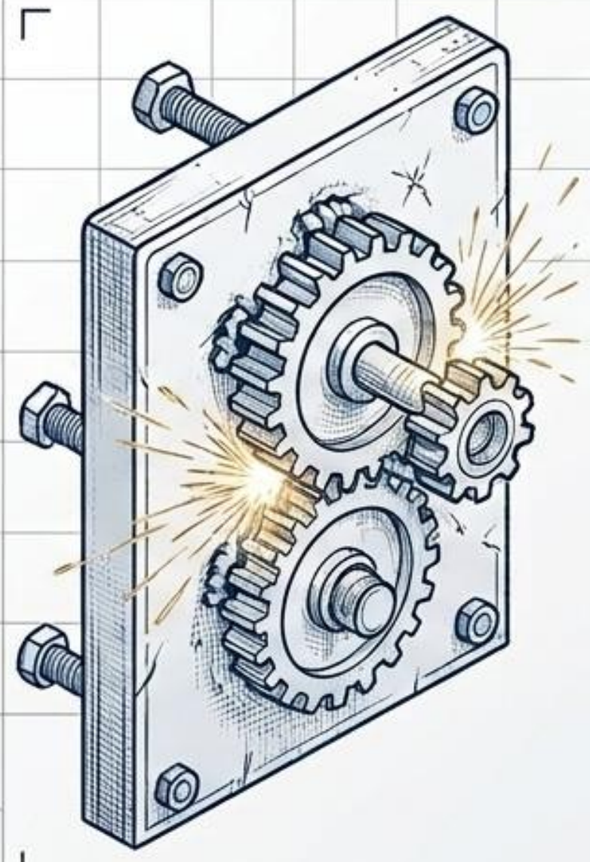
策略 2：盤點資產，建立 CBOM

不知道自己有什麼，就無法保護。依風險優先度限定範圍，建立可維護、可追溯的密碼技術清單 (CBOM)。

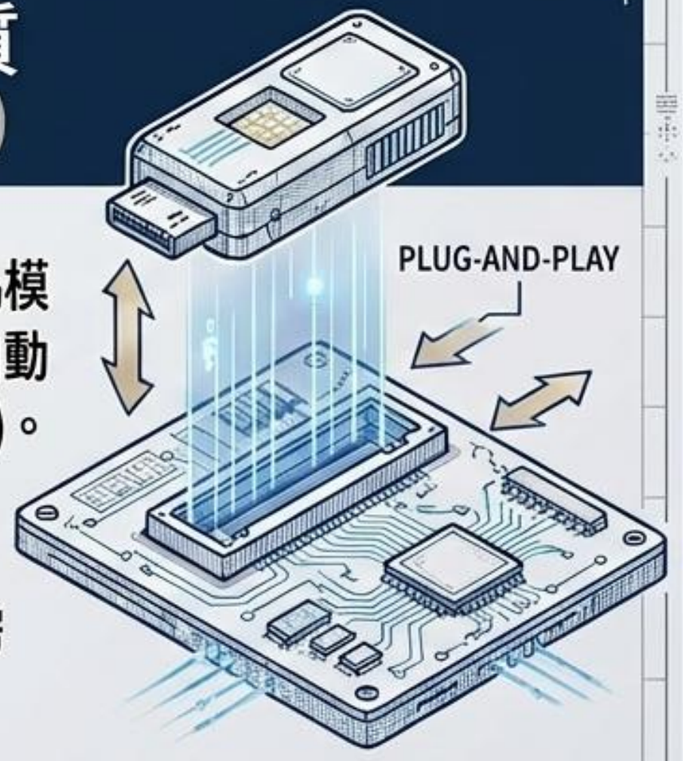


策略3：優先清除「密碼反模式」，打造「加密敏捷性」

PQC 標準仍持續演進，目標不是一次性替換演算法，而是打造隨時可無痛切換的敏捷體質。

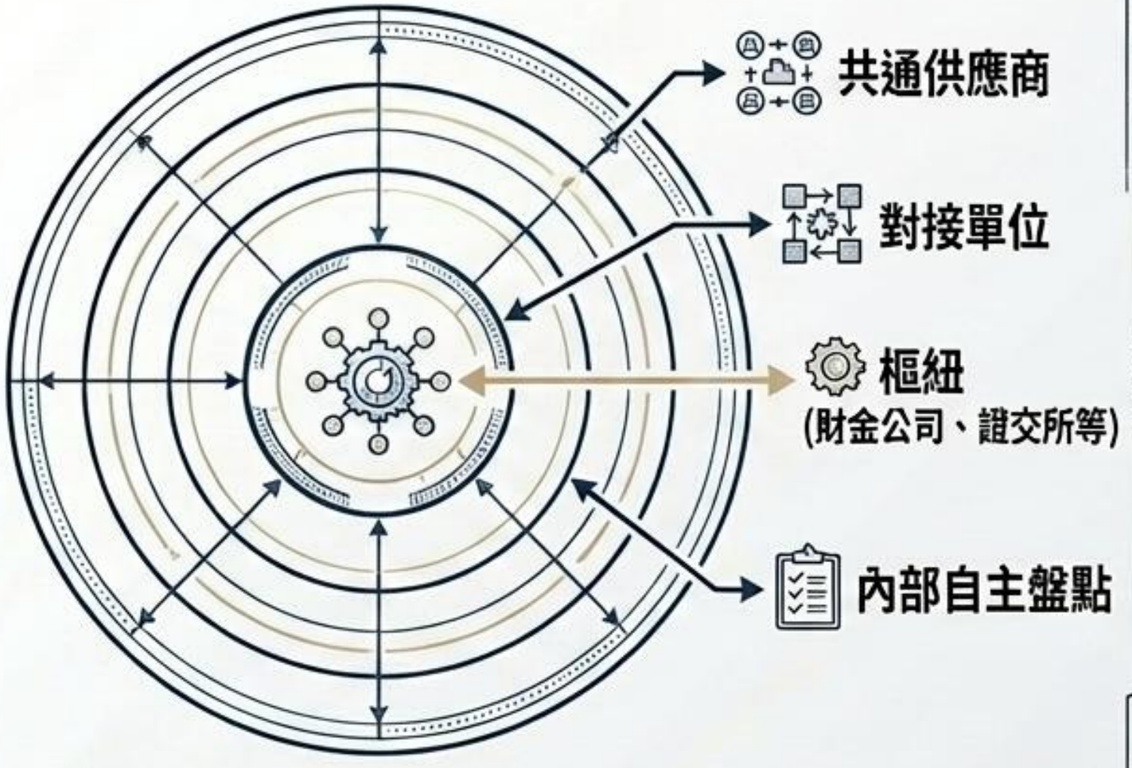


傳統加密體質 (密碼反模式)	敏捷加密體質 (Crypto-Agility)
特徵：加密演算法與憑證「硬編碼」寫死在程式碼中。手動管理憑證。	特徵：加密機制獨立為模組化設計。導入憑證自動化生命週期管理 (CLM)。
後果：每次更新都是浩大工程，極易引發系統崩潰與服務中斷。	後果：演算法迭代只需無痛抽換，集中處理，大幅降低升級風險。



聯防：以「四階生態系」協作，採風險導向排定優先序

策略 4：四階呈現生態協作 (Hub-and-Spoke)



由樞紐機構帶頭對齊步伐，制定共通標準，避免單一機構孤島式推進。

策略 5：風險導向優先序矩陣

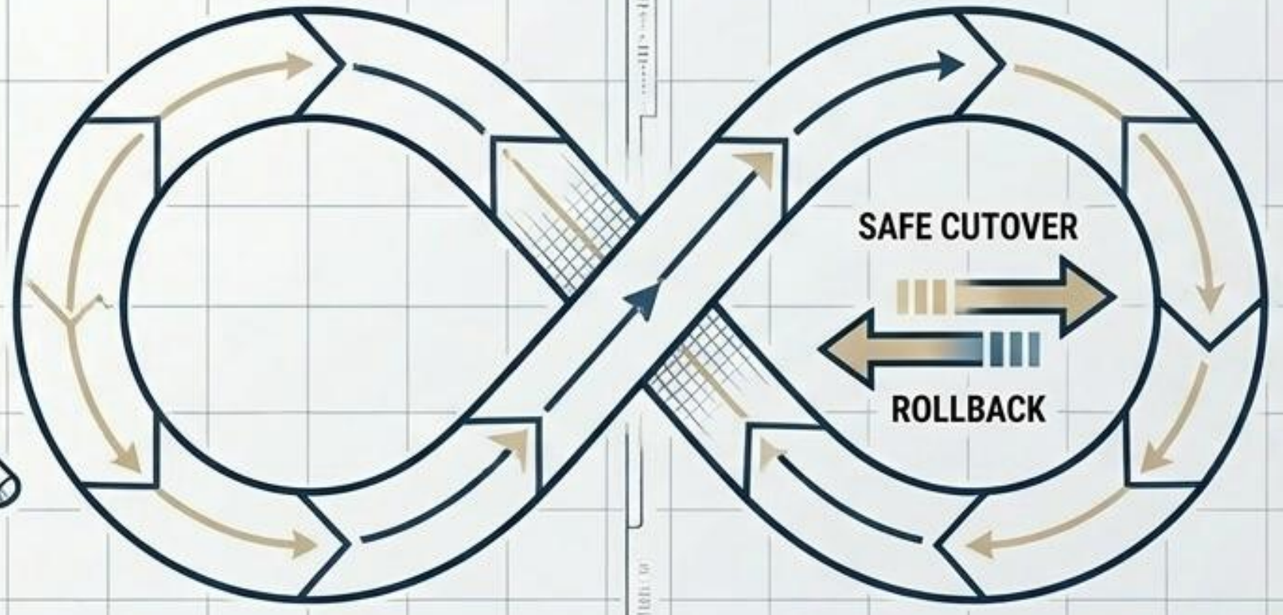
交叉評估資料敏感年限與外部依賴，精準配置遷移資源。

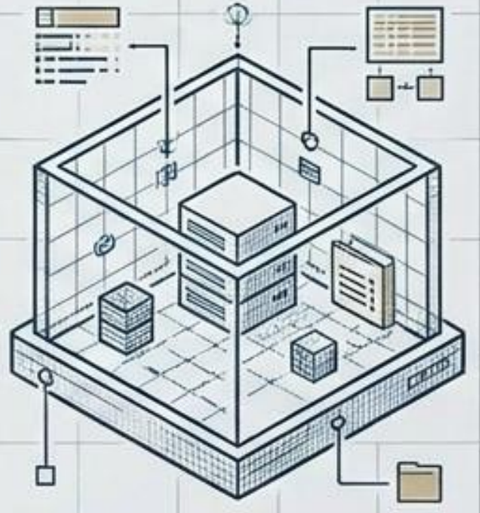
實戰：嚴控供應鏈，建立無痛測試與切換機制

策略 6：供應鏈管理

- 將 PQC 準備度納入採購與委外合約。
- 建立「卡關元件」提早處置機制，避免被單一舊設備拖累全局。

策略 7：測試與切換韌性





- 建立混合模式測試案例與灰度上線。
- 關鍵：把「回退機制 (Rollback)」視為必備能力，確保零服務中斷。

接軌國際，穩健推進：十年遷移路線圖

短期 (2026-2027) 打底期

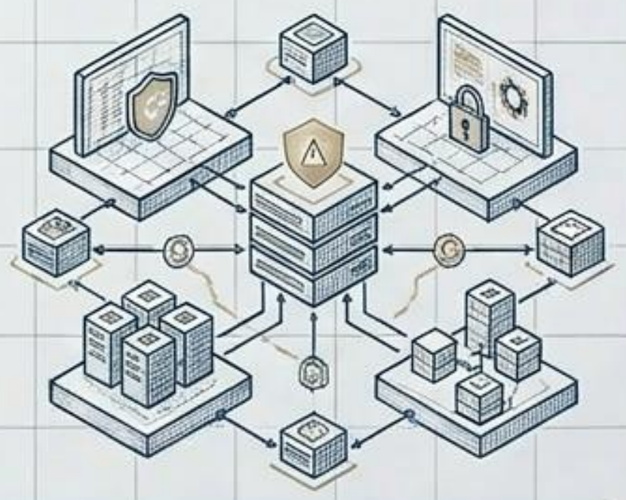
- 建立治理架構、盤點方法與 CBOM，優先清除密碼反模式，建立加密敏捷性基礎。

中期 (2027-2029) 試辦期

- 選定可控情境進行 PoC 試辦，評估效能衝擊。開始建立跨機構共同測試機制。

中長期 (至 2035) 全面擴大

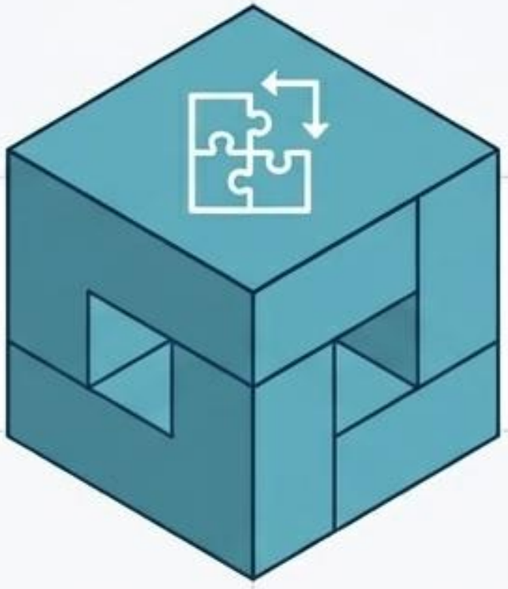
- 依風險排序，完成高風險及關鍵系統優先遷移，最終達成全體系接軌。



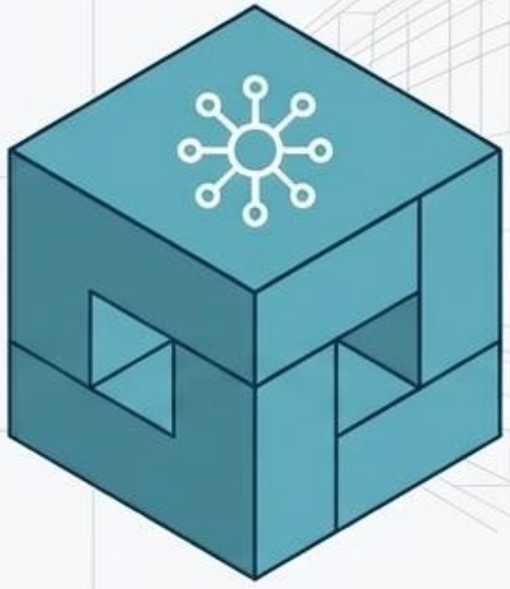
NIST 發布標準 → WEF 白皮書 → G7 呼籲 2035 遷移完成

指引三大設計理念 (Core Design Philosophy)

風險導向 (Risk-Oriented)：揚棄全面同步升級的非現實想像。採量子風險評分與外部依賴程度交叉評估，優先推動高敏感、長效期 (HNDL) 及關鍵驗證機制遷移。



加密敏捷性 (Crypto-Agile)：終極目標是將加密技術模組化。確保未來替換演算法僅需組態調整，而非大規模程式碼重構。



生態系驅動 (Ecosystem-Driven)：單一機構無法獨活。強調 Hub-and-Spoke 協作、跨境基礎設施同步、與嚴謹的供應鏈查核機制。

金融業的下一步：三條主線同步並進

1. 生態系對齊

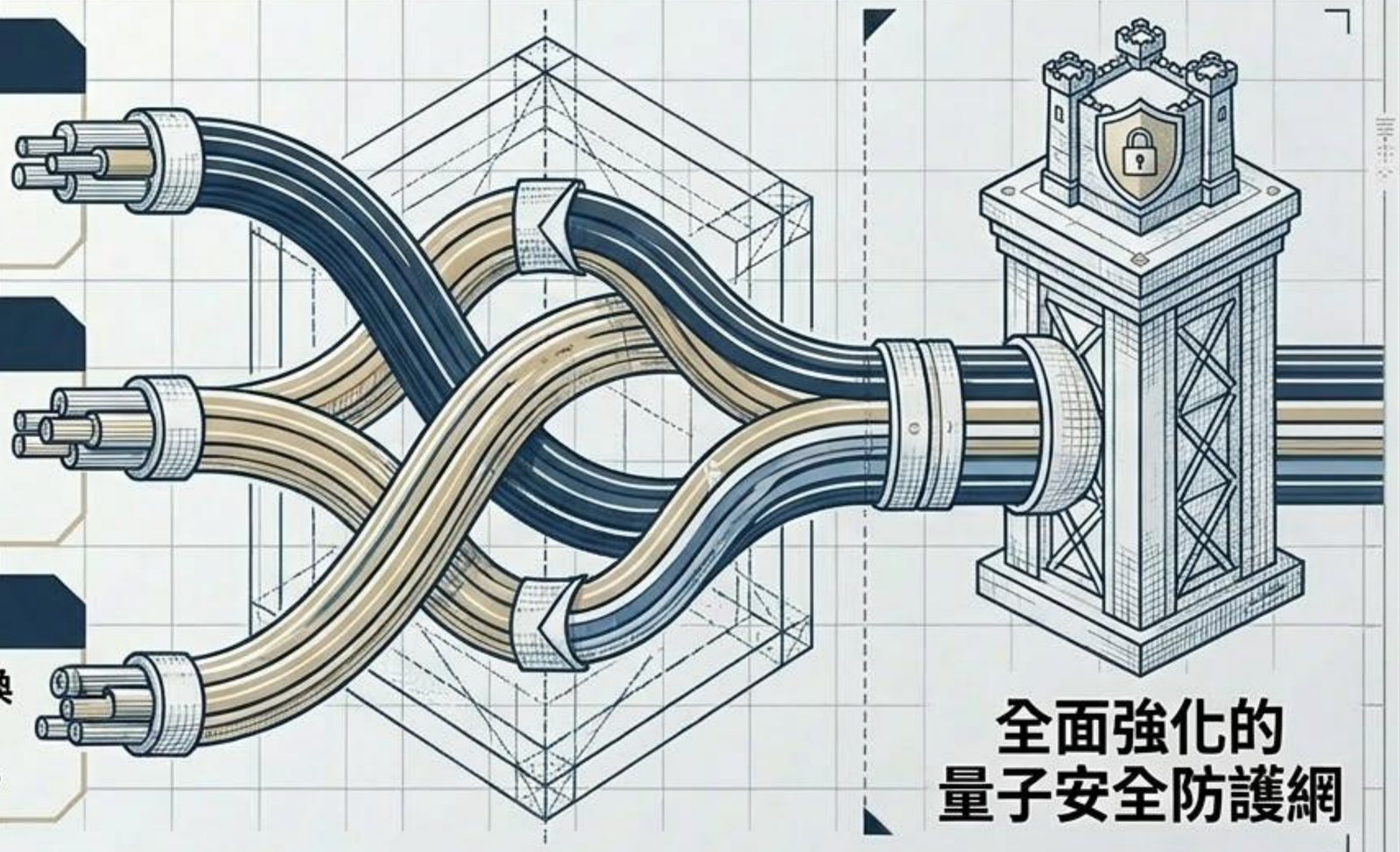
樞紐機構擬訂金融生態系遷移計畫，提出共同相容性矩陣。

2. 供應鏈治理

建置共通供應鏈調查與追蹤機制，彙整關鍵供應商準備度清冊。

3. 試辦與驗證

推動先導試辦，沉澱切換與回退 SOP，透過經驗分享形成全產業範本。



全面強化的量子安全防護網

化量子威脅為系統升級契機

金管會將引導金融業秉持**「循序漸進、風險導向」**原則，不追求盲目躁進，而是藉此機會**全面強化金融基礎設施**的加密體質。

終極目標：確保民眾交易安全、資料機密與金融體系的永續營運。

詳細內容請參閱《金融業後量子密碼遷移參考指引》