主題	**ISACA Journal 未雨綢繆的資安防護：邁向量子韌性的實務藍圖** **Future-Proofing Cybersecurity: A Practical Roadmap to Quantum Resilience**
類別	訊息新知 (Dec 2025)
內容	隨著量子運算技術快速成熟，現行依賴 RSA 與 ECC 的公鑰密碼體系將面臨被破解的風險，量子威脅已非遙遠的議題，而是需要立即啟動遷移計畫的結構性風險。量子時代最關鍵的挑戰在於「現在攔截、未來解密（HNDL）」攻擊模式，意指今日的加密資料在未來量子能力成熟時可能全面曝露。 本文提出量子密碼遷移的程序主要包含四大步驟： 1. 加密資產盤點：完整繪製組織所有密碼技術、演算法與依賴關係，作為治理與風險評估基礎。 2. 資料分級與長期保護策略：辨識需保存 5～20 年以上的敏感資料並優先導入 PQC 或混合加密。 3. 建立 PQC 跨部門治理架構：包含法律、內控、供應鏈與 IT，確保遷移符合監管、稽核與市場需求。 4. 試行混合密碼（Hybrid Crypto）：以 Kyber、Dilithium 等 NIST 標準為基礎，逐步測試 TLS、VPN、KMS、電子簽章等場景的相容性、效能與備援方案。 量子遷移是企業韌性、法遵與數位信任的核心工程，更是未來競爭力的重要指標。建議讀者深入閱讀全文，以掌握企業從架構、治理到技術層面的完整量子韌性藍圖，及早布局，避免未來量子運算到來時陷入被動。 全文詳閱: https://www.isaca.org/resources/isaca-journal/issues/2025/volume-6/future-proofing-cybersecurity