台灣資安法規對應一覽

資通安全管理法 × 個資法 × ISO 27001:2022 × 金融業 PQC 遷移指引(2026/6/18) 對應條目

AegisCode 內建中文化法規對應,讓資安修補與加密盤點的每一步都能直接連到 法規責任,適合金融、政府與高法遵組織的稽核情境。下表為四項法規／指引最常被 稽核的條目並列對照,可貼進稽核準備文件作為快速索引。

四項法規 / 指引並列對照

資通安全管理法

資安事件、弱點掃描、改善追蹤

- 資安事件分級與通報窗口
- 弱點掃描與修補時效要求
- 資安治理組織與責任歸屬
- 稽核紀錄保存與審查週期

個人資料保護法

個資處理、技術保護、外洩通報

- 個資處理目的與最小化原則
- 技術與組織保護措施
- 外洩通報與當事人告知
- 委外處理與第三方治理

ISO 27001:2022

資訊安全管理系統 (ISMS)

- A.5 組織控制 — 治理結構與責任
- A.6 人員控制 — 安全意識訓練
- A.8 技術控制 — 弱點管理與密碼學
- A.5.23 雲端服務與第三方風險

金融業後量子密碼遷移參考指引

金管會 2026/6/18 發布 • 準備期 2026–2027

- 密碼技術清冊 CBOM 盤點(AI 自動化輔助)
- 加密敏捷性與密碼反模式清除
- 風險導向遷移優先序評估
- 供應鏈 SBOM 與可離線驗證證據鏈

如何使用本表

稽核準備:將每項弱點對應到右側 ISO 27001 控制條目,可直接放進 ISMS 文件附錄。

管理層彙報:把技術修補映射到資安法 / 個資法的責任條目,讓主管 理解修補的法規意義。

供應商治理:第三方風險評估可參考此表,確認供應商在三條法規面的 覆蓋程度。

完整客製化對應

本表為公開速查版本。針對貴單位實際 Domain 範圍、業務類型(金融、 政府、醫療等)與既有 ISMS 文件的完整客製化合規對應,由 Surface 顧問服務交付。請聯絡 **sales@aegiscode.com**。