金融監督管理委員會
Financial Supervisory Commission R.O.C. (Taiwan)

金融資安韌性發展藍圖

共創安全、信賴、永續創新的金融未來

2025年12月30日

從合規到韌性：一個成果導向的新時代

過去：金融資安行動方案

· 合規導向
· 被動防禦

現在：金融資安韌性發展藍圖

· 成果導向
· 主動韌性
· 快速恢復

我們的目標：建構一個「可預測、可防禦、可復原」的金融生態系。

我們的藍圖：四大支柱建構金融韌性

第一軸：
目標治理

成果導向，強化決策鏈與問責鏈

第二軸：
全域防護

從安全設計到技術韌性的全鏈防護

第三軸：
生態聯防

建構跨域共防與智慧情資生態

第四軸：
堅實韌性

確保關鍵服務持續與快速恢復

第一軸：目標治理 - 從董事會開始，驅動成果

強化經營階層資安治理職能與問責機制，鼓勵資安法規調適

提升董事會資安監督能量，將資安納入公司治理核心。
建立資安長「責任、權限、資源」三位一體的治理架構，並推動法規調適與前瞻布局。

加強資安人才培育與交流，從共通基準邁向策略目標

藉由舉辦跨機構「主題式」論壇與工作坊，鼓勵分享前瞻規劃與典範實務，深化知識共享，引導從合規導向轉向「可量測、可成長、可差異化」的目標導向。

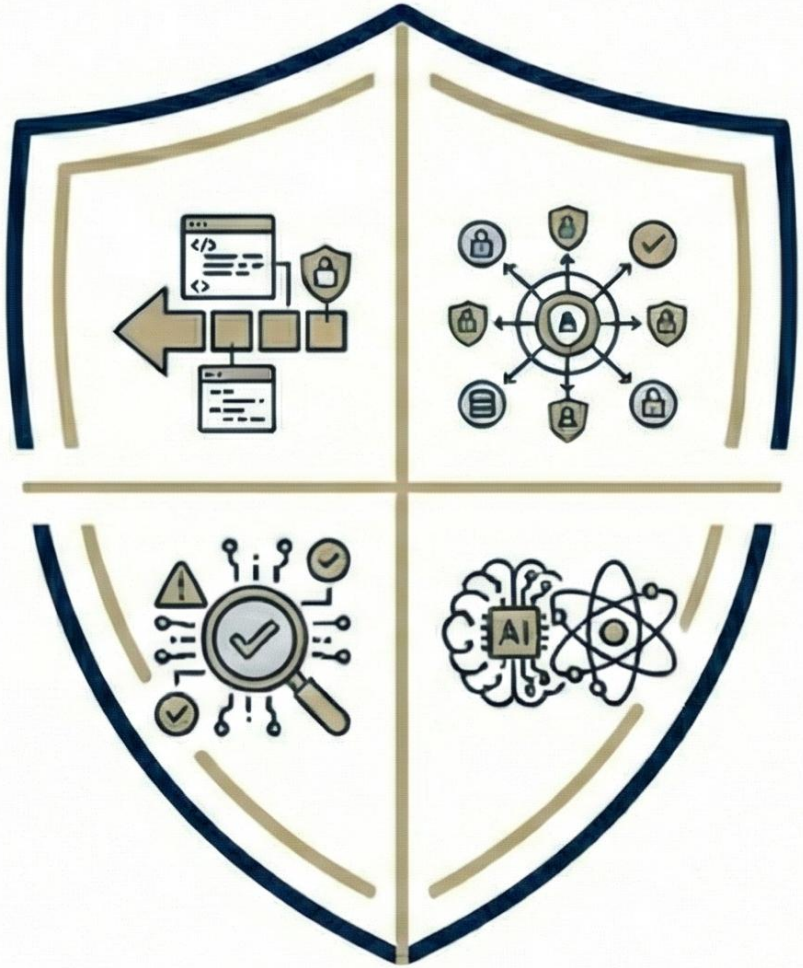
第二軸：全域防護 - 將安全內建，而非外加

資安左移，安全納入設計 (Secure By Design)

鼓勵導入安全軟體開發流程(SSDF)，於開發初期嵌入安全控制。
建立軟體物料清單(SBOM)追蹤機制，提升供應鏈透明度。
研訂API安全基準，強化安全防護。

推動零信任架構 (ZTA)

擇定高風險場域優先導入，漸進提升成熟度並納入基礎規範。



強化資安監控及防護有效性

擴增資安組態及監控基準，確保雲地資安水準一致性，並鼓勵透過演練方式評估有效性。

前瞻部署，因應新興科技的挑戰

研訂AI系統安全防護指引，以應對AI特有攻擊類型，並研訂金融業PQC遷移參考指引，布局後量子密碼遷移。

第三軸：生態聯防 - 單點防禦已不足夠

強化供應鏈資安，健全金融資安生態系

依供應商風險進行分級，研訂資安責任之委外契約參考條款，並鼓勵與關鍵供應商進行資安情資分享、強化控管與聯合演練。

加強資安情資分析與協同防禦

強化F-ISAC情資關聯分析，提升聯防SOC協同運作效能，並建立金融資安漏洞通報管道，及透過定期舉辦跨國會議深化國際合作。

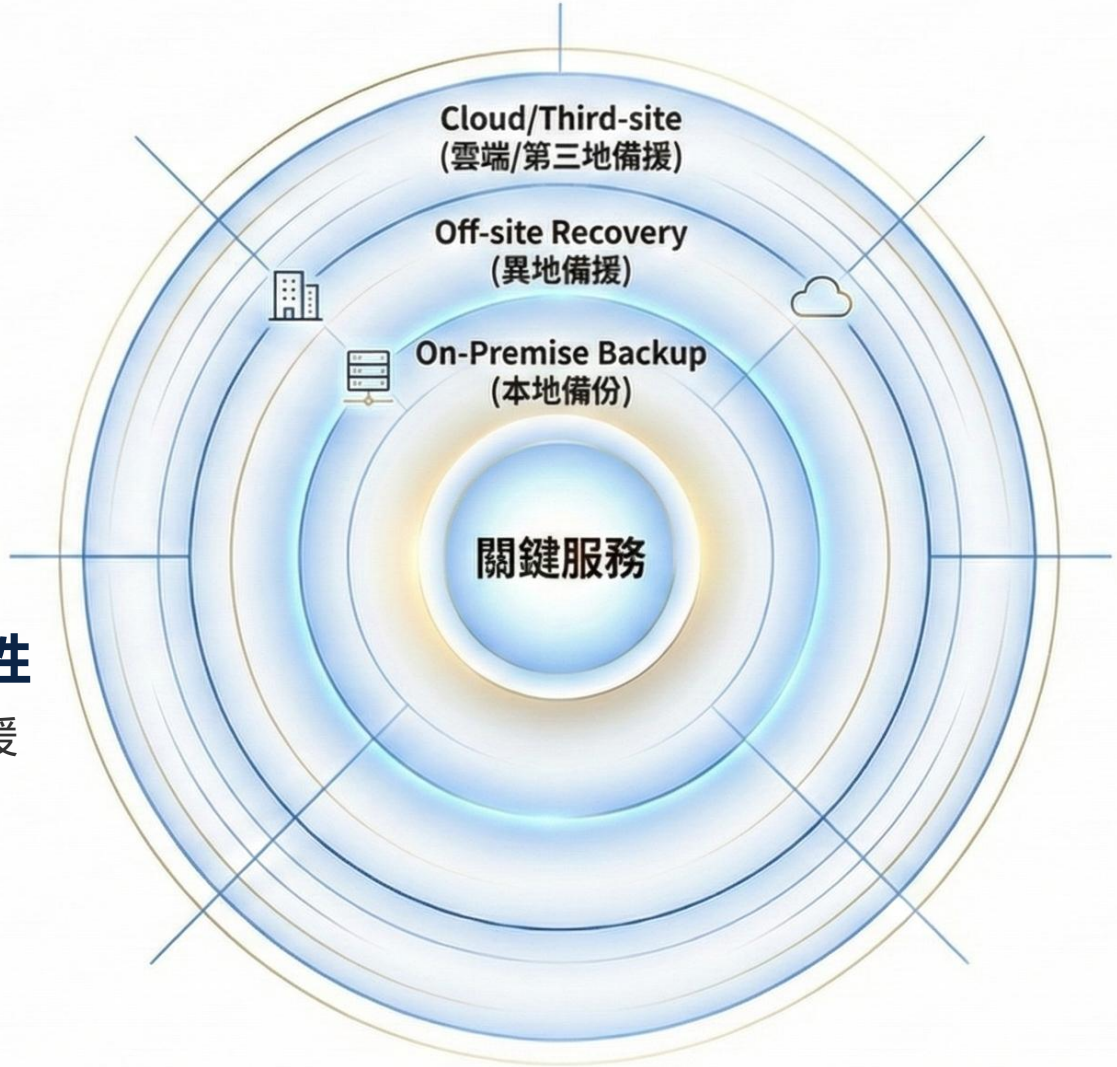
第四軸：堅實韌性 - 假設衝擊發生，並做好準備

辦理資安攻防演訓，強化應處能量

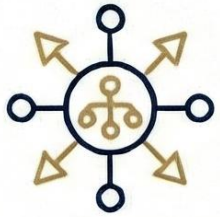
持續辦理DDoS、網路攻防演練等，並擴大演練情境(如勒索軟體、供應鏈攻擊)，驗證跨體系聯防之通報、協調及支援機制。

強化多層次備援機制，確保服務可用性

因應複合災難情境，規劃關鍵服務的多層次備援架構，並評估及建立關鍵金融服務生態系(含供應鏈夥伴)的備援協作機制。



共同實踐：我們的推動與管考原則

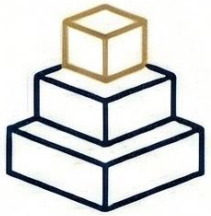


資源共享

發揮聯防功能，分享情資與應變資源。

公私協力

透過公部門、周邊單位與公會共同推動。



差異化管理

依機構規模與業務風險，分級規範。

激勵誘因

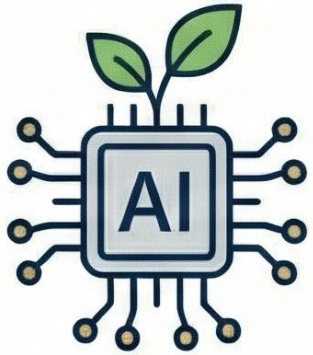
連結監理機制，引導機構主動強化資安。

國際合作

與國際金融資安機構交流，強化跨境預警。

* 自115年度起，每季檢討執行情形，滾動修訂推動策略。

預期效益：提升韌性，創造價值



政策面 (Policy)

堅實支撐金融創新
與AI應用安全落地。

管理面 (Management)

降低供應鏈衝擊，保障金融
穩定性。

技術面 (Technical)

增強攻擊預警能力，
並降低重大事故平均
恢復時間 (MTTR)。

國際面 (International)

提升台灣金融資安的國際
信任評等，有利跨國合作。

我們的願景

打造一個安全、可信、可持續創新的台灣金融生態系