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

近年國際資安監理趨勢

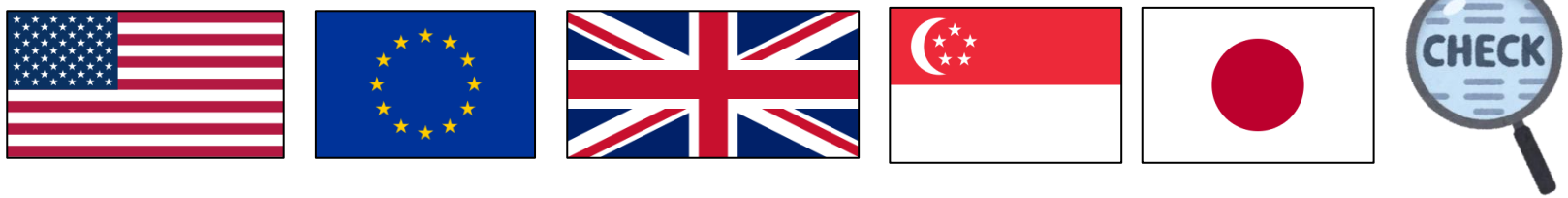
強化**高層責任**及提升**資安成熟度**

推動**資安左移**及**軟體物料管理**

推動**AI資安**治理與防護

規劃**後量子密碼遷移**準備

強化**供應商管理**與**營運韌性**



近年我國資安策略

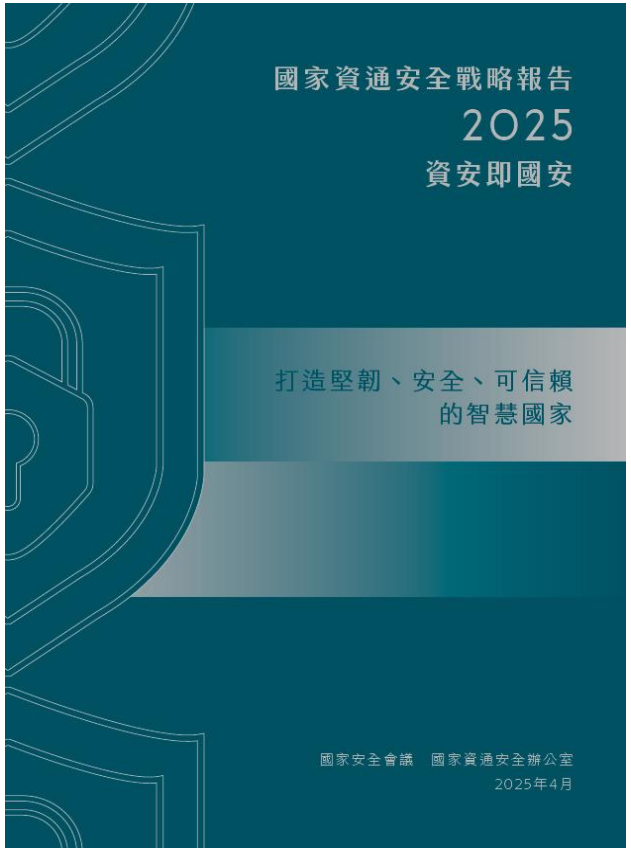
國家資通安全戰略 2025：資安即國安

- 零信任架構(ZTA)為近年資安治理中不可或缺的一環
- 發展後量子密碼之資安防護架構與管理
- 確保 AI 技術本身的安全性與可信任性
- 確保供應鏈的可視性與安全性
- 推動關鍵系統核心功能備援轉型，加強異地備援與容錯設計
- 推動第三方資安實兵演練及桌上兵推

在能源、通訊、交通、金融、醫療等領域的關鍵基礎設施分別**制定並執行「資通安全行動方案」**

國家資通安全發展方案(114年至117年)

- 1-2-2 培育高階型資安人才，強化實戰人才知能
- 2-2-1 強化關鍵基礎設施資安威脅監控
- 2-2-2 加強關鍵基礎設施情資分享運作，提升整體數位防護
- 2-2-3 關鍵基礎設施資安實地演練與稽核，提升資安韌性
- 2-3-1 落實各領域資安防護基準，強化關鍵基礎設施資安防護



金融資安政策進程

2020.08

- 金融資安行動方案1.0

2022.12

- 金融資安行動方案 2.0

2024.07

- 金融業導入零信任架構參考指引

2025.12

金融資安韌性發展藍圖

4 大構面
10 重點工作

四軸韌性治理架構

A.目標治理

以成果導向強化決策鏈與問責鏈

強化高層問責、法規調適與人才韌性。

B.全域防護

從安全設計到技術韌性的全域防護

推動「資安左移」與「零信任架構」，提升資安監控效能，前瞻部署 AI、PQC 等新興科技防護。

C.生態聯防

建構跨域共防與智慧情資生態

強化供應鏈資安管理與資安情資分析合作，深化國際聯防。

D.堅實韌性

確保關鍵服務持續與快速恢復

以演訓、備援與風險分層確保關鍵金融服務不中斷。

一、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

現行措施

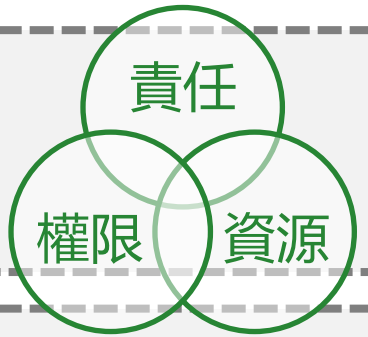
- 鼓勵金融機構遴聘具資安背景之董事或設置資安諮詢小組
- 推動一定規模或電子交易達一定比例之金融機構設置副總經理層級以上之資安長
- 開辦董監事資安教育訓練專設課程
- 辦理資安長聯繫會議
- 完備資安規範

延續並強化

ESG

提升董事會資安監督能量，資安納入公司治理核心

強化金融資安長問責及賦權機制



增修訂資安自律規範，鼓勵資安法規調適

– 採風險基礎方法(RBA)，授權一定理由或特定範圍可採取相當控制措施

二、加強資安人才培育與交流，從共通基準邁向典範實務

延續並強化

滾動修訂金融資安人才職能地圖，鼓勵**優化資安職能配置**及取得專業證照

鼓勵分享**前瞻**規劃暨**典範**實務

- 定期舉辦跨機構「主題式」論壇、工作坊或案例研討等，聚集相同領域之跨機構人才共同研討 NEW

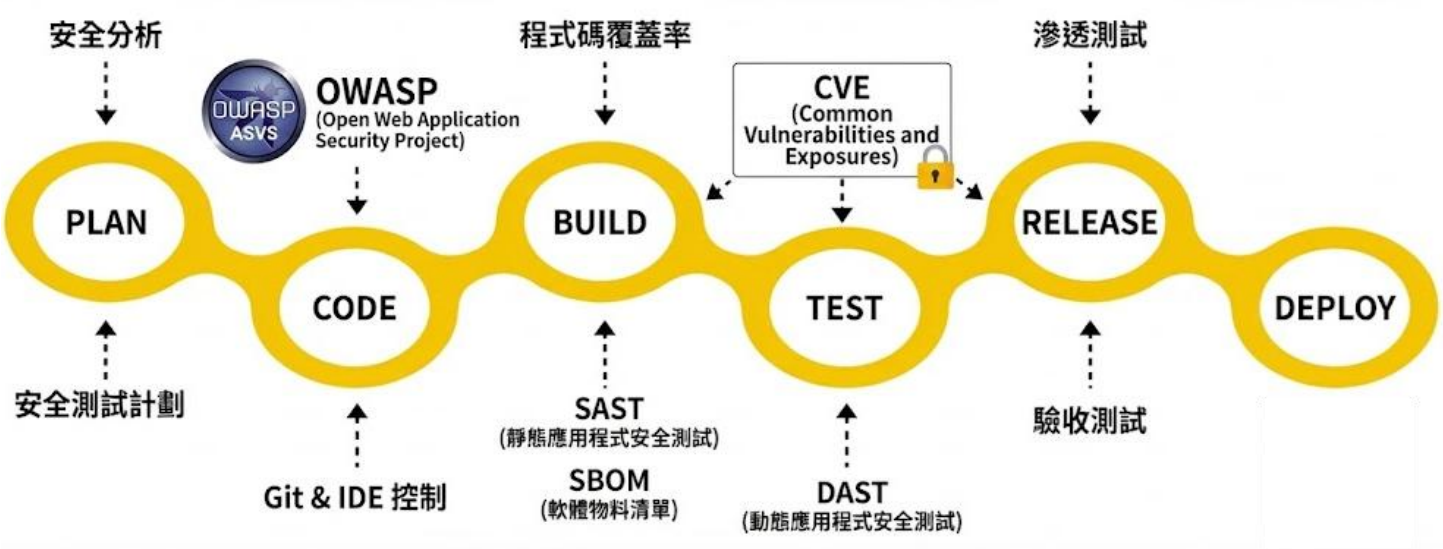
目標導向，銜接**防護基準**與**典範**實務

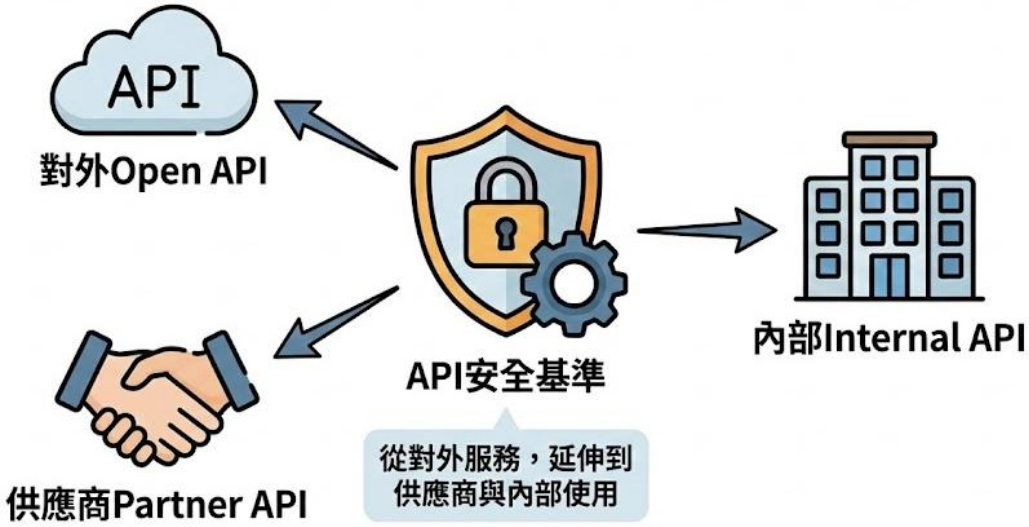
- 調修建立成熟度分級評估指標(可量測、可成長、可差異化)

三、資安左移，安全納入設計(Secure By Design)

新增措施 NEW

鼓勵導入**軟體安全**開發、測試及部署流程(CI/CD)	建立軟體**供應鏈透明化**(SBOM)與**弱點追蹤**機制	研訂**API安全基準**，建立API安全管理機制

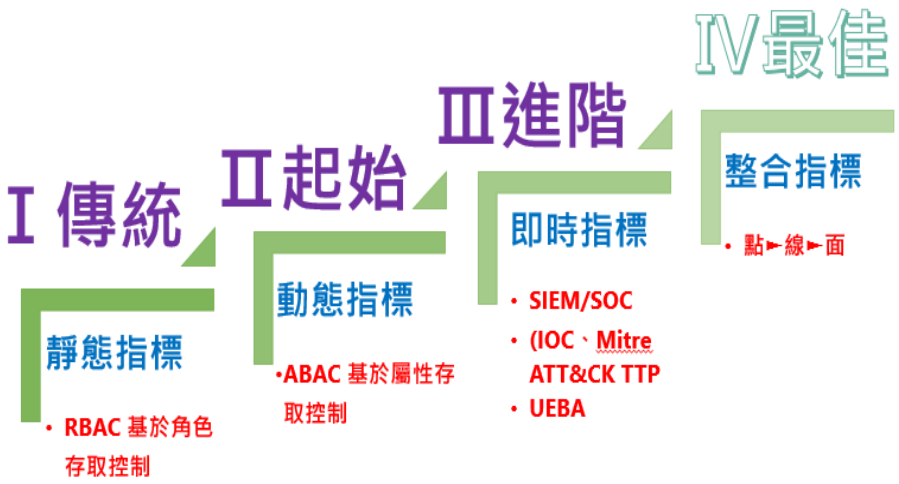




四、推動零信任架構(ZTA)，提升資安防護基準

延續並擴大

推動導入**高風險場域**， 漸進提升成熟度	鼓勵導入實務分享與交流	建立導入實務共識， 漸進納入**基礎規範** NEW



五、強化資安監控及防護有效性

延續並擴大

增修訂資安組態及監控作業基準

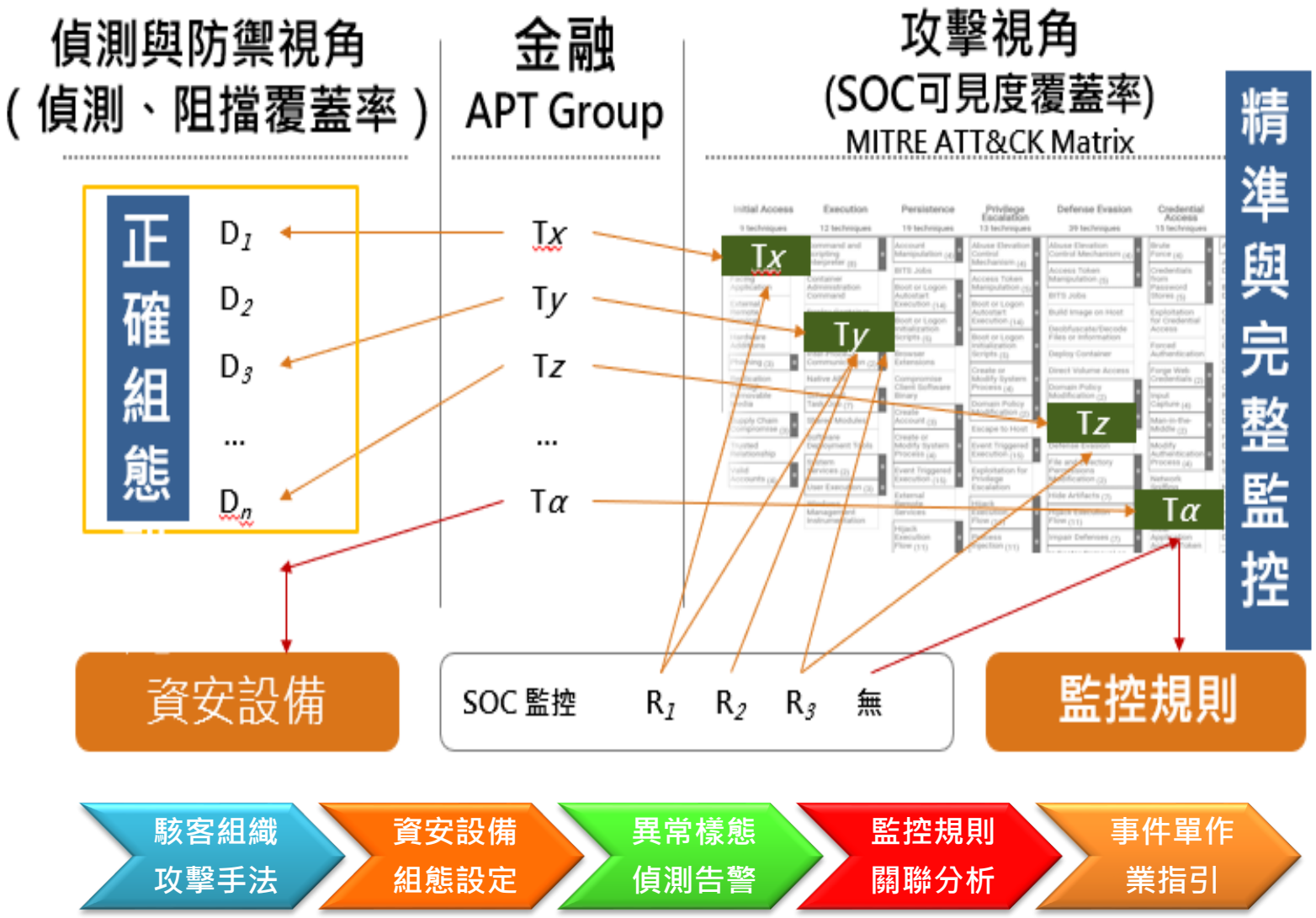
– 持續研析駭客組織攻擊手法

雲地資安接軌，確保資安水準

– 持續擴增雲端資安監控及組態基準範疇(如容器服務、PaaS等)

鼓勵資安監控及防護有效性評估

– 如DDoS攻防演練、紅藍隊演練、入侵與攻擊模擬等



六、前瞻部署，因應新興科技的挑戰

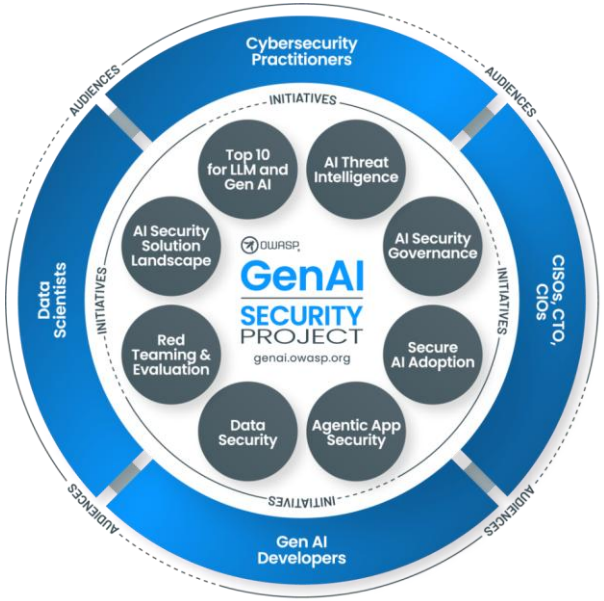
新增措施 NEW

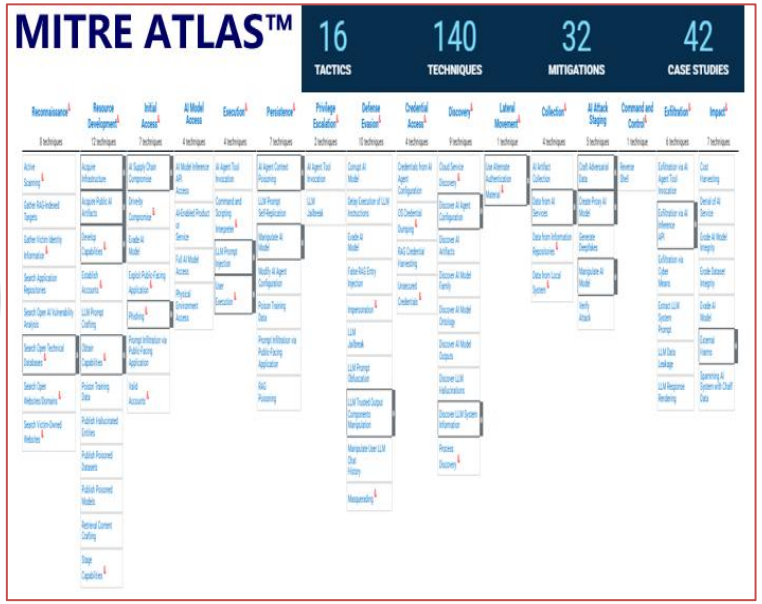
人工智慧(AI)強化效率，資安守護信任

– 研訂金融業AI系統安全防護及檢測參考指引

盤查加密態勢，布局後量子密碼(PQC)遷移

– 研訂金融業PQC遷移參考指引，適時推動遷移





七、強化供應鏈資安，健全金融資安生態系

現行措施

- 增修訂資安自律規範或作業指引，納入核心資訊系統供應商及第三方服務提供者之風險評估及查核等管理機制

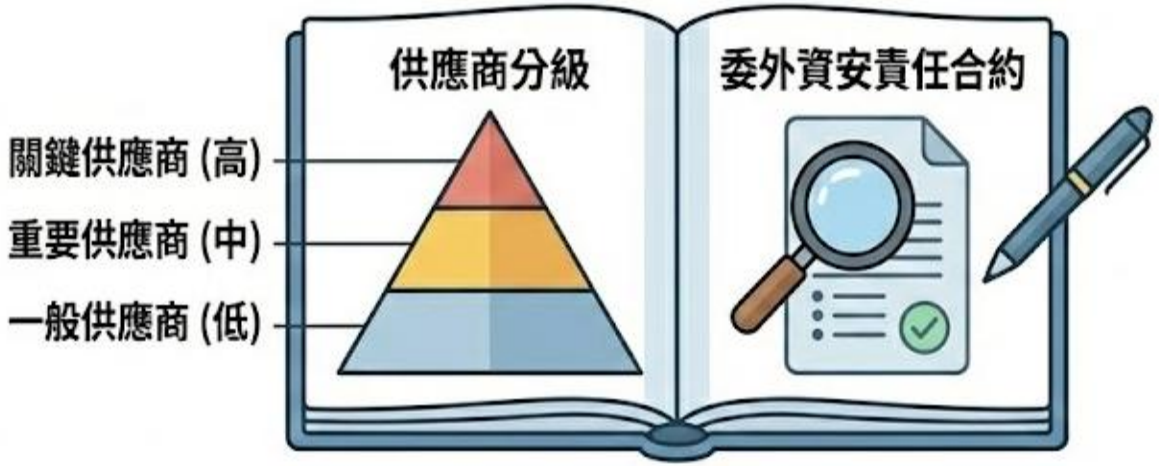
增修措施

研訂供應商分級及委外資安責任參考範本 NEW

– 依產業特性、供應商接觸資通系統之類別及資料敏感度等面向進行分級

鼓勵與關鍵供應商資安情資分享與協作 NEW

– 鼓勵與供應商分享威脅、保護資訊、強化控管，聯合資安演練等

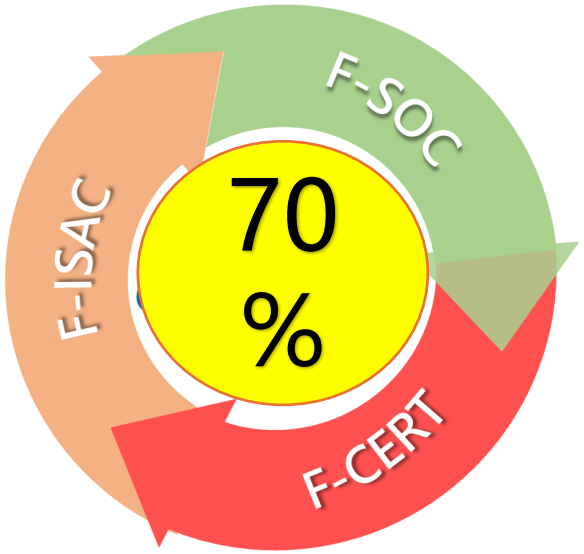


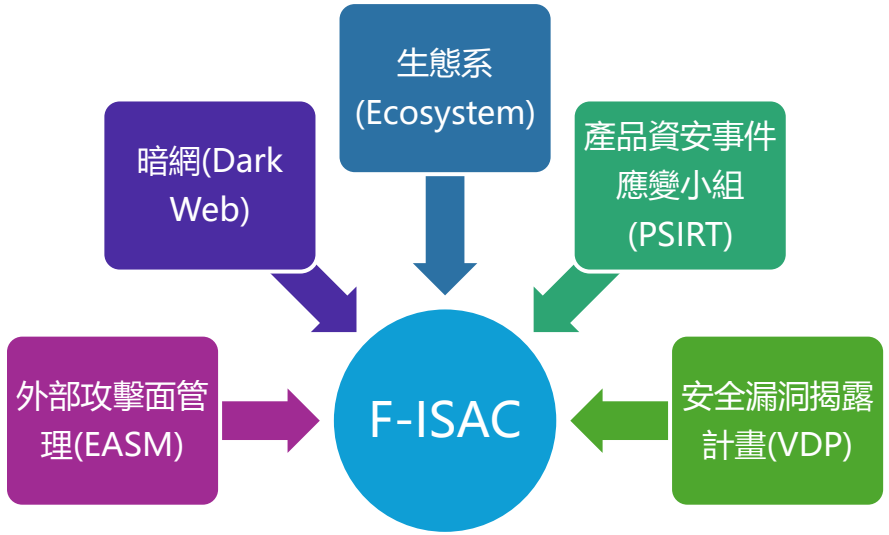
八、加強資安情資分析與協同防禦

金融資安資訊分享與分析中心
Financial Information Sharing and Analysis Center

延續並強化

強化資安情資關聯分析及情資分享動能	建立金融資安漏洞通報與回應管道 NEW	辦理提升金融機構SOC與聯防SOC協同運作效能	加強金融資安國際合作 – 定期舉辦跨國線上交流會議、提供我國報告等





FS-ISAC
FIRST
European FI-ISAC
APCERT
Asia Pacific Computer Emergency Response Team

九、辦理資安攻防演訓，強化資安事件應處能量

持續措施

辦理金融機構DDoS、網路攻防或其他資安演練

開設金融資安演訓專班

(體驗營/暖身場)

– 擴大攻擊防禦認知與技能培訓

辦理重大資安事件應變情境演練

– 擴大演練情境之廣度與深度

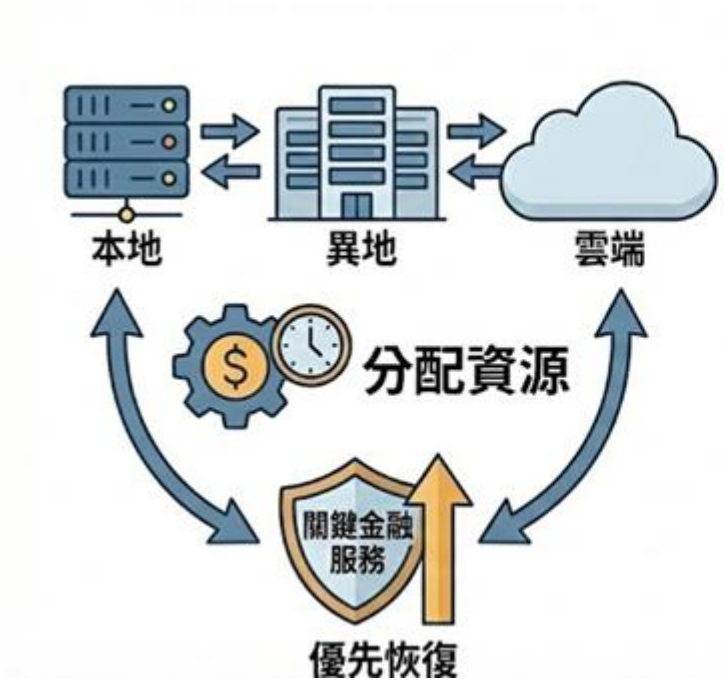
十、強化多層次備援機制，確保關鍵金融服務可用性

延續並強化

鼓勵導入國際**營運持續**管理標準及取得相關驗證

因應複合災難情境，建立**關鍵服務多層次備援**機制

評估建立**關鍵金融服務**生態系營運持續量能、**備援協作**機制 NEW



推動與管考

公私協力　**差異化管理**　**資源共享**　**激勵誘因**　**國際合作**

由金管會召集各業務局及相關周邊單位、同業公會共同訂定各項目之推動指標與執行進程。

自115年度起，每季檢討執行情形，滾動修訂推動策略、執行措施及各項推動指標。

預期成效

政策面

提升資安治理成熟度與韌性
堅實支撐金融服務創新與AI應用安全落地

管理面

提升跨業防護與復原能力
降低供應商資安事件對於金融業的衝擊

技術面

增強金融機構攻擊預警能力(TTP Intelligence)
降低重大事故平均恢復時間(MTTR)

國際面

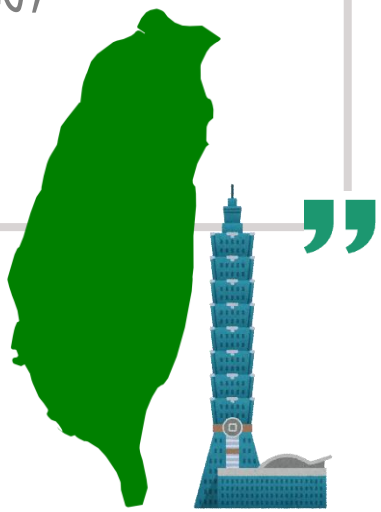
提升台灣金融資安的國際信任評等
有利金融機構跨國合作與外資布局

未來展望

從「防止發生」的心態，轉向「快速反應、快速恢復」的韌性

期於金融業建立一套：**可執行、可量測、可提升、可國際接軌**的韌性治理模式，

最終目標是打造：**安全、可信、可持續創新**的台灣金融生態系。



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