金融監督管理委員會
Financial Supervisory Commission

「金融資安行動方案」2.0

金融監督管理委員會

111年12月27日

簡報大綱

前言

01

02

近期金融資安威脅與挑戰

金融資安監理趨勢

03

04

金融資安精進措施

壹、前言

金融資安行動方案1.0 (109.8-)

願景：追求安全便利不中斷的金融服務

目標：
- 建立業者重視資安的組織文化
- 提升業者資安治理能力與水準
- 確保系統持續營運與資料安全

推動策略	具體措施
強化資安監理	1. 型塑金融機構重視資安的組織文化 2. 完備資安規範 3. 強化資安監理職能 4. 加強金融資安檢查
深化資安治理	1. 加強資安管理 2. 強化資安監控 3. 加強資安人才培育
精實金融韌性	1. 增進營運持續管理量能 2. 加強資安演練 3. 建構資料保全避風港
發揮資安聯防	1. 資安情資分享與合作 2. 建立金融資安事件應變體系 3. 建立金融資安事件監控體系

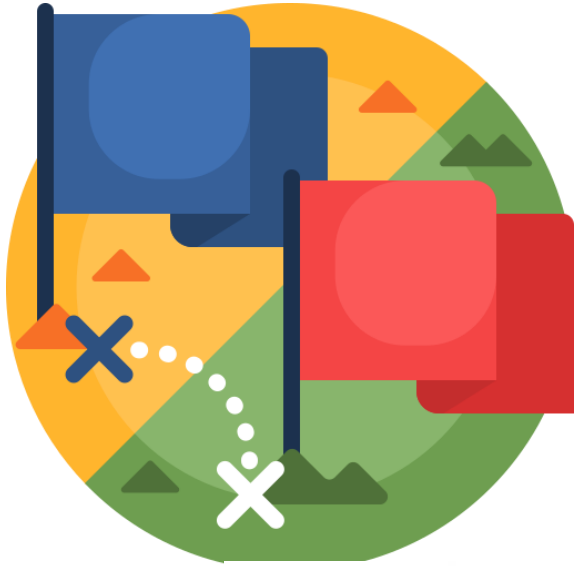
至111年之主要KPI均已達標(86%)

- 設置資安長
- 導入國際資安標準
- 辦理資安攻防演練與競賽
- 建立金融資安事件應變體系
- ....

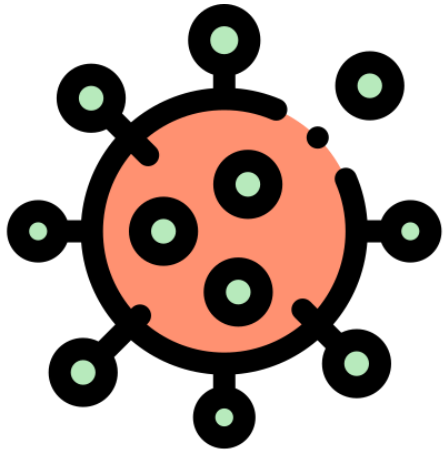
持續辦理中佔比14%
(原執行期程3~4年)

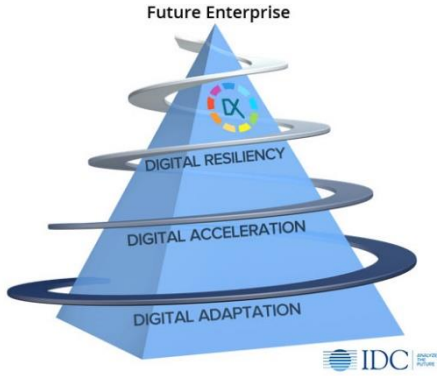
貳、近期金融資安威脅與挑戰

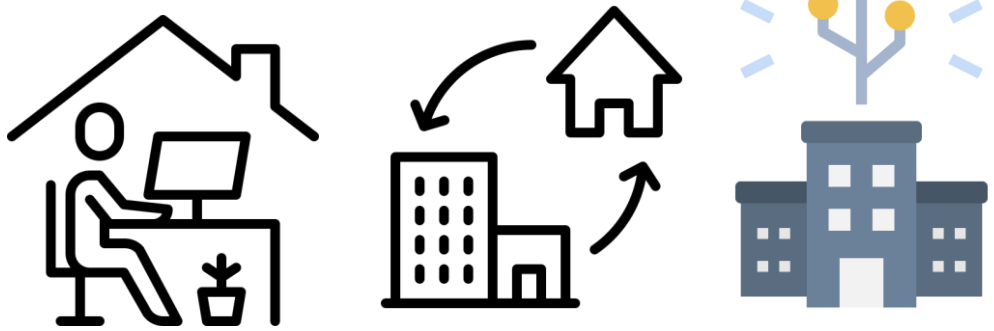
進階持續性威脅(APT)



新冠疫情





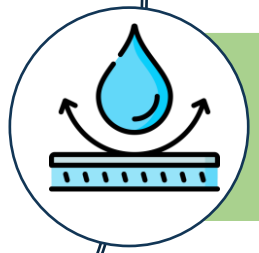


網路攻防　　數位韌性　　居家、異地辦公　　數位轉型

參、金融資安監理趨勢

重視經營階層資安職責、要求獨立資安職能

建立共通資安管理基準及自主評估機制



建構並實證作業風險抵禦能力

持續提升資安防護及其有效性評估

肆、金融資安精進措施 – 從 1.0 邁向 2.0

1.0

擴大適用

- 原KPI達標
- 已規劃導入中

落實深化

- 共通基準
- 精進有效

2.0

鼓勵前瞻

- 資安情勢
- 超前部署

金融資安行動方案2.0 - 精進重點

項次	推動措施	擴大適用	落實深化	鼓勵前瞻
1	擴大資安長設置，定期召開**資安長聯繫會議**	V	V	◎
2	因應數位轉型及及網路服務開放，增修訂自律規範		V	
3	深化**核心資料保全**及營運持續演練		V	V
4	擴大導入國際資安管理標準及建置資安監控機制	V	V	
5	鼓勵資安監控與防護之**有效性評估**		V	V
6	鼓勵**零信任網路部署**，強化連線驗證與授權管控			V
7	鼓勵配置多元專長資安人才，擴大**攻防演訓**量能		V	V
8	提升資安情資分享動能，增進資安聯防運作效能		V	
9	辦理資安攻防演練，規劃**重大資安事件支援演訓**		V	

推動藍圖

- 客戶
  - 2.1 eKYC與業務風險對照
- 第三方服務商
  - 2.2 第三方風險評估與管理
- 居家/異地辦公
  - 2.3 因應新型態資安攻擊

政策面

1.擴大資安長設置，定期召開資安長聯繫會議

管理面

4.1 擴大推動導入國際資安管理標準

7.鼓勵配置多元專長資安人才，擴大演訓量能

技術面

事前-資安部署 | 事中-資安監控 | 事後-營運持續

深化	6. 鼓勵零信任網路部署	4.2 擴大推動資安監控機制	3.1 金融核心資料保全
有效	5. 鼓勵資安監控與防護之有效性評估		3.2 對外服務營運持續實演練
聯防	8.1 提升資安情資分享動能	8.2 增進資安聯防運作效能	9 攻防演練及重大事件支援演訓

一、擴大資安長設置、定期辦理資安長聯繫會議

- 一定規模
- 電子交易達一定比例

資安長職責

- 定期向董事會與經營階層報告並受其問責
- 政策推動及資源調度
- 對資安情勢掌握
- 將資安風險納入經營決策考量，帶動重視資安組織文化

資安長聯繫會議

- 資安戰略研議推動
- 資安經驗分享與交流

重大資安事件因應

- 資安制度優化精進
- 資安事件指揮調度

二、因應數位轉型及及網路服務開放，增修訂自律規範

客戶

- 2.1 eKYC與業務風險對照
  - 自然人憑證
  - 金融憑證、金融卡
  - 雙因子認證
  - 視訊
  - 金融FidO、TW FidO
  - Mobile ID
  - …

第三方服務商

- 2.2 第三方風險評估與管理
  - 核心資訊系統**供應商**或跨機構資訊服務**合作廠商**之風險評估及查核
  - 金融服務韌性
  - 網路邊際防護
  - …

居家/異地辦公

- 2.3 因應新型態資安攻擊
  - DeepFake、混合式網路釣魚
  - 供應鏈攻擊、VPN
  - IOT、第三方元件
  - 勒索軟體
  - 資安預警情資…

三、深化核心資料保全及營運持續演練

沒有100%的資訊安全 - 建立平時及終極防護能量

營運持續管理

- **訂定核心系統備援演練指引**
- 識別核心業務、支持核心業務持續運作必要之系統
- 訂定最大可容忍中斷時間
- 演練、壓力測試

備援環境實作驗證

- 復原能力實證
  - 本地備援
  - 異地備援
- **實際對外服務業務運作驗證**

核心資料保全

- **檔案、資料庫 加密與分持儲存**
- **第三地或雲端備份**
- 資料可移性
- 資料復原性
- 關鍵服務持續性

四、擴大導入國際資安管理標準及建置資安監控機制

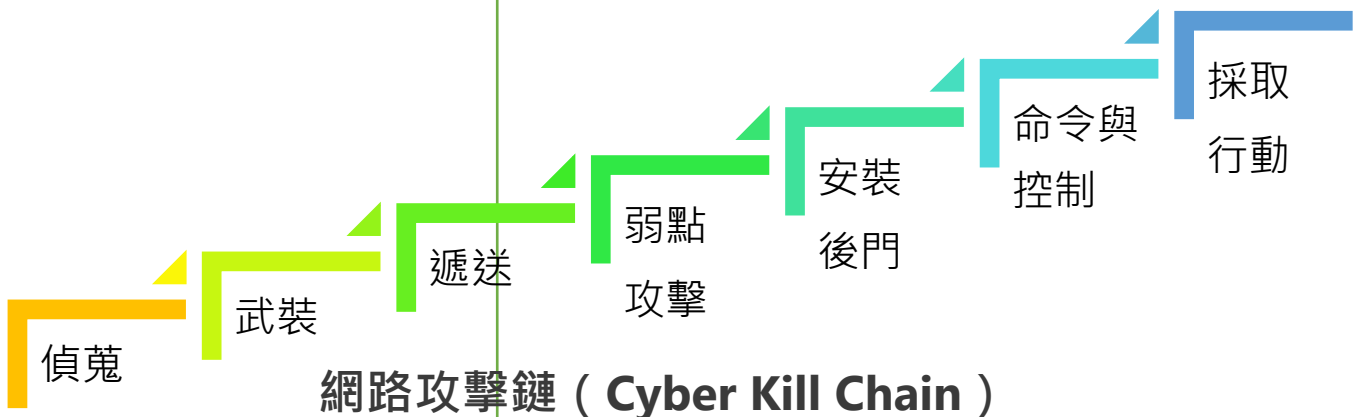
- 一定規模
- 電子交易達一定比例

國際資安管理標準(ISO27001)

- 為健全金融機構資訊安全管理制度，推動導入國際資安管理標準
- 透過第三方獨立機構檢視管理制度之有效性

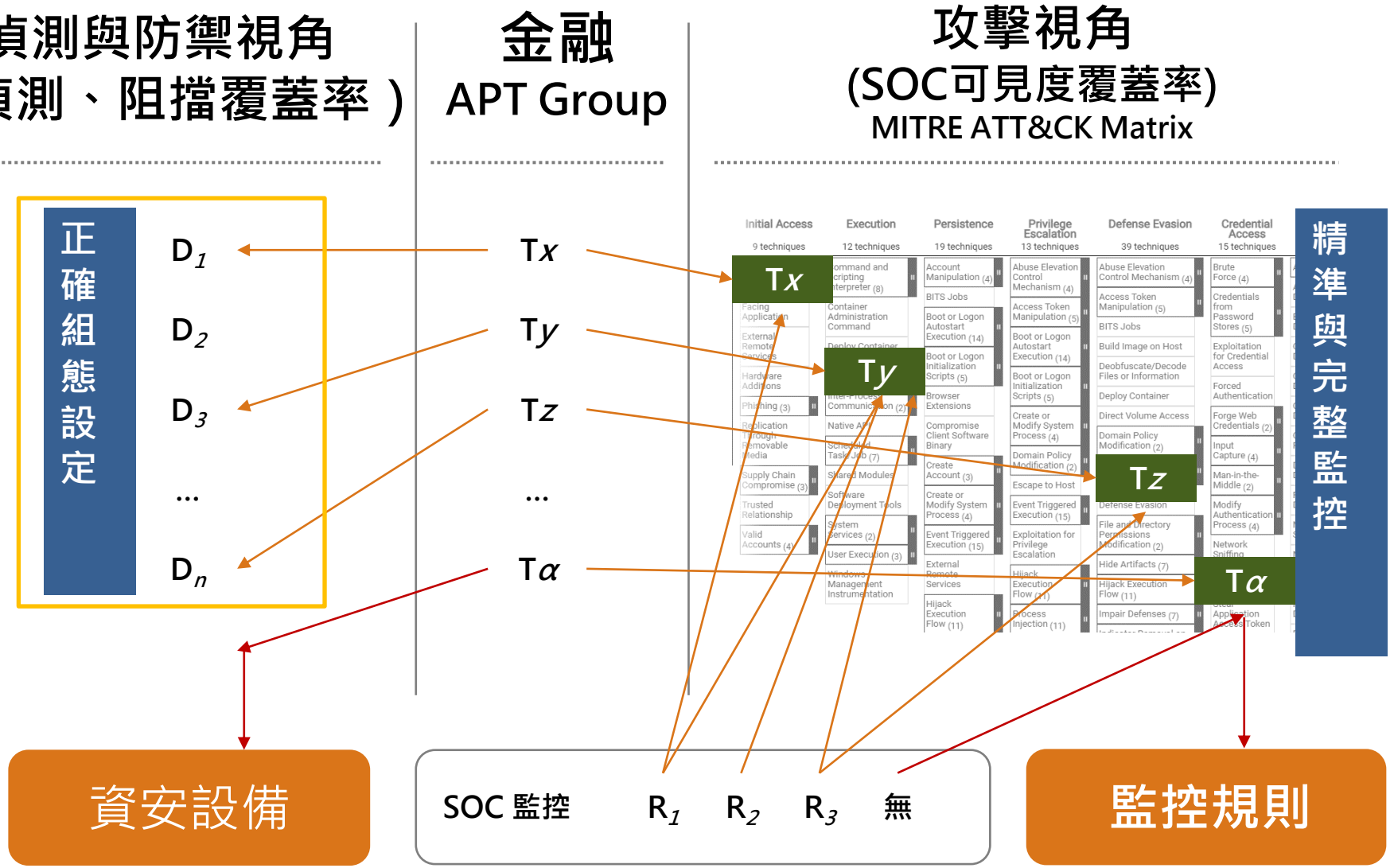
資安監控機制

- 資安監控組織、作業程序
- 監控範圍
- 事件關聯分析、事件單管理及應處
- 事件通報及應變



網路攻擊鏈（Cyber Kill Chain）

五、鼓勵資安監控與防護之有效性評估



- 運用 DeTT&CT 防禦方法論，將金融機構常用之資安、網路、應用系統等設備，映射至MITRE ATT&CK蒐整的網路攻擊手法，針對所對應到的攻擊技術，研析其特徵與手法，產出相對應之監控平台(SIEM)的金融機構資安監控規則

六、鼓勵零信任網路部署，強化連線驗證與授權管控

世界重要國家政府推動規劃

- 零信任已從概念探討階段進入實務部署規劃，世界重要國家之政府紛紛建立國家零信任網路安全戰略

美國

具體規劃2024年前聯邦網路完成初步遷移。

歐盟

2020年建立歐盟網安戰略，提出標準框架，協助成員國轉型。

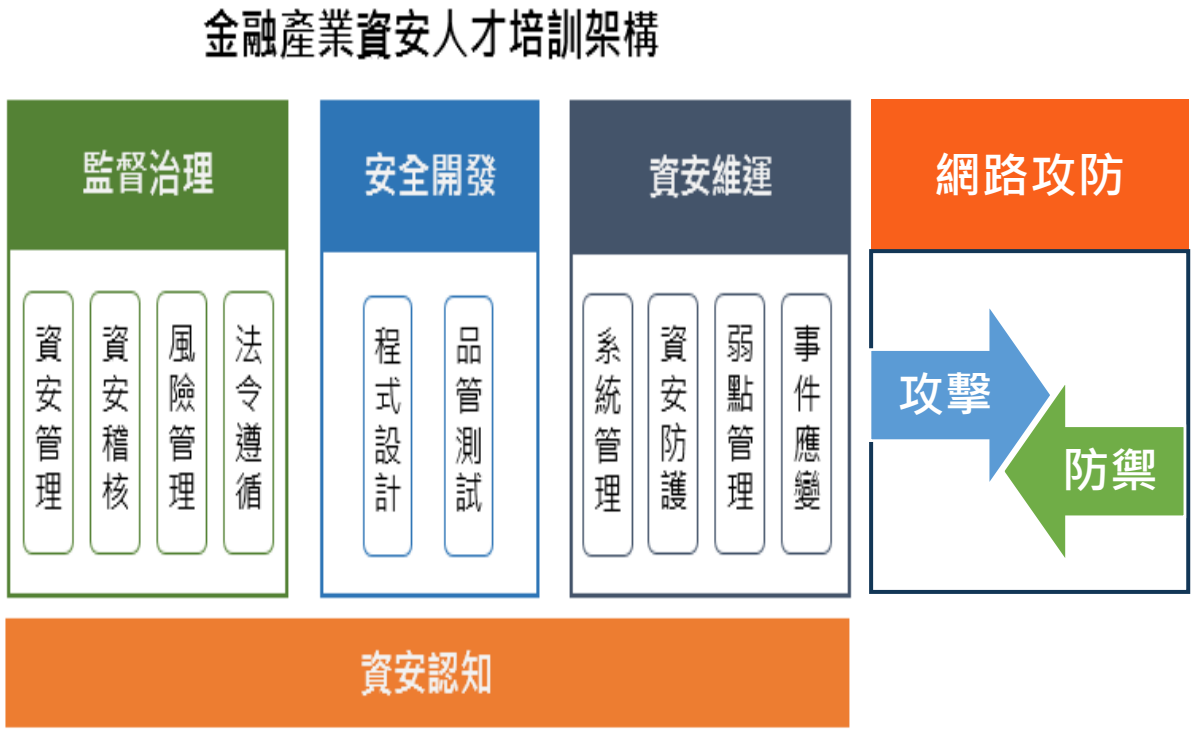
- 行政院「國家資通安全發展方案(110年至113年)」之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，發展零信任網路資安防護環境，**推動政府機關導入零信任網路**，完善政府網際服務網防禦深廣度

身分及設備兩相驗證，授予相應權限，並循環監控

七、鼓勵配置多元專長資安人才，擴大攻防演訓量能

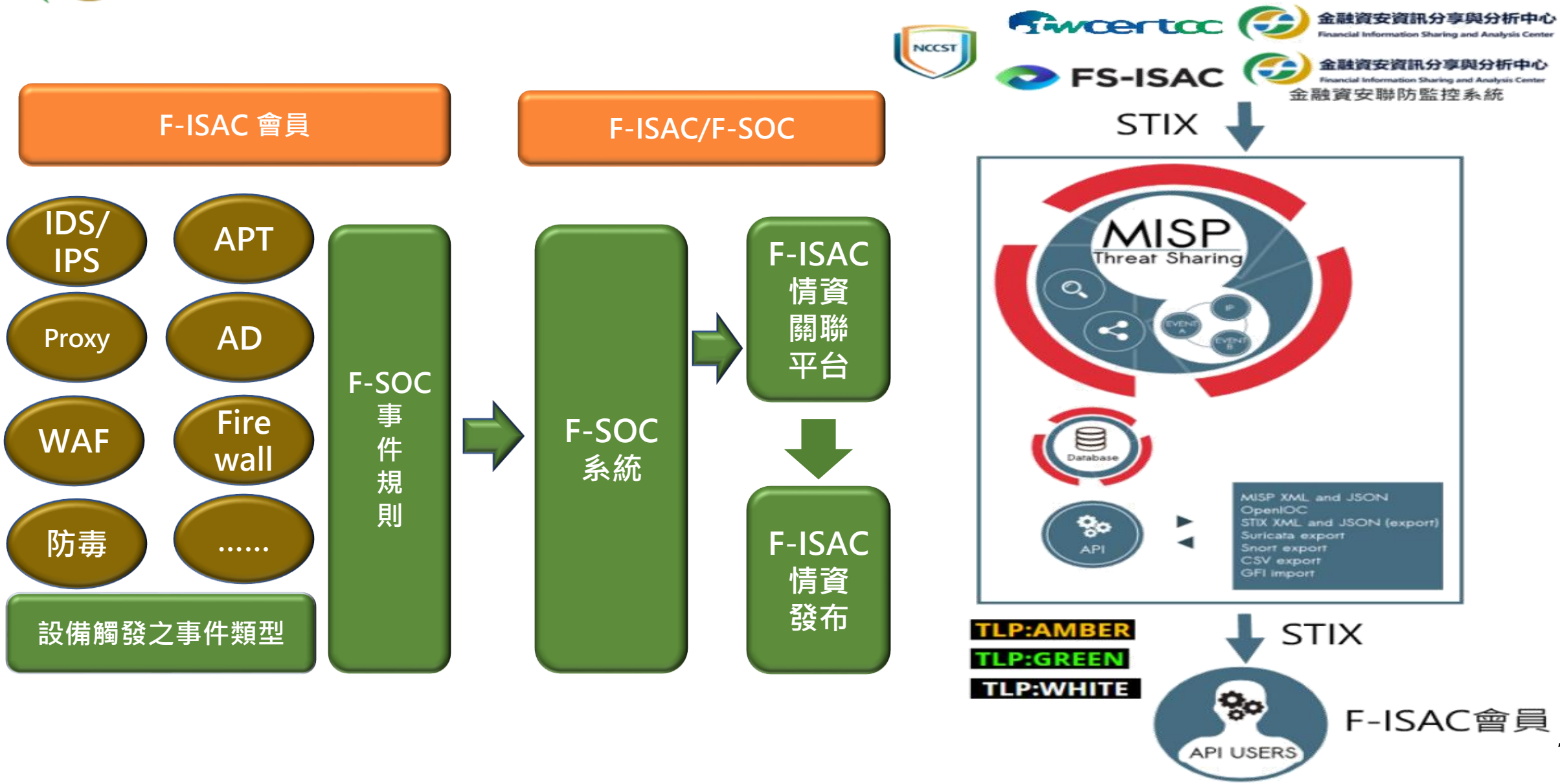
供給 → 職能配置 → 職涯發展 → 需求

- 訂定**人才培訓地圖**，強化金融資安人才能力建構
- 開設**金融資安人才養成專班**，結合科技公司，充實師資及課程
- 透過產學合作、跨業合作，**培育跨領域人才**
- 鼓勵資安人員**取得國際資安證照**，以提升專業能力

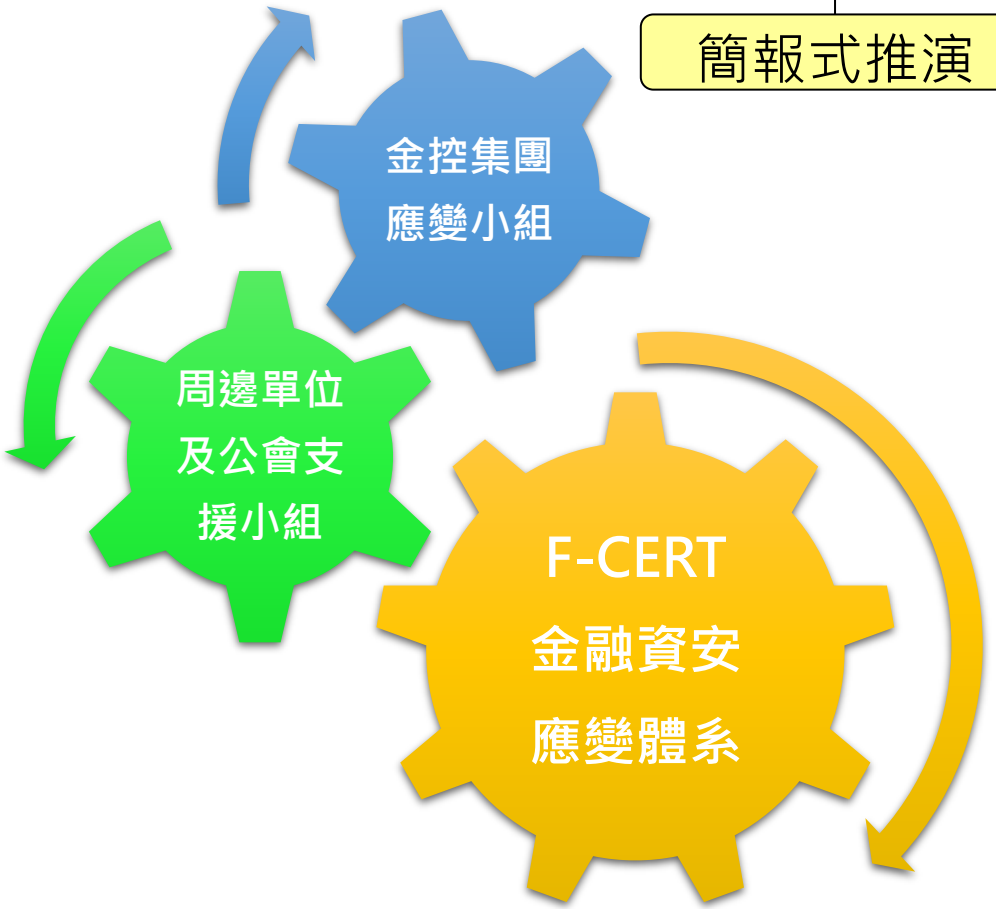


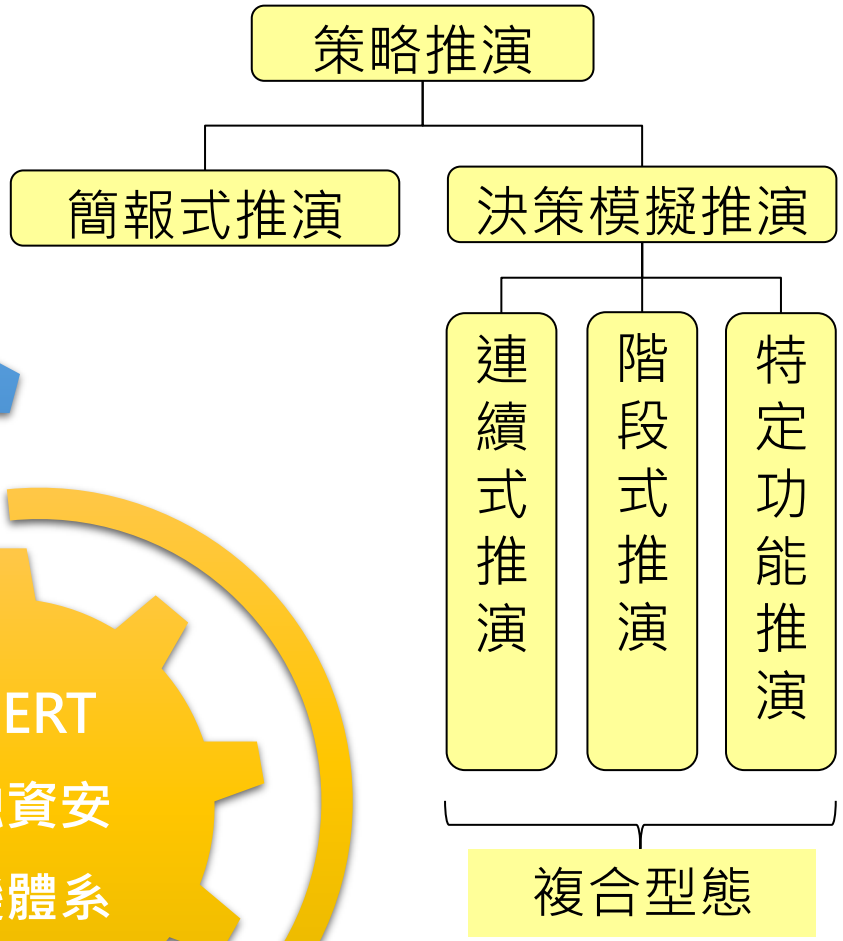
- ✓ 導入美國資安專業組織 **MITRE ATT&CK & Engage** 攻擊防禦方法論
- ✓ 自動化攻擊(包含SQL Injection、木馬、勒索軟體)情境腳本
- ✓ 強化資安人員處理資安事件之應變能力
- ✓ 提升**資安人才**培育容量
- ✓ **跨機構技術交流與人才庫**

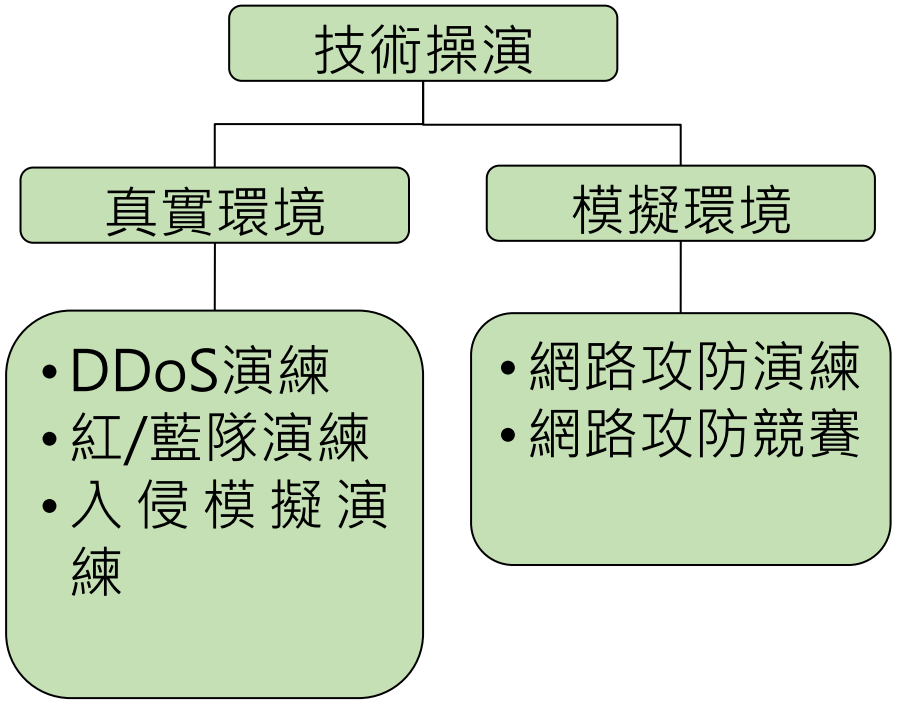
八、提升資安情資分享動能，增進資安聯防運作效能

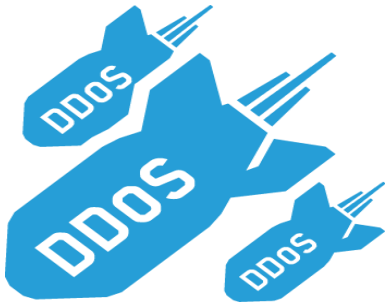


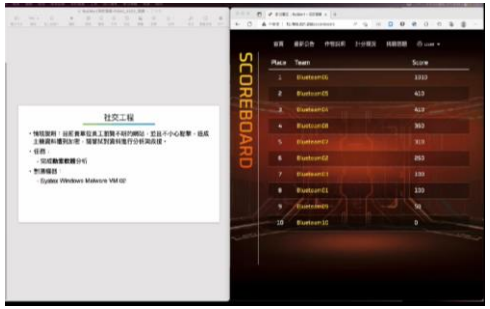
九、辦理資安攻防演練，規劃重大資安事件支援演訓











金融資安精進措施

40項措施：新增12項、擴大5項、持續23項

願景：追求安全便利不中斷的金融服務

目標：
- 建立業者重視資安的組織文化
- 提升業者資安治理能力與水準
- 確保系統持續營運與資料安全

推動策略

強化資安監理	深化資安治理	精實金融韌性	發揮資安聯防
1. 擴大資安長設置 2. 定期召開資安長聯繫會議 3. 建立網路身分驗證與業務風險對照 4. 強化第三方服務提供者風險評估與管理	1. 推動導入國際資安管理標準 2. 推動資安監控機制及鼓勵有效性評估 3. 鼓勵配置多元資安人才，提升攻防演訓量能 4. 鼓勵零信任網路部署	1.鼓勵對外服務之營運持續演練 2.辦理資安實兵攻防及重大事件情境演練 3.強化資料保全機制	1. 強化資安情資關聯分析及情資分享動能 2. 規劃重大資安事件支援演訓，建立虛擬指揮應變體系 3. 提升聯防SOC協同運作效能

精進措施

推動作法

依不同業別、規模及業務，給予不同資安要求，循序推動

透過資源共享，建立情資分享、事件應變及監控體系

做好資安的業者，給予費率優惠等降低經營成本的誘因，例如降存款保險費率

結合其他國家資安組織，掌握國際資安情勢，合作因應駭客攻擊

政府、本會周邊單位及各業別公會協力合作分工

願 景

安全、便利、不中斷
金 融 服 務

- 安全穩定的數位金融交易環境
- 保護消費者金融資產及個人資料
- 提供多元便捷的金融服務

簡報完畢
敬請指教