金融資安的發展現況

金融監督管理委員會
資服處蔡處長福隆
111年01月18日

2021資安威脅趨勢

一、國際遭駭事件頻傳，金融機構仍為主要目標

二、勒索攻擊成為常態

三、AI成為社交工程攻擊手法

四、供應鏈攻擊已成為金融機構風險

五、資通訊及物聯網設備漏洞零時差

六、國家級犯罪組織持續活動

資安的挑戰

- 沒有發生資安事件，無法感受資安的重要
- 資安只有投入成本，不易看到績效
- 資安與效率的矛盾；資安與資訊的衝突
- 資安的防守戰線太長，易攻難守
- 駭客愈來愈厲害(專業化、組織化)，不易抵擋

資安的因應之道

- 整體的思考與論述
- 善於對內協調、對外溝通
- 重視資安成為組織文化(資安不只是資安或資訊單位的事)
- 風險可控、踏實推動、落實執行
- 要心思細膩，不斷追根究底
- 最重要：不發生重大資安事件

金融資安行動方案

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

具體措施

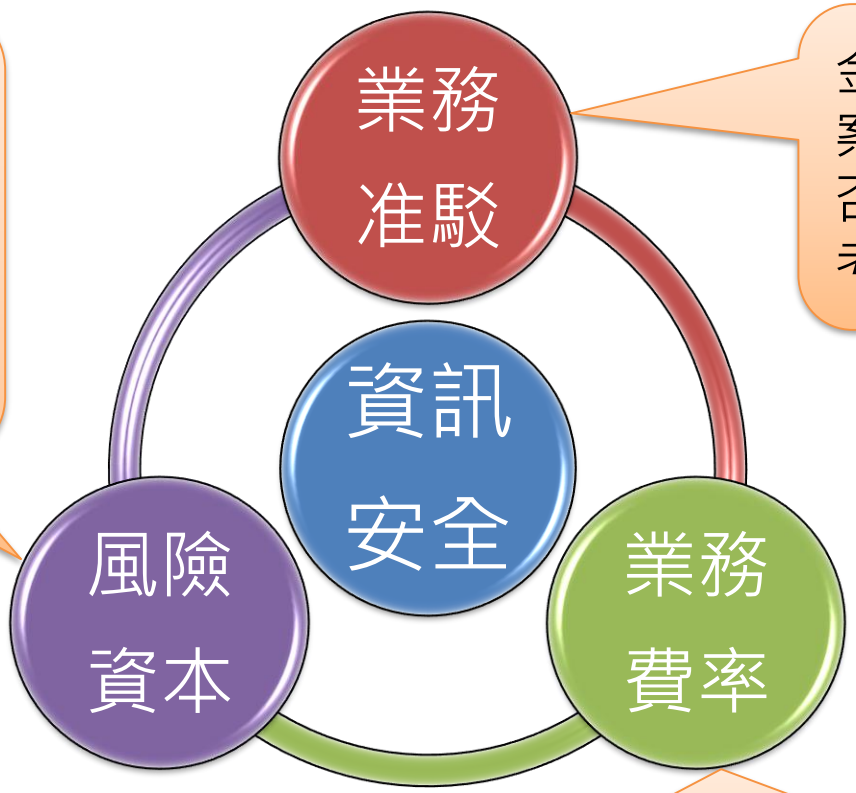
強化資安監理	深化資安治理	精實金融韌性	發揮資安聯防
1. 型塑金融機構重視資安的組織文化 2. 完備資安規範 3. 強化資安監理職能 4. 加強金融資安檢查	1. 加強資安管理 2. 強化資安監控 3. 加強資安人才培育	1. 增進營運持續管理量能 2. 加強資安演練 3. 建構資料保全避風港	1. 資安情資分享與合作 2. 建立金融資安事件應變體系 3. 建立金融資安事件監控體系

金融資安行動方案重點

- 結合監理工具提供激勵誘因
- 以戰代訓-強化資安演練廣度與深度
- 型塑金融機構重視資安的組織文化
- 資安情資分享與國際合作
- 強化新興科技的資安防護
- 建構資源共享的資安應變機制
- 系統化培育金融資安專業人才
- 落實災害應變復原運作機制

(一)結合監理工具提供激勵誘因

未落實資訊安全之金融機構，提高其作業風險法定資本之計提



金融業者申請開辦業務案件，資訊安全管理是否落實，作為本會准駁考量因素之一

資訊安全執行較好金融機構，適用較低費率：

- 存款保險
- 保險安定基金

(二)型塑重視資安的組織文化

執行措施	執行成效	研議作為
• 推動一定規模金融機構或純網銀設置**副總經理層級之資安長** • 鼓勵遴聘具資安背景之**董事、顧問或設置資安諮詢小組**。	• 已有12家重要金融機構由副總經理兼任資安長。 • 已有34家金融機構臨聘具資安背景之董事、顧問或設置資安諮詢小組	• 修法要求所有本國銀行、一定規模以上之保險公司及證券業設置資安長。 • 研議納入保發中心資訊安全推展卓越獎評分項目 • 研議納入安定基金計提指標項目

(三)強化新興科技的資安防護

兼顧服務創新與安全

金融機構運用新興科技發展創新業務，
亦須預先考量相關資安風險因子

＋

因應委外及跨業合作

強化金融供應鏈體系風險評估與
管理，降低體系風險

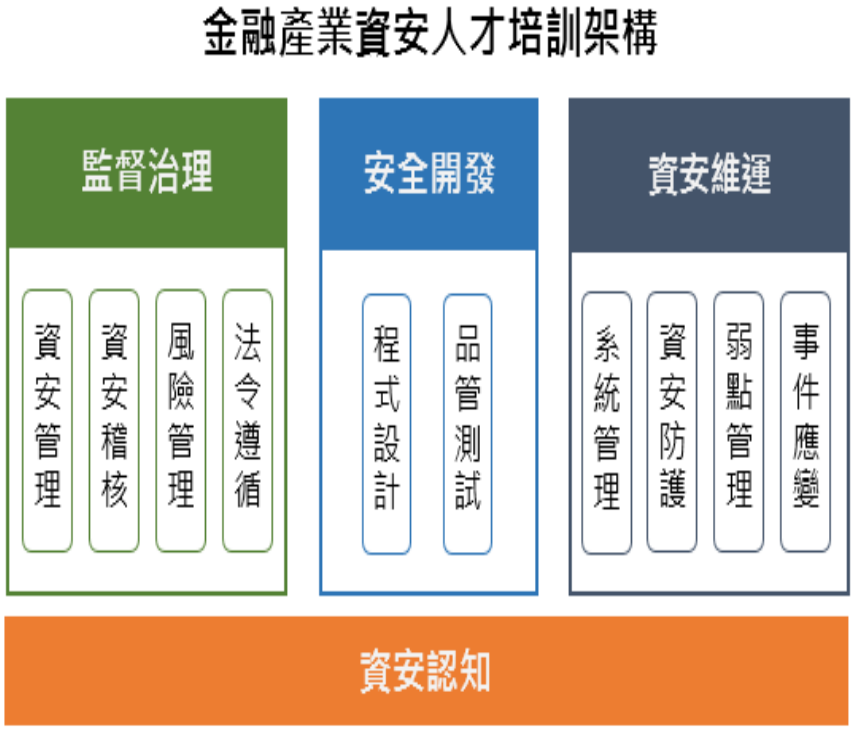
→

增修訂資安自律規範

- APP
- 雲端服務
- 開放銀行
- 網路身分驗證
- 供應鏈風險評估

(四)系統化培育金融資安專業人才

- 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



本會周邊培訓機構(金融研訓院、證基會、保發中心等)109年度共開辦79堂課程，受訓人數達2,630人。

(五)以戰代訓-強化資安演練廣度與深度

攻防演練/訓練

- DDoS演練
- 紅隊演練
- 藍隊演練
- 網路攻防演練實作
- Threat Hunting

建置攻防演練場域

- ✓ 情境腳本自動化攻擊(包含SQL Injection、木馬、勒索軟體)
- ✓ 透過模擬演練學習MITRE ATT&CK攻擊鏈知識
- ✓ 強化金融機構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

(六)金融資安聯防 F-ISAC

金融資安資訊分享與分析中心(106年12月成立)
Financial Information Sharing and Analysis Center

會員數376家

建立國際ISACs情資交流

- FS-ISAC 美國FS-ISAC (108年3月)
- enisa 歐盟FI-ISAC (108年5月)
- Financials ISAC Japan 日本F-ISAC (108年10月)
- CERT-IL 以色列CERT-IL
- 금융보안원 韓國FSI

防患未然 F-ISAC事前預防 → **防微杜漸** F-SOC事中監控 → **降低傷害** F-CERT事後復原

威脅預警

- F-ISAC發布威脅警訊計996則
- 推動會員情資分享計549則
- **推動弱點管理自動化機制**

人才培育

- 資安研討會23場
- 資安防護實作課程20梯次
- 資安職能認證課程2梯次

資安演練

- 13家銀行參加行政院跨國攻防演練(CODE2019)
- 辦理「金融DDoS攻防演練」計32家金融業者參演

聯防監控

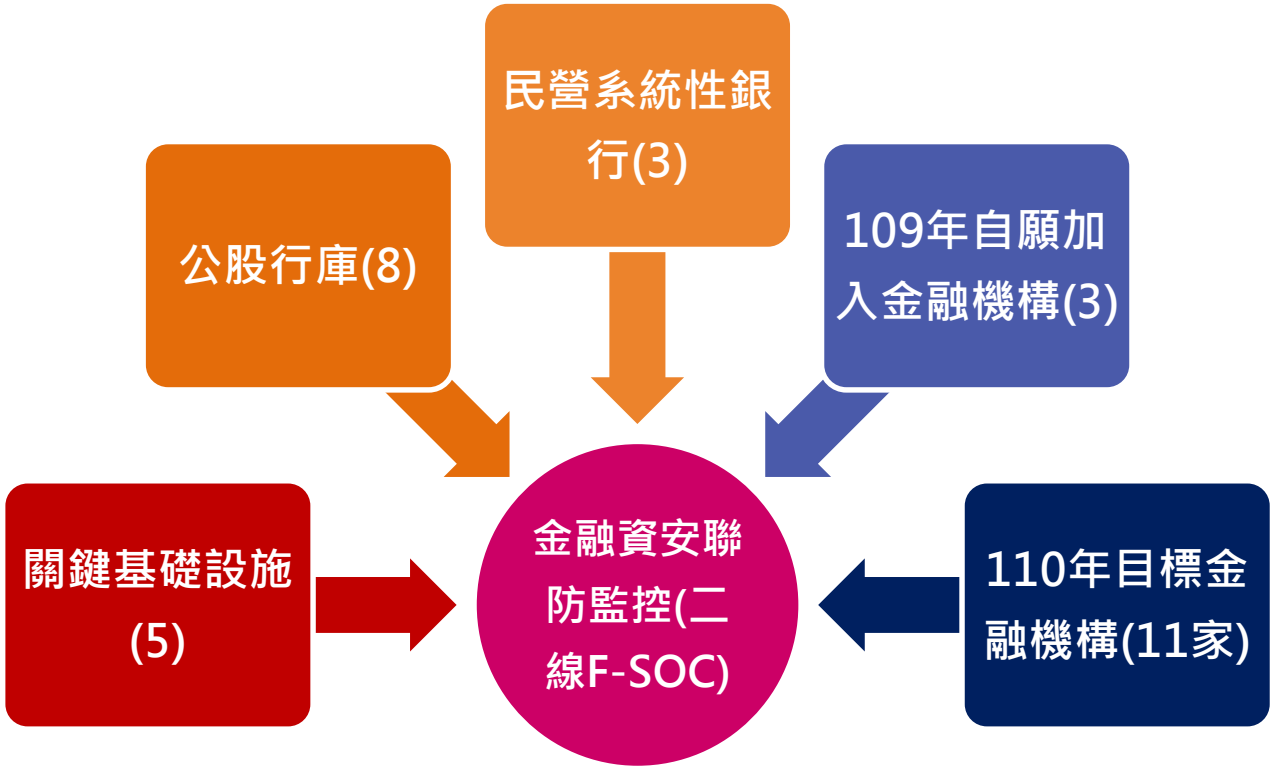
- 建置F-SOC二線金融資安聯防監控平台
- 制定資安事件聯防監控規則

事件處理

- 建置F-CERT二線金融電腦緊急應變小組
- 109年協助金融業者處理勒索軟體攻擊事件。

(六)金融資安聯防 F-SOC

- ◆建置F-SOC平台，訂定95條監控規則。
- ◆推動金融機構SOC與聯防SOC協同運作

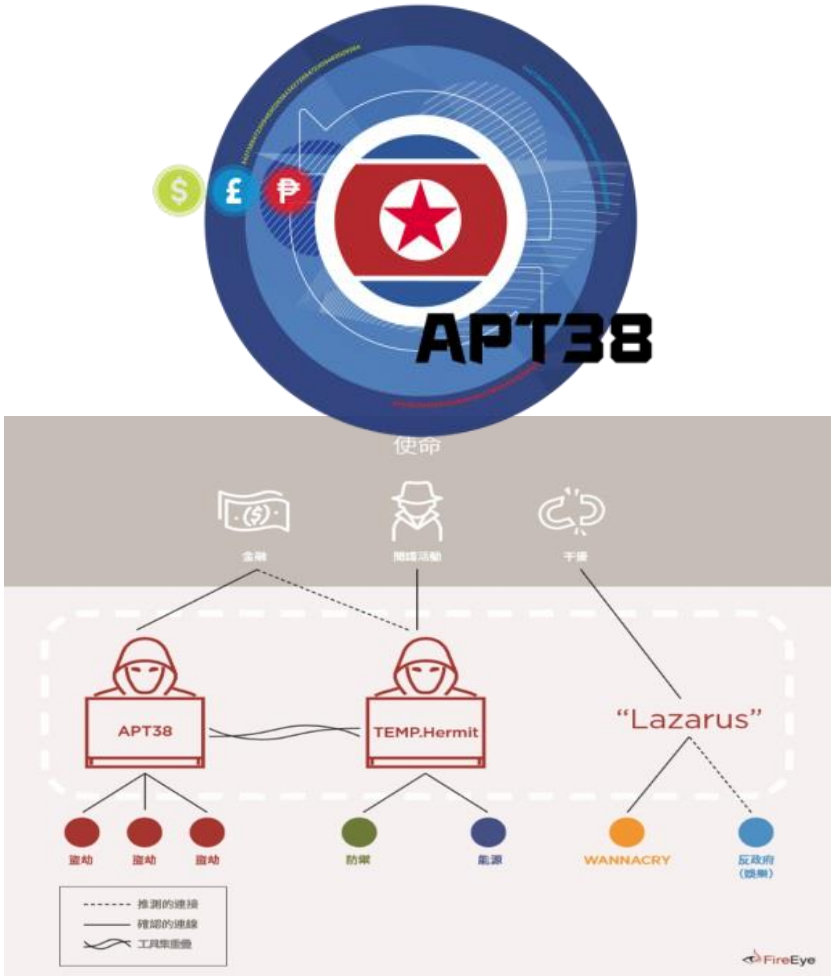


(六)金融資安聯防 F-SOC

駭客組織APT38，針對**全球金融產業**發動多起攻擊事件，如SWIFT系統盜轉、ATM盜領等

透過研究攻擊手法，並經過系統模擬及驗證，**制定相關監控規則**提供給金融機構SOC運用

F-SOC透過**分析**回傳事件單，**掌握**該組織於我國金融機構之相關**足跡**，**早期預警**，強化金融聯防監控成效



(七)建構資源共享的資安應變機制

因應資安事件應變處理具高度時效要求，單一機構資源有其限制，建立資源共享的資安應變機制

- 金控集團應變小組
- 周邊單位及公會支援小組
- F-ISAC/F-CERT應變體系

(八)落實災害應變復原運作機制

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

- 識別核心業務
- 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
- 實際業務運作驗證

關鍵資料保全

- 資料保護
- 資料可移性
- 資料復原性
- 關鍵服務持續性

(九)金融資安治理成熟度評估

- 5大評估類別
- 39題

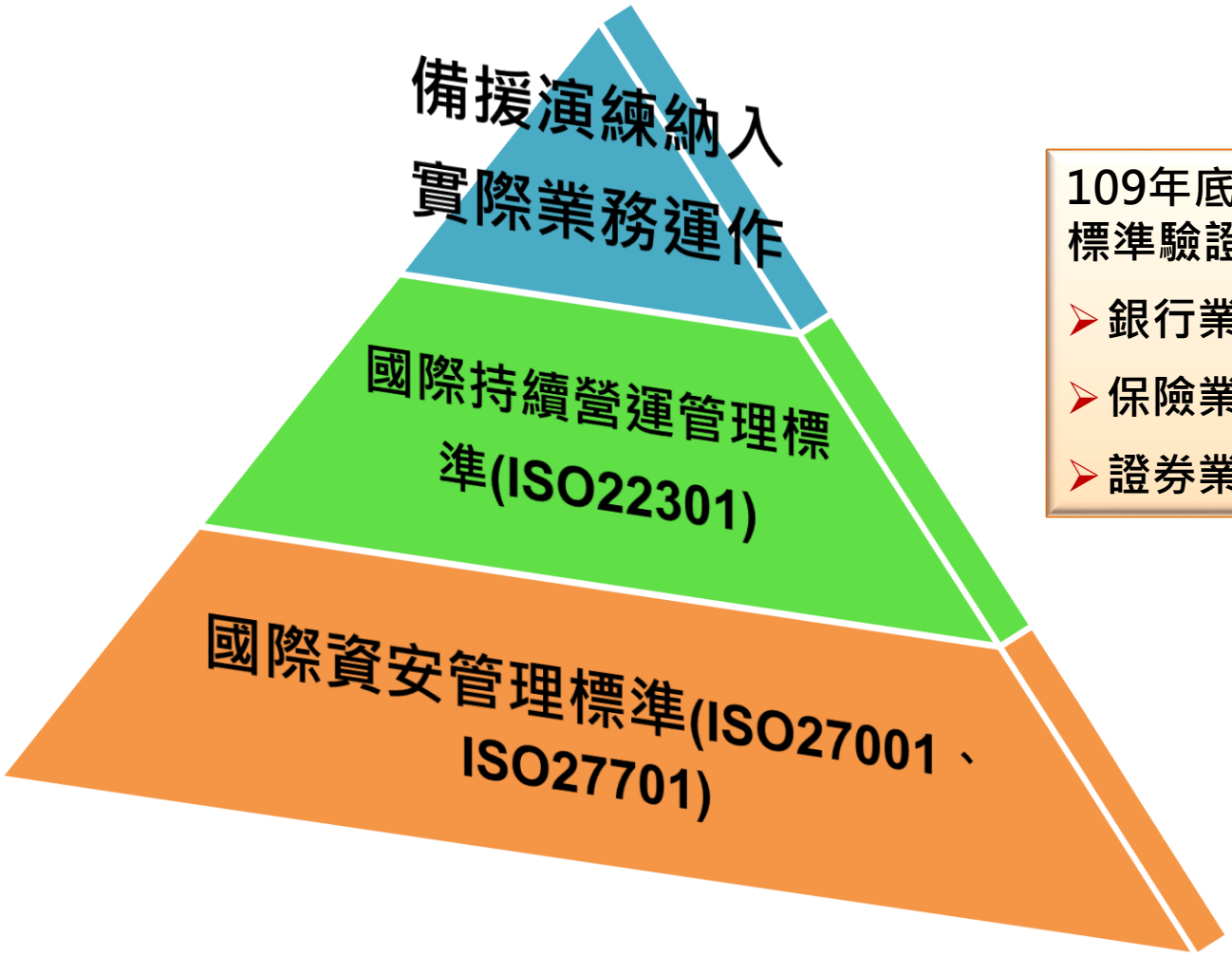
- 5大控制領域
- 494題

- 定期評估以制定資安管理方針及改善方案

- 建立風險/成熟度關聯矩陣

- 109年度-銀行業
- 110年度-保險業
- 111年度-證券業

(十)鼓勵導入國際資安標準



109年底取得國際資安管理標準驗證

- 銀行業：30家 (81%)
- 保險業：38家 (93%)
- 證券業：13家

(十一) F-ISAC偽冒網站偵測服務

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

偽冒網站偵測機制

金融業者網站

Step2:
發現疑似偽冒網站，將留存偽冒網頁快照紀錄並通知業者確認。

Step1:
7*24自動化搜尋偽冒網站，比對網址及網站相似度

Step3:通知偽冒網站情資

twcert/cc (DNS RPZ)

Google Microsoft

Step4:避免民眾連結偽冒網站

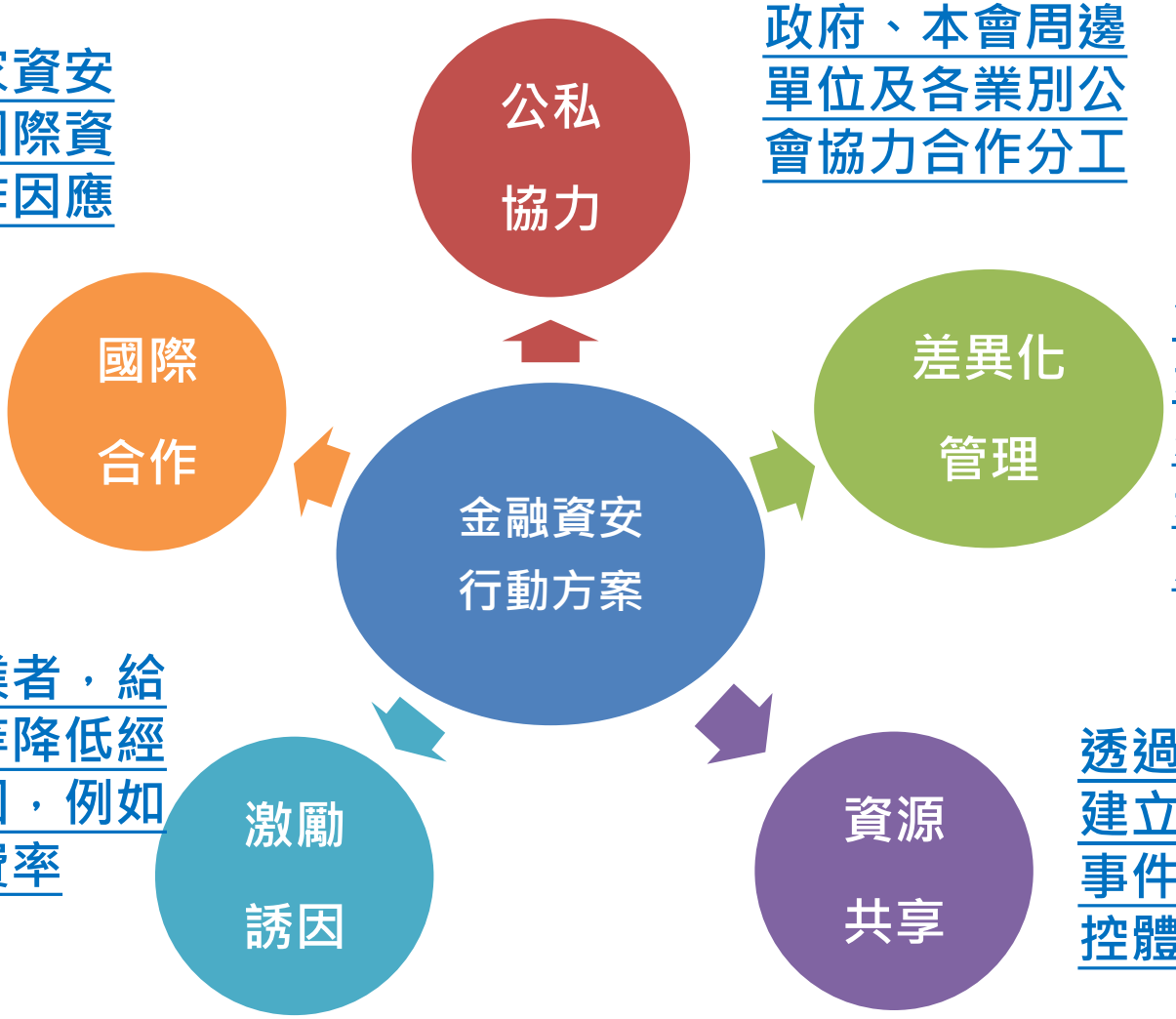
偽冒網站

詐騙集團

詐騙簡訊

民眾

推動作法


公私協力
政府、本會周邊單位及各業別公會協力合作分工
國際合作
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
金融資安行動方案
差異化管理
依不同業別、規模及業務，給予不同資安要求，循序推動
激勵誘因
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
資源共享
透過資源共享，建立情資分享、事件應變及監控體系

結語