推動「金融資安行動方案」

金融監督管理委員會
報告人：資訊服務處蔡處長福隆
109年9月17日

一、背景說明

金融資安

- 9月5、6日智利Estado銀行遭受勒索軟體攻擊，並於9月7日起關閉所有分行
- 8月25-28日紐西蘭證交所遭受分散式阻斷服務(DDoS)攻擊，暫停股票交易4天
- 8月26日美國國土安全部等政府機構發布惡意程式分析報告，北韓駭客組織HIDDEN COBRA利用FASTCash 2.0遠端存取後門工具程式，操控金融設備進行偽冒交易

金融穩定

- 2017年3月G20財長與央行總裁會議宣言：惡意的使用資通訊科技可能癱瘓掉一國或國際金融體系，破壞金融的安全與民眾的信任，並危及金融穩定

金融領域資安防護痛點

風險高 → 組織型駭客持續攻擊並勒索金融產業

威脅多 → 新興資訊技術(Fintech、AI、IoT)帶來新增威脅

溝通少 → 金融機構資安防護各自獨立，缺少訊息溝通管道

人才缺 → 金融資安專業人才短缺

二、方案架構

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

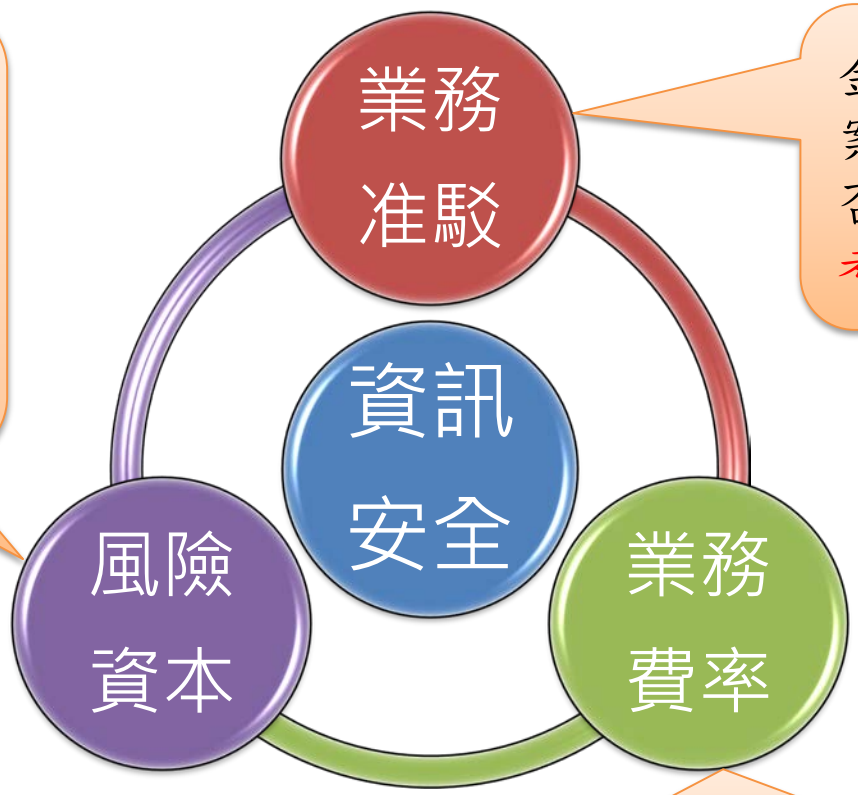
強化資安監理	深化資安治理	精實金融韌性	發揮資安聯防
1. 型塑金融機構重視資安的組織文化 2. 完備資安規範 3. 強化資安監理職能 4. 加強金融資安檢查	1. 加強資安管理 2. 強化資安監控 3. 加強資安人才培育	1. 增進營運持續管理量能 2. 加強資安演練 3. 建構資料保全避風港	1. 資安情資分享與合作 2. 建立金融資安事件應變體系 3. 建立金融資安事件監控體系

三、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

董事會

- 鼓勵遴聘具**資安背景之董事、顧問或設置資安諮詢小組**，增納專業人員參與董事會運作，帶動機構重視資安的組織文化

資安長

- 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**，統籌資安政策推動協調與資源調度

(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

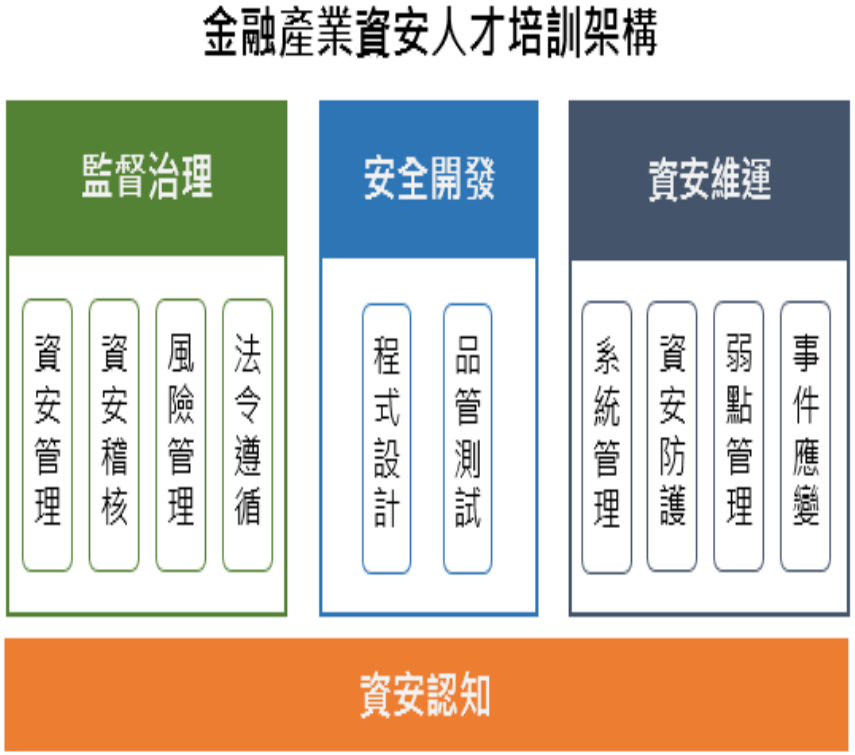
→

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



(五)以戰代訓-強化資安演練廣度與深度

106/107行政院攻防演練

- 跨域情境演練
- DDoS演練
- 電子郵件社交工程
- 外網滲透測試
- 內網滲透測試

108年-行政院跨國攻防演練
109年-攻防場域建置與演訓

金融核心系統實驗場域

紅藍軍對抗

(六)資安情資分享與國際合作

- 多元化情資來源
- 智能化情資分析
- 國際化情資合作

區間	弱點公告	威脅情資	定期週/月報	分析報告	合計
106.12~107	105	106	69	60	340
108年	36	156	63	50	305
109.1~109.6	20	121	32	6	179

截至109年8月底，F-ISAC會員總計376家

(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

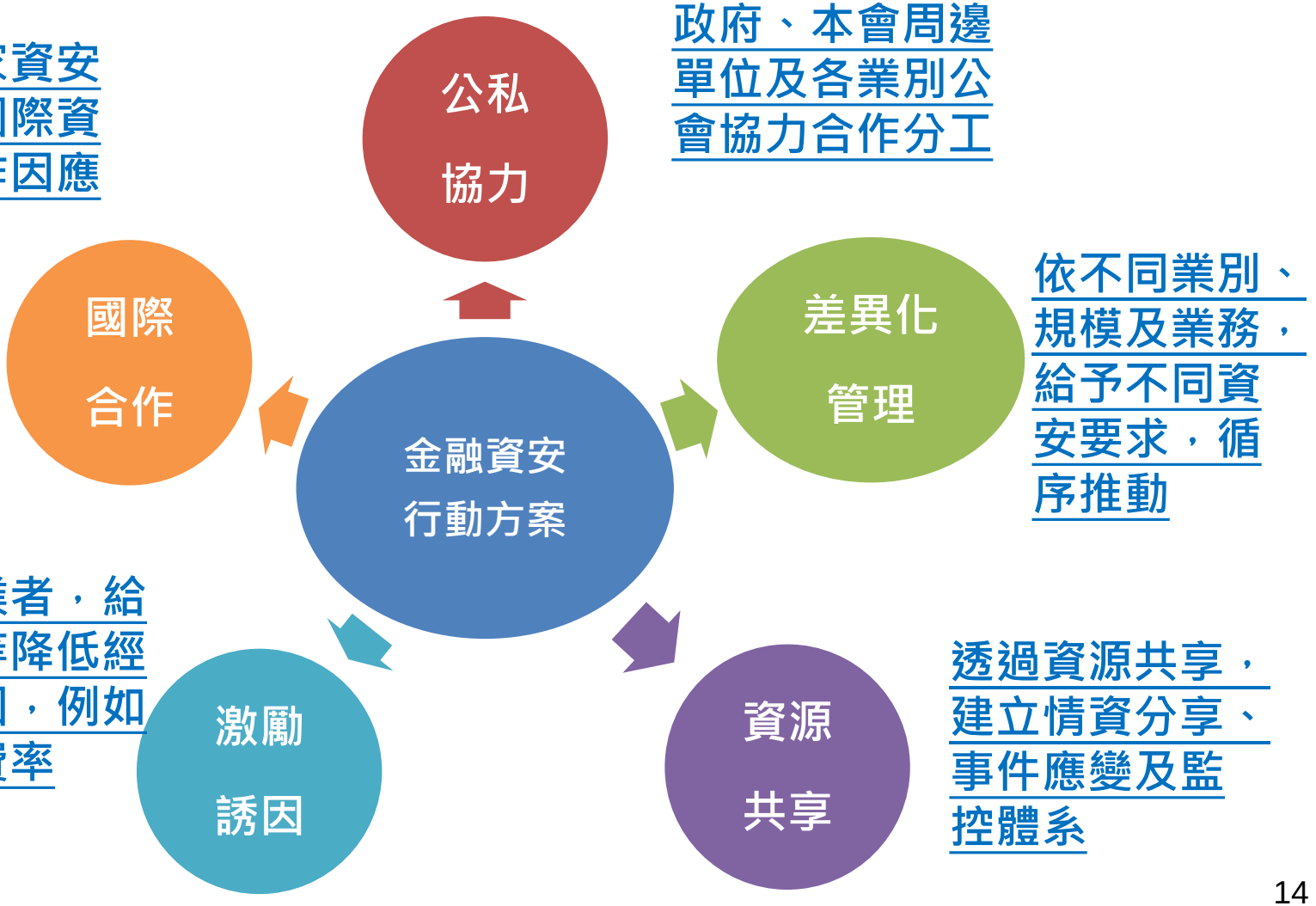
備援環境實作驗證

- 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

四、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

五、預期效益

金融機構

- 健全資安管理制度，提升資安防護能量。在資訊安全的基礎上，運用新興科技發展金融業務，**提供消費者更安心、便利與多樣金融服務**

金融產業

- 建構金融資安聯防體系，營造安全的金融服務發展環境，**奠立金融科技發展基石**

金融消費者

- 安心使用便利、不中斷的金融服務，**享受金融科技與服務創新，確保財產資訊及隱私**