金融監督管理委員會
Financial Supervisory Commission

金融資安行動方案

資訊服務處
109年8月6日

簡報大綱

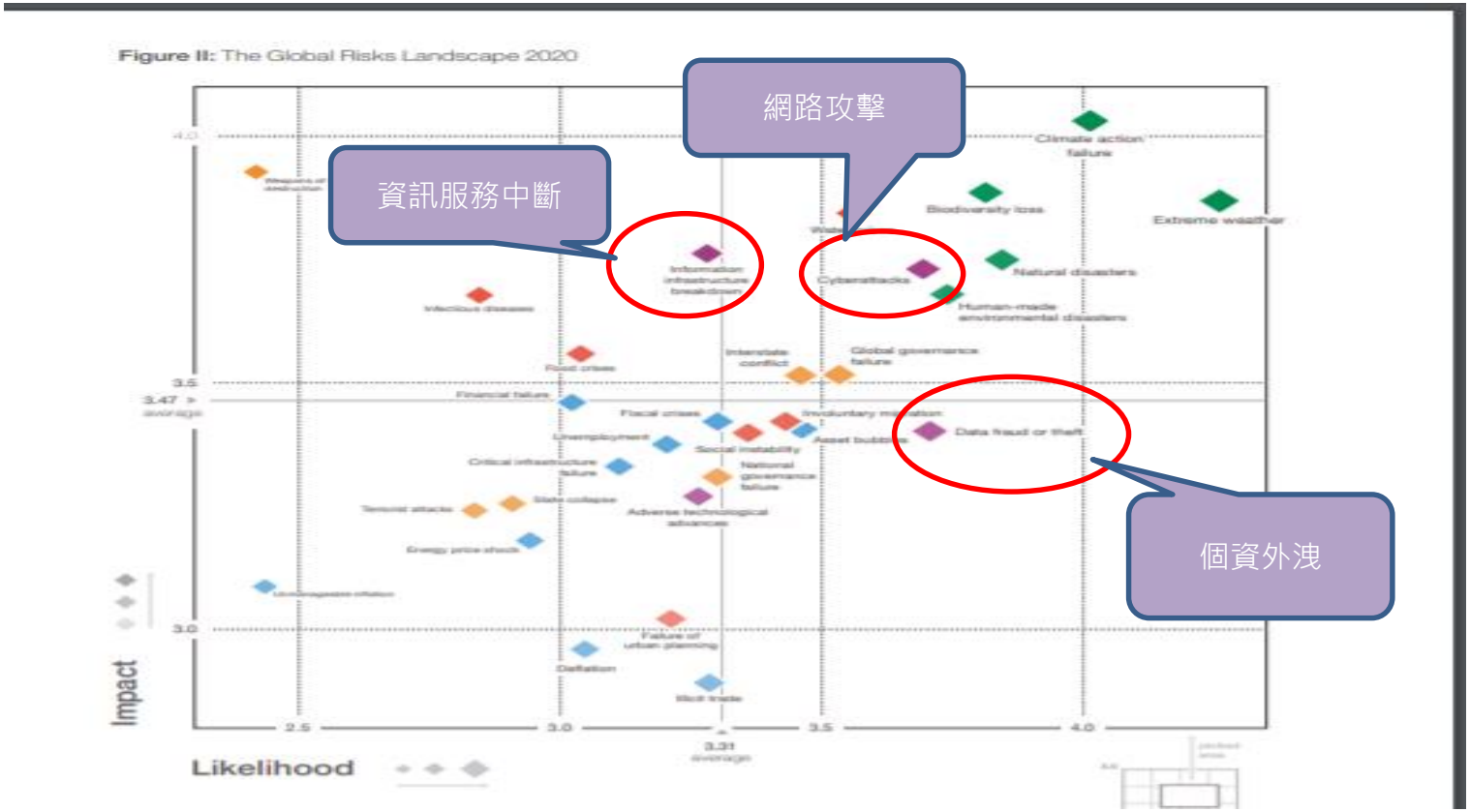
一. 背景說明
二. 資安威脅情勢
三. 國際金融資安監理趨勢
四. 金融資安行動方案
五. 金融資安行動方案八大特色
六. 一年內可完成之資安措施
七. 推動作法
八. 預期效益

一、背景說明

- **緣起**：
  - 金融科技創新改變金融業營運模式，提供客戶便利服務，同樣也帶來風險。
  - 資安威脅日益嚴峻，金融資安防護思維須更快速的調整因應
- **過程**：觀察國際金融資安情勢、國際金融資安監理趨勢，並檢討現行資安監理政策
- **方案**：訂定金融資安行動方案，以四年為期推動
- **目的**：提供民眾安心便利、穩定不中斷的金融服務，保護金融消費者的財產與隱私

二、資安威脅情勢(1/2)

依世界經濟論壇(WEF)「The Global Risks Report 2020」指出，
網路攻擊、個資外洩、資訊服務中斷是三大主要資安風險



二、資安威脅情勢(2/2)

- 國際頻傳遭駭事件，金融機構仍為眾所矚目標的
  如SWIFT系統遭盜轉、ATM遭盜領、藉DDoS攻擊勒索等事件
- 資安管理仍待持續強化與落實，供應鏈成為攻擊跳板
  包括資料傳輸安全性、人員資安意識、委外廠商或供應商資安管理等風險
- 具針對性攻擊潛伏期長影響大，防禦難度倍增
  金融資安事件已無法完全避免，相對考驗的是不僅是事前防禦，還有事中之緊急應變及事後之災害復原能力
- 國家級金融犯罪組織持續活動，防禦方相對勢單力薄
  駭客已從過去單打獨鬥，轉型為有組織、專業化及國際化發展，已難以完全防範，造成金融機構資安風險大幅增加

三、國際金融資安監理趨勢(1/2)

- 重視經營管理階層資安職責及要求獨立資安職能
  - 美國紐約州金融服務署(NYDFS)2017年「金融服務業網路安全要求規範」(23 NYCRR Part 500)
  - 歐洲銀行監理總署(EBA)2019「資通科技及安全風險管理指引」
- 建立共通資安管理基準及自我評估機制

  已有多個監理機關發布相關規範，內容包括資安政策、資安風險管理、作業安全、資安監控等各面向
  - 歐洲銀行監理總署(EBA)2019年底「資通科技及安全風險管理指引」
  - 新加坡金融管理局(MAS) 2019年8月「網路安全通告」
  - 美國聯邦金融機構檢查委員會（FFIEC）2015年6月「資訊安全評估工具」(CAT)
  - 美國FED、OCC、FDIC於2016年10月聯合發布「強化網路風險管理標準」草案預告

三、國際金融資安監理趨勢(2/2)

- 建構並實證作業風險抵禦能力
  - 英國英格蘭銀行(BOE)、審慎監理總署(PRA)、金融行為監理總署(FCA)於2018年聯名發布「建構英國金融業之作業風險抵禦能力之政策方向」討論文件
  - 美國商品期貨交易委員會(CFTC)2016年發布修正網路安全能力測試準則
  - 加拿大金融監理署(OSFI)於2013年10月公布資訊安全自行評估準則

四、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

(一)強化資安監理

型塑重視資安的組織文化	• 推動一定規模金融機構或純網銀設置副總經理層級資安長 • 遴聘具資安背景之董事、顧問或設置資安諮詢小組 • 定期檢視資安風險因子與金融監理工具連結之有效性
完備資安規範	• 訂定資通安全防護基準，納入網路安全防護及資訊系統安全防護基準 • 訂定新興金融科技資安規範，納入APP、雲端服務、開放銀行、OPEN API、物聯網、網路身分認證(eKYC)等 • 增修訂供應鏈風險管理規範，納入核心資訊系統供應商或跨機構資訊服務之風險評估及查核等管理機制
強化資安監理職能	• 推動本會資安人才培育計畫，包括訓練課程、赴周邊或公務機構實習、參加國際人才進修等措施 • 提升中高階主管資安知能
加強金融資安檢查	• 因應新興業務調整資安檢查重點 • 提升資安檢查人員專業技能

(二)深化資安治理

加強資安管理	• 鼓勵金融機構導入國際資安管理標準(ISMS)及取得驗證 • 推動金融資安治理成熟度，鼓勵金融機構自評，持續強化資安管理
強化資安監控	• 鼓勵金融機構建置資安監控機制(SOC)，及早發現網路異常行為，以扮演資安防護「防微杜漸」的關鍵角色
加強資安人才培育	• 訂定金融資安人才職能地圖、開設金融資安人才養成專班 • 鼓勵金融資安人員取得國際資安證照 • 推動攻防演練訓練課程，以戰代訓

(三)精實金融韌性

增進營運持續管理量能	• 訂定強化作業韌性參考規範，包括核心業務識別、最大可容忍中斷時間與災害應變運作、壓力測試、復原能力之實證等 • 鼓勵導入國際營運持續管理標準(BCM)及取得驗證 • 鼓勵實際作業之營運持續演練
加強資安演練	• 辦理金融資安攻防演練，如阻斷式服務攻擊(DDoS) • 辦理金融資安攻防競賽 • 辦理重大資安事件應變情境演練
建構資料保全避風港	• 研議資料保全運作機制，包括資料保護、資料可移性、資料復原性及關鍵服務持續性等項 • 推動成立資料保全中心

(四)發揮資安聯防

資安情資分享與合作	• 建立資安情資關聯分析平台，提供金融機構早期預警與防護建議 • 加強與國際金融資安機構合作或簽訂MOU
建立金融資安事件應變體系	• 鼓勵建立電腦資安事件應變小組(金控) • 推動建立資安應變支援小組(周邊單位或公會) • 建立金融資安應變體系(F-ISAC)
建立金融資安事件監控體系	• 建立二線資安聯防監控體制，訂定資安監控作業標準，透過協同運作，以即時有效關聯分析資安風險。 • 導入AI分析機制，提升情資分析量能。

五、金融資安行動方案八大特色

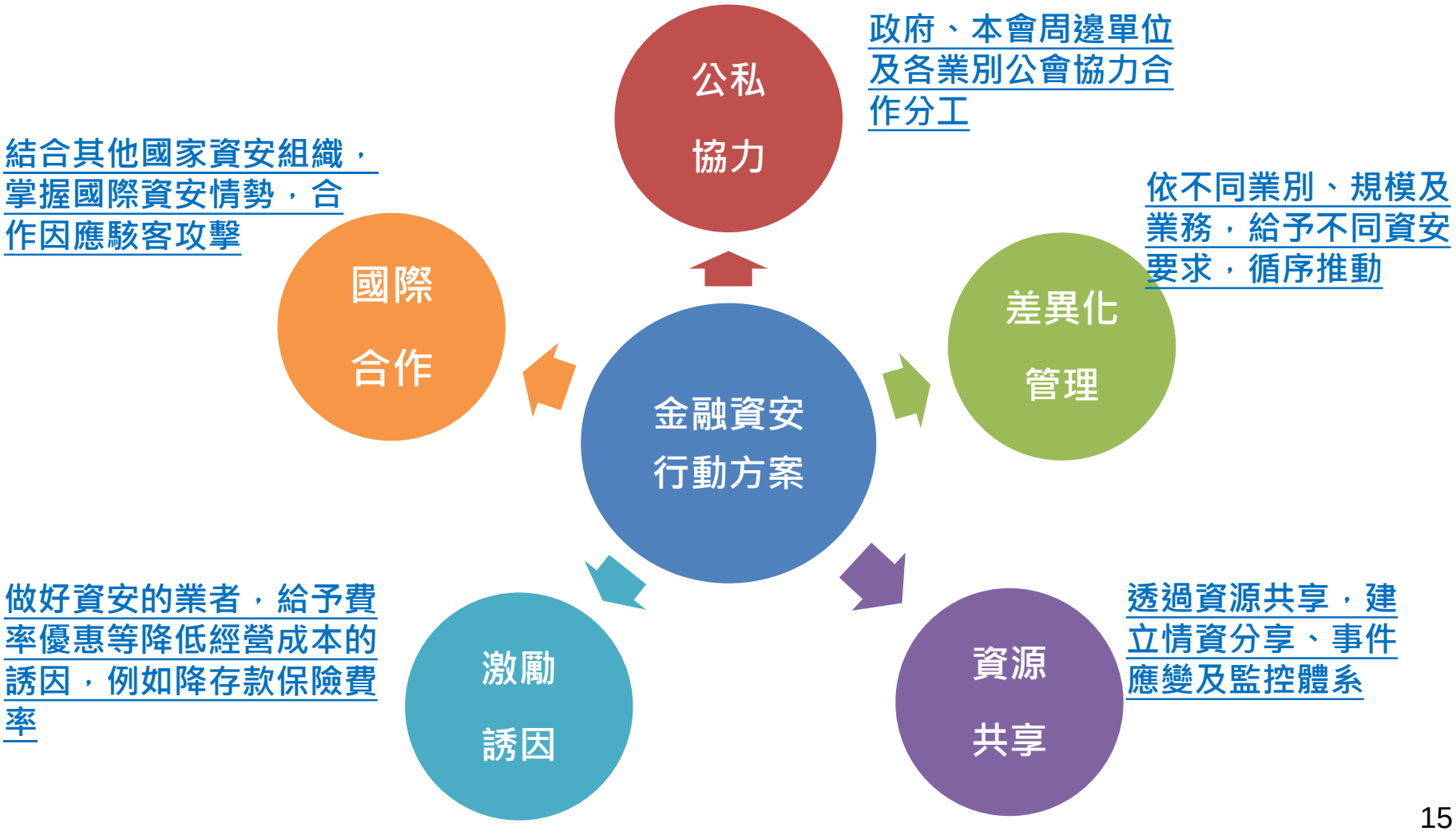
- 型塑金融機構重視資安的組織文化(設副總層級資安長及專業董事或顧問)
- 強化新興科技的資安防護
- 系統化培育金融資安人才(職能地圖、開設專班、國際證照)
- 建立營運資料保全避風港(保全金融營運關鍵資訊)

- 建構資源共享的資安應變機制
- 建置金融資安監控協同體系
- 鼓勵導入資安國際標準
- 落實復原應變運作機制

六、一年內可完成之資安措施

新增措施(計9項)	優化精進措施(計7項)
➢ 開辦董監事資安教育訓練專設課程	➢ 定期檢視資安風險因子與金融監理工具連結之有效性
➢ 推動本會資安人才培育計畫	➢ 因應新興業務調整資安檢查重點
➢ 提升中高階主管資安知能	➢ 提升資安檢查人員專業技能
➢ 鼓勵導入國際資安管理標準	➢ 訂定金融資安人才職能地圖
➢ 鼓勵建置資安監控機制(SOC)	➢ 協調周邊單位開設金融資安人才養成專班
➢ 鼓勵金融資安人員取得國際資安證照	➢ 辦理金融資安攻防演練
➢ 鼓勵金融機構導入國際營運持續管理標準	➢ 加強金融資安國際合作
➢ 鼓勵實際作業之營運持續演練	
➢ 鼓勵金控建立電腦資安事件應變小組	

七、推動作法(1/2)


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
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
金融資安行動方案
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

七、推動作法(2/2)

- 由金管會召集各業務局及相關周邊單位、產業公會共同訂定各項目之推動指標與執行進程。
- 自110年度起，每半年檢討執行情形，滾動修訂推動策略、執行措施及各項推動指標。

八、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、便利與多樣之金融服務。

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，奠立金融科技創新發展之基石。

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。