金融監督管理委員會
Financial Supervisory Commission

附件2

金融資安行動方案

金融監督管理委員會
報告人：資訊服務處林副處長裕泰
109年12月4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. 推動作法

六. 預期效益

一、背景說明

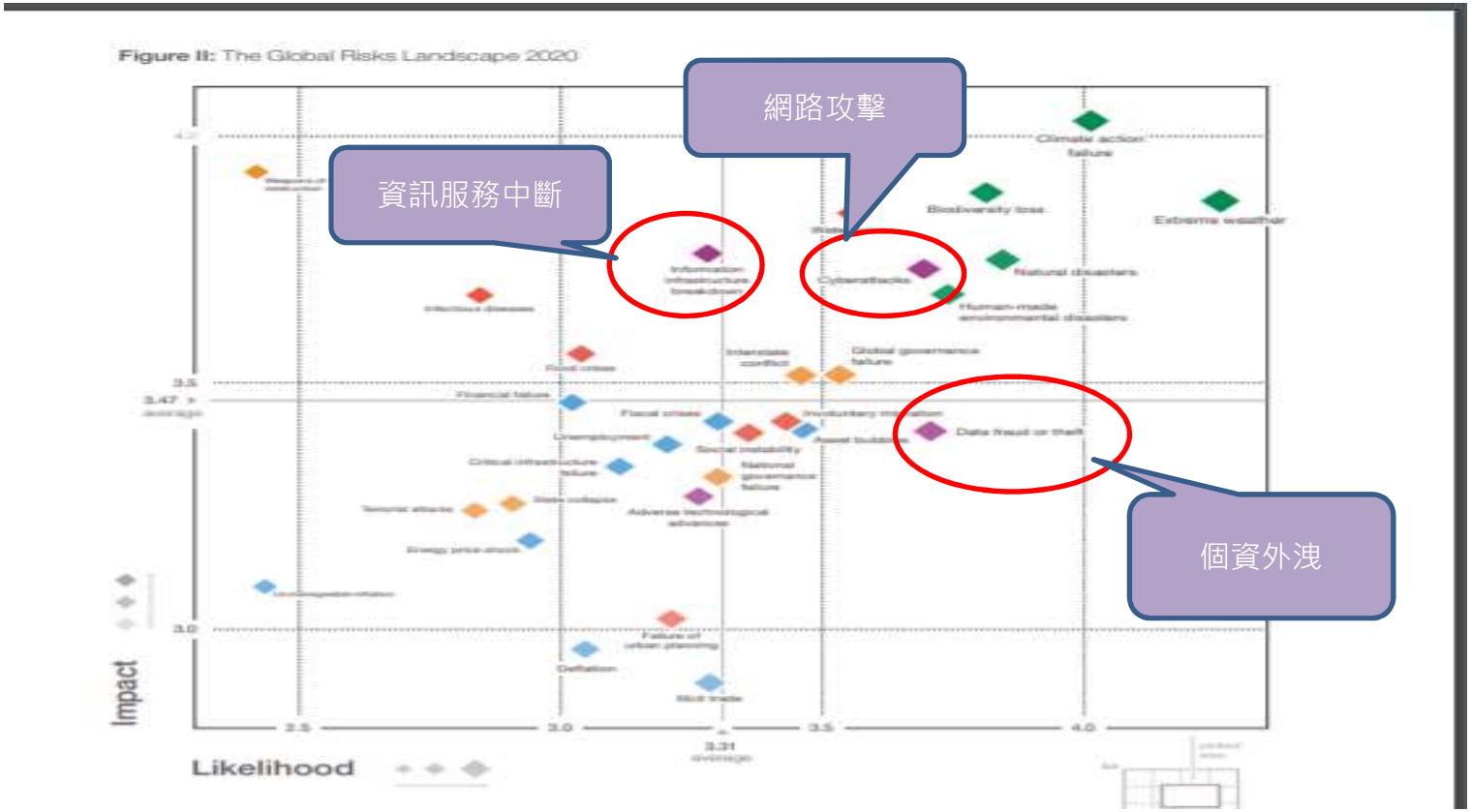
- **緣起**：
  - 金融科技創新改變金融業營運模式，提供客戶便利服務，同樣也帶來風險。
  - 資安威脅日益嚴峻，金融資安防護思維須更快速的調整因應
- **過程**：觀察國際金融資安情勢、國際金融資安監理趨勢，並檢討現行資安監理政策
- **方案**：訂定金融資安行動方案，以四年為期推動
- **目的**：提供民眾安心便利、穩定不中斷的金融服務，保護金融消費者的財產與隱私

二、資安威脅情勢(1/2)

- 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

二、資安威脅情勢(2/2)

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



三、國際金融資安監理趨勢(1/3)

重視經營管理階層資安職責、要求獨立資安職能

- 美國NYDFS-金融服務業網路安全要求規範(Part 500)：指定資安長，每年提交董事會決議或由資深主管簽署網路安全法遵聲明書。
- 美國FFIEC-資訊安全評估工具(CAT)：資安風險管理與監督列為五大評估面向之一，確保受董事會層級之監督。
- 歐盟EBA-資通科技及安全風險管理指引：隔離資安職能與資通作業流程相，定期直接向董事會報告，提供資訊安全及風險建議。
- 日本FSA-強化金融產業網路安全政策：強化高階管理人員的資安意識與積極參與，將網路安全問題提升至整個組織的經營與風險管理議題。

三、國際金融資安監理趨勢(2/3)

建立共通資安管理基準及自主評估機制

- 歐盟ESA-資通訊風險管理及網路安全聯名建議：透過修法使所有金融機構皆應遵循明確之規範，並提高各成員國資安規範之一致性。
- 歐盟EBA-資通科技及安全風險管理指引：涵蓋資安政策、資安職能、邏輯安全、實體安全、資通科技作業安全、資安監控、資安檢討、評估及測試、資安訓練及資安意識等各個面向。
- 新加坡MAS-網路安全通告：規範系統管理者帳號、弱點修補、系統安全基準、網路邊界防禦、惡意軟體防護及身分識別等控制措施。
- 美國FFIEC-資訊安全評估工具(CAT)：藉由比較資訊安全的風險與成熟度等級，找出資訊安全弱點，持續調和風險與強化內控之程序。
- 美國FED/OCC/FDIC-強化網路風險管理標準草案預告：分級管理，大型及功能性運作更重要之金融機構，採行更嚴格的標準。
- FED/OCC/FDIC、ESA、G7：加強第三方服務供應商之風險評估與委外管理。

三、國際金融資安監理趨勢(3/3)

建構並實證作業風險抵禦能力

- 英國BOE/PRA/FCA-建構英國金融業之作業風險抵禦能力之政策方向：辨識核心業務及設定可容忍中斷時間，並據以建立及實證其復原能力。
- 美國FFIEC-資訊安全評估工具(CAT)：網路資安事件之管理與復原為五大評估構面之一，確保準備度與資源配置，並受到監理機關及董事會之監督。
- 歐盟EBA/美國CFTC/G7/日本：加強金融機構因應資安事件之應變處置，支持以威脅驅動之滲透測試及駭客攻擊演練(Red Team Exercise)。
- 新加坡MAS-提升金融機構訂定營運持續管理計畫之標準，更重視跨營運部門之相依性，以及與外部服務供應商之連結。

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(1/2)

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

型塑重視資安的組織文化

董事會

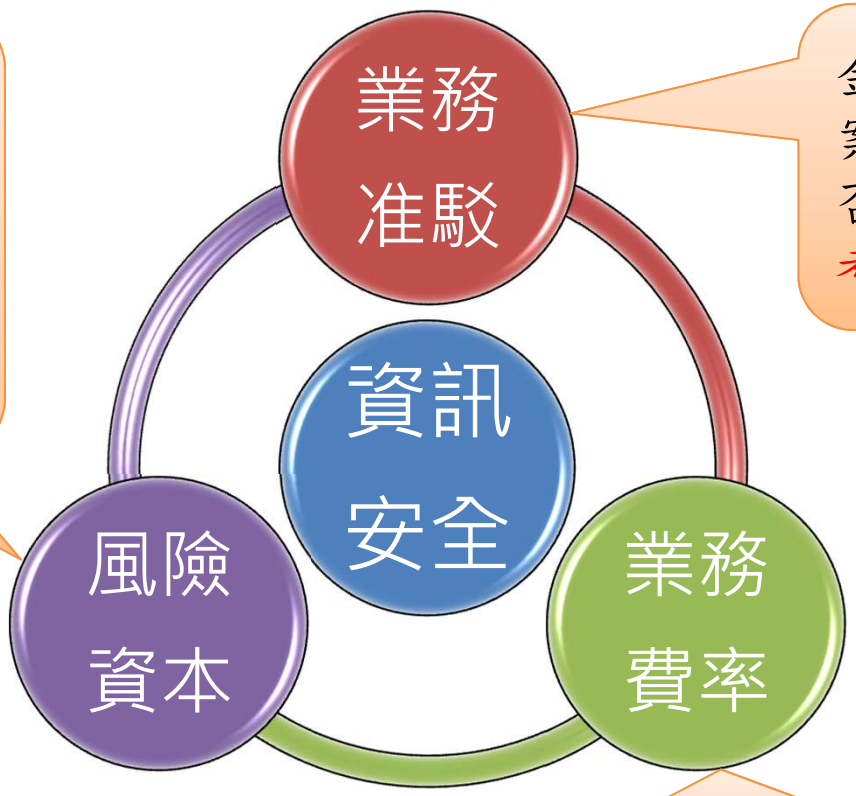
- 鼓勵遴聘具**資安背景之董事、顧問或設置資安諮詢小組**，增納專業人員參與董事會運作，帶動機構重視資安的組織文化

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

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

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

(一)強化資安監理(2/2)

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

鼓勵導入資安國際標準

- 鼓勵金融機構導入國際資安管理標準及國際營運持續管理標準，並取得相關驗證，透過第三方獨立機構檢視管理制度及持續營運之有效性。

金融監督管理委員會
Financial Supervisory Commission

推動金融資安治理成熟度

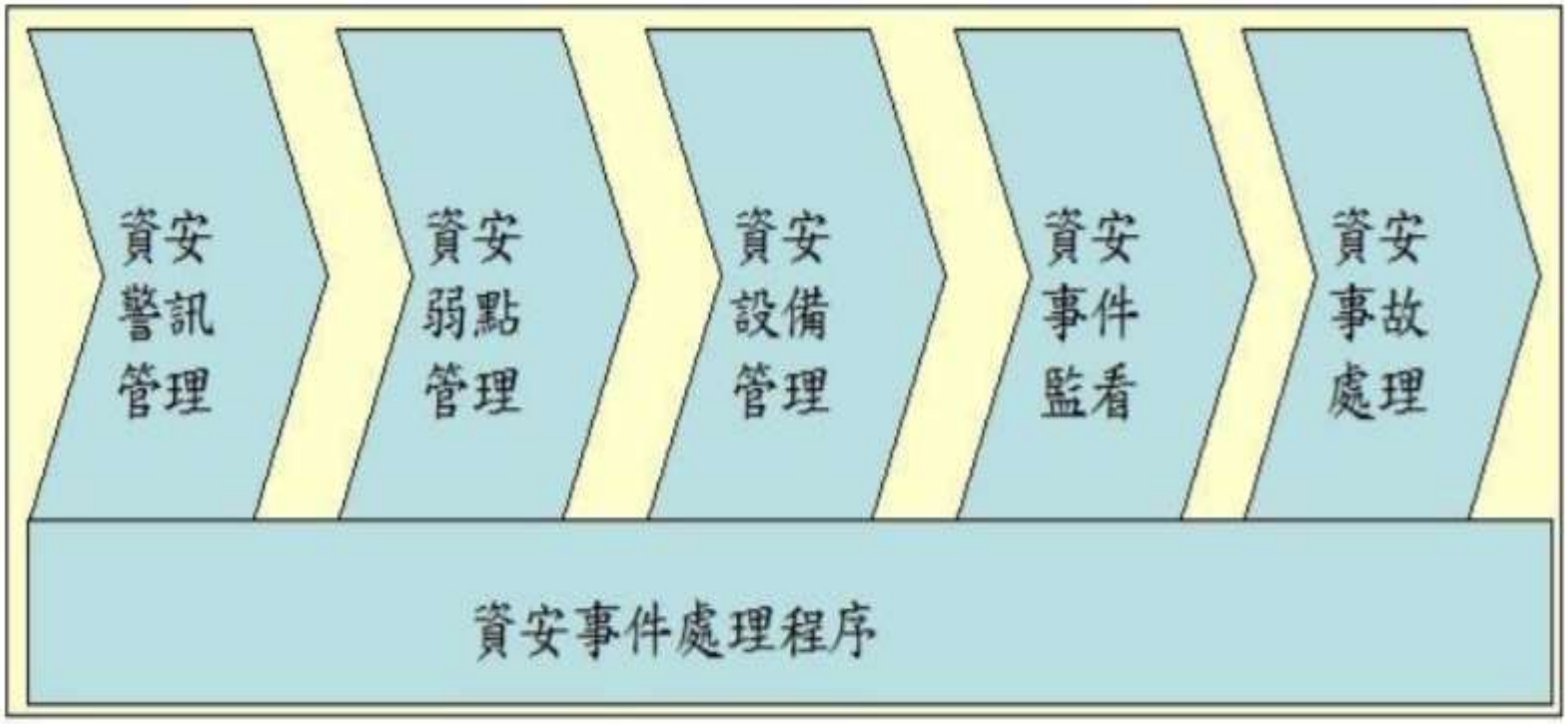
領域 *Domains*

- **網路風險管理與監督**
  包含資訊治理(Governance)、風險管理(Risk Management)、資源(Resources)、培訓與文化(Training and Culture)等4項評估因子。
- **威脅情資管理與合作**
  包含威脅情資(Threat Intelligence)、監測與分析(Monitoring and Analyzing)、資訊分享(Information Sharing)等3項評估因子。
- **網路安全管理**
- 包含預防(Preventative Control)、監測(Detective Control)、改善(Corrective Control)等3項評估因子。
- **委外及依賴關係**
  包含關係建立(Connections)、關係管理(Relationship Management)等2項評估因子。
- **網路事件管理與回應**
  包含事件處理策略(Incident Resilience)、偵測、回應與緩解(Detection, Response, & Mitigation)、升級與報告(Escalation & Reporting)等3項評估因子。

成熟度等級 *Maturity Levels*

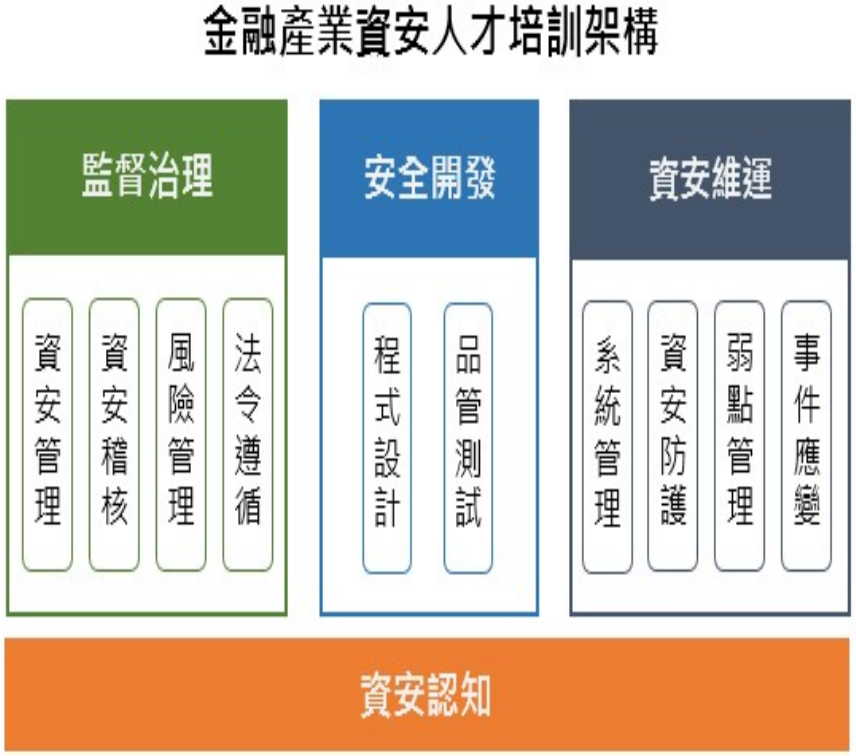
- **基本 *Baseline***
  達到法律及法規要求，或監理指引所建議的最低期望。此等級包括法規遵循目標，管理階層已審查且評估指引原則。
- **發展中 *Evolving***
  已訂定未明文要求之額外文件化程序和政策，組織已考量落實風險管理導向，網路安全責任已正式指派，且其保護範圍已擴及客戶資訊，包含整合資訊資產及系統。
- **中等 *Intermediate***
  已制定較詳細且文件化的程序，並高度落實。另已將風險管理實務及分析整合至企業營運策略。
- **進階 *Advanced***
  網路安全之實務及分析業以跨單位或跨業務方式進行整合。多數的風險管理流程已自動化，且包含持續性的流程改善。前線業務之風險決策責任已正式指派。
- **創新 *Innovation***
  為了組織及產業，藉由推動人員、流程及技術之創新以管理網路風險。此可能意味著需要發展新的控制措施、新的工具，或創造新的資訊分享平台。即時、預測性分析均與自動化回應相關。

鼓勵建置資安監控機制(SOC)



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



(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

增進營運持續管理量能

訂定災害應變運作、復原能力實證等作業韌性參考規範，作為業者遵循依據。

鼓勵金融機構於異地備援演練時，納入實際作業運作驗證。

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

建立關鍵資料保全避風港

資料保護

資料可移性

為提升金融機構客戶對金融系統對抗災難性事件的信心，參考美國推動之「避風港計畫」概念，研議資料保全運作機制，視研議結果評估推動方式，保護最關鍵資訊

資料復原性

關鍵服務持續性

金融監督管理委員會
Financial Supervisory Commission

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

(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。

資安情資分享與國際合作

多元化情資來源

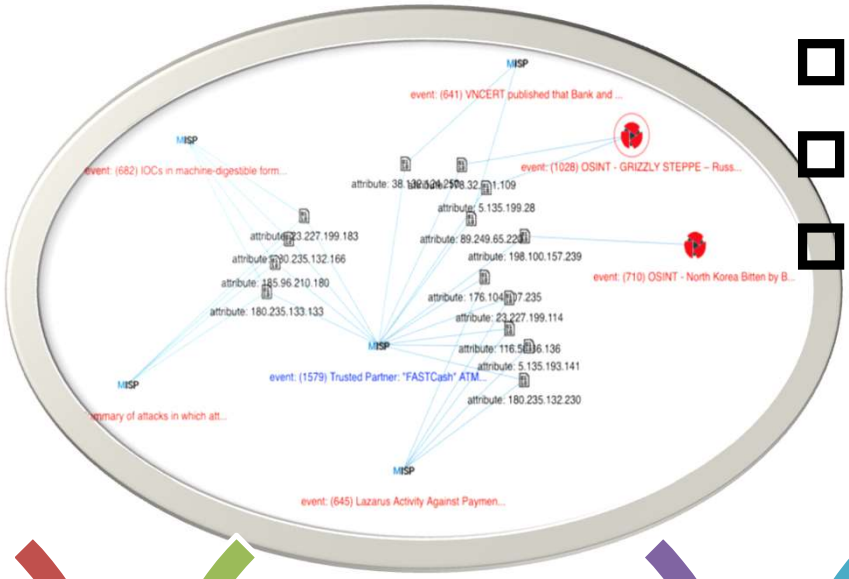
智能化情資分析

國際化情資合作

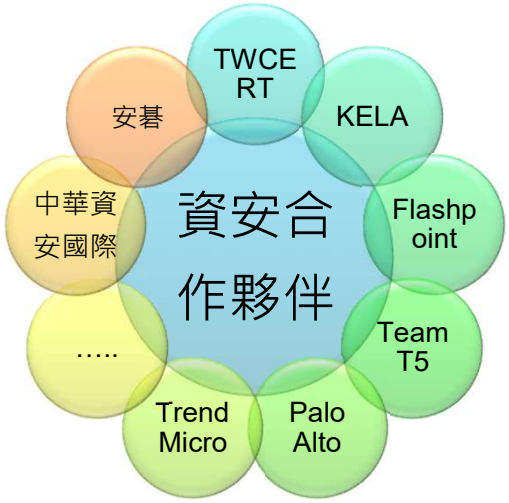
- 108年3月加入美國FS-ISAC會員
- 108年10月與日本F-ISAC簽署合作協議。
- 108年與歐盟FSI-SAC、以色列CERT-IL及南韓FSI建立情資交換管道

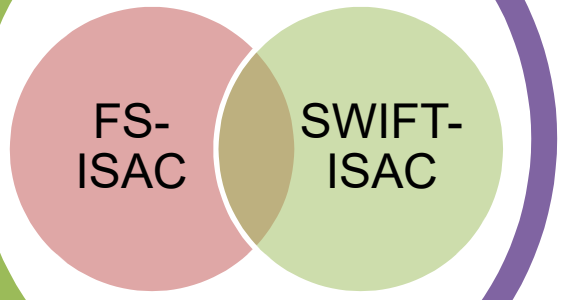
區間	弱點公告	威脅情資	定期週/月報	分析報告	合計
106.12~107	105	106	69	60	340
108年	36	156	63	50	305
109.1~109.6	20	121	32	6	179

智能化資安情資分析



- 多元化情資來源
- 智能化情資分析
- 國際化情資合作





國際金融-ISAC

美/歐/日/…

會員分享

建構資源共享的資安應變機制

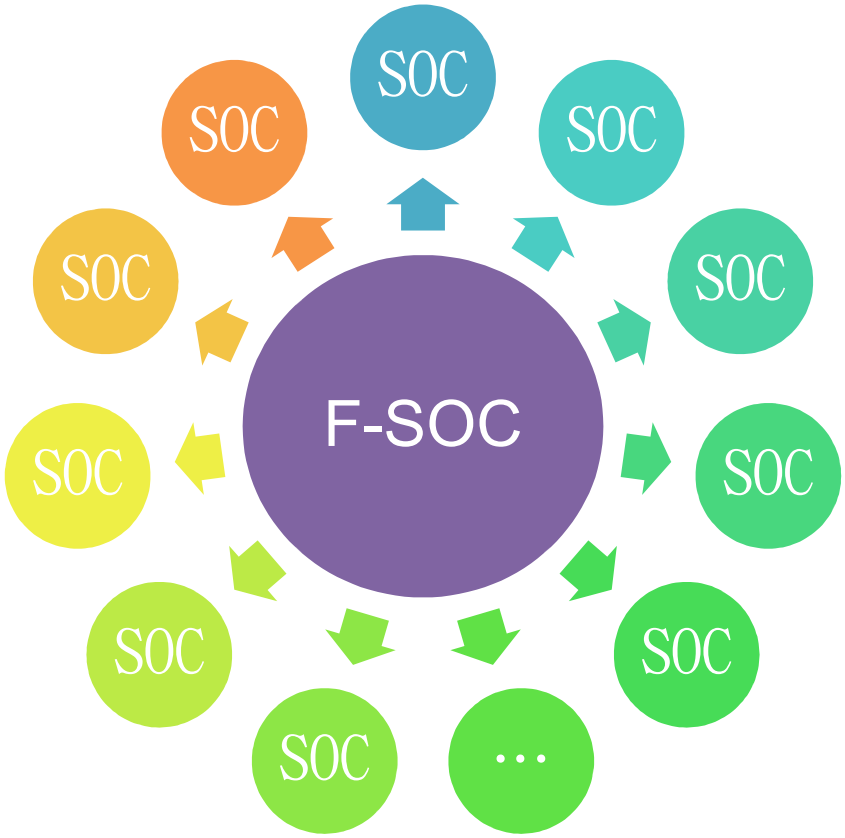
因應資安事件應變處理具高度時效要求，單一機構資源有其限制，建立資源共享的資安應變機制

- 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

建置金融資安監控協同體系

鼓勵金融機構自建資安監控機制(SOC)，及早發現網路異常行為，即時掌握資安風險

督導F-ISAC建置二線F-SOC及訂定資安監控作業標準，透過協同運作，有效監控整體資安風險，協助金融機構強化資安防護



五、推動作法(1/2)

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

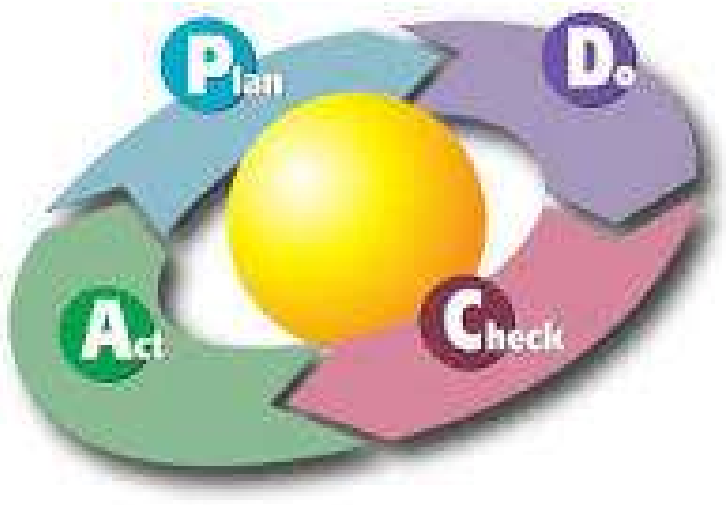
依不同業別、規模及業務，給予不同資安要求，循序推動

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

透過資源共享，建立情資分享、事件應變及監控體系

五、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工作計畫與執行進程。
- 自110年度起，每季、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。



六、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。