



## 金管會推動「金融資安行動方案」

2020/9/17

為強化金融業資安防護能力，達成安全、便利、營運不中斷目標，金管會已啟動「金融資安行動方案」計畫，透過「強化主管機關資安監理」、「深化金融機構資安治理」、「精實金融機構資安作業韌性」及「發揮資安聯防功能」4個面向，提出共計36項資安措施。除就現有資安措施再優化精進外，再規劃資安新思維方向，如推動一定規模金融機構或純網銀設置資安長，強化金融資安韌性，建立資安應變體系等。

金管會表示，將與周邊單位、各業公會及金融業者，分階段推動，每半年檢討成果，隨資安發展趨勢及實務運作情形，調整行動方案內容。本行動方案主要特色如下：

- 一、型塑金融機構重視資安的組織文化：為提升金融機構對資安議題之決策功能，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。並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。
- 二、強化新興科技的資安防護：為兼顧創新與安全之平衡，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，及因應金融服務委外及跨業合作發展，強化金融供應鏈體系風險評估與管理。建議公會增修訂資安自律規範，納入行動應用程式(APP)、雲端服務、開放銀行、Open API、網路身分驗證(eKYC)及資訊服務供應鏈之風險評估等當前關注議題，以配合金融科技發展與業務開放。



# 金融監督管理委員會 Financial Supervisory Commission

- 三、系統化培育金融資安專業人才：為強化金融機構資安人才能力建構，將依據金融資安職能需求訂定人才培訓地圖；協調周邊單位開設金融資安人才養成專班，與科技公司合作，充實師資及課程，透過產學合作、跨業合作，培育跨領域人才；並鼓勵金融資安人員取得國際資安證照，以培訓符合實務需要的資安人才。
- 四、深化資安情資分享與國際合作：為持續深化金融資安情資分享機制，除多元化資安情資來源外，將導入智能化情資分析方法，以人工智慧(AI)技術及大數據等分析技術提升情資分析效能，並擴大與國際資安機構合作交流，提升資安聯防整體效果，共同對抗國際駭客。
- 五、建構資源共享的資安應變機制：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，透過個別金融機構資安處理機制，加入金控集團資源、公會協力及 F-ISAC 聯防，建立資源共享的資安應變機制，協助業者資安應處。
- 六、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；並督導 F-ISAC 建置二線 SOC 及訂定資安監控作業標準，透過協同運作，以有效監控整體資安風險，協助金融機構強化資安防護。
- 七、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

八、落實復原應變運作機制：督導公會訂定災害應變運作、復原能力實證等作業韌性參考規範，作為業者遵循依據，並鼓勵金融機構於異地備援演練時，納入實際作業運作驗證。

為利行動方案推動，將依下列方式推動執行：

- 一、公私協力：透過公部門、金融周邊單位及各業別公會等，訂定相關管理規範標準、辦理資安人才培育、協力資安監控及應變，以協助金融機構提升資安防護能力。
- 二、差異化管理：針對各業別屬性、機構規模及業務風險等，分級規範適當的資安水準，兼顧金融機構實際資安防護業務需求及可執行性。
- 三、資源共享：賡續推動資安情資分享與合作、建立金融資安事件應變及監控體系，發揮資安聯防功能，並鼓勵金控或周邊單位(公會)建立資安事件應變小組，透過資源共享及合作，強化金融資安防禦能力。
- 四、激勵誘因：透過主管機關監理機制，如將資安風險因子納為業務准駁、資本計提、存款保險費率、保險安定基金費率之參考因子，引導金融機構主動積極執行資安措施。
- 五、國際合作：藉由加強與其他國家金融資安機構交流合作或簽定 MOU，掌握國際金融資安情勢，結合國際資安組織，共同對抗駭客。

金管會表示將持續提升金融機構資安防護能量，建構安全的金融服務發展環境，作為金融科技繼續發展之基礎，金融機構可運用新興科技發展金融業務，提供消費者安心、便利與多樣之金融服務。