金融資安行動方案 2.0 重要措施及成效

資料截至 113 年 12 月 31 日

目錄

壹、前言

金融業是高度利用資訊科技的產業，營業模式也因電子化、數位化、大數據及人工智慧的運用而轉變，客戶因為科技創新發展而享有極大便利。但隨著資安威脅日益嚴峻，金融資安防護的思維亦須更快速的調整因應，本會觀察國際金融資安情勢、國際金融資安監理趨勢，於 109 年 8 月 6 日發布「金融資安行動方案」，並因應業務發展與科技進步，經滾動檢討後，於 111 年 12 月 27 日發布「金融資安行動方案 2.0」，作為各金融機構及公會檢討資安策略、管理制度及防護技術等遵循的指引，以追求安全便利不中斷的金融服務。

金融資安行動方案 2.0 延續前期推動策略，分別從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、發揮資安聯防功能等四大構面切入，並以擴大適用、落實與深化、鼓勵前瞻為持續精進方向，提出 40 項資安措施。

本方案內容所涉面向廣泛，由本會整合相關資源，以三年為期循序漸進，並以公私協力、差異化管理、資源共享、激勵誘因及國際合作等方式推動執行，並每季檢討成果，隨資安發展趨勢及實務運作情形，調整行動方案內容。

貳、金融資安行動方案 2.0 重要措施辦理情形

一、 強化主管機關資安監理

（一）型塑金融機構重視資安的組織文化

1. 本會已要求金融機構應成立資安專責單位，將資安辦理情形定期提報董事會，另為提升金融機構對資安議題之決策能量，推動一定規模或電子交易達一定比例之金融機構設置副總經理層級以上之資安長，統籌資安政策推動協調與

資源調度。繼 110 年 9 月修正「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「保險業內部控制及稽核制度實施辦法」及「證券暨期貨市場各服務事業建立內部控制制度處理準則」，並發布相關令釋，要求所有本國銀行、資本額達新臺幣(下同)100 億元以上或電子下單比率符合一定條件之證券商、前一年度資產總額達 1 兆元以上之保險業設置資安長，本會於 113 年 1 月 4 日再修正相關函釋規定，推動證券商擴大設置資安長範圍，要求資本額 40 億元以上或電子下單比率符合一定條件之證券商設置資安長。截至 113 年底，已有 39 家本國銀行、26 家證券商及 11 家保險公司設置資安長。

2. 鼓勵金融機構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。截至 113 年底，已有 33 家金融機構遴聘具資安背景之董事、34 家金融機構聘有資安顧問、33 家金融機構設置資安諮詢小組。

3. 辦理董監事資安教育訓練課程，以增進董事會成員對資安情勢掌握，並實質將資安風險納入經營決策考量因子。本會周邊訓練機構 112 年度共開辦董監事資安課程 51 堂、受訓人數計 724 人次，113 年度開辦 41 堂課、受訓人數 677 人次。

4. 藉由定期召開資安長聯繫會議及重大資安事件情境應變演練等措施，研討當前資安情勢、推動策略及關鍵議題，以強化資安長職能。

（二）完備資安規範：督導金融同業公會增修訂資安相關自律規範，提供金融機構強化資安防護之準據，包括資通安全防

護基準、新興金融科技資安規範、供應鏈風險管理規範等項，並建立數位身分驗證等級與業務風險對照規範，以兼顧創新與安全之平衡，及符合實務需求。113 年度增修訂 8 項自律規範，包含：金融機構使用電子簽名機制安全控管作業規範、金融機構運用人工智慧技術作業規範、金融機構提供行動裝置應用程式作業規範、金融機構資通系統與服務供應鏈風險管理規範、金融機構作業委外使用雲端服務自律規範、證券暨期貨市場各服務事業網路安全防護參考指引、證券期貨市場相關公會新興科技資訊安全管控指引、保險業資訊安全防護自律規範等。

（三）加強金融資安檢查：金融資安檢查目的在驅策金融機構落實資安執行，為能快速因應金融服務資通訊環境及新興科技等之改變，本會每年定期檢視調整資安檢查重點，持續提升金融檢查之完整性及有效性。另為增進金融資安檢查之實效，本會並提供金融資安檢查人員與時俱進之專業訓練，持續提升資安檢查專業能力。

二、 深化金融機構資安治理

(一)加強資安管理：

1. 推動金融機構導入國際資安管理標準：為使金融機構於既有資安規範之遵循外，也能從整體面檢視資訊安全管理制度，建立良性改善循環，並借助第三方獨立機構找出執行盲點或驗證有效性，本會規劃請相關公會依業別特性，訂定各業別國際資安管理標準驗證之範圍，並推動一定規模或電子交易達一定比例之金融機構導入國際資安管理標準及取得相關驗證。截至 113 年底，已有 38 家銀行、22 家證券商及 37 家保險公司取得國際資安管理標準驗證。

2. 推動金融資安治理成熟度評估：本會已參考美國 FFIEC 重複量測工具(CAT)，調適訂定適用我國金融機構之資安治理成熟度評估方法，並鼓勵金融機構據以依其自有特性，自主風險評估其資安弱點，並持續強化其資安管理。截至 113 年底，已有 34 家銀行、20 家證券商及 27 家保險公司辦理評估作業。

(二)強化資安監控與防護

1. 推動建置資安監控機制(SOC)：對網路異常行為偵測告警之即時性及有效性，攸關其是否進階為資安事件及其後續災損控管，本會推動金融機構建置資安監控機制，扮演資安防護「防微杜漸」的關鍵角色，進而積極走向主動防禦。截至 113 年底，已有 39 家銀行、35 家證券商及 35 家保險公司建置資安監控機制。

2. 鼓勵辦理資安監控與防護有效性評估：資安監控與防護重在早期發現處置與防護網之綿密，惟純粹以守方思維，難免掛萬漏一，爰鼓勵已建置 SOC 並達一定規模之金融機構引入攻擊方思維，定期藉由網路攻擊手法，如 DDoS 攻防演練、紅藍隊演練、入侵與攻擊模擬等，檢驗資安監控及防禦部署之有效性。113 年度金融機構辦理入侵與攻擊模擬(BAS)計 39 家、DDoS 攻防演練 83 家、紅藍隊演練 39 家。

3. 鼓勵零信任網路部署一節：本會於 113 年 7 月 15 日發布「金融業導入零信任架構參考指引」，提供金融機構規劃/導入零信任架構參考。

(三)加強資安人才培育

1. 為利招募資安人才投入金融領域，並促使金融機構有計畫的培訓資安人才，本會依據金融資安職能需求，於 110 年 6 月 23 日發布金融資安人才職能地圖，並因應實務需求於 113 年 4 月 12 日修正職能地圖，俾提供金融機構、周邊單位及訓練機構參考運用。

2. 協調周邊訓練機構依據金融資安人才職能地圖及實務需求，開設金融資安人才養成專班，以利金融資安人員精進資安防護知能。本會周邊訓練機構 112 年度開辦 147 堂相關課程、受訓人數計 5,604 人次，113 年度開辦 109 堂課、受訓人數 3,593 人。

3. 鼓勵金融機構配置多元專長資安人員及取得國際或專業訓練機構核發之資安證照(書)，以完備機構內資安維運所需，強化金融機構防護能量，並利於金融資安人才之職涯發展。截至 113 年底，已有 39 家銀行、63 家證券商及 38 家保險公司聘有持國際資安證照之資安人員，計有 1,162 人取得國際資安證照，共取得 2,316 張國際資安證照。

三、精實金融機構資安作業韌性

(一)增進金融機構營運持續管理量能

1. 訂定強化作業韌性參考規範：金融服務資訊系統的破壞或癱瘓，可能影響民眾信心致危及金融穩定，本會參考英美歐等強化風險管理與作業風險抵禦能力等政策方向，請各業別同業公會依業別屬性訂定作業韌性參考規範，包含核心業務之識別、最大可容忍中斷時間之設定，災害應變之運作、壓力測試、復原能力之實證等，以利金融機構據以評估及強化其作業韌性，於時效內回復核心業務運作。

2. 鼓勵金融機構導入國際營運持續管理標準：為讓國際間對營運持續管理有共通語言及完整框架可供遵循，國際標準組織已訂有以營運持續管理為主題之國際標準，本會鼓勵金融機構導入國際營運持續管理標準，參採最佳實務做法，透過第三方獨立機構驗證符合來自內部、法規、及客戶的各種要求，並據以向利害關係人溝通其面臨衝擊之準備。截至 113 年底，計有 19 家銀行、8 家證券商及 17 家保險公司取得國際營運持續管理標準驗證。

3. 鼓勵實際作業之營運持續演練：為實證金融機構異地備份與備援環境運作機制於關鍵時刻能有效運作，爰規劃請公會依據行業特性訂定核心業務系統備援指引，以提供金融機構遵循，並鼓勵金融機構於異地備援演練時，納入實際業務運作驗證。截至 113 年底，計有 24 家銀行、41 家證券商及 19 家保險公司辦理實際作業之營運持續演練。

(二)加強資安演練：參考歐美等以滲透測試及駭客攻擊演練加強金融機構因應資安事件之應變處置之政策方向，參酌國際資安情勢駭客常用攻擊手法，並延續本會近年與行政院合辦或自辦之資安演練成效，規劃透過資安演練實證金融機構因應攻擊之防禦能量與應變能力，並據以督促金融機構資安實戰能量之提升。112 年及 113 年辦理 DDoS 攻防演練、網路攻防演練課程、金融資安攻防評比活動及重大資安事件應變情境演練等活動。

四、發揮資安聯防功能

(一) 資安情資分享與合作

1. 本會督導財金資訊股份有限公司持續營運 F-ISAC，加強情資分析之深度及廣度，賡續提供金融機構金融資安資

訊分享與分析、金融電腦緊急應變、金融資安聯防監控等服務，強化金融資安聯防功能。截至 113 年底，F-ISAC 會員數達 329 家，本會所管之重要金融機構均已加入 F-ISAC。

2. 為深化與會員間之情資分析與交流，以利及時提供更為精確完整的早期預警與資安防護建議，F-ISAC 鼓勵各金融機構積極分享相關情資，113 年度，F-ISAC 發布 510 則情資，其中源自會員分享情資經 F-ISAC 研析發布者計有 357 則，達 70%，有效建立 F-ISAC 與會員間互信及雙向情資分享機制，發揮資安聯防功能。

3. 加強金融資安國際合作：全球主要國家相繼設立金融資安資訊分享與分析機構，F-ISAC 成立後已先後加入美國 FS-ISAC 會員、出席歐盟 FI-ISAC 年會、與日本 F-ISAC 簽訂 MOU 等，因應網路攻擊無國界與掌握國際金融資安情勢之需，F-ISAC 於 110 年續與泰國 TB-CERT 簽訂 MOU，於 111 年成為資安事件應變及安全小組論壇(FIRST)之會員，於 112 年加入亞太地區電腦網路危機處理聯合組織(APCERT)，持續加強與其他國家金融資安機構交流合作。

(二)建立金融資安事件應變體系：考量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，本會推動金控集團、同業公會、證券暨期貨市場電腦緊急應變支援小組(SF-CERT)及金融資安資訊分析分享中心(F-ISAC)等建構資安事件應變支援體系，以協助個別金融機構之資安事件應處。

(三)建立金融資安監控體系：除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，即時掌握資安風險外，並督導 F-ISAC 建置聯防 SOC 及訂定資安監控作業標準，推

動金融機構導入資安監控組態基準及作業指引，強化金融機構資安監控中心與聯防監控中心協同運作機制，建立金融資安事件監控體系，即時有效關聯分析整體資安風險，強化金融機構資安防護，發揮資安聯防功能。截至 113 年底，共有 62 家金融機構參與聯防 SOC 運作。

參、結語

本會將推動金融機構強化資安防護列為重要政策之一，並偕同金融周邊單位、各金融同業公會與金融機構等，共同積極執行「金融資安行動方案 2.0」，引導金融資安持續精進，以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，並利金融機構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。