金融資安行動方案

2.0

金融監督管理委員會
中華民國 111 年 12 月

版次	摘　　要	發行/修訂生效日期
V1.0	訂定金融資安行動方案	109/08/06
V2.0	因應資安情勢、監理趨勢及執行成效等滾動檢討，依據精進方向增修執行措施。	111/12/27

目錄

壹、緣起

全球金融科技蓬勃發展，運用新興科技創新金融業務，借助數位化提供多元服務管道、提升客戶體驗、增強客戶關係，進而開創新興服務模式，已成為金融機構主要策略，而新冠疫情更加速金融機構數位轉型的發展。金融監督管理委員會（以下簡稱金管會）因應數位時代潮流，亦持續推動數位服務的開放與創新，包含開放設置純網路銀行、純網路保險、網路申辦金融業務之鬆綁、分階段推動開放銀行(Open Banking)等，期偕同金融機構善用數位科技，提供民眾更便捷的金融服務，提升金融服務品質。

於金融科技快速發展、金融服務創新開放的同時，資通安全也面臨嚴峻的挑戰，2017 年 3 月 G20 財長與央行總裁會議宣言中特別提出，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[1]。世界經濟論壇「2022 年全球風險報告」[2]亦指出，隨著數位系統廣泛使用及日漸複雜，不斷擴大的網路威脅正超過目前有效預防及管理的能量，攻擊門檻降低，甚至非技術人士也能使用惡意軟體進行攻擊。駭客的攻擊早已朝向系統化與組織化，甚至是企業化的黑色產業鏈，一旦受駭所帶來的衝擊較之諸往更鉅。

金管會於 109 年 8 月鑒於資安威脅日益嚴峻，觀察國際金融資安情勢、國際金融資安監理趨勢，並檢討當時資安監理政策，於 109 年 8 月發布「金融資安行動方案」，推動迄今已逾兩年，雖達主要績效指標，惟考量期間歷經新冠疫情驅動數位轉型、資安情勢加劇、重大災害及地緣政治等風險，推升金融資安韌性的重要性，爰滾動檢討金融

[1] https://www.bis.org/bcbs/publ/d454.htm
[2] https://www.weforum.org/reports/global-risks-report-2022/

資安行動方案，擴大及精進各項推動措施，以於賡續推動金融機構數位轉型、發展及運用金融科技、創新與開放金融服務的同時，能確保提供民眾安心便利、穩定不中斷的金融服務。

貳、 金融資安的威脅與挑戰

資安事件時有所聞，受駭者不乏國際知名大型機構，金管會亦持續蒐集資安情資並關注資安情勢的發展，綜觀近期金融資安情勢摘要如下：

一、國際頻傳遭駭事件，金融機構仍為眾所矚目標的

駭客藉由攻擊金融機構資訊系統竊取金錢，近年亞洲與歐美等均陸續傳出跨國電匯(SWIFT)系統遭盜轉、ATM 遭盜領等資安事件，駭客以系統化之攻擊策略，逐步探索出目標的脆弱點，攻擊手法除利用社交工程之外，還可利用資通訊及物聯網設備安全漏洞進行攻擊、撞庫攻擊及偽冒簡訊等，結合多階段攻擊等方式進行入侵，單一受駭事件甚至橫跨多個地區與國家。

另外，金融機構遭駭致帳戶等個資外洩、遭勒索軟體及分散式阻斷服務(DDoS)攻擊勒索金錢利益等事件亦時有所聞，顯示金融機構為受關注之對象。

二、資安管理仍待持續強化與落實，供應鏈成為攻擊跳板

研析近年金融機構資料外洩案例，多肇因於人員資安意識不足與資安管理未落實。駭客組織多數利用搜尋工具（如 Shodan），查找於網際網路上未做好安全管控之對外服務系統及資料庫，並利用暴力破解、

社交工程竊取、利用離職員工握有帳號密碼、或於暗網購得帳號密碼等手法，進行入侵並竊取敏感性資料，包含內外網路架構、存取控制及資料傳輸等，若未能落實控管，均會造成資安防護破口。

此外，金融機構為加速數位化的進程，越來越倚賴委外廠商或供應商；金融資訊服務亦不再侷限於單一機構，跨機構提供資訊服務之作業模式(如雲端服務、行動支付等)，亦成為駭客組織找尋資安防護脆弱點標的，以委外廠商、軟硬體供應商為跳板攻擊的案例逐漸增多，資安防禦陣線之延伸將是資安管理應積極面對的課題。

三、具針對性攻擊潛伏期長影響大，防禦難度倍增

近兩年勒索攻擊猖獗，國際多家金融機構遭到勒索攻擊導致客戶敏感資料外洩或是無法提供服務。美國重要油品業者遭駭導致短期間無法正常供油影響該國民生，我國亦有關鍵基礎設施及多家科技大廠受到攻擊等案例。

依近期國內外大型機構遭到勒索軟體攻擊，影響其營運並產生巨額營業損失之案例，事後鑑識均發覺係針對受駭機構資通訊環境特製之惡意程式及攻擊手法，且會避開受駭機構之防毒軟體等資安防護設備之偵測，入侵後長期潛伏等待最佳時機發動最後攻擊，一旦攻擊成功即造成嚴重影響，如無法維持正常業務運作，或營業資料滅失等。

金融資安事件難以完全避免，相對考驗的不僅是事前防禦，還有事中之緊急應變及事後之災害復原能力，以因應攻擊時能有效應變處置及迅速復原，降低

遭受攻擊之營運損失。

四、專業金融犯罪組織持續活動，防禦方相對勢單力薄

現今的駭客已少是單打獨鬥，而是有組織的朝向專業化及國際化發展，如 FireEye、Trend Micro、美國 FS-ISAC 等專業資安單位發布之報告，均觀察到有多個特定國際金融犯罪組織持續於各個重大金融資安事件扮演要角，並且是有規模、有計畫的發動攻擊，每次攻擊受影響的對象亦非侷限於單一機構。類此特別駭客組織的活躍、型態改變及專業技術的提升，造成金融機構資安風險大幅增加。

金融機構之資安防護如仍獨善其身，缺少橫向訊息溝通管道，相對於專業駭客組織的攻擊將更顯勢單力薄。

五、新冠疫情加速金融機構數位轉型，伴隨資安風險增加

新冠疫情自 2020 年以來襲捲全球，不僅衝擊全球的經濟，也改變生活與工作型態，帶動宅經濟、零接觸經濟的發展，並促使企業數位轉型。

金融機構於疫情期間調整相關營運作業方式，包含居家辦公、分區或異地辦公等。同時也觀察到攻擊方利用疫情大肆攻擊，包含偽冒客戶聯繫居家辦公同仁進行詐騙轉帳、藉由人工智慧(AI)技術進行深度偽冒詐騙 (DeepFake)、結合釣魚郵件及語音釣魚等社交工程攻擊手法進行詐騙等。

金融業是高度利用資訊科技的產業，新冠疫情更加速金融機構數位化進程，伴隨金融科技發展與業務開放，行動應用程式 (APP)、雲端服務、開放銀行、Open

API、eKYC 等多涉及資訊服務供應鏈與第三方服務供應商，其跨機構及跨業之資安風險評估與管理，更是應關注的重要議題。

六、觀察國際衝突情勢，網路攻擊已成關鍵攻防領域

2022 年 3 月發生俄烏戰爭，俄羅斯針對烏克蘭政府資料中心發動飛彈攻擊，並對烏克蘭電腦進行資料刪除、分散式阻斷服務(DDOS)等攻擊，企圖中斷烏克蘭金融、能源等國家關鍵基礎設施；甚至透過深偽技術(DeepFake)合成國家元首散布假影片，進行認知作戰。可以觀察到現代化戰爭已是實體軍事活動及網路攻擊破壞併行，網路攻擊所帶來的風險及損害亦不容忽視。

有鑒於金融事業係支撐國家經濟、穩定民生運作重要之關鍵基礎設施，爰金融資料的備份保全存放、防範大規模網路攻擊，均應持續研議推動。

參、 國際金融資安監理趨勢

因應金融資安威脅，對金融機構的資安監理也成為歐美等金融監理機關的重要議題，並陸續發布相關規範、草案或討論文件等，要求金融機構從各個面向加強資安防護。金管會持續關注國際間資安監理相關強化措施與趨勢，彙整摘要如下：

一、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)於 2017 年發布「金融服務業網路安全要求規範(23 NYCRR Part 500)」[3]，目前為美國金融監理機關唯一之法律層級的

[3]https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

防範網路攻擊之資通安全規範，要求金融機構應指定資安長負責執行、監督、強化新採行之計畫及政策，並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。美國聯邦金融機構檢查委員會(FFIEC)於 2017 年更新之資通安全評估工具(Cybersecurity Assessment Tool, CAT)[4]，亦將資安風險管理與監督列為五大評估面向之一，以確保該等評估受董事會層級之監督。

美國網路安全及基礎設施安全局（CISA）於 2022 年成立資安指引入口網站 Shields Up[5]，提供企業適用的資安指引，及近百項可運用的免費網路工具與服務，並對企業高階主管與執行長提供建言，其中包含應授權資安長參與公司風險的決策過程，以確保全體組織了解安全面向的投資是首要的。

歐洲銀行監理總署(EBA)於 2019 年發布「資通科技及安全風險管理指引」[6]，要求金融機構應將資安職能與資通作業流程相隔離，以確保其獨立性與客觀性，並監控資安政策與措施之落實情形，定期直接向管理部門（董事會）報告，依實際需要不定期提供有關資通安全及金融機構風險之建議等。

在亞洲，日本金融廳(FSA)於 2018 年修正「強化金融產業網路安全政策」[7]，特別提出應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。新加坡金融管理局

[4] https://www.ffiec.gov/cyberassessmenttool.htm
[5] https://www.cisa.gov/shields-up
[6] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
[7] https://www.fsa.go.jp/en/news/2019/20190115/cyber-policy.pdf

(MAS)於 2021 年修正發布「技術風險管理指引」[8]，明訂董事會和高階管理層應確保任命具有必要經驗和專業知識的資訊長和資安長，負責管理技術和網路風險；董事會應具有相關知識的成員，以對技術和網路風險進行有效監督。

二、建立共通資安管理基準及自主評估機制

歐盟銀行、保險、證券三大金融監理機關(ESA)於 2019 年發布聯名建議(Joint Advice)[9]，建議透過修法強化歐盟金融業之資通訊風險管理及網路安全規範，其政策目標係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。歐洲 EBA 於 2019 年底發布「資通科技及安全風險管理指引」[10]，規範涵蓋資安政策、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 於 2019 年公布「網路安全通告」[11]，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 採可重覆量測的金融機構資通安全評估工具(CAT)，辨識其風險並決定其資安準備度，框架包含資安風險管理與監督、威脅情報與合作、資通安全控管、外部供應商管理、網路資安事件之管理與復原等，藉由比較資通安全的風險與成熟度等級，

[8] https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
[9] https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk
[10] https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
[11] https://www.mas.gov.sg/regulation/notices/notice-655

找出資通安全弱點，持續調和風險與強化內控之程序。

美國聯準會(FED)、通貨監理署(OCC)、聯邦存款保險公司(FDIC)於 2016 年聯合發布「強化網路風險管理標準」草案預告[12]，揭示分級強化資安標準之方向，並擬從網路風險治理、網路風險管理、內部依存管理、外部依存管理及資安事件處理、網路韌性、情境意識等 5 面向制定應強化之資安標準，對大型及功能性運作更重要之金融機構，採行更嚴格的標準。

此外，前揭草案預告、歐盟 ESA 發布之聯名建議、以及七大工業國組織(G7)於 2018 年發布「金融業對委外廠商之資安風險管理基礎要素」[13]等，不約而同提出應加強第三方服務供應商之風險評估與委外管理，是應持續關注及強化資安管理之課題。

三、建構並實證作業風險抵禦能力，強化營運韌性

歐盟委員會於 2020 年發布數位營運韌性法案(Digital Operational Resilience Act,DORA)草案[14]，以強化歐洲金融機構對資通訊技術(ICT)相關事件的抵禦能力。該法案提供完整的數位營運韌性之框架，對於營運於金融領域網路及資訊系統的公司和組織，以及為其提供 ICT 相關服務（如雲平台或數據分析服務）之關鍵第三方，訂定一致性要求，包含：ICT 風險管理、ICT 相關事件管理、數位營運韌性測試、ICT 第三方風險管理、資安情資共享等。

[12]https://www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards

[13]https://www.bundesbank.de/resource/blob/764692/01503c2cb8a58e44a862bee170d34545/mL/2018-10-24-g-7-fundamental-elements-for-third-party-cyber-risk-data.pdf

[14]https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/

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 2021 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」[15]，要求金融機構自行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，再由監理機關以壓力測試考核其落實情形。

美國 FFIEC 則將網路資安事件之管理與復原列為其資通安全評估工具(CAT)五大評估面向之一，以確保其資通安全之準備度與資源配置，可因應其作業風險，並受到監理機關及董事會之監督。FED、OCC、FDIC 聯合發布之「強化網路風險管理標準」草案預告亦要求適用機關應加強網路恢復能力，並建立整體企業之資安事件回應機制。

另於加強金融機構因應資安事件之應變處置，歐盟 EBA「資通科技及安全風險管理指引」要求金融機構應支持滲透測試及駭客攻擊演練(Red Team Exercise)；美國商品期貨交易委員會(CFTC)於 2016 年修正「網路安全能力測試準則」[16]，要求受監理機構進行弱點測試、滲透測試、控制測試、資安事件處理計畫測試及企業科技風險評估等 5 種類型之測試。G7 於 2018 年亦發布「以威脅驅動之滲透測試基礎要素(TLPT)」[17]，供主管機關及金融機構規劃與執行之參考。

於亞洲，日本 FSA「強化金融產業網路安全政策」

[15] https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

[16] https://www.cftc.gov/About/CFTCOrganization/NFACybersecurityGuidance083118

[17] https://www.cftc.gov/sites/default/files/idc/groups/public/@newsroom/documents/file/syssafeguard_factsheet090816.pdf

也將攻防演練作為提升金融機構因應網路攻擊能力之重要工具，並將持續分析真實攻擊樣態、結合外部專家，讓演練更擬真化；也將研議辦理攻擊範圍包含大範圍公用基礎設施的複合情境跨域演練。另新加坡 MAS 分別於 2021 年、2022 年修正「技術風險管理指引」及「營運持續管理指引」[18]，目的均在強化金融機構作業韌性，技術風險增列網路監控、安全軟體開發、惡意攻擊模擬、物聯網風險管理等議題。營運持續管理指引更著重提升金融機構訂定營運持續管理計畫之標準，重視跨營運部門之相依性，以及對第三方服務供應商進行嚴格監督；另也鼓勵金融機構有獨立的稽核計畫，定期審查營運持續管理計畫之有效性。

四、因應資安威脅，持續提升資安防護及其有效性評估

美國國家標準暨技術研究院(NIST) 2020 年推出 SP 800-207 零信任標準後，美國總統在 2021 年 5 月發布行政命令「改善國家的網路安全」[19]要求聯邦政府應落實現代化的網路安全標準，遵循零信任架構，以強化政府鑑識威脅。新加坡 2021 網路安全策略，政府鼓勵關鍵資訊基礎設施(CII)服務提供者對關鍵系統採取零信任網路安全[20]。

FFIEC 於 2021 年修正「對金融機構服務及系統之身分驗證與存取之指南」[21]，為金融機構之客戶、員工及第三方機構於存取數位銀行服務及資訊系統時，提

18 https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management

19 https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

20 https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021

21 https://www.ffiec.gov/press/pr081121.htm

供身分驗證及存取之風險管理原則與實務案例，以因應網路安全威脅對金融機構持續帶來的重大風險，並加強金融機構有效驗證、控制用戶及客戶存取金融服務及系統資訊。

歐洲系統風險委員會(ESRB)2022 年 1 月向歐盟三大監管機構（ESA）提議[22]，呼籲應制定應變框架(EU-SCICF,Pan-European systemic cyber incident coordination framework)，以便在因應可能對歐盟金融體系造成系統性影響的重大跨境網路事件時，能夠於泛歐展開有效的溝通協調。

法國審慎監理暨清理局(ACPR)、法國央行(BdF)與新加坡 MAS 於 2022 年 6 月 17 日共同發布聯合聲明，進行跨境資安危機管理測試，由三個跨國金融監理機關聯合辦理，透過有效資訊共享機制，迅速因應跨境營運金融機構之重大資安攻擊，以提升營運韌性及全球金融穩定。

肆、 金融資安推動現況

109 年 8 月金管會發布金融資安行動方案，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個面向切入，提出 36 項資安措施。經整合相關資源，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，迄 111 年第 3 季推動辦理情形如下：

[22] https://www.eba.europa.eu/esas-welcome-esrb-recommendation-create-pan-european-systemic-cyber-incident-coordination-framework

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. 金管會已要求金融機構應成立資安專責單位，並將資安辦理情形定期提報董事會，惟為提升金融機構對資安議題之決策能量，推動一定規模機構及純網銀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。金管會於 110 年 9 月間陸續修正「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，要求銀行業及符合一定條件之保險公司、證券期貨各服務事業，應於 111 年 3 月底前指派副總經理以上或職責相當之人兼任資安長，綜理資訊安全政策推動及資源調度事務。截至 111 年第 3 季已有 40 家本國銀行、21 家證券商及 12 家保險公司，共計 73 家重要金融機構設置副總經理層級以上之資安長。

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 111 年第 3 季已有 24 家金融機構遴聘具資安背景之董事、22 家金融機構聘有資安顧問、21 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。110 年至 111 年第 3 季止，金管會周邊訓練機構共開辦董監事資安課程 77 堂，受訓人數計 1,507 人次。

(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，以兼顧創新與安全之平衡，並符合實務需求。110 年至 111 年第 3 季增修訂之自律規範或參考指引計有：修訂金融機構辦理電子銀行業務安全控管作業基準(新增電信認證網路身分驗證機制)、金融機構使用物聯網設備安全控管規範、保險業資訊安全防護自律規範及證券期貨市場相關公會新興科技資通安全自律規範，增訂金融機構資通安全防護基準、保險業資訊作業韌性參考原則、證券暨期貨市場各服務事業資通系統安全防護基準參考指引、網路安全防護基準參考指引、供應鏈風險管理參考指引、作業韌性參考指引等項。

(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，金管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，金管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) 鼓勵導入資安國際標準：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及驗證有效性，金管會鼓勵金融機構導入國際資

安管理標準及取得相關驗證。截至 111 年第 3 季，已有 32 家銀行、17 家證券商及 38 家保險公司取得國際資安管理標準驗證。

(二) 推動金融資安治理成熟度評估：資安規範係奠基於可共通遵循之防護基準，更積極的面向係藉由自我評估資安風險，持續精進資安管理，特別是大型及具重要功能性之金融機構，應於防護基準上有更嚴格的標準。金管會督導金融資安資訊分享與分析中心(下稱 F-ISAC)參考美國 FFIEC 量測工具(CAT)，調適訂定適用我國金融機構且可重複量測之金融資安治理成熟度評估工具，並鼓勵金融機構據以依其自有特性，自主風險評估資安弱點，持續強化資安管理。F-ISAC 並於 109 年至 111 年，分別輔導銀行業、保險業及證券業辦理自我評估作業，截至 111 年第 3 季止，已有 40 家重要金融機構辦理金融資安治理成熟度評估。

(三) 鼓勵金融機構建置資安監控機制(SOC)：對網路異常行為偵測告警之即時性及有效性，攸關其是否惡化為資安事件及後續需進行災損控管，金管會鼓勵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 111 年第 3 季，已有 34 家銀行、28 家證券商及 29 家保險公司建置資安監控機制。

(四) 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，金管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，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，以利金融資安人員提升資安防護知能。110 年至 111 年第 3 季，金管會周邊訓練機構已開辦 163 堂相關課程，受訓人數計 6,399 人次。

3. 鼓勵金融資安人員取得國際資安證照，以引導金融機構重視資安人員之資格能力，並利於金融資安人才之職涯發展。截至 111 年第 3 季止，已有 40 家銀行、25 家證券商及 39 家保險公司聘有持國際資安證照之資安人員，計有 785 人取得共 1,398 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，可能從而影響民眾信心致危及金融穩定，金管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，金管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 111 年第 3 季，計有 10 家銀行、3 家證券商及 7 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：為於區域性災損時可維持核心業務運作，金融機構多已建置異地備份與備援環境，惟異地之切換涉及內部資源人力等之配置調度、外部夥伴之協同作業及資訊網路等調整介接等，涉及層面廣泛。為實證其運作機制於關鍵時刻能有效運作，金管會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 111 年第 3 季，計有 25 家銀行、36 家證券商及 25 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，並延續金管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。110 年至 111 年第 3 季，共辦理 DDoS 攻防演練、網路攻防演練課程、2021 金融 DEFENSE 資安攻防大賽等活動。

四、發揮資安聯防功能

(一) 建構資源共享的資安情資分享與事件應變機制

1. 金管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 111 年第 3 季止，F-ISAC 會員數達 339 家，金管會所管之重要金融機構均已加入 F-ISAC。

2. 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，金管會推動金控集團、同業公會、證券暨期貨市場電腦緊急應變支援小組(SF-CERT)及金融資安資訊分享與分析中心(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。

(二) 建置金融資安監控協同體系：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，以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 111 年第 3 季止，共有 40 家金融機構參與聯防 SOC 運作。

(三) 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 簽訂合作備忘錄(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 年成為全球最大之資安事件應變及安全小組論壇 FIRST (Forum of Incident Response and Security Teams)之會員，持續加強與其他國家金融資安機構交流合作。

伍、 金融資安精進方向

金管會經綜合近兩年國際資安情勢、金融資安監理趨勢，並檢討金融資安行動方案自 109 年 8 月發布後之執行情形，以擴大適用、落實與深化、鼓勵前瞻為持續精進方向：

一、擴大資安長設置，定期召開資安長聯繫會議

金管會已修訂各業別內部控制規範，要求銀行及一定規模以上金融機構設置副總經理層級以上之資安長。考量電子交易達一定比例者，其資安防護對整體營運影響甚高，爰併納入推動設置資安長範圍，統籌資安政策推動協調與資源調度。

為強化資安長職責，期資安長更能增進對資安情勢掌握，定期向董事會及經營管理階層報告及問責，擔任將資安風險納入經營決策考量及帶動重視組織文化之關鍵要角，爰規劃定期辦理資安長聯繫會議，就當前資安情勢、推動策略及關鍵議題等共同研商，並增進金融機構間交流與聯防。

二、因應數位轉型及及網路服務開放，增修訂自律規範

公會近兩年已陸續增修訂資通安全防護基準、新

興金融科技資安規範、供應鏈風險管理規範等，提供金融機構強化資安防護之準據。考量金融機構因應疫情加速數位轉型的腳步，對數位金融服務之倚賴愈深，傳統金融服務場景已由金融機構擴展至「金融生態圈」，爰規劃參考數位身分驗證等級國際標準(ISO 29115)架構，將網路身分驗證(eKYC)依登錄、信物管理及驗證等階段運作機制，區分信賴等級，並建立與業務風險對照之規範，以利業者於提供網路金融服務遵循；並將與第三方服務提供者(TSP)業務合作之風險評估與管理納入自律規範研修課題。

另考量新興技術與新型態資安攻擊態樣之演化(如 IOT、第三方元件、DeepFake、勒索軟體等)，持續滾動檢討修正相關自律規範，納入因應資安情資或事件檢討後之資安防護強化措施，並就急要事項先以作業指引行之，以增進時效。

三、深化核心資料保全及營運持續演練

金融資訊安全影響金融穩定，金融核心業務資料之保全更攸關民眾於金融機構財產權之確保。為因應重大資安事件、天然災害等風險，及考量對民生之衝擊性，將研議並鼓勵重要金融機構強化重要核心資料保全機制(包含核心資料檔案、資料庫加密與分持、備份儲存於第三地或雲端等機制)，以強化備份及復原機制，提升數位韌性。

金融機構為於區域性災損時可維持核心業務運作，多已建置異地備份與備援環境，惟異地之切換涉及內部資源人力配置調度、外部夥伴協同作業及資訊網路調整介接等，涉及層面廣泛。為實證其運作機制

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演練指引(如本異地備援實際運作、切換時效要求等項)，以提供金融機構遵循，並持續鼓勵金融機構或周邊單位於異地備援演練時，納入對外服務實際運作，驗證其有效性。另考量金融機構資訊系統服務常涉及外部單位，其穩定性非僅靠金融機構單一機構可維持，爰鼓勵金融機構聯合外部關聯單位辦理資通系統聯合演練，以應災害備援實務需求。

四、擴大導入國際資安管理標準及建置資安監控機制

金管會自 109 年鼓勵金融機構導入國際資安管理標準及建置資安監控機制(SOC)，主要金融機構均已導入或已有規劃辦理時程中，惟為求落實及有效執行，爰規劃依據業別特性，訂定國際資安管理標準之驗證範圍（如資訊基礎設施、全部核心資通系統、核心業務流程、網路金融服務及相關人員資產等），並建立資安監控作業基準（如資安組織、作業程序、監控範圍、資安威脅偵測與管理機制等項），擴大推動至具一定規模或電子交易達一定比例之金融機構。

五、鼓勵資安監控與防護之有效性評估

金管會近兩年已陸續研訂資安監控作業指引，並藉由解析專業駭客組織入侵攻擊手法發展資安監控組態基準，提供金融機構作為資安防護設定、監控規則與事件關聯分析等資安監控機制導入建置參考，亦可供作資安監控有效性評估對照。

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(Breach and Attack Simulation)等，檢驗資安監控及防禦部署之有效性。

六、鼓勵零信任網路部署，強化連線驗證與授權管控

因應疫情帶動異地/居家辦公模式，亦隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已難以滿足新形態工作需求。國際間包含美國、歐盟等都將發展零信任網路資安防護環境視為網路安全戰略；我國「國家資通安全發展方案(110年至113年)」，亦將發展零信任網路資安防護環境，推動政府機關導入零信任網路，爰規劃鼓勵金融機構逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路3大核心機制，搭配網路及資源的細化權限管控，以更能因應後疫情時期及數位轉型之資安防護需求。

七、鼓勵配置多元專長資安人才，擴大攻防演訓量能

金管會於110年發布金融資安人才職能地圖，並從供給面協調周邊訓練機構開設金融資安人才養成專班，鼓勵金融資安人員取得專業資安證照。為利金融機構資安之全面防護，規劃從需求面鼓勵金融機構重視各式資安人才之配置，及取得相關國際或專業訓練機構核發之資安證照(書)，引導金融機構重視資安人員之資格能力，以完備機構內資安維運所需職能，強化整體資安防護能量，並利金融資安人才之職涯發

展。

另鑑於傳統的資安防禦方法較偏重防禦面，往往陷入被動守勢而受制於駭客；美國資安專業組織MITRE（即 CVE、CWE 威脅指標的管理機構）從駭客攻擊的動機、目的、技術、方法，建立駭客威脅模型並做出因應對策，進而對網路威脅實施主動反擊；亦或順勢誘使攻擊者進入預先設計的陷阱，以實現主動防禦，減少駭客的預期危害。為強化因應駭客攻擊之防禦能量，爰規劃導入 MITRE 發布之攻擊與防禦方法論(MITRE ATT&CK & ENGAGE)，開設金融資安演訓專班，提升資安攻防戰略/戰術思維，並擴大演訓量能。

八、提升資安情資分享動能，增進資安聯防運作效能

金融資安資訊分享與分析中心(F-ISAC)為持續加強情資分析之深度及廣度，於 111 年底建置資安情資關聯分析平台，並提供自動化情資介接功能及建立情資分享獎勵機制。為提升資安情資分享動能，督導 F-ISAC 持續加強情資分析之深度及廣度，並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防護建議。

金管會於擴大推動金融機構建置 SOC 的同時，居於二線之聯防 SOC 亦將持續精進與一線 SOC 間之協作。為能對參與金融機構回傳事件單為更有效率之關聯分析，將輔導金融機構 SOC 導入依據網路攻擊行為樣態(MITRE ATT&CK)研訂之資安監控組態基準(包含異常事件觸發及關聯分析規則等)，並以此為基準研訂與聯 SOC 協作之監控組態與事件單觸發規

則，以增進聯防 SOC 對金融機構饋送事件單關聯分析之即時性及有效性，並利資安監控情資之回饋，提升金融機構 SOC 與聯防 SOC 協同運作效能。

九、辦理資安攻防演練，規劃重大資安事件支援演訓

為強化金融機構資安事件應變能力，金管會將持續規劃辦理金融機構分散式阻斷服務攻擊(DDoS)攻防演練、網路實兵攻防演練、網路攻防競賽及重大資安事件情境演練。

金管會另自 109 年陸續推動金控集團、各業別公會或周邊單位，及 F-CERT 建立跨組織之金融資安應變體系，另亦透過威脅獵捕或攻防演練培訓資安事件應變處置人才庫，為利跨機構支援之實務運作，將規劃建立重大資安事件虛擬指揮及應變體系，結合重大資安事件演練，併同驗證資安事件督導指揮、跨機構協調聯繫及支援應處能量等之運作機制。

陸、 執行措施

金管會在追求安全、便利、不中斷的金融資訊服務之願景下，以 109 年 8 月發布之金融資安行動方案為基礎，從強化資安監理、深化資安治理、精實資安韌性、發揮資安聯防等四大構面，滾動檢討精進措施，於「金融資安行動方案 2.0」提列 40 項執行措施(詳附件 1-「金融資安行動方案 2.0」執行措施彙總表)：

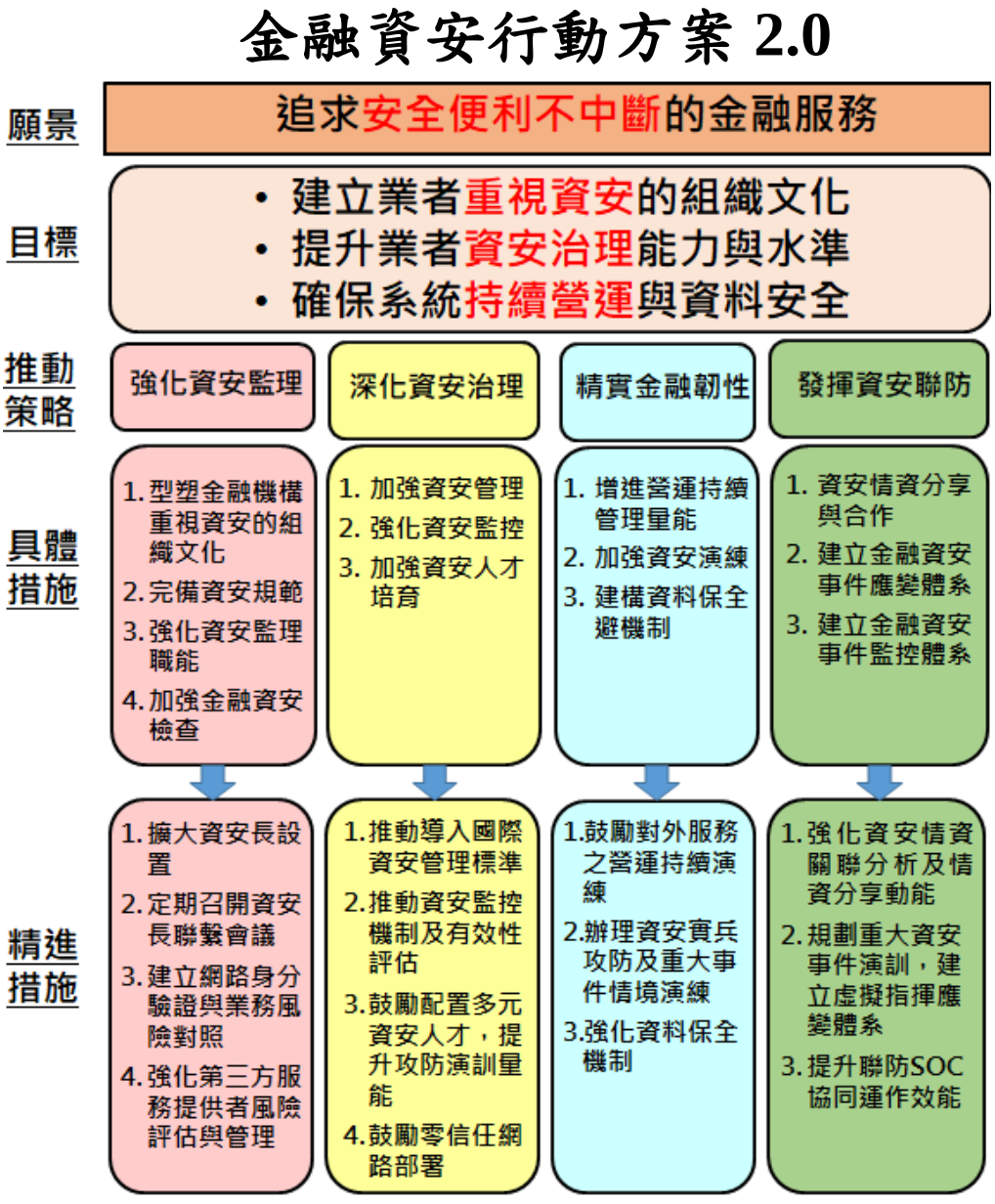

圖 1 、金融資安行動方案發展 2.0 藍圖

一、 強化資安監理

（一）型塑金融機構重視資安的組織文化

1. 增進經營階層對資安的監督職能

金管會已要求金融機構應成立資安專責單位並將資安辦理情形定期提報董事會，惟為再提升其對資安議題之決策能量，推動增設高階資安長統籌資安政策推動協調與資源調度，直接向董事會報告；並增納專業人員參與董事會運作，特設董監事資安課程，以增進對資安情勢掌握並實質將資安議題納入經營決策考量因子，帶動機構重視資安的組織文化。

金管會自109年推動一定規模之金融機構設置資安長，全體銀行及符合要件的保險業、證券期貨商、投信業皆已完成設置。考量金融機構電子交易達一定比例者，其資安防護對公司營運影響甚高，爰併納入推動設置資安長範圍。另針對已設置資安長之金融機構，定期辦理資安長聯繫會議，就當前資安情勢、推動策略及關鍵議題共同研商，強化資安長職責，並增進金融機構間交流與聯防。

2. 定期檢視資安風險因子與金融監理工具連結之有效性

為驅動金融機構對資安之重視，金管會已將其資安風險因子與金融監理工具連結，包含納入新申辦業務准駁、存款保險及保險安定基金費率計算、作業風險法定資本計提等。為掌握其有效性，並持續提供金融機構強化資安管理之誘因，續定期檢視並適時調整。

（二）完備資安規範：

1. 訂定資通安全防護基準

金管會銀、證、保三局已於各業別內部控制及稽核制度辦法中明訂公會應訂定資安自律規範並定期檢討。為求其更完備且與時俱進，參考我國資通安全管理法就資通系統訂定防護基準分級管理，以及為增加防禦縱深，採零信任架構思維重新檢視包含內外部網路之資源存取、網段隔離、邊界防護等議題，檢討修訂網路、資通系統安全等之自律規範，使其更臻明確與完整。

另參考資通安全管理法就資通訊環境訂定並要求政府機關導入組態基準，以及因應資訊系統委外風險於防護基準納入系統發展生命週期管理(包含需求、設計、開發、測試、部署與維運、委外、獲得程序、系統文件等)各階段控制措施等，對資安防護具有實效，爰參考以上做法，調適訂定參考指引，提供金融機構運用。

2. 增修訂新興金融科技與新型態資安攻擊樣態相關資安規範或作業指引

金融機構已逐步運用新興科技發展金融創新業務，為使金融機構運用新興科技時，能預先考量相關風險因子兼顧資安防護，將督導金融相關公會配合金融科技發展與金融業務的陸續開放，就行動應用程式(APP)、雲端服務、開放銀行 Open API、網路身分驗證(eKYC)等當前關注議題，併同新興技術與新型態資安攻擊樣態之演化(如 IOT、VPN、第三方元件、DDoS、DeepFake、勒索軟體、網頁置換等)，持續滾動檢討修正相關自律規範，納入資安事件檢討後之強化措施，並就急要事項先以作

業指引行之，以增進時效。

3. 增修訂供應鏈/第三方服務提供者風險管理規範或作業指引

因應金融服務委外及跨業之型態發展(如雲端服務、行動支付等)，及數位轉型後對數位金融服務之倚賴，為強化金融供應鏈體系及第三方服務提供者(TSP)之風險評估與管理，增修訂資安自律規範或作業指引，納入核心資通訊系統之軟硬體供應與維運商、第三方服務提供者(TSP)等之風險評估、邊際防護及委外稽核等。

4. 建立網路身分驗證強度與業務風險對照

因應網路金融服務持續擴大之身分驗證需求，參考數位身分驗證等級國際標準(ISO 29115)建立身分識別框架及標準，將身分驗證依登錄、信物管理及驗證等階段運作機，區分驗證強度等級，並建立與業務風險之對照。

（三）強化資安監理職能

透過專業及跨業課程訓練、赴周邊或公營機構實習、參加國際人才進修等措施，培育兼具金融與資安之跨域職能人才。另對中高階主管施以專設資安情勢、風險管理等高階課程，俾利資安監理政策之規劃與決策。

（四）加強金融資安檢查

1. 因應新興業務調整資安檢查重點

為能快速因應金融服務順應資通訊環境及新興科技等之改變，定期檢視調整資安檢查重點，俾

持續提升金融檢查之完整性及有效性，驅策金融機構落實資安執行。

2. 提升資安檢查人員專業檢查技能

為增進金融資安檢查之實效，因應資通訊環境及新興科技等之改變，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、 深化資安治理

（一）加強資安管理

1. 推動導入國際資安管理標準

為利資安管理制度之完備，國際標準組織已訂有標準可供遵循，我國資通安全管理法亦要求受管機關應導入資通安全管理標準，並透過公正第三方驗證資安管理之有效性。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，並借助第三方公正機構找出執行盲點及驗證有效性，爰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，並推動金融機構導入國際資安管理標準及取得相關驗證。

2. 推動金融機構資安治理成熟度評估

資安規範係奠基於可共通遵循之防護基準，更積極的面向係藉由自我評估資安風險，持續精進資安管理，特別是大型及具重要功能性之金融機構，應於防護基準上有更嚴格的標準。參考美國 FFIEC 採可重覆量測工具(CAT)供金融機構自主評量，調適訂定適用我國金融機構之評估方法，並鼓勵金融

機構據以依其自有特性，自主風險評估資安弱點，持續強化資安管理。

（二）強化資安監控

1. 推動建置資安監控機制(SOC)及辦理有效性評估

網路異常行為偵測告警之即時性及有效性，對異常行為是否惡化為資安事件及進行後續災損控管之影響甚鉅，透過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，並進而積極走向主動防禦。

金管會自109年鼓勵金融機構建置資安監控機制(SOC)，主要金融機構均已建置或規劃建置中，金管會亦已陸續研訂資安監控作業指引、監控組態基準等提供金融機構作為導入建置參考。考量資安監控於資安防護扮演關鍵角色，爰規劃進一步推動具一定規模或電子交易達一定比例之金融機構建置資安監控機制；並鼓勵藉由攻防演練等機制驗測資安監控及防禦部署之有效性。

2. 鼓勵金融機構以零信任原則進行網路部署

國際間包含美國、歐盟等都將發展零信任網路資安防護環境視為網路安全戰略；我國「國家資通安全發展方案(110年至113年)」，亦將發展零信任網路資安防護環境，推動政府機關導入零信任網路，爰規劃鼓勵金融機構採零信任網路部署，逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路三大核心機制，搭配網路及資源的細化權限管控，以更能因應後疫情時期及數位轉型之資安防護需求。

（三）加強資安人才培育

1. 鼓勵金融機構配置多元專長金融資安人才

金管會於 110 年訂定金融資安人才職能地圖，從供給面協調周邊訓練機構開設金融資安人才養成專班，以利招募資安人才投入金融領域，並鼓勵金融機構資安人員取得國際資安證照。為利金融機構資安之全面防護，規劃從需求面鼓勵金融機構重視各式資安職能人才之配置，以完備機構內資安維運所需職能。

2. 推動攻防演練訓練課程，強化第一線防守能力

資安訓練多以往僅著重被動防禦，金管會於 108 年與行政院合作辦理跨國攻防演練，增進資安人員對資安事件之通報應變能量，並獲致相當成效。該次演練已建置仿真電子銀行資訊系統，以此為基礎建置演練試驗場域，模擬以戰代訓，增進資安人員駭客思維與訓練成效。

美國專業資安組織 MITRE（即 CVE、CWE 威脅指標的管理機構）從駭客攻擊的動機、目的、技術、方法，建立駭客威脅模型並做出因應對策，進而對駭客威脅實施主動反擊；亦或順勢誘使攻擊者進入預先設計的陷阱，以實現主動防禦，減少駭客的預期危害。為強化因應駭客攻擊之防禦能量，爰規劃導入 MITRE ATT&CK & ENGAGE 方法論，開設金融資安演訓專班，提升資安攻防戰略/戰術思維，並擴大演訓量能。

三、 精實金融韌性

（一）增進營運持續管理量能

1. 訂定強化作業韌性參考規範

金融資訊服務的破壞或癱瘓，可能從而影響民眾信心致危及金融穩定，為強化金融機構風險管理與作業風險抵禦能力，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

國際標準組織已訂有以營運持續管理為主題之國際標準，藉由鼓勵金融機構導入國際營運持續管理標準及取得相關驗證，參採最佳實務做法，並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，據以向利害關係人溝通其面臨衝擊之準備。

3. 鼓勵實際作業之營運持續演練

為於區域性災損時可維持核心業務運作，金融機構多已建置異地備份與備援環境，惟異地之切換涉及內部資源人力等之配置調度、外部夥伴之協同作業及資訊網路等調整介接等，涉及層面廣泛，為實證其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演練指引(如本異地備援實際運作、切換時效要求等項)，以提供金融機構遵循，並持續鼓勵金融機構或周邊單位於異地備援演練納入對外服務實際業務運作，驗證其有效性。

另考量金融機構資訊系統服務多涉及外部單位，其穩定性非僅靠單一金融機構可維持，如證券

交易系統、跨行交易系統均涉及眾多金融機構，為確保金融資訊系統持續運作，爰鼓勵金融機構聯合外部關聯單位辦理資通系統聯合演練，以應災害備援實務需求。

（二）加強資安演練

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，包含：

1. 辦理金融資安攻防演練：定期辦理常被駭客用於利益勒索之 DDoS 或其他資安攻防演練。
2. 辦理金融資安攻防競賽：檢驗資安團隊實戰能力並促進跨機構良性競爭。
3. 辦理重大資安事件應變情境演練：考驗跨領域或跨機構橫向通報應變與協作。

（三）強化重要金融機構資料保全機制

為因應重大資安事件、天然災害及地緣政治等資料滅失之風險，及考量該等風險對民生所帶來之衝擊性，爰研議並鼓勵重要金融機構強化重要核心資料保全機制(包含核心資料檔案及資料庫加密與分持，並備份儲存於第三地或雲端等機制)，以強化備份及復原機制，提升數位韌性。

四、 發揮資安聯防

（一）資安情資分享與合作

1. 強化資安情資關聯分析及情資分享動能

F-ISAC 為持續加強情資分析之深度及廣度，於 111 年底建置資安情資關聯分析平台，並提供自

動化情資介接及建立情資分享獎勵機制，為提升資安情資分享動能，將督導 F-ISAC 持續加強情資分析之深度及廣度，並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防護建議。

2. 加強與國際金融資安機構合作

F-ISAC 成立後，已陸續加入美國 FS-ISAC 會員、出席歐盟 FI-ISAC 年會、與日本 F-ISAC、泰國 TB-CERT 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，持續推動與其他國家金融資安機構簽訂 MOU，並加強交流合作。

（二）建立金融資安事件應變體系

1. 鼓勵一定規模以上金控建立電腦資安事件應變小組

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，考量金控於集團內資源整合及相互支援之運作優勢，鼓勵金控建立電腦資安事件應變小組，俾利即時掌握及支援集團內成員資安事件之應變處置，降低事件損害。

2. 推動建立資安應變支援小組

考量部分小規模金融機構或未有充足能量與資源處理資安事件，爰推動由金融周邊單位或公會建立資安應變支援小組，適時協助體系成員處理資安事件。

3. 建立金融資安應變體系

重大資安事件往往非僅影響單一機構，如以共

同供應商為跳板發動之攻擊，恐同時波及體系中多數成員，為強化體系風險控管，建立跨機構甚至跨領域之橫向通報應變與支援協處之運作機制與能力，以降低重大事件之體系災損。

4. 規劃辦理重大資安事件支援演訓

金管會自 109 年陸續推動金控集團、各業別公會或週邊單位，及 F-CERT 建立跨組織之金融資安應變體系，另亦透過威脅獵捕或攻防演練培訓資安事件應變處置人才庫，為利跨機構支援之實務運作，爰規劃建立重大資安事件虛擬指揮及應變體系，結合重大資安事件演練，併同驗證資安事件督導指揮、跨機構協調聯繫及支援應處能量等之運作機制。

（三）建立金融資安事件監控體系

1. 建立聯防資安監控機制(F-SOC)

金管會於109年依據行政院國家資通安全會報「國家資通安全發展方案」，規劃建置金融資安聯防監控中心(F-SOC)，惟其能有效運作之關鍵在於金融機構一線 SOC 傳遞事件紀錄之即時性與完整性。藉由訂定與一線 SOC 協作之作業標準，包含事件資訊來源、事件分類與分級、事件資料格式與傳輸標準等，並據以推動與聯防 SOC 之協同運作，以能即時有效關聯分析整體資安風險，回饋金融機構加強資安防護。

2. 提升聯防 SOC 協同運作效能

金管會於擴大推動金融機構建置SOC的同時，居於二線之聯防 SOC 亦將持續精進與一線 SOC 間之協作。為能對參與金融機構回傳事件單為更有效

率之關聯分析，將輔導金融機構 SOC 導入依據駭客攻擊行為樣態(MITRE ATT&CK)研訂之資安監控組態基準(包含異常事件觸發及關聯分析規則等)，並以此為基準研訂與聯防 SOC 協作之監控組態與事件單觸發規則，以增進聯防 SOC 對金融機構饋送事件單關聯分析之即時性及有效性，提升金融機構 SOC 與聯防 SOC 協同運作效能。

柒、推動與管考

本方案內容所涉面向廣泛，由金管會整合相關資源，以三年為期循序漸進，推動作法如下：

一、公私協力：透過公部門、金融周邊單位及各業別公會等部門，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：針對各金融業別屬性、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需求及執行可達性。

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，並鼓勵金控及周邊單位(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新申辦業務准駁、作業風險法定資本計提、存款保險費率、保險安定基金費率之參考因子等措施，引導金融機構積極主動執行資安管控及強化措施。

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，共同強化資安防禦。

本方案發布後，由金管會召集各業務局及相關周邊單位、同業公會共同訂定各項目之推動指標與執行進程。自112年度起，每季檢討執行情形，滾動修訂推動策略、執行措施及各項推動指標。

捌、 預期效益

展望未來，金融科技的發展方興未艾，隨著金融服務與型態多元化、跨域創新連結與行動化，兼顧科技創新與風險管理，始能為社會謀求最大的福址。金管會推動本金融資安行動方案，期結合監理機關、金融周邊單位、各金融同業公會與金融機構，群策群力共創最佳效益：

一、金融機構：健全資安管理制度，提升資安防護能量；並得以在資通安全的基礎上，運用新興科技發展金融業務，提供消費者更安心、便利與多樣化之金融服務。

二、金融產業：建構金融資安聯防體系，厚植金融體系防禦能量，營造安全的金融服務發展環境，奠立金融科技發展之基石。

三、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。

附件 1「金融資安行動方案 2.0」執行措施彙總表

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
一、強化資安監理	1.型塑金融機構重視資安的組織文化	1.1增進經營階層對資安的監督職能	(1) 推動一定規模或電子交易達一定比例之金融機構設置資安長	113年	參考美國 NYDFS、歐盟 EBA 等要求金融機構應獨立資安職能、指定資安長及向經營階層(董事會）報告與問責等政策方向，本會繼要求金融機構應成立資安專責單位並將資安辦理情形定期提報董事會後，為再提升其對資安議題之決策能量，推動要求一定規模金融機構或純網銀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，向董事會報告，並增納專業人員參與董事會運作，辦理董監事資安課程，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，帶動重視資安的組織文化。 截至111年第3季止，全體銀行及符合要件的證券商有13家、期貨商有2家、投信業有5家、保險業有8家皆已完成設置資安長，考量金融機構電子交易達一定比例者，其資安防護作為對公司營運影響甚高，爰併納入推動設置資安長範圍。 另為強化資安長職責，期資安長能更增進對資安情勢掌握，定期向董事會及經營管理階層報告與問責，擔任將資安風險納入經營決策考量及帶動重視組織文化之關鍵要角，爰規劃定期辦理資安長聯繫會議，就當前資安情勢、推動策略及關鍵議題等共同研商，並增進金融機構間交流與聯防。	擴大適用
			(2) 鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組	持續		延續
			(3) 開辦董監事資安教育訓練專設課程	持續		延續
			(4) 辦理資安長聯繫會議	112年		新增

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
		1.2 定期檢視資安風險因子與金融監理工具連結之有效性	定期檢視現行資安風險因子與金融監理工具連結之有效性(如新業務申辦准駁、資本計提、存保費率、安定基金費率等)	持續	為驅動金融機構對資安之重視，本會已將其資安風險因子與金融監理工具連結，包含納入新申辦業務准駁、存款保險及保險安定基金費率計算、作業風險法定資本計提等。為掌握其有效性，並持續提供金融機構強化資安管理之誘因，續定期檢視並適時調整。	延續
	2.完備資安規範	2.1 訂定資通安全防護基準	(1)增修訂資安自律規範，納入網路安全防護及資訊系統安全防護基準內容	持續	歐盟 ESA 及亞洲新加坡等之金融資安監理政策均走向讓金融機構皆有明確可遵循之資安規範，本會銀、證、保三局亦已於各業別內部控制及稽核制度辦法中明訂公會應訂定資安自律規範並定期檢討。為求其更完備且與時俱進，爰參考我國資通安全管理法就資通系統訂定防護基準(包括存取控制、稽核與可歸責性、營運持續計畫、識別與鑑別、系統與服務獲得、系統與通訊保護、系統與資訊完整性等構面)分級管理；以及為增加防禦縱深，採零信任架構思維重新檢視包含內外部網路之資源存取、網段隔離、邊界防護等議題，檢討修訂網路、資通系統安全等自律規範，使其更臻完整明確。 另參考資通安全管理法就資通訊環境(包括個人電腦與伺服器作業系統、瀏覽器、應用程式、資安網路設備等)訂定並要求政府機關導入組態基準，以及因應資訊系統委外風險於防護基準納入系統	延續
			(2)訂定金融業電腦系統組態基準及資訊系統安全的發展生命週期相關防護基準等參考指引	113年		延續

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
					發展生命週期管理(包括需求、設計、開發、測試、部署與維運、委外、獲得程序、系統文件等)各階段控制措施等，規劃參考以上做法，訂定金融機構適用之參考指引，提供金融機構運用。	
		2.2增修訂新興金融科技與新型態資安攻擊樣態相關資安規範或作業指引	因應新興科技及新型態資安攻擊樣態滾動檢討修正自律規範或作業指引	持續	金融機構已逐步運用新興科技發展金融創新業務，為使金融機構運用新興科技時，能預先考量相關風險因子兼顧資安防護，將督導金融相關公會配合金融科技發展與金融業務的陸續開放，就行動應用程式(APP)、雲端服務、開放銀行 Open API、網路身分驗證(eKYC)等當前關注議題，併同新興技術與新型態資安攻擊樣態之演化(如 IOT、VPN、第三方元件、DDoS、DeepFake、勒索軟體、網頁置換等)，持續滾動檢討修正相關自律規範，納入資安事件檢討後之強化措施(如可視業別特性需要，導入自動流量清洗服務，以強化 DDoS 防護)，並就急要事項先以作業指引行之，以增進時效。	擴大範圍
		2.3增修訂供應鏈/第三方服務提供者風險管理規範或作業指引	增修訂資安自律規範或作業指引，納入核心資訊系統供應商及第三方服務提供者之風險評估及查核等管理機制	113年	因應近期以委外廠商、軟硬體供應商等做為跳板攻擊來源，有漸增之趨勢， G7及美國、歐盟金融監理機關均提出應加強第三方服務供應商之風險評估與委外管理；我國資通安全管理法施行細則亦揭示委外辦理資通訊系統之建置、維運或資通服務之提供，於選任及監督受託者時應注意事項，行政院也已將供應鏈風險管理列為重點項目。為因應金融服務委外及跨業之型態發展(如雲端服務、行動支付等)及強化金融	擴大範圍

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
					供應鏈體系之風險評估與管理，爰規劃增修訂資安自律規範，納入核心資通訊系統之軟硬體供應商與維運商、跨機構合作夥伴等之風險評估、邊際防護及委外稽核等。 另金融機構因應疫情持續加速數位轉型的腳步，對數位金融服務之倚賴愈深，傳統金融服務場景由金融機構擴展至「金融生態圈」已為趨勢，惟在建構金融服務生態圈時，如何因應第三方服務提供者之資安水準、服務水準等落差，確保安全可靠的金融服務亦是一大挑戰，爰除供應鏈外，規劃由公會研訂關鍵第三方服務提供者之範圍，並將其風險管理納入自律規範或作業指引研修。	
		2.4建立數位身分驗證等級與業務風險對照規範	因應數位轉型及網路服務開放，建立數位身分驗證等級與業務風險對照規範	113年	因應數位轉型及網路服務開放，並兼顧洗錢防制需求，可信賴的網路身分識別機制為各業別金融機構共同需求，為提供金融機構明確之執行準據，提升應用金融科技之效率，降低執行風險及減少消費者行政負擔，進而達到保障消費者權益之目的，爰規劃參考數位身分驗證等級國際標準(ISO 29115)架構，將身分驗證依登錄、信物管理及驗證等階段運作機制，區分信賴等級，並建立與業務風險對照之規範，以利業者遵循。	新增
	3.強化資安監理職	加強資安監理人才培育	(1) 推動本會資安人才培育計畫	持續	因應金融機構積極運用新興科技創新金融服務趨勢，監理機關應有超前部署之資安思維，一則洞察新興科技之應用與國	延續

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
	能				際金融監理趨勢，俾以資安為前題調適監理政策；另則具備督促金融機構落實並循環改善資安管理之職能。爰規劃以本會資訊人力及業務監理同仁為對象，透過專業及跨業課程訓練、赴周邊或公營機構實習、參加國際人才進修等措施，培育兼具金融與資安之跨域職能人才。另對中高階主管，施以專設資安情勢、風險管理等高階課程，俾利資安監理政策之規劃與決策。	
			(2)提升中高階主管資安知能	持續		延續
	4.加強金融資安檢查	4.1 因應新興業務調整資安檢查重點	定期因應新興業務調整資安檢查重點	持續	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順應資通訊環境及新興科技等之改變，定期檢視調整資安檢查重點，俾持續提升金融檢查之完整性及有效性。	延續
		4.2 提升資安檢查人員專業技能	提升資安檢查人員專業技能，以利檢查作業	持續	為增進金融資安檢查實效，順應資通訊環境及新興科技等之改變，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。	延續
二、深化資安	5.加強資安管理	5.1推動金融機構導入國際資安管理標準	(1)研訂國際資安管理標準驗證範圍	112年	為利資安管理制度之完備，國際標準組織已訂有標準可供遵循，我國資通安全管理法之子法-資通安全責任等級分級辦法亦要求受管機關應就全部核心資通系統導入資通安全管理標準，並透過第三方獨立機構驗證資安管理之有效性。本會前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	新增
			(2)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	113年		擴大適用

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
治理			及取得相關驗證		機構找出執行盲點及驗證有效性，鼓勵金融機構導入國際資安管理標準及取得相關驗證，截至111年底重要金融機構均已導入國際資安管理標準。另為提供金融機構驗證執行之準據，爰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（如資訊基礎設施、全部核心資通系統、核心業務流程、網路金融服務及相關人員資產等），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驗證。	
		5.2 推動金融資安治理成熟度評估	(1)研議訂定金融機構資安治理成熟度評估方法	完成	資安規範係奠基於可共通遵循之防護基準，更積極的面向係藉由自我評估資安風險，持續精進資安管理，特別是大型及具重要功能性之金融機構，應於防護基準上有更嚴格的標準。爰參考美國 FFIEC 採可重覆量測工具(CAT)供金融機構自主評量，調適訂定適用我國金融機構之評估方法，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。	
			(2)鼓勵金融機構辦理資安治理成熟度評估	持續		延續
	6.強化資安監控與防護	6.1推動建置資安監控機制(SOC)	推動一定規模或電子交易達一定比例之金融機構或周邊單位建置資安監控機制	114年	網路異常行為偵測告警之即時性及有效性，攸關其是否惡化為資安事件及需進行後續災損控管，爰透過鼓勵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，積極走向主動防禦。	擴大適用

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
					本會自109年鼓勵金融機構建置資安監控機制(SOC)，截至111年第3季，主要金融機構均已建置或規劃建置中，本會亦陸續研訂資安監控作業指引、監控組態基準等提供金融機構作為導入建置參考。考量網路攻擊無處不在，資安監控於資安防護扮演關鍵角色，爰進一步規劃依重要性推動具一定規模或電子交易達一定比例之金融機構或周邊單位建置資安監控機制（如包含資安組織、作業程序、監控範圍、資安威脅偵測與管理機制等項）。	
		6.2鼓勵辦理資安監控及資安防護有效性評估	鼓勵一定規模金融機構導入駭客思維，定期透過駭客攻擊手法實測資安監控與防護機制之有效性。	114年	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，藉由 DDoS 攻防演練、紅藍隊演練、入侵與攻擊模擬(Breach and Attack Simulation)等，定期檢驗資安監控及防禦部署之有效性。	新增
		6.3鼓勵零信任網路部署	鼓勵金融機構逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路3大核心機制。	114年	因應疫情帶動異地/居家辦公模式，亦隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於信任邊界之網路模型已難以滿足新形態工作需求。國際間包含美國、歐盟等都將發展零信任網路資安防護環境視為網路安全戰略；我國「國家資通安全發展方案(110年至113年)」，亦將發展零信任網路資安防護環境，推動政府機關導入零信任網路，爰	新增

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
					規劃鼓勵金融機構採零信任網路部署，逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路三大核心機制，搭配網路及資源的細化權限管控，以更能因應後疫情時期及數位轉型之資安防護需求。	
	7.加強資安人才培育	7.1鼓勵配置取得多元專長及資安證照	(1)訂定金融資安人才職能地圖	完成	金管會於110年訂定金融資安人才職能地圖，從供給面協調周邊訓練機構開設金融資安人才養成專班，以利招募資安人才投入金融領域，並鼓勵金融機構資安人員取得國際資安證照。為利金融機構資安之全面防護，規劃從需求面鼓勵金融機構重視各式資安職能人才之配置，及取得相關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職能，強化金融機構防護能量，並利金融資安人才之職涯發展。	
			(2)協調周邊單位開設金融資安人才養成專班	持續		延續
			(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)	持續		新增配置多元專長資安人力
		7.2推動攻防演練訓練課程，強化第一線防守能力	推動 F-ISAC 與金融研訓院等單位合作開設金融資安演訓專班	114年	傳統的資安防禦方法較偏重防禦面，往往陷入被動守勢而受制於駭客，金管會於108年與行政院合作辦理跨國攻防演練，增進資安人員對資安事件之通報應變能量，並獲致相當成效。該次演練已建置仿真電子銀行資訊系統，以此為基礎建置演練試驗場域，模擬以戰代訓，增進資安人員駭客思維與	新增

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
					訓練成效。 美國專業資安組織 MITRE（即 CVE、CWE 威脅指標的管理機構）從駭客攻擊的動機、目的、技術、方法，建立駭客威脅模型並做出因應對策，進而對駭客威脅實施主動反擊；亦或順勢誘使攻擊者進入預先設計的陷阱，以實現主動防禦，減少駭客的預期危害。為強化因應駭客攻擊之防禦能量，爰規劃導入 MITRE 發布之攻擊與防禦方法論(MITRE ATT&CK & ENGAGE)，推動 F-ISAC 與金融研訓院等單位合作開設金融資安演訓專班，提升資安攻防戰略/戰術思維，並擴大演訓量能。	
三、精實金融韌性	8.增進營運持續管理量能	8.1 訂定強化作業韌性參考規範	訂定金融作業韌性參考規範	113年	金融資訊服務的破壞或癱瘓，可能從而影響民眾信心致危及金融穩定，爰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，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。	延續
		8.2 鼓勵金融機構導入國際營運持續管理標準	鼓勵金融機構導入國際營運持續管理標準及取得相關驗證	持續	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，爰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，並透過第三方獨立機構驗證符合來自內部、法規、	延續

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
					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。	
		8.3鼓勵實際作業之營運持續演練	(1)研訂核心業務系統備援演練指引 (2)鼓勵金融機構及周邊單位於異地備援演練時，納入對外服務實際運作驗證 (3)鼓勵金融機構聯合外部關聯單位辦理資通系統聯合演練	113年 持續 持續	為於區域性災損時可維持核心業務運作，金融機構多已建置異地備份與備援環境，惟異地之切換涉及內部資源人力等之配置調度、外部夥伴之協同作業及資訊網路等調整介接等，涉及層面廣泛。為實證其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演練指引(如本異地備援實際運作、切換時效要求等項)，以提供金融機構遵循，並持續鼓勵金融機構或周邊單位於異地備援演練時，納入對外服務實際運作，驗證其有效性。 另考量金融機構資訊系統服務多涉及外部單位，其穩定性非僅靠單一金融機構可維持，如證券交易系統、跨行交易系統均涉及眾多金融機構，為確保金融資訊系統持續運作，爰鼓勵金融機構聯合外部關聯單位辦理資通系統聯合演練，以應災害備援實務需求。	新增 延續 新增
	9.加強資安演練	9.1 辦理金融資安攻防演練	定期辦理金融機構DDoS 或其他資安攻防演練	持續	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。	延續
		9.2辦理金融資安攻防競	定期辦理金融資安攻防演練競賽	持續(每兩		調整為定期辦

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
		賽		年)	演練類型包含常被駭客用於利益勒索之 DDoS 攻防、檢驗資安團隊實戰能力並促進跨機構良性競爭之攻防競賽，以及考驗跨領域或跨機構橫向通報應變與協作之重大資安事件情境演練。	理
		9.3 辦理重大資安事件應變情境演練	定期辦理重大資安事件應變情境演練	持續(每兩年)		調整為定期辦理
	10.強化資料保全機制	強化資料保全機制	鼓勵重要金融機構或周邊單位強化因應重大資安事件、天然災害等之資料保全	114年	金融資訊安全影響金融穩定，金融核心業務資料之保全更攸關民眾於金融機構財產權之確保，為因應重大資安事件、天然災害等風險，及考量該等風險對民生之衝擊性，爰研議並鼓勵重要金融機構強化重要核心資料保全機制(包含核心資料檔案、資料庫加密與分持，備份儲存於第三地或雲端等機制)，以強化備份及復原機制，提升數位韌性。	新增
四、發揮資安聯防	11.資安情資分享與合作	11.1強化資安情資關聯分析及情資分享動能	強化 F-ISAC 與會員間情資互動，帶動會員情資分析與分享量能	持續	F-ISAC 為持續加強情資分析之深度及廣度，於111年底建置資安情資關聯分析平台，並提供自動化情資介接及情資分享獎勵機制，為提升資安情資分享動能，將督導 F-ISAC 持續加強情資分析之深度及廣度，並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防護建議。	延續並強化
		11.2 加強金融資安國際合作	加強與國際金融資安機構合作或簽訂MOU，掌握國際金融資安情勢	持續	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、泰國 TB-CERT 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，持續推	延續

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
					動與其他國家金融資安機構簽訂 MOU，並加強交流合作。	
	12.建立金融資安事件應變體系	12.1 鼓勵金控建立電腦資安事件應變小組	鼓勵金控建立電腦資安事件應變小組，提供集團內成員必要協助	持續	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，考量金控於集團內資源整合及相互支援之運作優勢，鼓勵金控建立電腦資安事件應變小組，俾利即時掌握及支援集團內成員資安事件之應變處置，降低事件損害。	延續
		12.2 推動建立資安應變支援小組	推動周邊單位或公會建立資安應變支援小組，適時協助業者處理資安事件	持續	考量部分小規模金融機構或未有充足能量與資源處理資安事件，爰推動由金融周邊單位或公會建立資安應變支援小組，適時協助體系成員處理資安事件。	延續
		12.3 建立金融資安應變體系	建立因應重大資安事件，跨機構支援協處應變體系	持續	重大資安事件往往非僅影響單一機構，如以共同供應商為跳板發動之攻擊，恐同時波及體系中多數成員，為強化體系風險控管，爰規劃建立跨機構、跨領域之橫向通報應變與支援協處之運作機制與能力，以降低重大事件之體系災損。	延續
		12.4規劃辦理重大資安事件演訓	建立重大資安事件虛擬指揮及應變體系	113年	本會自109年陸續推動金控集團、各業別公會或周邊單位，及 F-CERT 建立跨組織之金融資安應變體系，另亦透過威脅獵捕或攻防演練培訓資安事件應變處置人才庫。為利跨機構支援之實務運作，將規劃建立重大資安事件虛擬指揮及應變體系，結合重大資安事件演練，併同驗證資安事件督導指揮、跨機構協調聯繫及支援應處能量等運作機制。	新增
	13.建立	13.1 建立聯	訂定資安監控作業	持續	本會109年依據行政院國家資通安全會報「國家資通安全發	延續

構面	工作項目	工作小項	執行措施	執行期限	說明	與1.0關聯性
	金融資安事件監控體系	防資安監控機制(SOC)	基準		展方案」，規劃建置金融資安二線監控中心(F-SOC)，惟其能有效運作之關鍵在於金融機構一線 SOC 傳遞事件紀錄之即時性與完整性，爰規劃訂定與一線 SOC 協作之作業標準，包含事件資訊來源、事件分類分級、事件資料格式與傳輸標準等，並據以推動與聯防 SOC 之協同運作，以能即時有效關聯分析整體資安風險，回饋金融機構加強資安防護。	
		13.2提升聯防 SOC 協同運作效能	提升金融機構 SOC 與聯防 SOC 協同運作效能	113年	本會於擴大推動金融機構建置 SOC 的同時，居於二線之聯防 SOC 亦將持續精進與一線 SOC 間之協作。為能對參與金融機構回傳事件單做更有效率之關聯分析，將輔導金融機構 SOC 導入依據駭客攻擊行為樣態(MITRE ATT&CK)研訂之資安監控組態基準(包含異常事件觸發及關聯分析規則等)，並以此為基準研訂與聯防 SOC 協作之監控組態與事件單觸發規則，以增進聯防 SOC 對金融機構饋送事件單關聯分析之即時性及有效性，提升金融機構 SOC 與聯防 SOC 協同運作效能。	新增

附件 2「金融資安行動方案 2.0」執行措施修正對照表

構面	工作項目	工作小項	修正執行措施	修正執行期程	原執行措施	原執行期程
一、強化資安監理	1.型塑金融機構重視資安的組織文化	1.1增進經營階層對資安的監督職能	(1) 推動一定規模或電子交易達一定比例之金融機構設置資安長	113年	(1)推動一定規模金融機構或純網銀設置資安長	二年
			(2) 鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組	持續	(2)鼓勵遴聘具資安背景之董事、顧問或設置資安諮詢小組	二年
			(3) 開辦董監事資安教育訓練專設課程	持續	(3)開辦董監事資安教育訓練專設課程	一年
			(4) 辦理資安長聯繫會議	112年		
		1.2 定期檢視資安風險因子與金融監理工具連結之有效性	定期檢視現行資安風險因子與金融監理工具連結之有效性(如新業務申辦准駁、資本計提、存保費率、安定基金費率等)	持續	定期檢視現行資安風險因子與金融監理工具連結之有效性(如新業務申辦准駁、資本計提、存保費率、安定基金費率等)	持續
	2.完備資安規範	2.1 訂定資通安全防護基準	(1)增修訂資安自律規範，納入網路安全防護及資訊系統安全防護基準內容	持續	(1)增修訂資安自律規範，納入網路安全防護及資訊系統安全防護基準內容	二年
			(2)訂定金融業電腦系統組態基準及資訊系統安全的發展生命週期相關防護基準等參考指引	113 年	(2)訂定金融業電腦系統組態基準及資訊系統安全的發展生命週期相關防護基準等參考指引	四年
		2.2增修訂新興金	因應新興科技及新型態資安攻擊樣	持續	增修訂資安自律規範，納入行動應	二年

構面	工作項目	工作小項	修正執行措施	修正執行期程	原執行措施	原執行期程
		融科技與新型態資安攻擊樣態相關資安規範或作業指引	態滾動檢討修正自律規範或作業指引		用程式(APP)、雲端服務、開放銀行 OPEN API、物聯網、網路身分驗證(eKYC)等新興科技安控規範。	
		2.3增修訂供應鏈/第三方服務提供者風險管理規範或作業指引	增修訂資安自律規範或作業指引，納入核心資訊系統供應商及第三方服務提供者之風險評估及查核等管理機制	113年	增修訂資安自律規範，納入核心資訊系統供應商及跨機構資訊服務之風險評估及查核等管理機制	二年
		2.4建立數位身分驗證等級與業務風險對照規範	因應數位轉型及網路服務開放，建立數位身分驗證等級與業務風險對照規範	113年		
	3.強化資安監理職能	加強資安監理人才培育	(1) 推動本會資安人才培育計畫	持續	(1)推動本會資安人才培育計畫	持續
			(2)提升中高階主管資安知能	持續	(2)提升中高階主管資安知能	持續
	4.加強金融資安檢查	4.1 因應新興業務調整資安檢查重點	定期因應新興業務調整資安檢查重點	持續	定期因應新興業務調整資安檢查重點	持續
		4.2 提升資安檢查人員專業技能	提升資安檢查人員專業技能，以利檢查作業	持續	提升資安檢查人員專業技能，以利檢查作業	持續
二深化	5.加強資安管理	5.1推動金融機構導入國際資安管理標準	(1)研訂國際資安管理標準驗證範圍	112年	鼓勵金融機構導入國際資安管理標準及取得相關驗證	持續
			(2)推動一定規模或電子交易達一定	113年		

構面	工作項目	工作小項	修正執行措施	修正執行期程	原執行措施	原執行期程
資安治理			比例之金融機構導入國際資安管理標準及取得相關驗證			
		5.2 推動金融資安治理成熟度評估	(1)研議訂定金融機構資安治理成熟度評估方法	完成	(1)研議訂定金融機構資安治理成熟度評估方法	二年
			(2)鼓勵金融機構辦理資安治理成熟度評估	持續	(2)鼓勵金融機構辦理資安治理成熟度評估	持續
	6.強化資安監控與防護	6.1推動建置資安監控機制(SOC)	推動一定規模或電子交易達一定比例之金融機構或周邊單位建置資安監控機制	114年	鼓勵金融機構建置資安監控機制	持續
		6.2鼓勵辦理資安監控及資安防護有效性評估	鼓勵一定規模金融機構導入駭客思維，定期透過駭客攻擊手法實測資安監控與防護機制之有效性。	114年		
		6.3鼓勵零信任網路部署	鼓勵金融機構逐步導入身分鑑別、設備鑑別及信任推斷等零信任網路3大核心機制。	114年		
	7.加強資安人才培育	7.1鼓勵配置取得多元專長及資安證照	(1)訂定金融資安人才職能地圖	完成	(1)訂定金融資安人才職能地圖	一年
			(2)協調周邊單位開設金融資安人才養成專班	持續	(2)協調周邊單位開設金融資安人才養成專班	一年
			(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	持續	(3)鼓勵金融資安人員取得國際資安證照	持續

構面	工作項目	工作小項	修正執行措施	修正執行期程	原執行措施	原執行期程
			發之資安證照(書)			
		7.2推動攻防演練訓練課程，強化第一線防守能力	推動 F-ISAC 與金融研訓院等單位合作開設金融資安演訓專班	114年	建置金融機構演練試驗場域，設計訓練教材及自動化攻擊機制，並辦理攻防演練訓練課程	二年
三精實金融韌性	8.增進營運持續管理量能	8.1 訂定強化作業韌性參考規範	訂定金融作業韌性參考規範	113 年	訂定金融作業韌性參考規範	四年
		8.2 鼓勵金融機構導入國際營運持續管理標準	鼓勵金融機構導入國際營運持續管理標準及取得相關驗證	持續	鼓勵金融機構導入國際營運持續管理標準及取得相關驗證	持續
		8.3鼓勵實際作業之營運持續演練	(1)研訂核心業務系統備援演練指引 (2)鼓勵金融機構及周邊單位於異地備援演練時，納入對外服務實際運作驗證 (3)鼓勵金融機構聯合外部關聯單位辦理資通系統聯合演練	113年 持續 持續	鼓勵一定規模金融機構於異地備援演練時，納入實際業務運作驗證	持續
	9.加強資安演練	9.1 辦理金融資安攻防演練	定期辦理金融機構 DDoS 或其他資安攻防演練	持續	定期辦理金融機構 DDoS 或其他資安攻防演練	持續
		9.2辦理金融資安攻防競賽	定期辦理金融資安攻防演練競賽	持續 (每兩年)	研議辦理金融資安攻防演練競賽	二年

構面	工作項目	工作小項	修正執行措施	修正執行期程	原執行措施	原執行期程
		9.3辦理重大資安事件應變情境演練	定期辦理重大資安事件應變情境演練	持續(每兩年)	規劃並辦理重大資安事件應變情境演練	持續
	10.強化資料保全機制	強化資料保全機制	鼓勵重要金融機構或周邊單位強化因應重大資安事件、天然災害等之資料保全	114年	10.1研議資料保全運作機制:研究核心資料類型、資料格式標準及資料安全保存及取用等運作機制及安全標準	二年
					10.2推動成立資料保全中心:視研議結果推動成立資料保全中心，並分階段推動試辦	四年
四發揮資安聯防	11.資安情資分享與合作	11.1強化資安情資關聯分析及情資分享動能	強化 F-ISAC 與會員間情資互動,帶動會員情資分析與分享量能	持續	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	二年
		11.2 加強金融資安國際合作	加強與國際金融資安機構合作或簽訂 MOU，掌握國際金融資安情勢	持續	加強與國際金融資安機構合作或簽訂 MOU，掌握國際金融資安情勢	持續
	12.建立金融資安事件應變體系	12.1 鼓勵金控建立電腦資安事件應變小組	鼓勵金控建立電腦資安事件應變小組，提供集團內成員必要協助	持續	鼓勵金控建立電腦資安事件應變小組，提供集團內成員必要協助	持續
		12.2 推動建立資安應變支援小組	推動周邊單位或公會建立資安應變支援小組，適時協助業者處理資安	持續	推動周邊單位或公會建立資安應變支援小組，適時協助業者處理資安	四年

構面	工作項目	工作小項	修正執行措施	修正執行期程	原執行措施	原執行期程
			事件		事件	
		12.3 建立金融資安應變體系	建立因應重大資安事件，跨機構支援協處應變體系	持續	建立因應重大資安事件，跨機構支援協處應變體系	二年
		12.4規劃辦理重大資安事件演訓	建立重大資安事件虛擬指揮及應變體系	113年		
	13.建立金融資安事件監控體系	13.1 建立聯防資安監控機制(SOC)	訂定資安監控作業基準	持續	(1)建置二線 SOC 及訂定資安監控作業標準 (2)推動金融機構 SOC 與二線 SOC 協同運作	二年
		13.2提升聯防 SOC 協同運作效能	提升金融機構 SOC 與聯防 SOC 協同運作效能	113年	研議導入 AI 分析機制，進行警訊及事件關聯分析	三年