「金融資安行動方案」執行措施彙總表

構面	工作項目	工作小項	執行措施	執行期程	說明
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)推動一定規模金融機構或純網銀設置資安長	二年	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，本會雖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，推動一定規模金融機構或純網銀設置高階資安長（副總經理，得兼任）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。
			(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	一年	
		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	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，以及中央存款保險、保險安定基金、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。

構面	工作項目	工作小項	執行措施	執行期程	說明
一、強化資安監理	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	二年	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)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	

構面	工作項目	工作小項	執行措施	執行期程	說明
一、強化資安監理	2.完備資安規範	2.2 增修訂新興金融科技資安規範	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、物聯網、網路身分驗證(eKYC)等新興科技安控規範。	二年	金融機構已逐步運用新興科技發展金融創新業務，為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，爰規劃配合金融科技的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)等當前關注議題增修資安自律規範，同時也持續關注未來環境變化進行滾動檢討。
		2.3 增修訂供應鏈風險管理規範	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	因應近期以委外廠商、軟硬體供應商等為跳板攻擊漸增之趨勢， 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。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)，為強化金融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。

構面	工作項目	工作小項	執行措施	執行期程	說明
一、強化資安監理	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	因應金融機構積極運用新興科技創新金融服務趨勢，監理機關應有超前布署之資安思維，一則洞察新興科技之應用與國際金融監理趨勢，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與之跨域職能人才。另對中高階主管，同施以專設資安情勢、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	
	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因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。
		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。

構面	工作項目	工作小項	執行措施	執行期程	說明
二、深化資安治理	5.加強資安管理	5.1 鼓勵導入國際資安管理標準	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	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，並透過第三方獨立機構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，並借助第三方獨立機構找出執行盲點或驗證有效性，鼓勵金融機構導入國際資安管理標準及取得相關驗證。
		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 (2)鼓勵金融機構辦理資安治理成熟度評估	二年	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資安風險的自我評估，持續精進資安管理，特別是大型及功能性更重要之金融機構，應於防護基準之上有更嚴格的標準。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。
	6.強化資安監控	鼓勵建置資安監控機制(SOC)	鼓勵金融機構建置資安監控機制	持續	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，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，進而積極走向主動防禦。

構面	工作項目	工作小項	執行措施	執行期程	說明
二、深化資安治理	7.加強資安人才培育	7.1 訂定金融資安職能地圖，培訓資安菁英人才，鼓勵取得國際資安證照	(1)訂定金融資安人才職能地圖	一年	本會已要求金融機構應設置資安專責單位，惟因應新興技術與金融服務、日益嚴峻的資安風險、以及資安法實施後各方競逐資安人力，如何有效培育並補充資安人力，為金融機構設置資安專責單位後亟需努力的議題。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，爰規劃依據金融資安職能需求訂定人才培訓地圖，並據以開辦金融資安人才養成專班，以符實務運作需求。 另參考資安管理法對列管機關有取得一定數量專業證照之要求，目前亦有金融機構將資安人員是否取得專業證照列為薪酬之參據，爰以鼓勵金融資安人員取得國際資安證照，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。
			(2)協調周邊單位開設金融資安人才養成專班	一年	
			(3)鼓勵金融資安人員取得國際資安證照	持續	
		7.2 推動攻防演練訓練課程，強化第一線防守能力	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	資安訓練多只著重被動防禦，本會近年與行政院合作，共同辦理跨域情境演練、分散式阻斷服務(DDoS)、實兵攻防、跨國攻防演練等，於增進資安人員對資安事件之通報應變能量，獲致相當成效。2019 年辦理之跨國攻防演練，已建置仿真電子銀行資訊系統，爰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。

構面	工作項目	工作小項	執行措施	執行期程	說明
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	四年	金融資訊服務的破壞或癱瘓，可能從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。
		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，爰藉由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、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	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	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界接等，涉及層面廣泛，為實證其運作機制於關鍵時刻能有效運作，爰鼓勵金融機構於異地備援演練時，納入實際業務運作驗證。

構面	工作項目	工作小項	執行措施	執行期程	說明
三、精實金融韌性	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。 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。
		9.2 辦理金融資安攻防競賽	研議辦理金融資安攻防演練競賽	二年	
		9.3 辦理重大資安事件應變情境演練	規劃並辦理重大資安事件應變情境演練	持續	
	10.建構資料保全避風港	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	金融資訊安全影響金融穩定，金融核心業務資訊之保全更攸關民眾於金融機構財產權之確保。爰參考美國為提升金融機構客戶對金融系統對抗災難性事件的信心，所推動之「避風港計畫」概念，預為就資料保護、資料可移性、資料復原性，以及關鍵服務持續性等研議其運作機制及以利相關資料與安全標準；再視研議結果評估推動方式。
		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	

構面	工作項目	工作小項	執行措施	執行期程	說明
四、發揮資安聯防	11.資安情資分享與合作	11.1 建立資安情資關聯分析平台	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	F-ISAC 成立後雖已建立資安情資蒐集及分析能量，惟因應資安情勢之日益嚴峻與情資來源的多元化，仍需持續加強情資分析之深度及廣度，爰規劃建立資安情資關聯分析平台，以增進分析量能，及時提供更為精確完整的早期預警與防護建議。
		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 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，續加強與其他國家金融資安機構交流合作。
	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。
		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	四年	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。

構面	工作項目	工作小項	執行措施	執行期程	說明
四發揮資安聯防	12.建立金融資安事件應變體系	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	二年	重大資安事件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。
	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)	(1)建置聯防 SOC 及訂定資安監控作業標準 (2)推動金融機構 SOC 與聯防 SOC 協同運作	二年	本會 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，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 導入 AI 分析機制	研議導入 AI 分析機制，進行警訊及事件關聯分析	三年	因應持續擴大推動金融機構參與聯防資安監控之中長期發展需求，爰研議善用智慧前瞻科技（大數據、AI）淬鍊有效情報，以自動化與智能化提升情資分析量能、即時有效將攻擊情資回饋至第一線資安監控主動防禦。