特　載

金融資安行動方案

本文係轉載 109 年 8 月 6 日
金融監督管理委員會新聞稿附件資料

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。金融監督管理委員會（以下簡稱金管會）因應數位時代潮流，亦陸續推動數位服務的開放與創新，包含開放設置純網路銀行、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，駭客的攻擊早已朝向系統化與組織化，除常見之分散式阻斷服務攻擊（Distributed Denial-of-Service, DDoS）、社交工程攻擊、勒索軟體等問題外，更不乏大型金融機構遭駭客跨國盜轉鉅額資金之案例，一旦受駭所帶來的衝擊較之諸往更鉅。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（註 1）。

金管會長期關注並督促金融機構資安防護，雖已行之有年也有一定的運作機制，惟鑒於資安威脅日益嚴峻，金融資安防護的思維亦須更快速的調整因應，爰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，提出「金融資安行動方案」，期以四年為期，更為提升金融產業資安能量，以於創新開放金融服務的同時，仍能提供民眾安心便利、穩定不中斷的金融服務，保護金融消費者的財產與隱私，亦為金融科技奠定發展的基石。

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，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、藉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，顯示駭客組織在利益導向下，多方覬覦可從金融機構獲取之非法利益。

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密、或於暗網購得帳密等手法，進一步運用取得帳密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），亦成為駭客組織尋求資安防護脆弱點覬覦標的，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

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，一旦發動成功即造成嚴重影響，如難以維持正常業務運作，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，以能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，面對不可控的外在環境。

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FirEye、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。

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 年即發布「金融服務業網路安全要求規範（23 NYCRR Part 500）」（註 2），目前為美國金融監理機關唯一之法律層級的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）（註 3），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。

歐洲銀行監理總署（EBA）於 2019 發布「資通科技及安全風險管理指引」[註4]，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」[註5]，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。

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）[註6]，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。歐洲銀行監理總署（EBA）於 2019 年底發布「資通科技及安全風險管理指引」[註7]，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。

新加坡金融管理局（MAS）於 2019 年公布「網路安全通告」[註8]，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，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 年已聯合發布「強化網路風險管理標準」草案預告[註9]，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」（註10）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

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2018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」討論文件（註11），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」（註12），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）」（註13），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」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於2019年發布修正「技術風險管理指引」及「營運持續管理指引」諮詢文件（註14），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。營運持續管理則在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；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。

肆、金融資安推動現況與檢討

因應近年金融資安情勢日益嚴峻，金管會已將金融機構的資通安全納為金融監理重點之一，以為金融市場風險管控的一部分，並透過強化政策驅動、完備資安規範、提升資安能量、落實資安執行及推動資安聯防等五個面向推升金融資安防護，相關措施推動現況暨檢討如下：

一、強化政策趨動

為驅動金融機構對資安的重視，金管會已將其資通安全辦理情形與監理工具相結合，包含新申辦業務准駁，以及納入中央存款保險、保險安定基金、作業風險法定資本計提等因子；也要求每年由資訊安全最高主管與董事長、總經理、稽核主管聯名出具「資訊安全整體執行情形聲明書」，提報董事會。

前開措施，與監理工具結合部分，係近一兩年陸續研議訂定，後續將持續檢視優化相關作業因子；另著眼於更進一步要求董事會重視資安並負實質決策責任，如何提升董事會的資安決策能量避免淪為橡皮圖章，將是未來持續推動的重點。

二、完備資安規範

為確保金融機構的資訊安全的執行，有共通的標準可供遵循，金管會已督導各業別公會自行訂定自律規範，並透過修訂金融機構內部控制及稽核制度實施辦法，提升自律規範之法律位階並作為各金融機構內部控制制度重要的一環。

自律規範之有效性，必須因應國內外資安威脅、新興科技的演進等滾動檢討修正。回顧過去一年的資安威脅，駭客從內部網路或自供應鏈發動攻擊事件頻傳，為增加防禦縱深，導入零信任架構[註 15]思維，重新檢視定義邊界防護；以更細緻的組態提升資訊系統防護基準；以及加強委外管理等，是應持續努力的方向。另

在新興科技部分，配合金融業務的開放，雲端服務、開放銀行 Open API、網路身分驗證（eKYC）等，也都是未來滾動檢討修正的重點。

三、 提升資安能量

專業的組織與充足的人力是金融機構完善資安管理重要的基礎。金管會已要求金融機構應設置資安專責單位及相當層級專責主管；銀行業及保險業資產總額達一兆元以上者，應設置具職權行使獨立性之資安專責單位，維持執行業務之獨立性。另在資安人力部分除了要求金融機構重視資安人才培訓外，近年也與行政院合作，共同辦理跨域情境演練、分散式阻斷服務（DDoS）演練、實兵攻防演練、跨國攻防演練等，於增進資安人員因應資安事件之通報與應變能量，獲致相當成效。

隨著新技術導入及外界快速變遷環境，新增作業風險更需仰賴專業人才處理，金融機構若無充足且優質的資安專職人力，將愈難以因應日益嚴峻的資安風險；而我國資安法實施後，各方競逐資安人力，如何有效培育並補充資安人力，亦為金融機構設置資安專責單位後亟需努力的議題。

此外，因應資安情勢日益嚴峻，國際金融資安監理也走向強調作業風險的抵禦能力，拉長資訊安全戰線，涵蓋資安事件前之有效監控、因應攻擊之應變處置、遭到入侵回復能力，美國 FS-ISAC 推動的「避風港計畫」[註 16]，更強調核心資料之最終保全。加強資安人員監控、應變、災害復原等能量及運作機制，為當前應努力的方向。

四、 落實資安執行

證之以往資安事件的發生，往往並非制度與規範不完備，而是各項資安標準程序與防護措施執行不落實或便宜行事。金管會已要求金融機構將資訊安全納為金融業者內部控制及稽核重點，也由檢查局負責規劃、執行金融機構之檢查，除定期辦理金融機構資安檢查外，也針對重點議題（如 ATM、SWIFT）辦理專案檢查，並就檢查發現缺失提列檢查意見，督促改善。

金融機構內部控制的三道防線，是督促其落實資安執行最重要的一環。金管

會檢查局的金融檢查，固然可以有效驅策金融機構重視資安，然畢竟人力資源有限，對數百家金融機構，也僅能以抽核方式辦理。囿於人力資源有限，未來策略性透過導入國際資安標準的第三方驗證，以及金融機構經營管理階層（如董事會、高層資安長）加強要求內部控制三道防線之落實，結合由外而內、從上而下的推升力道，內化資安監理思維，以進而型塑重視資安的組織文化，是應持續努力推動的方向。

五、 推動資安聯防

為健全金融產業資安防護能力，全球主要國家相繼設立金融資安資訊分享與分析機構，如美國有 FS-ISAC、英國有 CiSP 等資安分享中心。金管會也依據行政院國家資通安全會報「國家資通安全發展方案」（註 17），在 106 年底成立「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center, F-ISAC）」，108 至 109 年陸續建立「金融電腦緊急應變小組（Financial Computer Emergency Response Team, F-CERT）」及「金融資安監控中心（Financial Security Operation Center, F-SOC）」運作機制。

F-ISAC 成立以來，持續蒐集分析國內外金融資安情資，提供金融機構資安預警情資及強化資安防護建議，迄今銀行、產壽險、證券期貨、票證等各主要金融機構已全數加入成為會員，獲致相當成效。另 F-ISAC 亦積極與其他國家資安機構交流，包含美國 FS-ISAC、歐盟 FI-ISAC、日本 F-ISAC 等，於增進國際交流合作、擴大情資來源等亦有相當助益。

面對國家級駭客組織的持續精進，資安情資除了需要持續加強其深度及廣度外，未來更應著眼於有效性的提升，包含蒐集更具即時性之資安監控情資、增加自動化與智能化的情資分析量能，以及將攻擊情資回饋至第一線資安監控主動防禦等。另外，因應駭客系統化、組織化的攻擊，金融機構間除了情資分享外，如能進而建立跨機構之資安事件應變體系，以於重點期間支援單一機構應變能量不足之缺口，更能發揮資安聯防的效益。

伍、金融資安監理策勵方向

沒有 100% 的資訊安全，但民眾永遠期待更安心、便利、不中斷的金融服務。因應資訊與金融科技的快速發展，資安威脅的與日俱增，營造一個安全的金融服務發展環境，讓金融機構要可因應新科技與業務競爭快速發展新商品與服務，民眾也可以安心使用各項新金融商品服務，為金融發展一大挑戰。

金管會經綜合檢視前揭當前國際資安情勢、金融資安監理趨勢，並檢討現行金融資安監理政策，歸結四大後續策勵方向：

一、 強化資安監理

從金融監理機關角度，定期檢視金融監理工具與資訊安全連結之有效性、資安規範的完備性，並持續提升金融資安檢查量能。此外，亦須借力獨立第三方稽核、金融機構經營階層之監督職能，策略性由外而內、從上而下，型塑金融資安組織文化，以落實各項資安工作之執行。

二、 深化資安治理

從金融機構角度，應持續增補及培訓資安人力，並參照國際資安管理標準、資安治理成熟度等構面，建立自我評估機制，持續深化及落實資安管理，建立 PDCA（Plan-Do-Check-Act）良性改善循環。

三、 精實金融韌性

從金融消費者的角度，冀求便利不中斷的金融服務，於金融機構之財產權得以確保。金融機構必須以風險思維，精實遭遇嚴厲資安攻擊之金融服務韌性，包含加強因應資安攻擊之應變處置、災害復原、客戶財產資訊最終保全等，為最壞的打算做最好的準備。

四、 發揮資安聯防

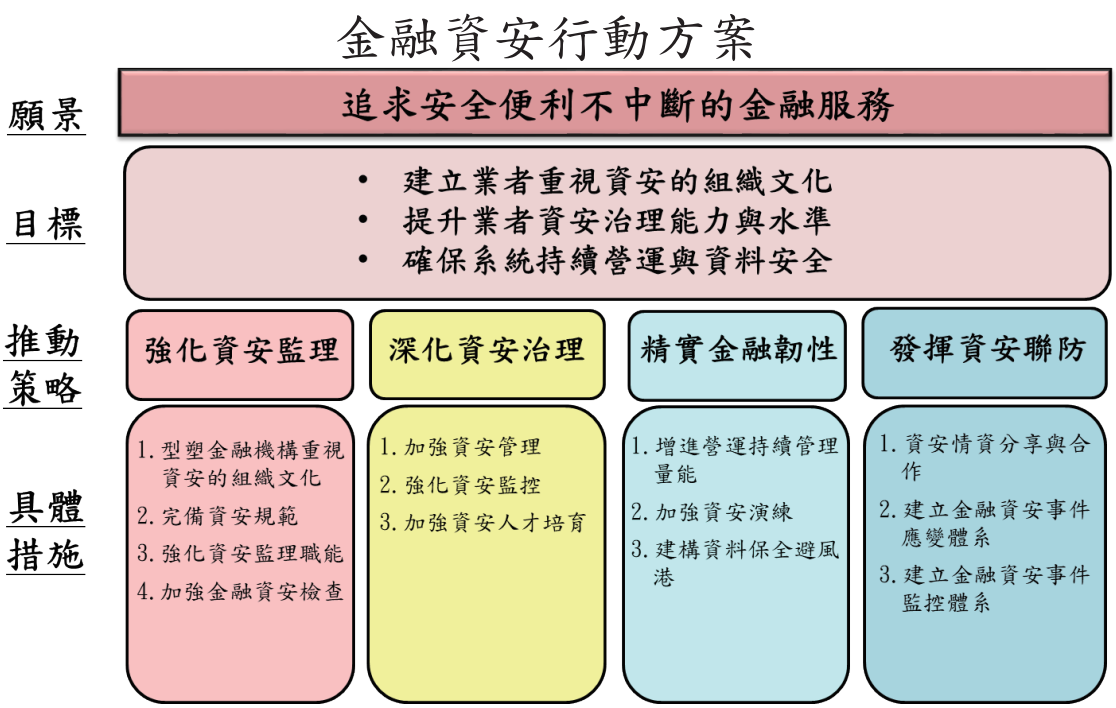
從聯防有效性的角度，持續加強情資蒐集的深度、廣度與即時性，除了整合 F-ISAC、F-CERT 及 F-SOC 運作機制外，續從智能化的資安情資分析，體系化的

資安事件應變、即時的資安監控等三個面向，持續推升資安聯防效能，從信任合作邁向更有效的主動防禦機制，凝聚金融資安生態體系。

陸、執行措施

金管會依四大金融資安策勵方向，訂定金融資安行動方案，方案願景在追求安全、便利、不中斷的金融資訊服務，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，提列 36 項執行措施（詳附件 -「金融資安行動方案」執行措施彙總表）：

圖 1　金融資安行動方案發展藍圖



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。

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，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。

(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具有實效，爰由參考以上做法，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資安規範

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，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。

3.增修訂供應鏈風險管理規範

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，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。

(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。

(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，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.鼓勵業者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。

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。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，持續強化其資安管理。

(二)強化資安監控 - 鼓勵金融機構建置資安監控機制

對網路異常行為偵測告警之即時性及有效性，對異常行為是否進階為資安事件及其後續災損控管之影響甚鉅，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，並進而積極走向主動防禦。

(三)加強資安人才培育

1.訂定金融資安人才職能地圖，培訓資安菁英人才，鼓勵資安人員取得國際資安證照

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，依據金融資安職能需求訂定人才培訓地圖，據以開辦金融資安人才養成專班，以符實務運作需求。另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.推動攻防演練訓練課程，強化第一線防守能力

資安訓練多只著重被動防禦，金管會 2019 年與行政院合作辦理跨國攻防演練，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。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。

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，鼓勵金融機構於異地備援演練納入實際業務運作驗證。

(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)建構資料保全避風港

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。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，以及相關資料與安全標準。再視研議結果評估推動方式與時程，分階段試辦。

四、 發揮資安聯防

(一)資安情資分享與合作

1.建立資安情資關聯分析平台

因應資安情勢之日益嚴峻與情資來源的多元化，需持續加強情資分析之深度及廣度，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。

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 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。

(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，建立跨機構甚或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。

(三)建立金融資安事件監控體系

1.建立二線資安監控機制（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。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，並據以推動與二線 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.導入 AI 分析機制

因應持續擴大推動金融機構參與二線資安監控之中長期發展需求，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。

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，以四年為期循序漸進，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，共同因應駭客組織化之攻擊。

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 110 年度起，每半年檢討執行情形，滾動修訂推動策略、執行措施及各項推動指標。

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，科技創新與風險管理要兼顧，才能為社會帶來最大的福址。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—「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	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。
			(2) 鼓勵金融機構辦理資安治理成熟度評估		

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	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。
	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	

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	7.2 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。
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。

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	8.2 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。

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	12.2 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。
		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 建立二線資安監控機制（SOC）	(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	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，並據以推動與二線 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。

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	13. 建立金融資安事件監控體系	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二線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。

註釋

註 1： https://www.bis.org/bcbs/publ/d454.htm

註 2： https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

註 3： https://www.ffiec.gov/cyberassessmenttool.htm

註 4： https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

註 5： https://www.fsa.go.jp/en/news/2019/20190115/cyber-policy.pdf

註 6： https://www.esma.europa.eu/press-news/esma-news/esas-publish-joint-advice-information-and-communication-technology-risk

註 7： https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

註 8： https://www.mas.gov.sg/regulation/notices/notice-655

註 9： https://www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards

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

註 11：https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

註 12：https://www.cftc.gov/About/CFTCOrganization/NFACybersecurityGuidance083118

註 13：https://www.bundesbank.de/resource/blob/764690/792725ab3e779617a2fe28a03c303940/mL/2018-10-24-g-7-fundamental-elements-for-threat-led-penetration-testing-data.pdf

註 14：https://www.mas.gov.sg/news/media-releases/2019/mas-consults-on-proposed-enhancements-to-trm-and-bcm-guidelines

註 15：https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

註 16：https://shelteredharbor.org/

註 17：https://nicst.ey.gov.tw/Page/296DE03FA832459B/f61d7cc8-d18a-45e5-ac38-0dc0cf96856e