金融資安韌性發展藍圖

金融監督管理委員會

中華民國 114 年 12 月

目錄

壹、 緣起

金融業為國家經濟運作的基石，金管會鑒於金融科技快速發展及金融服務創新開放，資通安全也面臨嚴峻挑戰，於 2020 年 8 月發布「金融資安行動方案」，期間歷經新冠疫情驅動金融業數位轉型，加劇資安威脅情勢，並為因應在重大災害及地緣政治等風險下，能持續提供民眾安心、便利、穩定不中斷的金融服務，於 2022 年 12 月發布「金融資安行動方案 2.0」，已引導金融業設立資安長及遴聘具資安背景之董事、顧問或設置資安諮詢小組，增進資安監理量能，並推動金融機構導入國際資安管理標準，建立資安監控機制、聯防機制及持續透過攻防演練等，提升防禦部署之有效性，並積極走向主動防禦。

然而，近年隨著雲端、人工智慧、量子計算等技術快速發展，也帶來新型態的資安風險，且金融機構間錯縱複雜的合作關係及供應商關係，也讓風險情勢變得更加不透明和難以預防；面對持續且不斷升級的資安威脅，金管會除了持續推動零信任架構，將資安防護邊界拓展至非屬傳統邊界的遠距辦公及雲端存取等場域，深化資安防護之廣度及深度，也觀察到國際間正積極推動「韌性導向」的監理，強調金融機構在面對網路攻擊、運作中斷或其他不確定性時，須具備快速回應與復原的能力。爰此，金管會賡續推出「金融資安韌性發展藍圖」，透過「目標治理」、「全域防護」、「生態聯防」及「堅實韌性」的四軸架構，目標是建構「可預測、可防禦、可復原」的金融生態系，並確保即使在極端情境下，金融關鍵服務也能持續運作。

貳、 全球資安的挑戰與趨勢

世界經濟論壇(WEF)「2025 年全球網路安全展望報告」[1]指出，地緣政治緊張局勢、供應鏈日益增長的相互依賴性，以及人工智慧(AI)技術快速發展帶來的應用和挑戰，都是造成網路環境複雜化的主要因素，其中國家級的威脅已蔓延至對關鍵基

[1] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

礎設施的攻擊，且當各組織越來越集中於特定供應商，也可能因為對這些供應商的攻擊或漏洞產生連鎖反應，進而對整個生態系統造成影響，爰 WEF 提出應加強公私部門合作、提升供應鏈的合作與透明度等建議，也呼籲組織領導者必須採取「安全優先」(security-first)的心態，將網路安全視為一項戰略投資，以確保在面對新興威脅時保持韌性，並應量化網路風險及其經濟影響，以便將投資與核心業務目標保持一致等。

美國貨幣監理署(OCC)於 2025 年 7 月發布「網路安全與金融系統韌性報告」[2]，也指出當前金融業主要的網路威脅包含勒索軟體、分散式阻斷服務攻擊(DDoS)攻擊、帳戶盜用、供應鏈風險、地緣政治威脅、人工智慧(AI)威脅、後量子密碼學等。

根據國際貨幣基金組織(IMF)「2024 年全球金融穩定報告」指出，一次資安事件就可能造成 25 億美元的損失，佔一般金融公司營業收入的 800%[3]，恐危及其清償能力與資本適足性；於 2025 年 10 月的報告中[4]，也指出網路攻擊所引發的營運中斷可能削弱外匯市場功能，進而造成流動性緊縮與市場劇烈波動，並強調即使是交易平台短暫的停擺，也足以衝擊市場流動性並導致結算延遲，甚至在跨市場間引發連鎖的系統性壓力，且當金融體系對少數關鍵技術服務供應商的高度依賴，更加劇了單點故障的風險，一旦這些關鍵節點遭駭，衝擊將迅速擴散至全球金融網路。

爰此，國際間也紛紛推出更全面、更主動的策略，並涵蓋監理政策、風險管理及防禦技術等面向，其最終目的都指向提升金融機構在面對極端情境下的營運韌性，以維護金融市場的長期穩定發展，包含：

一、 強化高層責任及提升資安成熟度

美國紐約州金融服務署(NYDFS)於 2023 年 11 月修訂金融

[2] https://www.occ.treas.gov/publications-and-resources/publications/cybersecurity-and-financial-system-resilience/index-cybersecurity-and-financial-system-resilience-report.html
[3] https://www.elibrary.imf.org/display/book/9798400257704/CH003.xml
[4] https://www.imf.org/en/publications/gfsr/issues/2025/10/14/global-financial-stability-report-october-2025

服務業網路安全要求規範(23 NYCRR Part 500)[5]，指定由董事會或其他適當委員會組成高階管理階層，且須具備妥適專業，負責督導網路資安風險之管理，及定期審查、核定資安相關政策與報告，並明確資安長職責，包含定期向高階管理階層報告資安執行情形、即時報告重大資安問題，及共同簽署資安符合性聲明等。

美國國家標準暨技術研究院(NIST)於 2024 年 2 月 26 日發布「網路安全框架」(CSF, Cybersecurity Framework)版本 2.0[6]，增加的「治理」(Govern)層面不僅貫穿整個框架，並涵蓋 6 大類別，包含：組織全景、風險管理策略、角色/職責/授權、政策、監管、網路安全供應鏈風險管理；由金融機構和產業協會組成的網路風險研究所(CRI, Cyber Risk Institute)緊接於 2024 年 2 月 29 日發布金融業專用的「網路安全評估框架」(CRI Profile)版本 2.0[7]，協助金融業於 CSF 2.0 的基礎上，透過標準化的問卷來衡量資安成熟度並進行風險管理。

歐盟於 2022 年 12 月發布數位營運韌性法案(DORA, Digital Operational Resilience Act)[8]，並自 2025 年 1 月 17 日起適用，第 5 條明確要求董事會必須對資通訊科技(ICT)風險管理負最終責任，及定期接受 ICT 相關培訓等，以確保其具備足夠的知識來理解和評估風險。

日本金融廳(FSA)於 2024 年 10 月發布的「金融業網路安全指引」[9]，指出網路安全非僅是 IT 部門的技術問題，董事會和高階主管需主導政策制定、資源分配，並對因管理不善造成的損失承擔潛在的法律責任，也強調金融機構應根據自身的業務環境、策略及風險承受能力，識別、評估並緩解網路風險，避免僅為符合規範而採取的表面功夫，並將應對措施分為「基本應對措施」(Fundamental response measures)是所有金融機構

[5] https://www.dfs.ny.gov/system/files/documents/2023/12/rf23_nycrr_part_500_amend02_20231101.pdf
[6] https://cyberriskinstitute.org/cri-issues-profile-version-2-0/
[7] https://cyberriskinstitute.org/the-profile/
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR
[9] https://www.fsa.go.jp/common/law/cybersecurity_guideline_en.pdf

都應實施的基礎實務，「建議措施」(Recommended measures)則是針對大型金融機構和金融市場基礎設施的進階最佳實踐。

二、 推動資安左移及軟體物料管理

美國國家標準與技術研究所(NIST)於 2022 年 2 月發布安全軟體開發框架(SSDF, Secure Software Development Framework)[10]，指出要確保軟體足夠安全，應將安全實踐在軟體開發生命週期(SDLC, Software Development Life Cycle)中，並將安全軟體開發分為 4 大構面，包含：組織準備、保護軟體、生產安全軟體、回應漏洞，分別提供實際任務及實作範例，協助組織將資安內化為軟體品質的一部分，及將資安問題左移至 SDLC 較前且較低成本的階段解決，並指出應於生產過程中獲取每個軟體元件的資訊(如軟體材料清單 SBOM)，才能在軟體發布後迅速且有效地應對新漏洞。美國網路安全暨基礎設施安全局(CISA)於 2023 年 10 月與 17 個美國及國際資安機構共同發布白皮書「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software」，提出了三個核心原則，指導軟體製造商在設計過程中將安全性納入考量，並提供安全設計策略(security by design tactics)最佳實務[11]。

針對軟體元件的管理，國際支付卡產業標準(PCI DSS)於 2022 年發布的第四版[12](2024 年 3 月 31 日生效、2025 年 3 月 31 日強制執行)，已在條款 6.3.2 要求機構維護客製化軟體及第三方軟體的元件清單，以便於漏洞管理與修補；美國網路安全與基礎設施安全局(CISA)於 2024 年發布「軟體元件透明度架構」(Framing Software Component Transparency)第三版[13]，進一步定義了軟體物料清單(SBOM)的屬性及建立流程，為軟體元件資訊共享的通用標準，可促進軟體供應鏈的透明度和問責制。

[10] https://csrc.nist.gov/projects/ssdf
[11] https://www.cisa.gov/securebydesign
[12] https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf
[13] https://www.cisa.gov/resources-tools/resources/framing-software-component-transparency-2024

而歐盟「網路韌性法案」(CRA, Cyber Resilience Act)[14]已於 2024 年 12 月 10 日生效(2027 年起將全面強制實施)，亦要求所有在歐盟銷售的「具數位元素產品」(包含軟體等)，其製造商必須記錄軟體物料清單(SBOM)，以便於製造商及用戶追蹤漏洞等。

三、 推動 AI 資安治理與防護

英國國家網路安全中心(NCSC)於 2023 年 11 月發布「安全 AI 系統開發指引」(Guidelines for Secure AI System Development)[15]，將 AI 開發生命週期分為 4 個關鍵領域：安全設計、安全開發、安全部署、安全運行和維護，並針對每個領域提出相應的注意事項和緩解措施，以降低 AI 系統開發流程的整體風險；英國科學創新與技術部(DSIT)並續於 2025 年 1 月發布「AI 網路安全實務守則」(Code of Practice for AI Cyber Security)及「AI 網路安全實務守則實作手冊」(Implementation Guide for the AI Cyber Security Code of Practice)[16]。

美國國家標準與技術研究所(NIST)於 2023 年 1 月 26 日發布「人工智慧風險管理框架」(AI RMF, Artificial Intelligence Risk Management Framework)第一版[17]，主要描述管理 AI 風險的方法，並指出 AI 系統特有的安全問題，2024 年 1 月則發布關於對抗式機器學習的報告[18]，詳細定義了針對預測式 AI、生成式 AI 的攻擊類型及緩解方法等，2024 年 7 月更進一步針對生成式 AI 的風險管理提出建議[19]。

資安領域著名的非營利組織 OWASP(Open Web Application Security Project)也於 2023 年 10 月發布「生成式 AI 安全專案」(GenAI Security Project)第一版[20]，提供軟體開發人員有關生成式 AI 的安全建議等，另一著名的非營利組織 MITRE 所提出的資安攻擊與防禦框架 ATT&CK (Adversarial

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847
[15] https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development
[16] https://www.gov.uk/government/publications/ai-cyber-security-code-of-practice
[17] https://www.nist.gov/itl/ai-risk-management-framework
[18] https://csrc.nist.gov/pubs/ai/100/2/e2023/final
[19] https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
[20] https://genai.owasp.org/

Tactics, Techniques & Common Knowledge)[21]自 2024 年起也陸續加入 AI 相關攻擊指標。

歐盟「人工智慧法案」(AI Act)[22]於 2024 年 8 月 1 日生效，第 15 條更明確要求高風險 AI 系統必須具備適當的安全性(附件 3 指出金融領域包含用於評估自然人信用狀況或建立其信用評分的 AI 系統，及用於自然人相關的保險評估與定價的 AI 系統等)，並確保具有抵禦惡意第三方攻擊的能力等。

四、 規劃後量子密碼遷移準備

美國國家標準與技術研究所(NIST)與摩根大通(J.P. Morgan)於 2020 年建議金融業應立即建立加密敏捷性[23]，美國總統並於 2022 年 12 月簽署「量子運算網路安全準備法」(Quantum Computing Cybersecurity Preparedness Act)，推動關鍵基礎設施及政府機關將資訊系統加密機制轉移為可抵禦量子電腦威脅的後量子密碼學(PQC, Post-Quantum Cryptography)系統，隔(2023)年美國網路安全暨基礎設施安全局(CISA)、美國國家安全局(NSA)和 NIST 併提出量子遷移步驟建議[24]，NIST 並於 2024~2025 年間已推出 3 項全球通用的 PQC 演算法標準。歐盟網路安全局(ENISA)則於 2022 年 10 月發布報告[25]，建議在過渡期採用混合機制(PQC+傳統加密)，以避免新演算法風險。

美國 FS-ISAC(Financial Services Information Sharing and Analysis Center)則成立工作小組，陸續發布盤點基礎設施加密技術、因應後量子密碼準備路線圖、建構加密敏捷性、對支付卡產業衝擊等報告[26]；新加坡金融管理局(MAS)於 2024 年 2 月函知金融機構有關解決與量子相關的網路安全風險的建議[27]，包含盤點加密資產、與第三方供應商接觸、規劃遷移時間表等，並於 2024 年 7 月發布量子運算計畫(Quantum Computing

[21] https://atlas.mitre.org/
[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
[23] https://www.nccoe.nist.gov/sites/default/files/2021-10/6-Yassir-NIST-%2020200819-8.pdf
[24] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography
[25] https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study
[26] https://www.fsisac.com/knowledge/pqc
[27] https://www.mas.gov.sg/regulation/circulars/advisory-on-addressing-the-cybersecurity-risks-associated-with-quantum

Programme)[28]，承諾投入 1 億新元支持量子及人工智慧領域的創新。

五、 強化供應商管理與營運韌性

美國金融監管機構(Fed、FDIC、OCC)於 2023 年 6 月聯合發布「第三方關係風險管理指引」(Interagency Guidance on Third-Party Relationships)[29]，將第三方風險管理的生命週期分為 5 個階段，包含：規劃、盡職調查與選擇、合約談判、持續監控、終止，並描述每個階段的風險管理原則，也提到應根據第三方的「關鍵性」(Criticality)採取依風險為基礎的管理手段，及明確指出對第三方的依賴並不能免除其對客戶的法律與合規責任。

針對第三方與供應鏈風險，金融穩定委員會(FSB)於 2023 年 12 月提出一套風險管理工具[30]，協助金融機構識別關鍵第三方服務，及管理第三方服務關係於整個生命週期中的潛在風險，也為金融主管機關設定了監督、識別和管理系統性風險的標準，並強調跨境監管合作和資訊共享的重要性；另考量事件報告是監管機構監控營運中斷的關鍵工具，FSB 於 2025 年 5 月發布 FIRE 框架(Format for Incident Reporting Exchange)[31]，旨在建立一套國際通用的金融營運事件報告格式，並涵蓋事件初始階段到結案的完整生命週期，使各監管機構能夠以標準化資料交換方式共享事件資訊。

歐盟於 2022 年 12 月發布數位營運韌性法案(DORA, Digital Operational Resilience Act)[32]，並自 2025 年 1 月 17 日起適用，要求金融機構應建立資通訊科技(ICT)風險管理框架、即時通報重大資安事件及測試數位營運韌性等，及金融機構與供應商簽約的相關要求，以確保金融機構具備承受、回應並從各

[28] https://www.mas.gov.sg/schemes-and-initiatives/quantum-computing-programme
[29] https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html
[30] https://www.fsb.org/2023/12/final-report-on-enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities/
[31] https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/
[32] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR

類 ICT 中斷和威脅中恢復的能力。

另在實戰演練方面，除了要求金融機構自身進行韌性測試，國際間也持續辦理不同形式的聯合演練，來測試金融業在面對不同情境下的韌性，以 2024 年為例，模擬網路攻擊的有英國 CBEST[33]、歐盟 TIBER-EU[34]等，模擬跨機構大規模中斷的有英國 SIMEX[35]、美國 Hamilton Series[36]、新加坡 Exercise Raffles[37]等，進行營運壓力測試的有英國 CORST[38]、歐盟 CRST[39]等，這些演練不僅為驗證金融機構是否能足夠人力及資源，得以快速應對網路威脅與恢復中斷，更著重於跨機構溝通協調、流動性危機處理以及市場信心維持機制等。

參、 金融資安推動現況與發展策略

金融領域為我國關鍵基礎設施之重要一環，為保障民眾財產權及提供穩定的金融服務，金管會自 2020 年底推動金融資安行動方案以來，多項措施執行已達目標，並納入常態運作，如定期檢視資安風險因子與金融監理工具連結之有效性、因應新興業務調整資安檢查重點、滾動檢討修訂資安規範，多數主要金融機構並已取得國際資安管理標準驗證、辦理金融資安治理成熟度評估及建置資安監控機制(SOC)，並建立包含金控集團、周邊單位或公會及 F-CERT 等金融資安事件應變體系，另以法規要求達一定規模之金融機構設置資安長，並定期辦理資安長聯繫會議，在推動金融業界之資安意識及增強資安風險管理等方面取得了顯著進展；另在促進資安合作與國際交流方面，金管會自 2017 年底成立金融資安資訊分享與分析中心(F-ISAC, Financial Information Sharing and Analysis Center)，已推動金融業資安情資分享與合作、建立聯防 SOC 機制等，並先後加入美國 FS-ISAC 會員、出席歐盟 FI-ISAC 年會，與日本 F-ISAC、

[33] https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/2024-cbest-thematic
[34] https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
[35] https://www.bankofengland.co.uk/news/2024/october/simex-24-testing-the-uk-financial-sector-resilience
[36] https://www.chicagofed.org/events/2025/midwest-cyber-workshop
[37] https://www.mas.gov.sg/news/media-releases/2024/business-continuity-exercise-to-bolster-financial-sector-operational-resilience
[38] https://www.bankofengland.co.uk/prudential-regulation/letter/2024/thematic-findings-2024-cyber-stress-test
[39] https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html

泰國 TB-CERT 等簽訂 MOU，成為資安事件應變及安全小組論壇(FIRST)之會員、加入亞太地區電腦網路危機處理聯合組織(APCERT)等。

為持續提升金融機構資安防護能力及應變能力，在人才培育方面，金管會於 2021 年訂定「金融資安人才職能地圖」[40]，從供給面協調周邊訓練機構開設金融資安人才養成專班，並從需求面鼓勵金融機構重視各式資安人才之配置及取得資安證照(書)；在防護技術方面，2024 年 7 月發布「金融業導入零信任架構參考指引」[41]，建議金融機構以風險導向，擇高風險低衝擊之場域先行，漸進導入相關控制措施，並責成 F-ISAC 陸續發布「金融機構組態基準」及「金融雲端資安監控基準」等，提供金融機構資安防護設定、監控規則等監控機制建置參考，亦透過持續辦理 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，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。

基於各類資通安全威脅日益嚴重，我國「國家資通安全戰略 2025：資安即國安」[42]針對國家級資安威脅、新興科技挑戰、網路犯罪猖獗等外部威脅，提出國家策略四大支柱：全社會防衛韌性、國土防衛與關鍵基礎設施、關鍵產業與供應鏈安全、人工智慧應用與安全，其中跨支柱準則之一「堅實資安治理機制及防護」，強調零信任架構(ZTA)已成為近年資安治理中不可或缺的一環，透過「絕不信任，永遠驗證」的理念，可有效降低網路攻擊的影響範圍，並提到運作韌性是資安治理的另一核心要素，而韌性的實現包括推動關鍵系統核心功能朝境外雲端備援轉型，加強基礎設施的異地備援與容錯設計等；另我國「國家資通安全發展方案(114 年至 117 年)」[43]並針對關鍵基礎設施，提出培育高階型資安人才、強化資安威脅監控、加強情資分享、

[40] https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202405061552070.pdf&filedisplay=金融資安人才職能地圖_11304 版.pdf
[41] https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202410210854050.pdf&filedisplay=金融零信任架構參考指引.pdf
[42] https://www.president.gov.tw/Page/317/1870
[43] https://www-api.moda.gov.tw/File/Get/acs/zh-tw/tcWbCXvyTtLkaRY

辦理實地演練與稽核、落實各領域資安防護基準等執行措施。

為應國家資通安全戰略及國家資通安全發展方案，並從前述國際趨勢可以推得，除了最低的合規標準，透過將資安議題上升至公司治理層級，採可監控、可量測、可成長的方式，持續提升資安成熟度，並從軟體根本的開發和使用上進行安全性管控，才得以更主動、更有效地面對不斷演進的資安威脅，金融機構並應改變傳統以系統為中心的「營運持續」思維，朝向以服務為中心的「營運韌性」，將整個生態系(包含供應商及合作夥伴等)視為服務的一部分，從預防災難發生到假設災難發生，持續針對複合情境進行測試演練，才得以有效控制、降低損失及維持信譽。

因此，本發展藍圖採「四軸架構」，引導金融體系由「合規導向」轉向「成果導向」，旨在形成一個不斷提升資安治理的良性循環，使金融機構的資安防護具備可預測性、可防禦性與可復原性。

	軸線	核心目標	達成路徑
一	目標治理	成果導向，強化決策鏈與問責鏈，建立可衡量、可提升的治理體系。	強化高層問責、法規調適與人才韌性。
二	全域防護	從安全設計到技術韌性的全鏈防護，建構可持續演進的安全技術藍圖。	推動「資安左移」與「零信任架構」，提升資安監控效能，前瞻部署AI、PQC 等新興科技防護。
三	生態聯防	建構跨域共防與智慧情資生態，提升整體生態系資安成熟度。	強化供應鏈資安管理與資安情資分析合作，深化國際聯防。
四	堅實韌性	確保關鍵服務持續與快速恢復，達成可持續運作與快速恢復。	以演訓、備援與風險分層確保關鍵金融服務不中斷。

肆、 推動措施

根據前述四大軸線，推動 10 個工作項目計 29 項執行措施如下：

一、 目標治理：以成果導向強化決策鏈與問責鏈

由合規導向轉為成果導向，建立具前瞻性與彈性的資安治理模式，強化高層問責、法規調適與人才韌性，建立可衡量、可提升的治理體系。

(一) 強化經營階層資安治理職能與問責機制，鼓勵資安法規調適

1. 提升董事會資安監督能量，資安納入公司治理核心

金管會要求金融機構應將資安辦理情形定期提報董事會，為提升董事會對資安議題之決策能量，前於金融資安行動方案持續鼓勵金融機構遴聘具資安背景之董事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。將持續推動提升董事會資安監督能量，資安納入公司治理核心，並將資訊安全目標與組織的整體業務目標相結合，確保資安策略能為企業創造價值、降低風險並實現永續發展。

2. 強化金融資安長問責及賦權機制

金管會已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，為進一步強化資安長職責與權責，確保其有足夠職能、資源和權限執行資安業務，爰續參考美國 NYDFS Part 500 明訂資安長之職責，包含資安長應對資安業務之合規性負一定責任，每年向董(理)事會報告資安整體執行情形等。另考量各金融機構業務、規模、環境之差異性，適度授權資安長於執行上基於一定理由或特定範圍可採取相當控制措施，以提升資安治理之效率與彈性，建立具「責任、權限、資源」三位一體的金融資安治理架構強化問責鏈、確保決策獨立、提

升資安治理彈性與韌性。

3. 增修訂資安自律規範，鼓勵資安法規調適

延續金融資安行動方案，持續督導金融同業公會因應資安威脅、業務需求及新興科技等增修訂資安相關自律規範或作業指引，提供金融機構強化資安防護之準據。另考量資安法遵要求因應愈趨繁複，且更新速度可能難以因應資安威脅演變，爰鼓勵於法規之增修，併同就既有法規重疊、滯礙或策略目標進行法規調適或前瞻布局，亦鼓勵採風險基礎方法(RBA)，適度授權資安長於執行上基於一定理由或特定範圍可採取相當控制措施，以提升資安治理之效率與彈性。

(二) 加強資安人才培育與交流，從共通基準邁向策略目標

4. 滾動修訂金融資安人才職能地圖，鼓勵優化資安職能配置及取得專業證照

金管會於 2021 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，並從需求面鼓勵金融機構重視各式資安人才之配置及取得資安證照(書)，以強化金融機構防護能量，並利金融資安人才之職涯發展。為應對全球化、國家級的資安威脅，將於前述基礎上，持續因應新興科技發展、金融政策及法規調適、實務需求等滾動修訂；並鼓勵金融機構參考美國 NICE 框架[44]盤點現行金融資安人才分布情形及缺口，據以健全資安職能配置。

5. 鼓勵分享前瞻規劃暨典範實務

金管會自 2017 年底成立 F-ISAC 推動金融資安聯防，已建立金融機構間的橫向鏈結，就資安情資分享、網路攻防演練、重大資安事件情境演練及零信任架構導入等，辦理金融業分享交流活動並獲回饋意見。金管會亦藉由定期

[44] https://niccs.cisa.gov/tools/nice-framework

召開資安長聯繫會議，就當前重要資安政策措施與監理重點、資安情勢及資安聯防等議題交換意見。配合目標導向治理之推動，規劃以此為基礎，藉由定期舉辦跨機構「主題式」論壇、工作坊或案例研討，聚集相同領域之跨機構人才，共同研討金融資安前瞻規劃暨典範實務，深化資安人才之知識共享及技術提升，並做為轉型目標治理之關鍵策略。

6. 目標導向，銜接防護基準與典範實務

資安規範係奠基於可共通遵循之防護基準(即最低的資安合規要求)，惟僅以合規要求作為防線勢難以因應網路攻擊之高速演化，金管會前參考美國 FFIEC 採可重覆量測之網路安全評估工具(CAT)[45]，調適訂定成熟度等級，鼓勵金融機構據以自主評估並持續強化相關資安管理作業。惟經檢視討現行規範與成熟度指標間尚未能完全接軌，爰規劃以既有資安規範為基準、「典範實務(Best Practice)」為目標，調修建立成熟度分級評估指標，引導金融機構從合規導向轉向目標導向，建立「可量測、可成長、可差異化」監理架構。

二、 全域防護：從安全設計到技術韌性的全域防護

推動「資安左移」與「零信任架構」，提升資安監控效能，前瞻部署 AI、PQC 等新興科技防護，建構可持續演進的安全技術藍圖。

(三) 資安左移，安全納入設計(Secure By Design)

7. 鼓勵導入軟體安全開發、測試及部署流程(CI/CD)

傳統軟體開發流程著重於功能實現與滿足使用者需求，安全性檢測常被延後至測試階段或功能上線前才進行，導致系統設計初期的安全缺陷未能及早發現，增加潛在資安風險，且一旦開發後期或上線前才發現安全漏洞，再緊

[45] https://www.ffiec.gov/sites/default/files/media/resources/FFIEC_CAT_May_2017.pdf

急進行修補或採行減緩措施，將增加修復成本及延宕專案期程。爰規劃參考美國 NIST SSDF 框架[46]、國際組織 OWASP SAMM 模型[47]及相關應用程式安全驗證標準(如 OWASP ASVS 等)，鼓勵金融機構導入軟體安全開發、測試及部署流程，如於分析設計階段進行風險評估或威脅建模，將安全控制嵌入設計、開發、測試與部署流程中，於實作與測試階段以安全開發為原則，並適時將安全性工具(SAST/DAST)整合到後續發佈與部署(CI/CD)流程。

8. 建立軟體供應鏈透明化與弱點追蹤機制

於軟體生命週期藉由軟體成分分析(SCA)，識別其使用的組件(含開源、第三方元件)及其依賴組件，產出軟體物料清單(SBOM)，提升軟體組件透明度與可追溯性，並連結弱點資料庫(CVE)[48]或已知被利用漏洞(CISA KEV)[49]，建立漏洞監控與版本更新之機制。

9. 研訂 API 安全基準，建立 API 安全管理機制

考量 API 為金融業系統間溝通之重要橋樑，且 API 常具有較高之權限與風險，OWASP 亦已發布 Top 10 API Security Risks[50]，爰規劃於銀行公會既有開放銀行 Open API 規範之基礎上，研訂更完整且涵蓋 Partner API 及 Internal API 之 API 安全基準，依據存取資料之機敏性及對象等，區分 API 類別及等級，落實 API 資安管控。

(四) 推動零信任架構(ZTA)，提升資安防護基準

10. 推動導入高風險場域，漸進提升成熟度

金管會於 2024 年 7 月 15 日發布「金融業導入零信任架構參考指引」[51]，建議金融機構以風險導向，擇高風險低衝擊之場域先行，並依該高風險場域之完整存取路徑

[46] https://csrc.nist.gov/projects/ssdf
[47] https://owasp.org/2020/02/11/SAMM-v2
[48] https://www.cvedetails.com/
[49] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[50] https://owasp.org/www-project-api-security/
[51] https://www.fsc.gov.tw/websitedowndoc?file=chfsc/202410210854050.pdf&filedisplay=金融業導入零信任架構參考指引.pdf

(即身分、設備、網路、應用程式、資料 5 大支柱)，評估既有資安防護機制之完備度，依傳統、初始、進階及最佳等四階段循序漸進導入相關控制措施。據至 2025 年調查，多數金融機構已陸續擇場域導入/規劃零信任架構，以此為基礎持續推動高風險場域優先導入，並漸進提升成熟度。

11. 鼓勵導入實務分享與交流

為推動金融機構導入零信任架構，持續由各業別重點推動對象組成先導小組，並由 F-ISAC 協助建立交流平台，進行零信任架構之技術交流，分享導入規劃及實務，帶動持續深化及擴散。

12. 建立導入實務共識，漸進納入基礎規範

定期調查各金融機構於零信任架構之導入規劃及進程，召集相關周邊單位、同業公會共同依據各金融業別屬性、規模及業務風險等，衡量實際資安防護需求及執行可達性，滾動修訂推動策略及實施進程，並評估將實作參考原則漸進納入資安基礎規範，提升整體資安防禦水準。

(五) 強化資安監控及防護有效性

13. 增修訂資安組態及監控作業基準

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，金管會自 2020 年起鼓勵金融機構建置資安監控機制(SOC)，隔(2021)年起研析駭客組織攻擊手法，制定金融資安監控及組態基準，提供金融機構設定資通訊設備組態及建置營運 SOC 參考，構成 F-ISAC、金融機構及資通訊設備廠間互利共好生態圈。

配合零信任架構之導入與提升成熟度，資安監控及組態基準亦不可或缺且仍需持續精進，爰規劃持續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，並持續研析駭客組織新興攻擊手法及擴增資安監控及組態基準涵蓋範圍。

14. 雲地資安接軌，確保資安水準

金融機構原於地端資安防護已有一定的基礎，惟雲端環境與傳統地端架構存在資安管控責任差異與技術挑戰，依雲端共同責任模型，雲端服務提供者及金融機構各自所應負責處理安全性工作，如管理不當易造成管理縫隙與風險外溢。

金管會於 2024 年起規劃將資安監控及組態基準延伸至雲端服務環境，並於 2025 年 3 月先以 MITRE ATT&CK Cloud Matrix[52]及網際網路安全中心(Center for Internet Security, CIS)就公有雲基礎服務所發布的 CIS Benchmarks(如帳號管理、靜態資料儲存、託管虛擬機、稽核紀錄、無伺服器運算、機密與金鑰管理及 IaaS 等)[53]為範圍，提供金融雲端資安監控及組態基準以供金融機構於規劃導入雲端服務時參考運用。為因應雲端服務的快速發展，爰規劃持續擴增其範疇(如容器服務、PaaS 等)，確保在雲地接軌上維持一致且高水準的資安防護。

15. 鼓勵資安監控及防護有效性評估

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，爰持續鼓勵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。

(六) 前瞻部署，因應新興科技的挑戰

16. 人工智慧(AI)強化效率，資安守護信任

AI 技術快速發展，加速金融機構應用 AI 技術，考量

[52] https://attack.mitre.org/matrices/enterprise/cloud/
[53] https://www.cisecurity.org/cis-benchmarks

AI 系統的資安風險與傳統系統雖有交集，但更複雜與隱蔽，使得傳統資安政策無法直接套用，需延伸出 AI 專屬資安框架，爰規劃參考 OWASP 已成立生成式 AI 安全性專案[54]，以及 MITRE 以 MITRE ATT&CK 為藍本，補充發布 MITRE ATLAS (Adversarial Threat Landscape for AI Systems)[55]，將其相關安全設計及檢測機制納為後續研議重點，研訂金融業 AI 系統安全防護及檢測參考指引，引導金融業於 AI 系統設計納入風險評估或威脅建模作業，以涵蓋傳統網路威脅及 AI 特有攻擊類型，並應視情境導入隱私強化技術，及適時對 AI 系統進行安全性相關測試、驗證與演練等，降低其 AI 曝險程度。

17. 盤查加密態勢，布局後量子密碼(PQC)遷移

量子電腦已證實對「非對稱式加密技術」構成嚴重威脅，影響網路交易、電子簽章及身分驗證等加密安全，美國國家標準暨技術研究院(NIST)已於 2025 年 3 月發布三項後量子密碼(Post-Quantum Cryptography, PQC)演算法標準文件[56]。

為因應量子運算發展帶來的風險，美國 FS-ISAC 已成立 PQC 工作小組，自 2023 年起陸續發布盤點基礎設施加密技術、因應後量子密碼準備路線圖、建構加密敏捷性、對支付卡產業衝擊等報告[57]。金管會已於 2025 年 7 月籌組先導小組，召集具代表性利害關係成員，並透過 F-ISAC 建立溝通討論平台，凝聚推動共識並研擬 PQC 遷移準備事項，將陸續進行技術清單，識別組織應用在 ICT 中的加密技術(包含網路協議、硬體設備及軟體套件等)，並據以評估其安全等級及業務風險(至少包含資料保密期間、業務衝擊、業務相依性、生態系關聯性 、國際接軌、加密技術脆弱性等因子)，及辦理其他準備工作(至少包含培訓

[54] https://genai.owasp.org/
[55] https://atlas.mitre.org/
[56] https://csrc.nist.gov/projects/post-quantum-cryptography
[57] https://www.fsisac.com/knowledge/pqc

技術人力、調查主要供應商、提升加密敏捷性、制定系統汰換採購策略等)，研訂金融業 PQC 遷移參考指引，提供金融業據以建立 PQC 遷移計畫，及視量子電腦及 PQC 發展成熟度適時推動金融機構辦理 PQC 遷移作業。

三、 生態聯防：建構跨域共防與智慧情資生態

強化供應商於資安之透明性及可歸責性，並透過跨業聯防協作提升供應鏈之資安成熟度，增進資安聯防運作效能，提升整體金融生態系韌性。

(七) 強化供應鏈資安，健全金融資安生態系

18. 研訂供應商分級及委外資安責任參考範本

因應數位轉型與金融生態系的發展，金融業對於第三方服務供應商與外包商的依賴程度日益加深，供應鏈的組成也愈趨於多元且複雜。因應供應鏈攻擊增溫趨勢，爰規劃依產業特性、供應商接觸資通系統之類別及資料敏感度等面向進行分級，研訂資安責任之委外契約參考條款，如資安服務水準協議(SLA)、資料保護責任、對於資安事件之通報時限及資安風險揭露等；又如金融機構對於軟體安全開發階段，要求供應商提供其產品或服務之安全性檢測證明及軟體物料清單、配合一定程度之資安測試及演練等，提供金融機構參考強化其供應商資安管理。

19. 鼓勵與關鍵供應商資安情資分享與協作

除由 F-ISAC 持續自 TWCERT/CC 及同業資安聯盟等資安情資來源，取得供應商異常資訊，並分享供應商相關漏洞資訊及其攻擊手法與防禦策略外，亦鼓勵金融機構建立供應鏈風險評估機制，與其關鍵供應商、第三方服務商、系統整合商等上下游合作，分享威脅、保護資訊、強化控管，聯合資安演練，降低整體供應鏈的資安風險。

(八) 加強資安情資分析與協同防禦

20. 強化資安情資關聯分析及情資分享動能

金管會自2017年底成立F-ISAC推動金融資安聯防，已建立金融機構間的橫向鏈結，另於2022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。為增加情資介接可用性及廣度，規劃強化既有情資自動化(API)分享機制，提供會員可依需求種類取得情資，並研議修訂情資分享獎勵辦法，鼓勵會員蒐集分享生態系關聯曝險情資。

21. 建立金融資安漏洞通報與回應管道

金管會為降低金融機構外部曝險，自2025年起模擬駭客角度，檢測金融業者對外之網際網路服務是否存在未修補之漏洞、使用不安全的加密機制或錯誤的組態設定等，並將檢測結果轉化為資安情資由F-ISAC通報金融機構應處，除將賡續辦理外，另由F-ISAC規劃建立金融資安漏洞通報與回應管道，擴大金融資安漏洞通報來源，並於初判後轉介金融機構應處，降低網路攻擊的風險。

22. 提升金融機構SOC與聯防SOC協同運作效能

金管會持續鼓勵金融機構建置資安監控機制(SOC)，並督導F-ISAC建置聯防SOC，為能對參與金融機構回傳事件單做更有效率之關聯分析，責由F-ISAC輔導金融機構SOC導入資安監控及組態基準，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。為更增進聯防SOC對事件單的分析價值，規劃導入自動化分析機制，強化事件單中關鍵資訊(如攻擊手法、影響範圍、攻擊鏈位置)的萃取與比對，並結合威脅情資庫進行關聯分析，藉由建立事件單內容分類與優先度標準，提升SOC在事件研判、趨勢掌握與預警通報上的精準度與即時性，進而提供金融機構更高效的分析結果。

23. 加強金融資安國際合作

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 等簽訂 MOU，並成為資安事件應變及安全小組論壇(FIRST)、亞太地區電腦網路危機處理聯合組織(APCERT)。為持續強化與國際合作夥伴互享資安威脅情資，規劃定期舉辦跨國線上交流會議，分享我國近期攻擊案例、趨勢及防禦策略等，並定期提供我國英文版威脅分析報告及整體威脅態勢報告，深化與國際合作夥伴交流及提升國際能見度，並強化跨境事件的預警與應變效益。

四、 堅實韌性：確保關鍵服務持續與快速恢復

以演訓、備援與風險分層確保關鍵金融服務不中斷，達成可持續運作與快速恢復。

(九) 辦理資安攻防演訓，強化資安事件應處能量

24. 辦理金融機構 DDoS、網路攻防或其他資安演練

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，爰金管會為強化因應駭客攻擊之防禦能量，導入 MITRE 發布之攻擊與防禦方法論(MITRE ATT&CK & ENGAGE)，延續金融資安行動推動措施，透過辦理金融資安攻防演練，增進第一線防守量能。

25. 開設金融資安演訓專班

除持續辦理前揭攻防演練外，考量金融機構規模與資安人力資源之差異，為擴大對攻擊防禦認知與技能培訓，規劃與訓練機構合作，另以演訓專班方式擴大參與量能。

26. 辦理重大資安事件應變情境演練

除延續辦理攻防演練及演訓專班外，為驗證於重大資安事件之指揮體系運作，擴大演練情境之廣度與深度，如勒索軟體、供應鏈攻擊、雲端供應商服務中斷等應變情境演練，並適度驗證金融機構與金控集團電腦資安事件應變

小組、周邊單位或公會之資安應變支援小組、F-ISAC 等資安聯防體系間之通報、協調及支援機制。

(十) 強化多層次備援機制，確保關鍵金融服務可用性

27. 鼓勵導入國際營運持續管理標準及取得相關驗證

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。

28. 因應複合災難情境，建立關鍵服務多層次備援機制

金管會發布金融資安行動方案2.0時考量金融核心業務資料之保全攸關民眾於金融機構財產權之確保，為因應重大資安事件、天然災害及地緣政治等風險，除金融機構既有的本地及異地備份及備援機制外，已將強化金融機構關鍵資料保全機制(如第三地或雲端備份等)列為推動重點之一。為持續提升災難復原能力及業務持續運作的韌性，爰規續推進強化關鍵金融服務多層次備援架構，依據營運衝擊分析(BIA)評估於各式備援情境之最小復原需求，設定復原時間目標(RTO)與資料復原點目標(RPO)，作為備援設計與資源分配的依據，並考量實際災難發生時的跨區資源調度與指揮運作，透過定期測試與演練驗證，以於任一層故障時皆能切換運作，優先恢復關鍵金融服務。

29. 評估建立關鍵金融服務生態系營運持續量能、備援協作機制

考量金融服務高度依賴外部供應商與生態系合作夥伴(如核心系統廠商、電信業者、支付處理機構、API 介接對象等)，爰金融機構應同步針對關鍵供應鏈夥伴評估其災難復原與備援能力是否足以支援關鍵金融服務，並建

立相關備援協作機制或研擬替代措施，併納入備援及演練規劃。

伍、 推動與管考

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。

本藍圖發布後，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 115 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。

陸、 預期成效

一、 **政策面**：採雙軌制，透過推動產業規範(標準化)與典範實務(最佳化)並行，奠立短、中、長程目標，逐步降低金融業法遵負擔，並由金融機構經營層級帶動提升資安治理成熟

度與韌性，以堅實支撐金融服務創新與 AI 應用安全落地。

二、 **管理面**：透過推動金融業強化軟體安全、供應鏈安全管理與協作機制等，提升跨業防護與復原能力，降低供應商資安事件對於金融業的衝擊，保障金融穩定性。

三、 **技術面**：透過推動金融業逐步導入零信任架構、建立多層次備援機制及擴大演練範疇等，以增強金融機構攻擊預警能力(TTP Intelligence)及降低重大事故平均恢復時間(MTTR)。

四、 **國際面**：透過持續提升本國金融機構營運韌性，加強與國際金融資安組織合作，提升台灣金融資安的國際信任評等，並有利金融機構跨國合作與外資布局。

柒、 未來展望

未來的資安威脅不會因金融機構防禦能力提升而減弱，反而會因科技持續性的革新而更加複雜。因此，金融體系必須從「防止發生」的心態，轉向「快速反應、快速恢復」的韌性邏輯。

本藍圖提出的四軸架構，結合國際監理趨勢、台灣實務現況與科技發展方向，透過強化高層治理的問責鏈、導入前瞻的技術防護(如資安左移、零信任、AI/PQC 部署)、擴大供應鏈的協同防禦，並透過多層次備援與常態化演訓，期於金融業建立一套：可執行、可量測、可提升、可國際接軌的韌性治理模式，最終目標是打造：安全、可信、可持續創新的台灣金融生態系。

附件、執行措施彙總表

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
一、目標治理	1.強化經營階層資安治理職能與問責機制，鼓勵資安法規調適	(1)提升董事會資安監督能量，資安納入公司治理核心	金融機構	持續	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，本會前於金融資安行動方案已推動一定規模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，並鼓勵金融機構遴聘具資安背景之董事或設置資安諮詢小組，增納專業人員參與董事會運作，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。將持續推動提升董事會資安監督能量，資安納入公司治理核心，並將資訊安全目標與組織的整體業務目標相結合，確保資安策略能為企業創造價值、降低風險並實現永續發展。 為進一步強化資安長職責與權責，確保其有足夠職能、資源和權限執行資安業務，續參考美國 NYDFS，推動金融機構應明訂資安長之職責聲明(如列出其於資安治理、風險管理、事件應對等方面之具體職責)，資安長應對資安業務之合規性負一定責任(如簽署聲明書)，並於每年向董(理)事會報告前一年度資安整體執行情形(包含但不限於：資安計畫執行及變更情形、重大資安事件與改善措施、現行資安風險評估情形及控制措施之有效性、資安預算運用與資源配置情形等)。另考量各金融機構業務、規模、環境之差異性，適度授權資安長得就資安相關規範及成熟度未達事項，提出改善方案及期程或相當控制措施並定期追蹤，建立具「責任、權限、資源」三位一體的金融資安治理架構強化問責鏈、確保決策獨立、提升資安治理彈性與韌性。	延續並強化
		(2)強化金融資安長問責及賦權機制	各業務局/金融機構	持續		延續並強化

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
		(3)增修訂資安自律規範，鼓勵資安法規調適	公會、周邊單位	持續	美國 NYDFS、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，近年已增修訂之項目包含資通安全防護基準、供應鏈風險管理規範、作業韌性參考規範等項，並已建立數位身分驗證等級與業務風險對照規範，兼顧創新與安全之平衡，將延續金融資安行動方案，持續督導金融同業公會因應資安威脅、業務需求及新興科技等增修訂資安相關自律規範或作業指引，提供金融機構強化資安防護之準據。另考量金融機構資安法遵要求愈趨繁複，部分內容重疊或衝突，形成執行負擔與落實困難，且法規更新速度可能難以因應資安威脅演變，爰將透過本會法規調適平台收集產官學界之意見，或召集各業務局、金融同業公會，鼓勵於法規之增修，併同就既有法規重疊、滯礙或策略目標進行法規調適或前瞻布局，及適度授權資安長於執行上基於一定理由或特定範圍可採取相當控制措施，以提升資安治理之效率與彈性，及有效降低金融機構在法遵作業之重複投入。	延續並強化
	2.加強資安人才培育與交流，從共通基準邁向策略目標	(4-1) 滾動修訂金融資安人才職能地圖	本會/F-ISAC	持續	本會於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)，以強化金融機構防護能量，並利金融資安人才之職涯發展。 為應對全球化、國家級的網路威脅，將持續因應新興科技發展、金融政策及法規調適、金融機構實務需求等，滾動增修訂金融資安人才職能地	延續
		(4-2) 開設金融資安人才養成專班	訓練機構	持續		延續
		(4-3) 鼓勵優化資	金融機構	持續		延續

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
		安職能配置及取得資安證照(書)			圖，如新增經營階層(如資安長、董監事等)之領域及相關課程，增設相關實務課程(如零信任架構、雲端監控與防護、攻防演練、供應鏈管理、軟體安全左移、AI 系統安全防護等)；並鼓勵金融機構參考美國 NICE 框架盤點現行金融資安人才分布情形及缺口，據以健全資安職能配置。	
		(5)鼓勵分享前瞻規劃暨典範實務	本會/ F-ISAC	持續	本會自2017年底成立 F-ISAC 推動金融資安聯防，已建立金融機構間的橫向鏈結，就資安情資分享、網路攻防演練、重大資安事件情境演練及零信任架構導入等，辦理金融業分享交流活動並獲回饋意見，亦已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，並藉由定期召開資安長聯繫會議，就當前重要資安政策措施與監理重點、資安情勢及資安聯防等議題交換意見。 配合目標導向治理之推動，將藉由定期舉辦跨機構「主題式」論壇、工作坊或案例研討，鼓勵金融機構主動投稿或聚集相同領域之跨機構人才，共同研討前瞻規劃暨典範實務(Best Practice)，深化資安人才之知識共享及技術提升，並做為轉型目標治理之關鍵策略。	新增
		(6)目標導向，銜接防護基準與典範實務	F-ISAC/ 公會、周邊單位/金融機構	持續	資安規範係奠基於可共通遵循之防護基準(即最低的資安合規要求)，惟僅以合規要求作為防線勢難以因應網路攻擊之高速演化，本會為鼓勵金融機構評估並持續追求資安治理最佳實務，前參考美國 FFIEC 採可重覆量測之網路安全評估工具(CAT)，調適訂定適用我國金融機構之評估方法及成熟度等級，鼓勵金融機構據以依其自有特性，自主風險評估其資安能力及弱點，並持續強化相關資安管理作業。截至114年第3季止，已有86家金融機構辦理資安治理成熟度評估作業。 為因應美國 FFIEC CAT 已於2025年8月31日停止使用，既有成熟度評估	延續並強化

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
					方法除將參考美國 NIST CSF2.0、CRI Profile 或 CISA CPG 等工具進行適度調整及精簡，經檢視討現行規範與成熟度指標間尚未能完全接軌，並將參考美國財政部及 CISA 設立金融產業特定目標(FS-SSGs)之精神，以既有資安規範為基準、「典範實務(Best Parctice)」為目標，由 F-ISAC 調修建立成熟度分級評估指標，引導金融機構從合規導向轉向目標導向，建立「可量測、可成長、可差異化」監理架構。	
二、全域防護	3. 資安左移，安全納入設計(Secure By Design)	(7)鼓勵導入軟體安全開發、測試及部署流程(CI/CD)	金融機構	持續	傳統軟體開發流程著重於功能實現與滿足使用者需求，安全性檢測常被延後至測試階段或功能上線前才進行，導致系統設計初期的安全缺陷未能及早發現，增加潛在資安風險，且一旦開發後期或上線前才發現安全漏洞，再緊急進行修補或採行減緩措施，將增加修復成本及延宕專案期程。 參考美國 NIST SSDF 框架、國際組織 OWASP SAMM 模型及相關應用程式安全驗證標準(如 OWASP ASVS 等)，鼓勵金融機構構導入軟體安全開發、測試及部署流程，如於分析設計階段進行風險評估或威脅建模，將安全控制嵌入設計、開發、測試與部署流程中，於實作與測試階段以安全開發為原則，適時將安全性工具(SAST/DAST)整合到後續發佈與部署(CI/CD)流程，並藉由進行軟體成分分析(SCA)，識別其使用的組件(含開源、第三方元件)及其依賴組件，產出軟體物料清單(SBOM)，提升軟體組件透明度與可追溯性，並連結弱點資料庫(CVE)或已知被利用漏洞(CISA KEV)，建立漏洞管理與即時版本更新之機制。另考量 API 為金融業系統間溝通之重要橋樑，且 API 常具有較高之權限與風險，OWASP 亦已發布 Top 10 API Security Risks，爰將於銀行公會既有開放銀行 Open	新增
		(8)建立軟體供應鏈透明化與弱點追蹤機制	金融機構	持續		新增
		(9)研訂 API 安全基準，建立 API 安全管理機制	F-ISAC/ 公會	一年		新增

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
					API 規範之基礎上,研訂更完整且涵蓋 Partner API 及 Internal API 之 API 安全基準，依據存取資料之機敏性及對象等，區分 API 類別及等級，落實 API 資安管控。	
	4.推動零信任架構(ZTA),提升資安防護基準	(10)推動導入高風險場域，漸進提升成熟度	金融機構	持續	本會於2024年7月15日發布「金融業導入零信任架構參考指引」,建議金融機構以風險導向，擇高風險低衝擊之場域先行，並依該高風險場域之完整存取路徑(即身分、設備、網路、應用程式、資料5大支柱)，評估既有資安防護機制之完備度，依傳統、初始、進階及最佳等四階段循序漸進導入相關控制措施。	延續並強化
		(11)鼓勵導入實務分享與交流	本會/F-ISAC	持續		新增
		(12)建立導入實務共識，漸進納入基礎規範	公會、周邊單位	持續	據至2025年調查,多數金融機構已擇至少1個場域導入/規劃零信任架構,已導入者多以遠距辦公為優先導入場域(系統維運管理次之)，將以此為基礎持續推動高風險場域優先導入，並漸進提升成熟度。另為推動金融機構導入零信任架構，持續由各業別重點推動對象等組成先導小組，並由 F-ISAC 協助建立交流平台，進行零信任架構之技術交流，分享導入規劃及實務，帶動持續深化及擴散，並定期調查各金融機構於零信任架構之導入規劃及進程，召集相關周邊單位、同業公會共同依據各金融業別屬性、規模及業務風險等，衡量實際資安防護需求及執行可達性，滾動修訂推動策略及實施進程，並評估將實作參考原則漸進納入資安基礎規範，提升整體資安防禦水準。	新增
	5.強化資安監控及防護有效性	(13-1)推動建置資安監控機制	金融機構、周邊單位	持續	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，爰本會自109年起鼓勵金融機構建置資安監控機制(SOC)，隔(110)年起研析駭客組織攻擊手法，制定金融資安監控組態基準，提供金融機構設定資通訊設備組態及建置 SOC 參考，構成 F-	延續並擴大
		(13-2)增修訂資安組態及監控	F-ISAC	持續		延續並擴大

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
		作業基準			ISAC、金融機構及資通訊設備廠間互利共好生態圈。 配合零信任架構之導入與提升成熟度，資安監控及組態基準亦不可或缺且仍需持續精進，爰持續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），並持續研析駭客組織新興攻擊手法及擴增資安監控及組態基準涵蓋範圍。	
		(14)雲地資安接軌，確保資安水準	金融機構、周邊單位/F-ISAC	兩年	金融機構原於地端資安防護已有一定的基礎，惟雲端環境與傳統地端架構存在資安管控責任差異與技術挑戰，依雲端共同責任模型，雲端服務提供者及金融機構各自所應負責處理安全性工作，如管理不當易造成管理縫隙與風險外溢。本會於2024年起規劃將資安監控及組態基準延伸至雲端服務環境，並於2025年3月先以 MITRE ATT&CK Cloud Matrix 及網際網路安全中心(Center for Internet Security, CIS)就公有雲基礎服務所發布的 CIS Benchmarks（如帳號管理、靜態資料儲存、託管虛擬機、稽核紀錄、無伺服器運算、機密與金鑰管理及 IaaS 等）為範圍，提供金融雲端資安監控及組態基準以供金融機構於規劃導入雲端服務時參考運用。為因應雲端服務的快速發展，並提升金融業對於雲地架構的風險辨識及一致性防護能力，將請 F-ISAC 持續擴增雲端資安監控基準研究範疇，如115年增加容器服務，116年補齊尚未涵蓋之 PaaS 範疇(如雲端資料庫、無伺服器應用、雲端 SOAR 等)，確保金融機構在雲地接軌上維持一致且高水準的資安防護。	延續並擴大
		(15)鼓勵資安監控及防護有效性	金融機構	持續	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，爰持續鼓勵已建置 SOC 之金融機構引入攻擊方思	延續

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
		評估			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，定期檢驗自身資安監控及防禦部署之有效性。	
	6. 前瞻部署，因應新興科技的挑戰	(16)研議訂定 AI 系統安全防護及檢測參考指引	本會/F-ISAC	一年	近年人工智慧(AI)技術發展迅速，加速金融機構應用 AI 技術，考量 AI 系統的資安風險與傳統系統雖有交集，但更複雜與隱蔽，使得傳統資安政策無法直接套用，需延伸出 AI 專屬資安框架，爰為應國際間強調金融機構應導入 AI 生命週期治理機制等，將參考國際組織 OWASP 已成立生成式 AI 安全性專案、MITRE 以 MITRE ATT&CK 為藍本，補充發布 MITRE ATLAS 等，將其相關安全設計及檢測機制納為後續研議重點，研議訂定金融業 AI 系統防護及檢測參考指引，引導金融業於 AI 系統設計初期納入風險評估或威脅建模作業，以涵蓋傳統網路威脅及 AI 特有攻擊類型，並應視情境導入隱私強化技術，及適時對 AI 系統進行安全性相關測試、驗證與演練等，降低其 AI 曝險程度。	新增
		(17-1)辦理 PQC 遷移準備，並研訂 PQC 遷移參考指引。	本會、公會、金融機構、周邊單位、F-ISAC	一年	量子電腦已證實對「非對稱式加密技術」構成嚴重威脅，影響網路交易、電子簽章及身分驗證等加密安全，美國 NIST 已於2025年3月發布三項 PQC 演算法標準文件，美國 FS-ISAC 已成立 PQC 工作小組，自2023年起陸續發布盤點基礎設施加密技術、因應後量子密碼準備路線圖、建構加密敏捷性、對支付卡產業衝擊等報告。 本會已於2025年7月籌組先導小組，召集具代表性利害關係成員，並透過 F-ISAC 建立溝通討論平台，凝聚推動共識並研擬 PQC 遷移準備事項，將陸續建立加密技術清單，識別組織應用在 ICT 中的加密技術(包含網路協議、硬體設備及軟體套件等)，並據以評估其安全等級及業務風險(至少包含資料保密期間、業務衝擊、業務相依性、生態系關聯性 、國際接	新增
		(17-2)推動金融機構辦理 PQC 遷移作業	金融機構、周邊單位	持續		新增

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
					軌、加密技術脆弱性等因子)，及辦理其他準備工作(至少包含培訓技術人力、調查主要供應商、提升加密敏捷性、制定系統汰換採購策略等)，研訂金融業 PQC 遷移參考指引，提供金融業據以建立 PQC 遷移計畫，及視量子電腦及 PQC 發展成熟度適時推動金融機構辦理 PQC 遷移作業。	
三、生態聯防	7.強化供應鏈資安，健全金融資安生態系	(18)研訂供應商分級及委外資安責任參考範本	公會、周邊單位	一年	因應數位轉型與金融生態系的發展，金融業對於第三方供應商與外包商的依賴程度日益加深，供應鏈的組成也愈趨於多元且複雜，然現行主要由金融機構自行於委外契約或相關文件，約定各項服務要求、定義資安相關權責及罰責等，缺乏共通性原則及較明確之要求，較難以確保最低資安水準。 因應供應鏈攻擊增溫趨勢，將督導金融同業公會依其產業特性、供應商接觸資通系統之類別及資料敏感度等面向進行分級，研訂資安責任之委外契約參考條款，訂定差異化審查項目及標準(如不同風險等級之供應商應符合之國際標準、資安曝險程度要求等)，並參考我國資安法施行細則及歐盟 DORA 等法規，確保委外契約包含必要的資安條款，如資安服務水準協議(SLA)、資料保護責任、對於資安事件之通報時限及資安風險揭露等；又如配合金融機構對於軟體安全開發，要求金融機構之供應商應提供其產品或服務之安全性檢測證明及軟體物料清單(SBOM)、配合共同進行一定程度之資安測試及演練，與違反時相關罰則、保留金融機構之稽核權等，提供金融機構參考強化其供應商資安管理；另除由 F-ISAC 持續自 TWCERT/CC 及同業資安聯盟等資安情資來源，取得供應商異常資訊，並分享供應商相關漏洞資訊及其攻擊手法與防禦策略外，	新增
		(19)鼓勵與關鍵供應商資安情資分享與協作	金融機構	持續		新增

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
					亦鼓勵金融機構建立供應鏈風險評估機制，與其關鍵供應商、第三方服務商、系統整合商等上下游合作，分享威脅、保護資訊、強化控管，聯合資安演練，降低整體供應鏈的資安風險。。	
	8.加強資安情資分析與協同防禦	(20)強化資安情資關聯分析及情資分享動能	F-ISAC	持續	本會自2017年底成立 F-ISAC 推動金融資安聯防，已建立金融機構間的橫向鏈結，並於111年底建置資安情資關聯分析平台，提供自動化情資介接及情資分享獎勵機制。 為增加情資介接可用性及廣度，規劃強化既有情資自動化(API)分享機制，提供會員可依需求種類取得情資，並研議修訂情資分享獎勵辦法，鼓勵會員蒐集分享生態系關聯曝險情資。	延續並強化
		(21)建立金融資安漏洞通報與回應管道	F-ISAC	一年	本會為降低金融機構外部曝險，自114年起模擬駭客角度，檢測金融業者對外之網際網路服務是否存在未修補之漏洞、使用不安全的加密機制或錯誤的組態設定等，並將檢測結果轉化為資安情資，由 F-ISAC 通報金融機構應處。 除持續定期辦理上述網際網路檢測，規劃由 F-ISAC 建立金融機構資安漏洞通報與回應管道，擴大金融資安漏洞通報來源，並由 F-ISAC 於初步判斷後轉介金融機構應處，降低網路攻擊的風險，並發布報告供各金融機構參辦。	新增
		(22)提升金融機構 SOC 與聯防 SOC 協同運作效能	F-ISAC	持續	本會持續鼓勵金融機構建置資安監控機制(SOC)，並督導 F-ISAC 建置聯防 SOC，為能對參與金融機構回傳事件單做更有效率之關聯分析，責由 F-ISAC 輔導金融機構 SOC 導入資安監控組態基準，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。 為更增進聯防 SOC 對事件單的分析價值，規劃導入自動化分析機制，	延續並強化

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
					強化事件單中關鍵資訊(如攻擊手法、影響範圍、攻擊鏈位置)的萃取與比對，並結合威脅情資庫進行關聯分析，藉由建立事件單內容分類與優先度標準，提升 SOC 在事件研判、趨勢掌握與預警通報上的精準度與即時性，進而提供會員更具行動性的分析結果。	
		(23)加強金融資安國際合作	F-ISAC	持續	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，並成為資安事件應變及安全小組論壇(FIRST)、亞太地區電腦網路危機處理聯合組織(APCERT)成員。 為持續強化與國際合作夥伴互享資安威脅情資，規劃定期舉辦跨國線上交流會議，分享我國近期攻擊案例、趨勢及防禦策略等，並定期提供我國英文版威脅分析報告及整體威脅態勢報告，深化與國際合作夥伴交流及提升國際能見度，並強化跨境事件的預警與應變效益。	延續
四、堅實韌性	9.辦理資安攻防演訓，強化資安事件應處能量	(24)辦理金融機構DDoS、網路攻防或其他資安演練	本會/F-ISAC	持續	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，爰本會為強化因應駭客攻擊之防禦能量，導入 MITRE 發布之攻擊與防禦方法論(MITRE ATT&CK & ENGAGE)，並透過辦理金融資安攻防演練、金融資安攻防演練評比活動、重大資安事件情境演練等，增進第一線防守量能，實證金融機構因應攻擊之防禦能量與應變能力，及考驗跨領域或跨機構間之橫向通報應變與協作。 除延續辦理前揭攻防演練外，考量金融機構規模與資安人力資源之差異，為擴大對攻擊防禦認知與技能培訓，規劃與訓練機構合作，另以演訓專班方式擴大參與量能。另為驗證於重大資安事件之指揮體系運作，擴大演練情境之廣度與深度，如規劃勒索軟體、供應鏈攻擊、雲端供應	延續
		(25)開設金融資安演訓專班	F-ISAC、訓練機構	持續		延續
		(26)辦理重大資安事件應變情境演練	本會	持續		延續

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
					商服務中斷等應變情境演練，並適度驗證金融機構與金控集團電腦資安事件應變小組、周邊單位或公會之資安應變支援小組、F-ISAC 等資安聯防體系間之通報、協調及支援機制。	
	10. 強化多層次備援機制，確保關鍵金融服務可用性	(27)鼓勵導入國際營運持續管理標準及取得相關驗證	金融機構	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，本會持續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，並鼓勵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。	延續
		(28-1)因應複合災難情境，規劃關鍵服務多層次備援機制	各業務局/金融機構、周邊單位	持續	本會2022年12月發布金融資安行動方案2.0時，考量金融核心業務資料之保全攸關民眾於金融機構財產權之確保，爰為因應重大資安事件、天然災害等風險，除金融機構既有的本地、異地之備份及備援機制外，已將強化金融機構關鍵資料保全機制(如第三地或雲端備份等)列為推動重點之一。 為持續提升災難復原能力及業務持續運作的韌性，爰將續推進強化關鍵金融服務備援機制，由各業務局召集相關周邊單位、同業公會共同依據營運衝擊分析(BIA)評估於各式備援情境之最小復原需求，設定復原時間目標(RTO)與資料復原點目標(RPO)，作為備援設計與資源分配的依據，並考量實際災難發生時的跨區資源調度與指揮運作，透過定期測試	新增
		(28-2)因應複合災難情境，建置關鍵服務多層次備援機制	金融機構、周邊單位	持續		

構面	工作項目	執行措施	執行單位	執行期限	說明	與2.0關聯性
		(29)評估及建立關鍵金融服務生態系營運持續量能、備援協作機制	各業務局/金融機構、周邊單位	持續	與演練驗證，以於任一層故障時皆能切換運作，優先恢復關鍵金融服務；另考量金融服務高度依賴外部供應商與生態系合作夥伴(如核心系統廠商、電信業者、支付處理機構、API 介接對象等)，爰金融機構應同步針對關鍵供應鏈夥伴評估其災難復原與備援能力是否足以支援關鍵金融服務，並建立相關備援協作機制或研擬替代措施，併納入備援及演練規劃。	新增