

出國報告（出國類別：開會）

2026 英國金融資安韌性交流活動

服務機關：金融監督管理委員會

姓名職稱：林裕泰 處長

派赴國家/地區：英國倫敦

出國期間：115 年 6 月 7 日至 13 日

報告日期：115 年 9 月 8 日

摘要

本次參訪團於 115 年 6 月 7 日至 6 月 13 日赴英國參訪，觀察其金融體系在面對重大資安事件、雲端與供應鏈中斷、支付詐欺及新興科技風險時，如何維持重要金融服務持續運作。拜會對象涵蓋金融產業協會、跨國銀行、共同防禦組織、金融科技新創聚落、資安科技業者、支付網路業者及金融市場基礎設施。本次參訪重點不僅在瞭解個別機構之技術作法，更在觀察英國如何將資安治理、營運韌性、情資共享、第三方管理及新興科技風險控管，轉化為金融體系層級之協作機制。

參訪結果顯示，英國金融資安韌性之推動，已由單一機構內部防護，擴展為金融機構、金融市場基礎設施、支付網路、關鍵第三方、科技平台、電信、執法及政府部門共同參與之生態系治理。其制度特色在於以重要業務服務與影響容忍度為核心，結合產業級應變框架、跨市場演練、可行動情資、共同供應商治理及事件溝通機制，使重大事故處理不僅著重技術復原，也強調跨機構資訊一致、資源協調、服務不中斷及市場信心維持。

整體而言，本次參訪所見英國金融業相關制度設計與實務作法，與本會去年底發布之「金融資安韌性發展藍圖」政策方向具有高度呼應。其由機構治理、技術防護、跨域協作至重大事件復原之整體推動經驗，可作為我國持續深化金融資安韌性政策之重要參考；另亦見證我國金融資安資訊分享及分析中心（F-ISAC）與英國網路防禦聯盟（Cyber Defence Alliance, CDA）簽署合作備忘錄。

目錄

壹、前言.....	4
貳、參訪行程	5
參、參訪紀要與觀察.....	7
一、IBM Innovation Studio London：量子安全轉型與密碼韌性....	7
二、UK Finance：產業級營運韌性與跨機構協作	8
三、Standard Chartered Bank：全球 SOC 營運、MTTC 與 AI 輔助 防禦.....	10
四、Cyber Defence Alliance：高信任情資共享與可行動共同防禦	12
五、Level39：金融科技新創聚落與會員企業分享	14
六、Darktrace：資安 AI 應用與代理式 AI 安全治理	15
七、Visa Cyber Fusion Center：支付網路資安、反詐與數位資產韌 性治理	16
八、London Stock Exchange Group：金融市場基礎設施營運韌性與 AI 治理	18
肆、F-ISAC 與 CDA 簽署合作備忘錄（MOU）	21
伍、心得與建議.....	22

壹、前言

近年金融服務高度數位化，雲端服務、人工智慧、第三方供應鏈、跨境支付及金融市場基礎設施之相互依賴日益加深，使金融資安風險已不再只是單一機構的內部防護議題，而是關係金融體系穩定、重要業務服務持續運作及跨機構應變能力之整體韌性議題。為配合我國金融資安韌性政策推動需求，並觀察主要國際金融市場在營運韌性、資安治理、共同防禦及新興科技風險管理之制度與實務，本次規劃赴英國進行金融資安韌性研習與參訪。

英國具全球領先的金融科技與金融創新地位，倫敦長期位居世界重要金融中心與金融科技聚落前列。在資安治理方面，英國除有國家級資安機構與金融業建立風險共享與事件協作機制外，亦重視跨市場營運韌性與公私協力聯防；在人工智慧治理方面，近年積極推動 AI 安全與責任治理，兼顧技術創新、應用落地與風險控制；在支付與資料共享方面，具備快速支付及成熟支付基礎設施；在新興金融與市場基礎設施方面，亦發展出兼顧創新、法遵與營運韌性之制度環境。上述特色使英國成為觀察金融資安韌性、產業協作、支付治理與新興科技監理的重要參訪對象。

本次參訪目的在於瞭解英國金融業如何透過監理要求、產業協作、跨機構演練、威脅情報共享、關鍵第三方管理及資安事件應變機制，在重大資安事件、雲端或供應鏈中斷、詐欺威脅及新興科技風險下，維持重要金融服務持續運作，並作為我國後續金融資安政策研議、監理溝通及產業協作之參考。參訪期間亦透過與金融機構、產業協會、資安聯防組織、支付網路業者、金融科技新創聚落、資安科技業者及金融市場基礎設施交流，蒐集人工智慧、代理式人工智慧、後量子密碼、數位資產與跨境支付等新興議題之治理趨勢與實務經驗；另亦促成我國金融資安資訊分享及分析中心（F-ISAC）與英國網路防禦聯盟（Cyber Defence Alliance, CDA）簽署合作備忘錄。

貳、參訪行程

日期	參訪單位	單位簡介與參訪重點
6 月 8 日	IBM Innovation Studio London (IBM 倫敦 創新工作室)	IBM Innovation Studio London (IBM 倫敦創新工作室) 為 IBM 於倫敦設置之創新展示與交流場域，聚焦雲端、人工智慧、資安、量子運算及產業數位轉型。本次參訪聚焦量子安全轉型、後量子密碼遷移、加密資產盤點與密碼敏捷性治理。
6 月 9 日 上午	UK Finance	UK Finance 為英國金融業主要產業協會，代表銀行、支付、金融科技及相關金融服務業者，並參與營運韌性、資安政策、第三方風險及跨市場事件應變協作。
6 月 9 日 下午	渣打銀行 (Standard Chartered Bank)	渣打銀行為總部設於英國之國際性銀行，業務遍及亞洲、非洲與中東等市場。本次交流重點包括全球資安營運中心 (Security Operations Center, SOC) 營運、平均遏制時間 (Mean Time to Contain, MTTC) 管理、告警分流與 AI 輔助防禦。
6 月 10 日 上午	網路防禦聯盟 (Cyber Defence Alliance, CDA)	Cyber Defence Alliance 為由金融機構組成之非營利共同防禦組織，重視高信任情資共享、威脅排序、可行動情資、反詐協作及資料共享來源控制。本次參訪重點在觀察其共同防禦運作模式及與金融機構間之情資協作實務，並促成 F-ISAC 與 CDA 簽署合作備忘錄。
6 月 10 日 下午	Level39	Level39 為倫敦 Canary Wharf 地區之金融科技與科技新創聚落，由 Canary Wharf Group 設立，透過會員篩選、彈性辦公空間、社群

日期	參訪單位	單位簡介與參訪重點
		活動、導師與投資人連結，支持快速成長科技企業發展。本次參訪重點在瞭解其平台定位、會員服務及倫敦金融科技創新生態。
6 月 11 日 上午	Darktrace	Darktrace 為資安科技業者，本次交流如何運用行為式偵測、告警關聯分析、自動化回應邊界及 AI 使用監控，提升資安營運效率與代理式 AI 治理能力。
6 月 11 日 下午	Visa Cyber Fusion Center (融合式資安 指揮中心)	Visa 為全球支付網路業者，其 Cyber Fusion Center 整合資安事件應變、威脅情報、反詐、雲端安全、身分存取及治理風險合規功能，維持支付服務安全與韌性。
6 月 12 日	倫敦證券交易所集團 (London Stock Exchange Group, LSEG)	London Stock Exchange Group 為全球金融市場基礎設施與資料服務集團。本次參訪聚焦金融市場基礎設施之 AI 治理、第三方風險、供應鏈安全、威脅導向測試與營運韌性。

參、參訪紀要與觀察

本章依參訪機構整理會議主軸、交流內容及參訪觀察。各場次先說明參訪議題定位，再整理英方機構介紹、雙方交流重點與具體案例，最後歸納對我國金融資安治理、營運韌性、共同防禦、人工智慧資安、後量子密碼遷移、支付風控及金融市場基礎設施韌性之觀察。

一、IBM Innovation Studio London：量子安全轉型與密碼韌性

(一) **會議主軸**：本場聚焦量子運算對金融業加密體系之潛在衝擊，以及金融機構如何以治理、技術與供應鏈協作方式推動後量子密碼遷移。

(二) 交流內容

1. **量子威脅與長期資料保護**：量子運算成熟後，可能影響現行非對稱加密機制，尤其是「先收集、後解密」風險，即攻擊者先大量蒐集具長期保密價值之金融資料，待未來量子運算能力成熟後再行解密。
2. **企業級 PQC 遷移框架**：後量子密碼遷移可從加密資產發現與清點、風險評估、自動化與現代化、治理機制到業務團隊分工等面向推動，重點不僅是替換演算法，而是建立可持續管理密碼風險的治理能力。
3. **遷移時程與聯邦式執行模型**：全球主要監理機關已提醒金融業須及早規劃後量子密碼遷移，並以 2035 年前完成關鍵遷移作為重要時間壓力。實務推動上，可採中央指導、各業務與開發團隊分散執行之聯邦式執行模型，使密碼治理要求能實際落入系統開發、營運維護與供應鏈管理流程。
4. **加密資產與依賴盤點**：後量子密碼遷移需建立密碼物料清單 (CBOM)，並掌握硬體安全模組 (HSM)、金鑰管理服務

(KMS)、公開金鑰基礎設施(PKI)及憑證生命週期管理等底層依賴。

5. **供應鏈與新系統納管**：PQC 準備度需納入新系統開發、安全開發與維運流程、採購契約、第三方供應商管理與變更流程，避免今日新增系統成為未來無法遷移的新技術債。
6. **工具化支援與分工**：PQC 遷移宜結合加密使用探索、加密資產可視化、風險排序及過渡期補救等工具化支援，以降低僅依賴人工清查之限制，並協助金融機構逐步建立持續管理密碼風險之實務能力。

(三) 參訪觀察：

1. **長期密碼治理定位**：PQC 遷移應被定位為長期密碼治理工程，涵蓋治理責任、資產盤點、系統改造、測試切換、供應鏈管理與營運韌性。
2. **高價值場景與工具化支援優先**：金融業宜優先針對支付、清算、結算、跨機構連線及長期保存資料等高價值場景，建立風險導向遷移優先序，並將加密資產盤點、風險排序、技術債管理、新系統 PQC 準備度及工具化支援納入實務檢視，以利後續從清查、可視化管理到過渡期補救逐步落地。

二、UK Finance：產業級營運韌性與跨機構協作

(一) **會議主軸**：本場聚焦 UK Finance 作為英國金融業主要產業協會，如何在政策倡議、產業協調與系統性事件應變間扮演樞紐角色，並透過跨市場營運韌性小組(CMORG)、金融產業應變框架(SRF)、跨機構演練及關鍵第三方協同測試，協助金融業將監理要求轉化為可運作的產業級韌性機制。

(二) 交流內容

1. **政策倡議與產業協調角色**：UK Finance 代表英國金融服務業逾三百家會員機構，除就營運韌性、資安政策、第三方風險及事件通報等議題彙整產業意見，向政府與監理機關溝通外，也透

過常設委員會、工作小組與實務指引，協助會員理解監理要求並轉化為可執行之內部管理作法。

2. **營運韌性監理要求落地：**英國營運韌性架構強調識別重要業務服務、設定影響容忍度、執行情境測試，並將人員、流程、科技、設施、資訊、第三方與第四方依賴納入端對端盤點。其重點不在要求所有服務完全不中斷，而是在嚴重但可合理預見情境下，驗證重要服務能否在容忍範圍內維持或恢復。
3. **跨市場營運韌性治理：**跨市場營運韌性小組（Cross-Market Operational Resilience Group, CMORG）由 UK Finance 與英格蘭銀行共同推動，採公私協力及自願參與模式，結合主要銀行、金融市場基礎設施、保險業、監理機關、財政部及國家網路安全中心等成員，作為跨市場韌性議題之策略論壇。其工作計畫涵蓋跨部門韌性、第三方風險管理、產業應變、安全創新、資安威脅及韌性文化等面向。
4. **金融產業應變框架與分層運作：**UK Finance 說明，金融產業應變框架（Sector Response Framework, SRF）係重大跨市場事件下之產業協調架構，並透過跨市場業務連續性小組（CMBCG）、金融業網路協作中心（FSCCC）及事件溝通小組（ICG）等機制，分別支援高階決策、資安事件協作、產業資訊彙整及對外訊息一致，確保事件期間能依嚴重程度快速升級並維持共同語言。
5. **共同情境圖像與一致溝通：**在系統性事件或跨機構資安事故發生時，前述機制可彙整會員回報、掌握受影響服務與依賴關係、形成產業共同情境圖像，並透過標準化情勢更新與一致對外訊息，降低資訊落差、市場誤解、重複通報及各機構各自對外說明所造成的次生風險。
6. **跨市場演練與關鍵第三方測試：**英國透過兩年一次之全國性金融市場演練 SIMEX（Sector-wide Simulation Exercise）測試嚴重

但可合理預見情境下的跨機構應變能力，並於演練後檢討聯絡窗口、升級流程、資訊格式與溝通落差。另針對關鍵第三方（Critical Third Party, CTP）推動協同情境測試，由多家金融機構共同檢視雲端、支付處理或其他共同供應商之復原能力，以降低重複保證負擔並提升測試實效。

7. **共同供應商治理與新興風險議題：**彙整會員主要供應商清單、辨識共同關鍵供應商並進行集體溝通，有助降低個別金融機構重複查核負擔，也能促使大型供應商更願意回應金融業對資安與營運韌性的共同要求。另 UK Finance 亦持續關注事件通報、勒索軟體、後量子密碼、人工智慧、重大弱點修補潮與供應鏈風險等政策議題，並透過產業意見彙整，使監理要求與實務可行性之間保持對話。

（三）參訪觀察：

1. **產業共同治理：**英國金融業已將營運韌性由個別機構內部控制提升為產業共同治理，透過標準化通報、共同情境圖像、跨市場演練及共同供應商治理，強化金融體系於重大事故下之持續服務能力。
2. **共同供應商與事件溝通：**共同供應商辨識、集體溝通、金融產業應變框架（SRF）及事件溝通機制，有助於我國思考在重大事件期間，如何降低重複通報負擔、提升資訊一致性、強化關鍵第三方風險管理，並維持市場信心。

三、Standard Chartered Bank：全球 SOC 營運、MTTC 與 AI 輔助防禦

- （一）**會議主軸：**本場聚焦渣打銀行全球資安營運中心（Security Operations Center, SOC）之全天候偵測、分析與事件處理能力，並以平均遏制時間（Mean Time to Contain, MTTC）、告警分流、偵測規則調校及 AI 輔助分析為核心，觀察跨國銀行如何提升資安營運效率並縮短高速度攻擊下之應變時間。

（二）交流內容

1. **全球 SOC 營運模式：**渣打銀行資安防禦中心採全球接力式（follow-the-sun）SOC 模式，由不同區域輪值支援，維持全天候偵測、分析與事件應變能力。此一模式重點在於讓告警監控、事件研判與處置流程能隨時區接續運作，支援跨市場業務之持續服務。
2. **營運指標與 MTTC 管理：**資安營運管理可透過告警處理量、調查啟動情形、偵測規則更新、資料外洩防護掃描、端點惡意活動處置及平均遏制時間（Mean Time to Contain, MTTC）等指標，檢視 SOC 偵測覆蓋、分析效率與處置品質。MTTC 之意義不在追求單一數字，而在協助管理者判斷告警分流、人工研判、自動化輔助與處置流程是否有效銜接。
3. **高速度攻擊下之偵測與遏制：**面對攻擊者可能在入侵後快速擴散或觸及關鍵系統之情境，金融機構需縮短從告警產生、啟動調查、確認事件到遏制擴散之時間。此一流程涉及偵測規則有效性、告警優先排序、分析人員判斷、自動化輔助與處置授權，亦是 SOC 能否將技術偵測轉化為實際防禦效果之關鍵。
4. **AI 輔助告警分流與分析：**AI 可協助 SOC 進行告警初步分類、事件脈絡整理、重複告警降噪及疑似攻擊路徑提示，提升分析效率與判斷一致性。惟金融機構導入 AI 輔助資安營運時，仍須保留人工複核、權限控管、品質檢視及可稽核紀錄，避免誤判、漏判或自動化處置對重要業務服務造成影響。
5. **資安文化與攻防回饋：**除 SOC 技術營運外，該行亦透過年度資安訓練、釣魚郵件演練、員工通報獎勵、紅隊、藍隊與紫隊協作，以及軟體與實體滲透測試，將攻防演練結果回饋至偵測規則、告警調校與應變流程。其中，紫隊協作係整合攻擊模擬、偵測應變與雙方回饋調校，使資安文化與技術營運相互支援。

（三）參訪觀察：

1. **SOC 營運量化與 MTTC 管理**：本場交流可供參考者，在於以全球 SOC、營運指標及 MTTC 等方式，將資安偵測、研判與處置能力轉化為可衡量、可追蹤及可改善之管理項目。相關經驗可作為我國金融機構檢視資安營運成熟度之參考，惟具體指標仍須依機構規模、業務型態及風險特性調整。
2. **AI 輔助防禦與人工覆核**：面對高速度攻擊、大量告警及複雜攻擊路徑，AI 可協助提升告警分流、事件脈絡整理與分析效率；惟其定位宜為分析輔助與營運支援，仍須搭配人工覆核、權限控管、品質檢視及明確治理邊界，避免自動化判斷或處置形成新的營運風險。

四、Cyber Defence Alliance：高信任情資共享與可行動共同防禦

(一) **會議主軸**：本場聚焦 CDA 如何以高信任會員關係、來源控制及可行動情資為基礎，將金融機構分散掌握之威脅線索，轉化為共同威脅排序、攻擊手法分析、歸因研判、反詐協作及事件協調。同時，本場亦觀察其在資料共享法遵、供應鏈風險與前沿 AI 弱點治理等議題上的作法。

(二) 交流內容

1. **高信任共同防禦模式**：CDA 並非單純情資交換平台，而是以會員信任、作業安全（Operational Security, OPSEC）、來源控制、即時聯絡網及與政府、執法機關之合作關係為基礎，支援金融機構在重大威脅、詐欺案件或跨會員事件中進行共同研判與必要協調。
2. **Top Threats Project 與威脅排序**：Top Threats Project 彙整會員關注的主要威脅行動者與攻擊類型，並對不同供應商命名進行去重與標準化，再依共同重要性收斂為優先威脅清單。後續透過 TTP、MITRE ATT&CK 對應、攻擊階段及可偵測行為分析，協助會員將共同威脅認知轉化為偵測邏輯與控制改善。

3. **可行動情資與歸因研判：**CDA 強調情資價值在於能否支持具體行動。除一般技術指標外，其作法包括整合會員事件資料、外部基礎設施線索及來源可信資訊，形成可供追查、下架、阻斷或會員自我防禦之情資彙整，並透過歸因會議（Attribution Sessions）快速整合不同機構資料與工具，協助會員補強偵測規則、確認自身是否受影響、優先處理高風險曝露點，並在必要時支援惡意網域、基礎設施或詐欺服務之通報、阻斷與下架。
4. **反詐與跨域協作：**金融詐欺常透過電信、社群平台、數位廣告、可疑電話、釣魚網域及遠端控制工具擴散，因此共同防禦須跨越金融機構邊界，結合電信、平台、執法及技術服務業者。Operation Elaborate（針對 iSpooof 電話號碼偽冒平台）及 Operation Stargrew（針對 LabHost 釣魚即服務平台）等案例顯示，高信任通報、基礎設施下架與跨域協作，可將反詐情資轉化為可阻斷、可調查之具體行動。
5. **弱點排序、供應鏈與前沿 AI：**弱點處理不宜僅依 CVSS 分數排序，而應結合是否已遭利用、是否具概念驗證程式、外部曝露程度、是否涉及金融業或供應鏈常用技術，以及地下論壇討論熱度等因素。面對前沿 AI 可能加速弱點發現及增加修補壓力，治理重點在於以可利用性、曝露程度與關鍵系統影響進行精準排序，而非僅要求更快修補。

（三）參訪觀察：

1. **情資研析重點在共同排序與攻擊手法分析：**CDA 之經驗顯示，金融資安情資分享若要提升實用性，重點不在大量交換零散技術指標，而在於透過會員共同關注之威脅清單、TTP 分析、MITRE ATT&CK 對應、攻擊階段拆解及可偵測行為整理，協助會員形成一致的威脅認知與防禦優先順序。
2. **情資行動化需連結偵測、防禦與外部處置：**可行動情資的價

值，在於能協助會員補強偵測規則、確認自身是否受影響、優先處理高風險曝露點，並於必要時支援惡意網域、犯罪基礎設施或詐欺服務之通報、阻斷與下架。對我國而言，後續推動情資分享機制時，可進一步強化情資研析、影響範圍查核、會員防禦措施與外部處置管道之連結，使情資分享更能支援實際防禦與事件處理需求。

3. **AI 時代下更需風險排序與精準處置：**面對前沿 AI 可能加速弱點發現、攻擊鏈規劃及修補壓力，資安治理不宜僅以弱點分數或修補速度作為判斷依據，而應結合是否已遭利用、外部曝露程度、概念驗證程式、金融業常用技術與供應鏈依賴等因素進行風險排序，使有限資源優先投入最可能影響金融服務之威脅與弱點。

五、Level39：金融科技新創聚落與會員企業分享

(一) **會議主軸：**本場由 Level39 介紹其作為倫敦 Canary Wharf 金融科技與科技新創聚落之定位，並由現場會員企業分享其在 AI 資料分析、資安顧問服務及憑證治理等領域之產品與服務經驗。

(二) 交流內容

1. **Level39 平台與社群支持：**Level39 由 Canary Wharf Group 設立，定位為支持快速成長科技企業之新創聚落，透過會員申請與篩選、彈性辦公空間、策展式課程、活動、導師與投資人連結，以及國際代表團交流，協助會員企業建立曝光、交流與合作機會。
2. **AI 與資料分析服務分享：**會員企業分享對話式分析、特定領域 AI、分析引擎及專用算力在大量資料處理與金融市場資料分析之應用，並提及資料處理速度、運算成本、資料來源控制及降低分析錯誤等實務考量。

3. **資安顧問、AI 治理與憑證控制分享：**資安顧問業者分享中小企業資安服務、資安營運、滲透測試、第三方盡職調查、教育訓練及自動化工具應用，並說明影子 AI、資料外洩、問責與人工介入等議題。另憑證治理業者以數位主權為切入，說明企業掌握存取憑證、使用者不自行保管密碼、加密分段憑證、即時存取檢視、稽核軌跡及一鍵撤銷等產品設計。

(三) 參訪觀察：

1. **新創聚落與會員企業分享：**Level39 場次主要呈現新創聚落平台運作及會員企業產品與服務經驗，相關分享涉及 AI 資料分析、資安顧問、自動化服務及憑證治理等議題，可協助瞭解倫敦金融科技新創在產品定位、技術應用與市場連結上的實務作法。

六、Darktrace：資安 AI 應用與代理式 AI 安全治理

- (一) **會議主軸：**本場聚焦金融機構資安營運面對高告警量、未知威脅、雲端與身分濫用，以及生成式與代理式 AI 使用管理等挑戰時，如何運用行為式偵測、告警關聯、事件脈絡分析及適度自動化回應，提升偵測與研判效率，並保留人工覆核、授權邊界及可稽核性。

(二) 交流內容

1. **行為式偵測與事件脈絡建立：**面對未知威脅與身分濫用，資安營運不宜僅依賴已知特徵或固定規則。透過使用者、裝置、端點、網路、雲端、身分及 SaaS 活動建立正常行為基準，可協助發現偏離常態之異常訊號，並將零散活動整理為較完整的事件脈絡。
2. **告警關聯、降噪與優先排序：**在 SOC 面臨大量告警時，重點不在產生更多訊號，而在於依事件脈絡、攻擊階段、資產重要性及 MITRE ATT&CK 對應關係進行關聯與彙整，協助分析人

員降低雜訊、掌握優先處理順序，並將有限人力集中於較高風險事件。

3. **重大漏洞與高速度攻擊下的早期偵測：**在重大漏洞剛公開、攻擊手法尚未完全明朗，或攻擊者嘗試快速擴散時，行為式偵測可透過異常程序、外部連線、命令控制活動、挖礦行為或異常行為序列等訊號，協助及早辨識可能攻擊鏈，爭取分析與處置時間。
4. **AI 使用監控與自動化回應邊界：**生成式與代理式 AI 導入後，資安治理需關注影子 AI、提示內容、工作階段、工具調用、資料外洩風險及代理行為監控。自動化回應可在高速度攻擊或大量告警情境下爭取時間，但仍須事前定義啟用條件、回應範圍、人工覆核、授權層級、回復程序及中止機制，確保回應行為可控、可追溯且不影響重要業務服務。

（三）參訪觀察：

1. **由告警處理轉向事件脈絡研判：**本場觀察顯示，行為式偵測與告警關聯之價值，在於協助 SOC 將使用者、裝置、網路、雲端、身分與 SaaS 活動整理為可分析的事件脈絡，而非僅增加告警數量。
2. **AI 與自動化應設定清楚邊界：**生成式與代理式 AI 可協助提升資安營運效率，但其監控、工具調用及自動化回應仍須搭配政策比對、人工覆核、授權範圍、稽核紀錄、回復程序及中止機制，避免自動化處置影響重要業務服務。

七、Visa Cyber Fusion Center：支付網路資安、反詐與數位資產韌性治理

- （一）**會議主軸：**本場聚焦 Visa Cyber Fusion Center 如何整合資安事件應變、威脅情報、反詐、交易監控、雲端安全、身分存取與治理風險合規功能，以支援全球支付網路安全；並觀察其在支付詐欺模型、告警分流、資料品質、零信任架構、生成

式與代理式 AI 應用，以及數位資產與跨境支付等議題上的實務經驗。

（二）交流內容

1. **支付反詐與交易模型**：Visa 分享支付網路在帳戶對帳戶支付、即時支付、商戶詐欺、申請詐欺及洗錢相關異常交易等場景下，如何運用跨機構交易資料、行為分析與交易模型進行風險判斷。相關模型須在偵測效果、誤判率、客戶體驗、客服負擔及風險胃納間取得平衡。
2. **模型啟用、資料品質與持續校準**：在新支付場景或歷史資料不足時，可先以初始風控模型建立基本風險判斷，並隨交易資料累積持續校準模型表現。模型訓練不宜過度依賴品質不一或已過期之外部外洩資料，而應結合可信資料來源、實際營運流程、誤判成本及法遵邊界進行調整。
3. **融合式資安指揮中心**：Visa Cyber Fusion Center 整合資安事件應變、威脅情報、反詐、雲端安全、身分與存取管理及治理風險法遵等功能，並以全球接力式營運支援支付服務安全與韌性。此一模式重點在於將資安、防詐與交易監控資訊整合於同一營運視角，以利事件期間快速研判與協調。
4. **AI 輔助與零信任存取控管**：生成式 AI 可協助告警分流、弱點掃描、異常事件整理及分析輔助，但其分析或建議仍須建立在明確的身分驗證、最小權限、情境式授權及存取活動監控基礎上；代理式 AI 若需調用工具或存取系統，更須搭配安全護欄、工具調用邊界、第三方套件防護與即時授權控制。相對而言，零信任架構下累積之身分、裝置、應用程式與交易環境存取訊號，也可作為 AI 輔助研判異常行為與風險優先序之重要依據。

5. **新興支付與長期韌性議題**：穩定幣結算、代幣化存款、跨境支付實驗及 PQC 準備等議題，與支付資料保護、交易信任及長期服務韌性相關，宜作為支付服務未來發展之觀察議題。

（三）參訪觀察：

1. **資安、反詐與支付監控整合**：Visa Cyber Fusion Center 將資安事件應變、威脅情報、反詐、交易監控、雲端安全及身分存取等功能整合於同一營運視角，有助於在支付網路異常或資安事件發生時，快速彙整告警、交易與存取訊號，支援事件研判與協調處理。
2. **AI 輔助分析與零信任相互支援**：AI 可協助告警分流、弱點掃描、異常事件整理及風險優先排序；惟其分析與建議仍須建立在零信任所強調之身分驗證、最小權限、情境式授權及存取活動監控基礎上。對代理式 AI 而言，工具調用邊界、即時授權、人工覆核與稽核紀錄更是確保資安應用可控的重要條件。

八、London Stock Exchange Group：金融市場基礎設施營運韌性與 AI 治理

- （一）**會議主軸**：本場聚焦金融市場基礎設施在 AI、第三方依賴、供應鏈攻擊、營運韌性監理及重大事件應變下的治理方式，並觀察 LSEG 如何將資安韌性與市場穩定、跨境服務及公共信任連結。

（二）交流內容

1. **金融市場基礎設施韌性定位**：金融市場基礎設施之資安韌性不僅是內部 IT 風險，而是關係市場連續運作、跨境服務、關鍵第三方依賴及金融體系信任之治理議題。
2. **AI 風險分層與前沿 AI 挑戰**：AI 風險可依預測式 AI、生成式 AI、代理式 AI 及前沿 AI 等不同型態進行觀察；前沿模型可能加速弱點發掘、攻擊鏈規劃及自動化攻擊，企業須同時運用 AI 檢視自身暴露面並建立治理邊界。

3. **代理式 AI 控制與機器速度攻防**：針對代理式 AI，核心控制包括代理清冊、代理身分、權限邊界、工具使用範圍、行為監控、稽核軌跡及異常中止能力。若攻擊進入機器速度，防禦亦須重新評估人工覆核與自動化回應之平衡。
4. **第三方、供應鏈與情資共享**：第三方及供應鏈風險仍是金融市場基礎設施韌性的核心挑戰，需透過威脅情報團隊、FS-ISAC、NCSC 及金融業協作管道，將供應商監控、威脅情報與監理要求結合。
5. **營運韌性測試與工程治理**：英國營運韌性框架強調重要業務服務、影響容忍度與嚴重但可合理預見之情境；CBEST／TIBER 等威脅導向滲透測試、分段部署、經核准之軟體套件來源、CI/CD 控管、類生產環境測試、回復機制及攻擊路徑修復，則有助於驗證真實攻擊或重大更新失效情境下的防禦與復原能力，降低單一更新或供應鏈事件對市場連續運作造成的系統性衝擊。
6. **重大事故後根本原因分析**：除即時通報與服務復原外，金融市場基礎設施亦重視事件後根本原因分析（Root Cause Analysis, RCA）、控制缺口修補、變更流程檢討及經驗回饋，以避免相同弱點或系統性風險重複發生。

（三）參訪觀察：

1. **以市場服務韌性為核心**：當 AI 應用、第三方依賴、供應鏈事件或重大技術變更影響關鍵服務時，單純通報或修補並不足夠，仍須確認服務影響範圍、替代處理方式、復原順序及對市場參與者之溝通。
2. **前沿 AI 應納入情境測試**：前沿 AI 可能加速弱點發現、攻擊鏈規劃及自動化攻擊，也可能造成修補量暴增與判斷壓力。相關風險可轉化為較具體的演練情境，例如重大弱點短時間內被利用、開源套件或供應鏈元件遭攻擊、重大更新失效、以及自動

化偵測或回應判斷錯誤等，以檢視金融市場基礎設施在高壓情境下之偵測、決策、復原與溝通能力。

3. **代理式 AI 治理應可控：**相較一般 AI 分析工具，代理式 AI 若可自主規劃步驟、調用工具或存取系統，應明確掌握其代理身分、任務範圍、可使用工具、權限邊界、行為紀錄、人工覆核及異常中止條件。此類控制可避免代理式 AI 在未經授權或判斷錯誤時擴大對市場服務之影響。

肆、F-ISAC 與 CDA 簽署合作備忘錄（MOU）

本次參訪期間，我國金融資安資訊分享及分析中心（F-ISAC）與英國網路防禦聯盟（Cyber Defence Alliance, CDA）簽署合作備忘錄（Memorandum of Understanding, MOU）。此一合作係在雙方既有交流基礎上，進一步建立金融資安情資分享、威脅趨勢交流與事件聯繫之合作管道，具有深化我國金融資安國際合作之意義。

就實務面而言，F-ISAC 與 CDA 後續可在可行動情資互享、重大威脅趨勢交流、金融業常見攻擊手法研析、最佳實務分享及事件應處經驗交流等面向持續合作。於發生重大跨境資安事件或涉及共同威脅行動者時，雙方亦可透過既有聯繫管道，強化必要之資訊交換與協調聯繫，使情資合作更能支援金融機構實際防禦與應變需求。



伍、心得與建議

一、綜合觀察

本次參訪雖涵蓋營運韌性、共同防禦、資安營運、支付安全、後量子密碼、人工智慧及金融市場基礎設施等不同議題，但可歸納出一項共同趨勢：金融資安治理已由個別機構是否完成資安控制，轉向金融服務在重大衝擊下是否具備持續運作、快速復原與協調應變能力。此一趨勢與我國近期推動金融資安韌性、後量子密碼遷移及人工智慧治理之政策方向相互呼應，亦可作為既有政策持續精進與落實之參照。

就金融資安韌性而言，重點應回到重要金融服務能否持續運作。無論是重要業務服務、影響容忍度、跨市場演練、支付服務安全，或金融市場基礎設施之復原安排，均顯示資安治理不能只停留在事件發生後的通報與修補，而須事前掌握關鍵服務、依賴關係、可能中斷影響及復原順序。此可協助金融機構在重大事故發生時，較快判斷服務影響範圍、優先維持或恢復之功能，以及對客戶、市場參與者與主管機關之溝通重點。

就共同防禦與供應鏈風險而言，金融機構面對的威脅、弱點、異常活動及第三方依賴，往往具有跨機構與跨域特性。情資分享若僅停留於技術指標交換，效果有限；更重要的是透過情資研析、共同威脅排序、攻擊手法分析、曝險查核及防禦建議，提升產業整體風險感知。供應鏈風險亦屬此一聯防脈絡之一環，共同供應商或關鍵外部服務一旦發生異常，可能同步影響多家金融機構或重要金融服務，有必要與情資研析、風險感知及事件聯繫機制相互銜接。

就後量子密碼而言，其性質較接近準備期長、影響範圍廣的結構性風險，宜及早從加密資產、長期保存資料、跨機構連線、憑證與金鑰管理、供應鏈契約及新系統建置等面向盤點，逐步建立遷移優先序與密碼敏捷性。相關工作不宜被視為單次演算法替換，而應

納入金融機構系統開發、維運、採購、第三方管理及營運韌性流程。

在人工智慧方面，應先正視 AI 對攻擊風險的放大效果。攻擊者可能運用 AI 加速弱點探索、社交工程、惡意程式產製、攻擊路徑規劃及攻擊鏈自動化，使攻擊準備時間縮短、誘騙內容更具個人化，並增加資安團隊辨識與應處壓力。相對地，金融機構亦可運用 AI 提升防禦效率，例如協助告警分流、事件脈絡整理、弱點排序、異常交易偵測及分析輔助；惟其定位應為輔助研判與營運支援，仍須搭配人工覆核、品質檢視及可稽核紀錄。進一步而言，生成式或代理式 AI 若可調用工具、存取系統或產出處置建議，更應明確掌握 AI 使用清冊、代理身分、任務範圍、資料與權限邊界、工具調用、人工覆核、稽核紀錄及異常中止條件，避免影子 AI 或代理式 AI 在未被識別、未經授權或缺乏檢視的情況下擴大營運與資安風險。

二、政策建議

綜合前述觀察，英國經驗可作為我國既有政策持續精進與落實之參照。後續除持續推動金融資安韌性、PQC 遷移及 AI 治理等議題外，建議可在現行基礎上，續研議推動下列事項：

(一) 以資安營運指標強化高速度攻擊整備：面對重大弱點快速利用、攻擊鏈自動化及 AI 加速攻擊等情境，金融機構應以少數核心指標檢視偵測、研判、遏制與復原能力，包括告警分流、事件脈絡建立、平均遏制時間（MTTC）、重大弱點修補及改善追蹤等；並應透過攻防演練或情境測試，檢視資安監控、人工研判、自動化輔助及處置授權是否能有效銜接，以提升早期發現與快速應變能力。

(二) 推動情資行動化，支援實際防禦與應變：建議情資分享機制由技術指標交換，進一步形成可操作之防禦輸出，包括共同威脅排序、攻擊手法分析、曝險查核方向、偵測規則建議及必要事件聯繫。相關輸出應能協助金融機構確認是否受影

響、補強防禦措施、優先處理高風險曝露點，並於重大事件發生時支援快速研判與協調應處。

(三) 將共同或關鍵供應商納入聯防體系：辨識金融業共同依賴或對重要金融服務具關鍵影響之供應商，建立聯繫窗口、異常通報及風險提示機制。對於重大弱點、重大系統更新或關鍵外部服務異常，可透過共同情境測試或集體溝通，檢視資訊傳遞、備援啟動及復原協調情形，降低供應商事件造成之連鎖影響。

(四) 研議代理式 AI 控管要求：針對可調用工具、存取系統或產出處置建議之代理式 AI，研議使用清冊、代理身分、任務範圍、資料與權限邊界、工具調用限制、人工覆核、稽核紀錄及異常中止等基本要求。涉及重要金融服務或高風險作業者，宜採分級授權或人工確認，並透過情境測試檢視其控管有效性。