出國報告（出國類別：考察）

赴2024美國金融科技及資安產業考察團

服務機關：臺灣銀行 資通安全處
姓名職稱：顏志達 領組
派赴國家/地區：美國
出國期間：**113**年**6**月**1**日～**113**年**6**月**9**日
報告日期：**113**年**8**月**5**日

摘要

在目前全球金融產業的發展趨勢下，金融科技(FinTech)是發展競爭力的關鍵要素，其對應的主管機關監理、法令遵循與資訊安全防護亦有所必要，皆為金融業數位轉型不可或缺的一部分。透過中華民國銀行公會特別組織的「美國金融科技及資安產業考察團」，得到對國際金融監理、金融科技與資安領域的最新趨勢、技術應用以及創新策略的進一步了解機會。

舊金山與矽谷，是為全球科技創新的重鎮，除具美國加州的監理機關，更有不少一流的金融科技應用與資安科技企業總部設置於此，其監理政策、經營理念、創新策略與實務經驗都值得參考學習。本次考察團即透過參訪舊金山與矽谷的監理機關、金融機構和資安企業，可更全面地了解美國金融相關領域的發展情況與趨勢，並期建立深厚的交流和合作機會。

在銀行公會與台灣金融研訓院的安排下，本次參訪主題大致可分為金融監理、永續金融與金融科技暨資訊安全，深入瞭解金融科技的應用、資訊安全研發、應用和人才培育的領先策略和實務經驗，期相關經驗對國內金融業發展有所助益。

目　次

壹、　前言（目的）

銀行公會已屢次舉辦考察團，常有金融監督管理委員會與中央銀行等重要機構參團共同跟國際機構、先驅企業進行深度交流。本次舉辦的「美國金融科技及資安產業考察團」，由銀行公會雷理事長仲達帶隊，金融監督管理委員會、中央銀行、金融聯合徵信中心、財金資訊股份有限公司、全盈支付金融科技股份有限公司、國泰金融控股股份有限公司、永豐商業銀行、台中商業銀行等機單位派員參與該團，成員亦不乏總經理、副總經理、處長等高階主管，個人則是有幸首次參與考察團。

本次參加美國金融科技及資安產業考察團的目的，除了解美國監理機關的監管策略與要求金融機構的風險責任態度，亦包含美國金融業與科技公司都戮力於推動 ESG 或綠建築，另有新創公司與科技公司分享擬透過金融工具或透過 AI 提升服務與執行效率，以及資安公司關注近期 AI、零信任網路等相關議題對金融業的幫助和衝擊，並有美國監理機關分享因應臺美背景不同應就風險考量發展各自的金融策略，實收益良多。

貳、 過程

美國金融科技及資安產業考察團所安排的行程主題大致可分為金融監理、永續金融與金融科技暨資訊安全，下述將根據行程主題逐一描述：

一、 金融監理

金融監管政策主為拜訪在舊金山的監理機關，包含舊金山聯邦準備銀行(Federal Reserve Bank of San Francisco, FRBSF)與加利福尼亞州的監理機關－金融保護與創新局(Department of Financial Protection and Innovation, DFPI)。

美國聯邦準備理事會(Federal Reserve System)是為美國之中央銀行，舊金山聯邦準備銀行作為美國中央銀行的一部分，服務於第十二聯邦儲備地區，本考察團的第一站即為舊金山聯邦準備銀行。

這場是我在本次觀察團看到較特別的場面，是由我國向舊金山聯邦準備銀行的成員們先分享本國內容再進行交流。由金管會綜合規劃處胡則華處長、國泰金融控股股份有限公司吳建興資深副總經理、上海商業儲蓄銀行資訊研發處狄景力資深協理三位就 Fintech 的監理觀點與創新途徑、金融創新的系統性風險管理、金融領域的資安進行分享，內容不乏有金融科技發展路徑圖與其相關的快速認證架構、未來關注負責任的

AI(Responsible AI)、雲端服務風險、金融機構運用人工智慧技術作業規範、臺灣近期較受注目的資安事件與銀行公會自律規範等。

1. 對於 Fintech 的監理觀點與創新途徑，舊金山聯邦準備銀行也分享了所關注的趨勢是數位轉型、加密貨幣與其 DLT(Distributed Ledger Technology)技術、快速支付和 AI，其分別可能相關於第三方廠商管理、貨幣經濟、DLT 技術應用、工具與市場機制，以及 AI 可能帶來的作業方式與商業模式，對此考察團也分享了臺灣的經驗，另可看出金融機構在不少趨勢有機會尋求第三方廠商處理，在第三方廠商管理的風險控管與實務上有不少討論，監理機關都希望幫助金融機構正視相關風險管理措施以降低相關風險。

2. 接下來的環節更深入地探討雲端、AI 與 GEN AI (Generative AI)的風險與監理作為，舊金山聯邦準備銀行分享在這塊新興科技的應用通常不會要求金融機構事先獲得監理機關的同意或審查，金融機構應就風險管理制度的角度自我管理，後續監理機關會要求金融機構就實務上提出其風險管理是否已考量所有面向、有無盡職調查等，惟有加密貨幣相關活動需先報知監理機關；即金融機構僅要可以有效管理風險，就可自由創新與部署相關技術，另有提及美

國的 AI 原則，並需留意 AI 的模型透明度及可解釋性議題。

3. 壓軸為資安攻擊與 AI 深偽技術(Deepfake)的議題，舊金山聯邦準備銀行對此回應攻擊者將目標放在較弱的驗證、零時差漏洞、N 日漏洞與水電等基礎建設，而以多因子認證應對較弱的驗證是有效的；舊金山聯邦準備銀行期望金融機構自建治理能力，如成立治理委員會管理相關風險，將策略與相關新技術進行關聯並監控風險，制訂適當的政策與標準，也包含了日常基準，如可接受等級與應處、通報與決策層級，才能說有治理能力。後續分享識別風險、保護關鍵資產或關鍵業務、回應與復原，也提出關鍵業務復原的程序與時間亦為監理機關關心之標的，亦關注事件發生後的分析與復原工作，以讓其他金融機構可就相關挑戰中進行學習，並認同簡報韌性(Resiliency)一詞，提出系統應具備韌性。

最後舊金山聯邦準備銀行與考察團互相肯定本次的交流在相互學習與經驗分享非常有幫助，希望未來可以保持並有更緊密的合作。

第二站監理機關為金融保護與創新局，其前身為商業觀察部(Department of Business Oversight, DBO)，目標為健全服務金融系統、監管與消費者保護，係因應加

州消費者金融保護法案(California Consumer Financial Protection Law, CCFPL)改組、擴充職權與監管範圍，在分享中亦有提及；而本場主題包含金融機構分類、加州消費者金融保護法案、金融科技創新方法與加州數位金融資產法(Digital Financial Assets Law, DFAL)。

1. 金融機構分類：主要提及監管的銀行類型與牌照發行數量，並以去年矽谷銀行倒閉為例提出監管的事後檢討，包含(1)對大型銀行的監管流程、遠距監控與檢查資源，改善早期預警指標，提前發現潛在危機；(2)根據未保險存款在銀行組合達一定比例加強盡職調查與審查；(3)社交媒體的時代，要留意其會帶來的聲譽與其他風險影響，現金也可能因其影響而快速地透過電子交易移走。另關於檢查趨勢與重點提出下列項目：(1)網路安全與 IT 應定期測試網路韌性並發現脆弱點，不再等被入侵才加強，另應留意所採用的安全措施本身是可靠的；(2)確保反洗錢工作到位；(3)遠距工作帶來的商業房地產問題；(4) 經濟擔憂、供應鏈問題、通貨膨脹、高利率等議題。另針對社交媒體監督相關的議題，講者說明該機關不是銀行的管理者，銀行的管理階層(包含董事會)有責任將銀行的風險管理做好，機關會去檢視銀行的風險管理計畫

與風險管理品質。

2. 加州消費者金融保護法案：介紹該法案於2020年疫情期間通過，除了影響加州消費者金融保護局，也給予該機關新名稱－金融保護與創新局，法定了雙重使命－保護消費者與促進負責任的創新；提及該法案是透過活動而非機構/產業決定範圍，如涉及存款、支付、貸款等活動，即可根據該法案要求相關人員正式接受機關的監督，這些金融產品和服務的提供者須進行登記，每次登記期間為4年，除提供數據亦須接受機關檢查，認為立法機構除立意良善也保持溝通，並透過良好的數據確保金融監管框架；另該機關有權採取實質行動抑止組織有關非法、不公平、具欺騙或擾亂的行為。

3. 金融科技創新方法：主要在講部門的核心功能－參與、教育與協調，以達成部門的消費者保護及應對協調之雙重使命。參與部分以開放對話、教育採用活動或創新會談、協調包含各地的創新辦公室及機關夥伴，並有舉例紀錄今年約花費57小時在反詐騙技術上，也有建立專門團隊研究在生成式AI時代下的公平貸款。

4. 加州數位金融資產法：提及該法汲取紐約近10年的經驗並於2022年通過，認

為針對數位金融資產，包含比特幣與 FDX，應該要有足夠的透明度以保護顧客權益。

二、 永續金融

考察團在永續金融選擇參訪全球大銀行之一的富國銀行(Wells Fargo Bank)，總部亦位於舊金山，兼具跨國與多元金融業務，其金融創新與科技投入勢必走在銀行業的前端，藉此機會了解該銀行的最新金融科技應用與永續金融相關經驗：

1. 富國銀行有設定2030年的永續金融目標為500B 美元，去年已達約130B 美元，主要是透過債券市場達成，另為了淨零排放，有關資助客戶相關的財務碳排放(Financed Emissions)納入考量，亦對石油與天然氣、電力、鋼鐵、汽車、航空五項產業制定不同的階段性里程碑，設定碳排放的基準線，該銀行也觀察到所進行之鼓勵在市場有獲得值得鼓舞的反應。

2. 有關淨零排放的 Scope 3碳排放計算較為困難，且包含員工的通勤等。富國銀行分享其約有28萬名員工，為避免迷失在細節中，勢必需要有可接受的假設前提並發佈計算方法給各部門，目前雖有不少協會提供指引，但尚未有完美的解決方案，在財務碳排放計算亦有同樣狀況，需可運作並靠滾動式修正。

3. 指出整個集團一直常駐永續維運(Operational Sustainability)的觀念且思考前衛，可以說是已深植進 DNA 中，分享在2014年投注資金與美國國家再生能源實驗室(National Renewable Energy Laboratory, NREL)合作啟動了 Wells Fargo Innovation Incubator (IN^2)計畫，致力於創新與提高市場對潔淨科技(Clean Technologies)的接受率，以應對極端氣候的挑戰，並提出永續除了極端氣候還包含公正轉型(Just Transition)與社會層面議題。

4. 分享對再生能源融資業務，會對開發商進行大量的盡職調查，以支持和加強承保，亦有強健的稅惠權益(Tax Equity)業務因應「通脹削減法案」，該法案對再生能源等開放稅收抵免，亦為銀行業務的新興領域，另提到人工智能的挑戰是資料中心需要大量的電與水，如何讓資料中心更永續即會成為議題。

三、 金融科技暨資訊安全

金融科技暨資訊安全參訪的企業包含了 Uber、Palo Alto Networks、Google、Microsoft 與 Nvidia。

Uber 為知名的全球線上平台，透過 APP 促使共享經濟蔚為風潮，包含了乘車服務與食品配送服務，另在金融服務也跨足了 Uber Cash 及 Uber Cash Card，在本參訪可考

察相關商業模式創新、金融科技應用及信任安全議題處理方式。

1. Uber 的出發點即是試圖讓更多人共乘，並舉根據研究，如果道路上每輛車都可加入共乘，則僅需3%的車輛，顯示還有97%的空間可以努力；另提及Uber的原點為2009年的叫車，於2014開始有 Pool 的共乘概念，在臺灣非常受歡迎的 Uber Eats 則發想於計程車後座給人點餐的三明治。

2. Uber 的業務遍及約70個國家、1萬個城市，所要遵循的法規各有所不同，是以城市為基礎開展業務，如車輛是否僅能於特定街道上接送乘客，相關法規根據不同地區，可能由市長或議會制訂，並認為從遵法與公共機構合作的角度來看，比同行遍布更大的範圍與詳細的關聯。

3. 介紹Uber的神奇體驗，從叫車、乘車、下車，不需要掏出信用卡、現金或索取發票，一切都在後台完成，對於相關乘客體驗非常重視。舉巴西 Uber Conta 與美加的 Uber Pro Card 為例，說明司機的收取與支付機制，司機在完成服務後獲得的報酬是透過Uber墊付，供司機可立即使用，另除了提供司機備用餘額與折扣，亦不斷嘗試根據司機屬性推薦不同的金融商品，並研究跨境匯款相關的金融服務中。

4. 提到有商家的加入，以 Pizza 店為例，會對商家盡職調查、交易監控等，並切入詐欺對這商業模式的影響。對 Uber 的主要兩種詐欺為支付詐欺(Payment Fraud)、退款或補償(Refunds & Appeasements)：所有業務都可能有支付詐欺，如對已經完成的搭乘執行退款或拒付，通常較容易衡量損失；退款或補償，跟客戶請求退款較有關，如未拿到食物、食物涼了、物品亂放等，雖嘗試估計詐欺與實際需求，實難以具體。對此 Uber 建立相關防詐欺機制，收集歷史評分紀錄與 GPS 等資訊，經以風險規則為基礎的 Mastermind 與機器學習的 Michelangelo，可以獲得相關的決策，也提到有些地區要求要人工輸入不可自動決策，如允許支付或阻止交易。

5. 永續的部分，提及電動車與永續的配套措施，在臺灣是跟 Gogoro 合作，對機車與充電的夥伴提供折扣；另提到在災難救援和社區支持方面有所作為，包含疫情期間對夥伴提供經濟支持、對醫護人員等提供優惠餐點，也對地震當地提供優惠等。

Palo Alto Networks (PA)為知名的防火牆公司，供應包含了入侵防禦系統與次世代防火牆等產品，亦提供協助客戶資安相關服務，本參訪有助於了解資安產業的最新發

展與相關風險趨勢。

1. 介紹 PA 是15年前在美國成立，主要產品為第七層防火牆，需要有可視性(Visibility)，方看得到敵人並消滅掉；另大約6年前開始跨足雲資安，適逢疫情帶來的數位轉型，應用普及約在3-4年前，未來目標是作為資安平台整合，提供平台式服務。

2. 分享 PA 有組成紅隊(Red Team)並每季執行作業，用來檢視需要投入更多資源或防護的區域，由紅隊自主選擇目標與技術，於成功時提出入侵路徑與應修補項目，並提案例為利用 AI模擬資安長的聲音打給同事作為示範，讓同事理解最新趨勢，不過演練用的假音訊要有驗證碼以避免後續問題。

3. 對於深偽技術(Deepfake)，指出有開源函式庫可以訓練模型進行偽冒，如銀行透過聲音或影像執行 KYC，暗網甚至出售可以利用 AI 繞過相關驗證的工具。

4. AI 的滲透舉了 Copilot 為例，PA 亦有訓練自己的 Copilot，除了尋找漏洞外，應考量應用程序有無額外的攻擊面議題，並提出一是使用上是否會造成注入或越獄(打破內容審核)，另就客戶使用上，A 客戶不應該看到 B 客戶的內容，

根據上述設計自動化注入與越獄測試。在關於組織採用 ChatGPT，提出應要求大型語言模型(Large Language Model, LLM)服務提供者不可將組織的資料用在AI訓練上，且傳輸過程要滿足組織的保護措施，列入契約中並由服務提供者提出相關的保證。

5. 舉物聯網、居家辦公、網站瀏覽、須持續不斷驗證身分與授權的零信任網路為例，強調資安平台化的重要，並可透過機器學習了解行為模式避免資安問題，另認為亦可透過機器學習讓網站過濾從白名單調整到體驗較佳的狀況，亦認為平台化才可讓縱深防禦的各設備形成聯防，發揮價值。

6. 對於中小企業的資安管理，建議可以採簡化作業或外包給專家，專注在控制點上，如服務以透過瀏覽器為主，可嘗試專注在瀏覽器的保護上，另如網際網路提供商的網站過濾，可在可承受風險下選擇嚴謹或簡單設定；認為大公司需關注較多領域，常需要其他供應商來整合各領域方案，後面須面對培訓成本，提及過程整合花時間、資安花時間、人亦難找，分享 PA 徵才也需花費3-6個月期程。

Google 搜尋引擎家喻戶曉，今次所參訪的是總部 Google Cloud 部門，許多企業有

採用其雲服務 Google Cloud Platform，而這次主題包含 Google 的 AI 大型語言模型 Gemini 與相關應用案例，以及近期收購 Mandiant 所提供的資安服務。

1. 先談生成式 AI 的基礎應為負責任(Responsible AI)，鑒於 AI 非常強大，在於各領域(不論好壞)皆可發揮效果，須要在原則下開發與應用，包含對社會有益、不具偏見的基本(如不可用於不當目的)，再透過科學方法進行檢驗。

2. 舉 Gemini 為例說明 AI 訓練過程，AI 訓練是需要大量的數據，讓 AI 可以理解這個世界，而這些數據又需要經過合法授權，是一個嚴謹的過程；即使獲得了合法授權內容，也需要進行清洗，如同網際網路會有人性最好的一面跟最壞的一面，就需要把不應進入模型的數據清洗；當然維運上是不斷精進，舉在地化語言服務可能會有些內容過濾無法正確運作，會需要不斷滾動式修正。

3. 舉過去洗錢偵測是規則告警為主，透過 AI 分析的效果較佳，也減少了誤判，匯豐銀行即有使用相關技術，且該 AI 符合可解釋性與合規，亦不需寫入商業規則，後續 AI 讀取企業的數據訓練，完成後便可開始預測並跳出告警給單位確認；有提到團隊亦會與監管機構討論，作為供應商共同合作讓 AI 符合規範

相關內容；另提到 Google 有發佈 Google's Secure AI Framework，客戶的資料不會交出去，內部亦有採三道防線的做法。

4. 介紹 Google 因駭客問題，約於14年前即開始建立零信任網路架構(Zero Trust Architecture, ZTA)，以抵禦不同的威脅，也是對內部網路的未雨綢繆，亦提及 Security built in not bolted-on 的概念；除靜態加密與傳輸加密確保所有元素皆有保護，亦提及涉身分鑑別流程、確認流程經合法簽章且確保使用者在授權範圍及時機內存取該存取之資料的強式身份識別(Strong Identity)。

5. 介紹 Mandiant 威脅情資團隊會應對世界矚目的重大事件，分析如何鎖定目標組織、惡意軟體、相關技術、突破防線的方式，及所竊取的數據等，再將其回饋並提升 Google 產品及雲平台安全性，亦可讓雲端使用者檢視相關威脅活動報告，並說明政府與金融業仍是風險較高的標的，另建議要留意零時差漏洞有持續成長的趨勢；在生成式 AI 威脅的部分，有提到巴西有透過深偽技術繞過巴西銀行 KYC 控制措施的案例，生成式 AI 亦可能有助於攻擊者快速生成惡意程式。對於資安事件應變(Response)策略，認為要預期防線可能會被突破滲透，萬一發生可如何降低災損或儘早偵測到入侵行為，藉由威脅情資學

習與嘗試預測，以建立穩健具韌性的組織。

Microsoft 的 Windows 作業系統應無人不知，近年來亦投注 AI 領域的發展且成果卓越，包含搜索引擎 Bing、Copilot 及 Azure OpenAI 服務，本次考察其 AI 應用、責任及倫理相關議題。

1. 提及AI已從大型語言模型衍生到推理引擎，經觀察目前主要是建立內部應用模型而不是直接為客戶建立內容，而是對員工建立內容，再由員工監督確認相關內容；二是在網站上在聊天機器人增加生成式AI功能，讓客戶可以更方便的找到內容，且組織須有一定程度的監督；三是基於生成式AI提供新的產品或服務，過程須建立對技術的信心與訓練技術以適用使用情境。

2. Microsoft 長期以來一直對 OpenAI 有投資與合作，一方面促使建置更佳更大型的硬體堆疊(Hardware Stack)，以利符合所需高算力跟大規模基礎架構，一方面則共同致力於模型的安全，亦有共同發表的論文。

3. 介紹組織如採用 Azure OpenAI，Microsoft 不會利用客戶的數據與產品去改善自身模型，亦不會將數據提供給其他第三方 Microsoft 產品或服務，亦即客戶的模型改善僅對自身有效，舉 Costco 改善模型也不會給可口可樂。

4. 舉目前金融領域應用的客戶案例

(1) 新加坡華僑銀行(OCBC)應用於客服中心，透過私有 Microsoft Azure 環境建立 Gen AI 聊天機器人，人員透過 Teams 使用該聊天機器人起草電子郵件，讓人員可管理更多的互動跟確保回應內容的一致性

(2) 安盛銀行(AXA)建立了員工用的 Gen AI 助手，稱 AXA Secure GPT，可讓員工查詢金融商品資料的答案與資料來源，正確率約90%。

(3) 穆迪(Moody)則正與 Microsoft 合作共同建置下一代數據、研究、協作和風險的 Gen AI 解決方案。

5. 在程式碼現代化(Code Modernization)方面，舉 Github Copilot 提高程式開發效率，生產力上升70%；介紹 Microsoft 365 Copilot 產品，除即時翻譯，舉其 GEN AI 整理摘要會議紀錄等能力，可以快速掌握未參加會議的內容、更專注在特定主題、每日約可節省11分鐘。

6. 討論中提到 AI的強大會帶來內部威脅，包含員工的安全意識，如即時翻譯因為環境因素漏抓幾個字而讓字幕結果不同、員工透過 AI詢答存取到機密文件等；而 GEN AI 的使用不同於其他技術或產品，是足以改變員工工作與思維

方式的文化轉型，如何活用或發展 GEN AI 的提問(Prompt)將逐顯重要。

NVIDIA(輝達)為全球知名的半導體公司，過去最常見的即為顯示卡跟圖形處理器(Graphic Processing Unit, GPU)，而作為人工智慧的推動者，在近期更是名滿天下，國內亦有許多國內供應鏈受惠。

1. 提及 NVIDIA 轉型為 Full-stack Accelerated Computing 公司，除了底層 GPU 外，建置 Framework 供客戶開發，解決方案就是提供平台與 Framework 讓客戶發展軟體，並指創辦人黃仁勳在 Computex 秀出臺灣為中心及相關夥伴的 Ecosystem 頗令人感動，希望未來金融業也會是呈現在上的夥伴。

2. 透過影片介紹 AI 可以是 Visionary、Helper、Transformer、Trainer、Navigator 啟發思考 AI 用途，再舉 Paypal 防詐偵測從基於規則轉為機器學習與深度學習，認為金融業仍是值得投入發展AI的行業，指出可考量從表格化資料轉為非結構化儲存，資料更有活化利用的機會。

3. 介紹 NVIDIA AI Enterprise，為企業解決方案，有不同的 AI 開發工具，讓企業更快加速開發生成式AI或大型語言模型，可以封裝並快速部署至雲端、地端、邊緣(Edge)，簡介元件有可擴展的雲端原生之 GEN AI 框架 Nemo

Framework，方便使用者有效地創建、客製化與部署新的 GEN AI 模型；透過 API 調用 GEN AI 模型的 NIM Microservices；雲端原生的網路安全框架 Morpheus，可用於加速偵測日常未能檢測到的攻擊或病毒，提及約可加速 200倍；主要用於開發數位孿生(Digital Twins)的 Omniverse 平台，指製造業已有應用，並提銀行業可用於作為銀行領域知識庫的虛擬客服，亦可用於創建新分行時模擬人員動線，範例另有 Earth 2模擬氣候變遷。

參、 心得與建議

本次赴美國進行學習參訪，參與長官成員多為個人參與課程或研討會的講者，實有幸從中了解長官對於各項議題的切入點與著重重點，其預先設想及運籌帷幄的能力可見一斑，讓人多有學習之處。本考察團涉及專業範圍廣泛，包含金融監理、永續金融與金融科技暨資訊安全，個人本專研資訊安全範疇，雖對其他領域資訊接收較為吃力，不失為多多學習其他領域的機會，其中對富國銀行的 ESG 文化或治理頗為佩服，尤其是被詢問到如何讓員工配合 Scope 3碳排放計算時，自信地說員工只要妥善說明原則都很願意配合，組織擁有 ESG 的 DNA，亦猶如已建置好資安文化與制度的銀行或企業，員工都應共同做好資安，在研討會上都可自信地說出員工都內建資安的 DNA。

有關體現 ESG 的部分，可見到矽谷企業的建築尤為明顯，受其氣候資源限制，多有水再循環利用的設施；光線的部分則外牆多會採用玻璃帷幕增加採光，Microsoft 則再增加物聯網調節光線以調整溫度；亦多有太陽能板產生綠能；另屋頂常有花圃園地可供單位同仁認領，同休閒設施讓同仁陶冶性情。

在資安方面，Security built in not bolted-on 實中個人心坎，常見到資訊業務為了個別資安要求或規範不斷疊床架屋，持續累加檢核表做表面功夫，如能實際落實到程序內各步驟或系統內應能更加順遂；當然，如果執行單位皆能了解對應的資安要求背景再去落實，想必更能達到內建資安 DNA 的程度。

最後，本次銀行公會舉辦的考察團實可圈可點，讓成員充實國際對相關領域的觀念跟做法，可帶回各自企業審視成長，亦也帶動同業合作，於考察期間互相交流深化，透過此考察團實收穫良多。