出國報告（出國類別：開會）

2025 年金融檢查與稽核系列研討會

服務機關：臺灣土地銀行稽核處
姓名職稱：羅瑞芬副處長
派赴國家：英國
出國期間：114 年 09 月 06 日至 09 月 13 日
報告日期：114 年 10 月 20 日

摘　　要

中華民國銀行公會與台灣金融研訓院「金融檢查與稽核系列研討會」（Bank Examiners and Auditors Program）自 1998 年推動以來，為銀行業監理及內稽專業社群營造跨國交流平台，藉由導入國際經驗與最佳實務趨勢，提升國內金融業對於風險之因應能力，為金融的穩健發展奠定良機。

本（2025）年度研討會係以「國際金融監理、企業營運韌性、金融科技應用以及永續金融規範」作為活動主軸，並於英國倫敦舉行，透過機構考察活動形式，安排參訓人員與英國當地金融監理機關及具代表性之跨國銀行集團高階稽核主管進行交流，期藉由雙邊經驗分享與反饋，加速台灣金融監理與內部稽核實務向國際標竿邁進。

本次研討主題分為兩大主軸（監管與內部治理、創新與未來發展）及四項議題（國際金融監理、企業營運韌性、金融科技應用、永續金融規範），透過簡報、機構考察及線上課程等形式，與英國審慎監理局（Prudential Regulation Authority, PRA）、Chartered Institute of Internal Auditors、跨國銀行集團（包含匯豐銀行 HSBC Bank 及渣打銀行 Standard Chartered Bank）、國際知名會計師事務所（EY、PwC）等機構進行交流與學習，探討英國金融監理法規對外國銀行之監理要求與期待；面對網路威脅與技術不斷進化，金融機構的因應之道；利用動態風險評估進行金融犯罪風險偵測並提高報送準確率；以及在人工智慧蓬勃發展、各類風險與治理挑戰持續升高的環境下，如何善用新興科技進行內部稽核數位轉型，以期能更全面、即時、有效地規劃與執行稽核作業，並結合組織目標提升稽核的整體價值。

目錄

壹、目的.....1

貳、過程.....2

一、PRA 關鍵關注領域和 2025 年的監理重點.....3

二、網路安全及營運韌性.....4

三、英國對外國銀行的監管政策.....6

四、ESG 風險管理與實務.....7

五、全球內部稽核準則.....8

六、人工智慧在金融犯罪預防的應用.....10

參、心得與建議.....12

壹、目的

為促進金融監理與稽核制度與國際接軌，導入國際前瞻趨勢，協助國內金融機構內部稽核單位認識日新月異的新興風險，了解國外監理重點與銀行同業最新實務發展，中華民國銀行公會（簡稱銀行公會）及台灣金融研訓院本年度於英國倫敦舉辦 2025 年「金融檢查與稽核系列研討會」，由金融監督管理委員會（簡稱金管會）檢查局賴局長親自率團，期透過國內外主管機關、同業及會計師事務所與台灣金融業稽核主管暨法遵主管經驗分享，了解金融業所面臨之新挑戰及因應戰略，提升本國稽核品質及法遵文化，加速內稽轉型，特邀探討以下重要議題：

一、PRA 監管架構與原則、關注領域及 2025 年的監理重點

二、網路安全及營運韌性

三、英國對外國銀行的監管政策

四、ESG 風險管理與實務

五、全球內部稽核準則在英國及愛爾蘭當地之應用及挑戰

六、人工智慧在金融犯罪預防的應用

貳、過程

本次研討會期間為 114 年 9 月 8 日至 12 日（9 月 12 日上午為學員分組心得分享活動），由金管會檢查局賴局長欣國擔任團長，率領檢查局林組長靜瑜、中華民國銀行公會內部稽核委員會陳妙娟主任委員、柳蜀君副主任委員及張麗珠諮詢委員、中央銀行易專員重威、台灣金融研訓院呂副院長子立、相關工作人員及金融同業之稽核/法遵主管共 29 員，研討會列表如下：

日期	參訪機構	交流主題	演講者
114.9.8 (一)上午	PRA	Sound Management and Risk Resilience	➢ Chris Forster, Senior Manager ➢ Vishmi Sapukotanage, Assistant Supervisor
114.9.8 (一)下午	EY UK	Current regulatory policies for Foreign Banks operating in the UK	➢ Corinne Kaufman, Director
114.9.9 (二)上午	HSBC Bank	Application of AI in Financial Crime	➢ Nish Ranatunga, Head of Financial Crime Risk Models and Monitoring Oversight ➢ Mattew Farrar, Senior Fraud Risk Manager-Financial Crime Fraud Risk Stewardship ➢ Richard Hayden, Senior Fraud Risk Manager-Financial Crime Fraud Risk Stewardship ➢ Dennis Wong, Global Head of Financial Crime Risk Audit
114.9.9 (二)下午	Chartered IIA	Internal Audit and Organizational Culture	➢ Sandro Boeri, President
114.9.10 (三)上午	PwC UK	Cybersecurity and Information Technology Risk	➢ Christian Anrdt, Head of Cyber Strategy ➢ Maya Chehab, Cyber Partner ➢ Duncan Scott, Operational Resilience Leader ➢ Adam Bee, Senior Manager
114.9.10 (三)下午	Standard Chartered Bank UK	ESG Risk Management and Practical Implementation	➢ Dana Barsky, Global Head of Sustainability Strategy and Net Zero ➢ Vincent Paulger, Group Regulatory Affairs
114.9.11 (四)上午	Chartered IIA	Global Internal Audit Practices and Challenges	➢ Anne Kiem OBE, CEO, Chartered IIA-UK & Ireland
114.9.11 (四)下午	British Standards Institution	ESG Compliance and Information Disclosure	➢ David Fatscher, Interim Head of Standards Development-Sustainability & ESG, BSI

	UK		➢ Daan van der Wekken, Head of Sustainability, BSI ➢ Mark Manning, visiting Sr fellow, Centre for Economic Transition Expertise, London School of Economics and Political Science

一、PRA 關鍵關注領域和 2025 年的監理重點

(一) PRA 監管架構與原則

1. PRA 監管主要目標包括促進受監管機構的安全與穩健、為保單持有人提供適度保障，次要目標為促進企業間有效競爭及促進英國經濟（特別是金融服務業）的國際競爭力及其中長期成長，次要目標不得與主要目標衝突。

2. PRA 的監理模式是在 2008 年金融危機後建立的，目的是在金融穩定與國際銀行業的開放間取得平衡，對國際銀行與本地銀行採用相同的監理架構。PRA 的國際監理原則如下：

   (1)採判斷式監理（Judgment-based Supervision），以監管人員的判斷為核心，評估受監管機構是否穩健，是否持續符合最低要求，以及如何解決問題。

   (2)前瞻性（Forward looking）：不僅應對當前風險，也針對可能出現的潛在風險提前採取行動。

   (3)聚焦關鍵風險（Focused on key risks）：不以合規為唯一導向，而是聚焦對金融穩定及其法定目標影響最大的議題及銀行；採用比例原則(Proportionality)，監理強度及頻率取決於該銀行對英國金融穩定的潛在影響。

(二) PRA 關鍵關注領域

1. PRA 每年發布監理優先事項信函（Priorities Letter），一份針對英國公司，一份針對國際公司，2025 年的英國優先函側重於「信用風險」，國際優先函則側重於「交易對手信用風險」。信件內容專注於非公司特定問題，應與個別公司的反饋函一併閱讀，作為風險框架的一部分。

2. 2024 年整體銀行業獲利強勁，但 2025 年的挑戰加劇。全球風險上升：包括地緣政治、氣候變遷、貿易關稅政策不確定性（尤其與台灣高度相關）、供應鏈中斷等。經濟壓力導致信用與市場風險上升，流動性雖仍充足，但壓力已在醞釀，銀行可能提高風險胃納（Risk Appetite）以維持獲利。

3. PRA 持續關注資料、職能運作效率及風險文化對其影響，網路韌性（Cyber Resilience）亦成為關鍵焦點。此外，第三方供應商集中度高恐帶來額外風險，PRA 要求銀行採取全面性的風險管理，監控及降低委外風險，並推動強化風險文化，控制風險承擔行為，確保資本充足、流動性穩定、風險控管健全，且強調與母國監管機關合作。

(三) 2025 年的監理重點

1. 資料品質

(1)資料品質是 PRA 監理重點之一，與風險文化並列為風險管理與控制的核心，金融機構須具備蒐集、管理及整合資料之能力，以有效管理其業務及風險。

(2)準確地向 PRA 回報相關資料，讓監管機構能做出正確決策，特別是在設定資本要求和流動性要求時，只有資料精準的情況下，監管決策才最有效，若資料品質不佳，會削弱整個風險辨識、監控與控制流程。

2. 營運韌性、數位轉型及委外監管

(1)PRA 透過委外管理的成熟度，間接評估分行的營運韌性。PRA 要求系統重要性銀行提交自我評估報告，內容須包括高衝擊事件的衝擊容忍度（Impact Tolerance）、重大情境測試（Severe but Plausible Scenarios）的證據資料，不僅依靠專家判斷，還需提供實際測試數據。

(2)數位轉型驅動因素包括淘汰舊系統、提升效率與韌性，常見挑戰如缺乏大規模轉型經驗、董事會缺乏 IT 專業背景，監督力不足、委外依賴度過高（第三方、第四方的複雜依存關係）、流程改變與內部稽核脫節。

(3)重大委外計畫須提前通報 PRA，依比例原則審查其對金融穩定的影響，雲端委外為主要審查焦點，且 PRA 要求企業具備壓力退出計畫（Stressed exit planning），確保第三方供應商長時間停擺時，尚能維持關鍵功能運作。

二、網路安全及營運韌性

(一) 網路安全與趨勢威脅環境與技術演進

1. 威脅環境與技術演進：2024 年網路威脅環境極度活躍，攻擊者不僅延續前一年的活動，還採用新技術與工具。地緣政治（如戰爭與國際衝突）為主要的攻擊動機來源，而勒索軟體的發展也未因執法干預而減弱，反而更加成熟與擴散。攻擊者大量使用公開的惡意工具與程式碼，讓技術門檻降低，導致更多人投入網路犯罪。這些工具不僅容易使用，還具備高度複雜性，使得攻擊行動更具破壞力。另針對邊界設備（Edge

Device）的零日漏洞（Zero-day Exploits），企業需迅速判斷漏洞是否存在、影響程度、修補時間與成本，否則可能遭受重大損害。這些漏洞遍及各大廠牌，顯示邊界防禦已成為攻擊焦點。

2. 身分登入取代直接入侵：現代攻擊者不再依靠技術侵入系統，而是透過合法憑證登入系統（logging in, not breaking in），繞過傳統防禦機制，身份管理與存取控制成為資安策略的核心。社交工程與外包客服成為弱點，雲端環境使駭客可直接存取企業資源，繞過傳統防線。金融業雖資安成熟度高，但仍面臨內部威脅與第三方供應商風險，尤其是員工行為偏差與供應鏈漏洞。

3. 勒索病毒與第三方供應商風險：勒索軟體攻擊廣泛影響各行業，受害者數量創新高。攻擊者透過洩漏網站施壓受害者，並集中攻擊高價值產業。勒索軟體生態系已形成完整的商業模式，從初始存取、憑證提供、工具部署到資料加密與勒索金支付，皆有明確分工，具高度韌性。這種模式讓更多人能參與攻擊行動，擴大影響力。

4. 資安韌性與監管趨勢：企業需更公開資安風險與事件，建立韌性防禦架構，具備災後營運能力與恢復計畫。資安已成為企業營運核心議題，董事會與監管機關將要求更清晰的風險報告與量化分析。

5. AI 影響與未來挑戰：AI 技術雖提升資安工具效能，但也加速攻擊手法演化，若授權不當，可能成為新風險來源，駭客能快速生成攻擊工具與釣魚郵件。未來幾年，網路威脅將更複雜，漏洞利用不會減少，反而可能更頻繁。地緣政治仍是主要驅動力，企業需強化防禦並關注國際情勢對資安的影響。

(二) 營運韌性與歐盟數位營運韌性法案（Digital Operational Resilience Act, DORA）

1. 監管架構與企業轉型挑戰：當前威脅環境活躍，包括網路攻擊、第三方供應商、雲端服務、人員與資料風險。韌性不只是合規，而是企業應具備的核心能力。英國韌性監管架構包括：識別重要業務服務→服務映射（Map Dependencies）→設定容忍度→情境測試→自我評估→建立韌性文化。韌性不只是防止事件發生，更是確保在事件發生後能迅速恢復營運。英國監管機構的核心理念是「失敗是必然的」，企業應以此為前提設計營運架構。

2. 整合測試與營運模式：測試不應僅限於既定場景，而應根據實際威脅進行設計。建議企業從自身風險紀錄、稽核報告、合規問題出發，結合外部情資，制定測試計畫。測試目標應是「讓服務失效」，以找出真正的弱點與改善空間。

3. 第三方供應商韌性與未來趨勢：歐盟 DORA 法案要求企業對第三方供應商進行韌性測試與合約審查。PwC 指出，目前企業普遍面臨第三方供應商配合度低、資料掌握困難

等挑戰。建議透過合約條款強化審核權、逐步提升成熟度，並考慮由企業主導測試並分享結果。

4. 韌性文化與治理架構：韌性應由第一線業務單位主導，而非僅由後勤部門負責。建議設立「重要業務服務負責人」，並將韌性納入績效與獎酬制度。董事會與高階主管需定期審查韌性報告，並透過情境演練提升全員意識。

三、英國對外國銀行的監管政策

(一) 英國的監管機構：

1. 在金融海嘯後，英國在 2013 年大幅修改金融監理架構，首先分拆金融監理總署（Financial Service Authority，FSA），除了穩定金融的考量，亦兼顧金融效率的提升，並在英格蘭銀行增設獨立之金融政策委員會（Financial Policy Committee, FPC）負責總體審慎監理，而其下轄新成立的審慎監理局（Prudential Regulation Authority, PRA），與另一獨立運作的金融行為監理局（Financial Conduct Authority, FCA）負責個體審慎監理，均脫胎於消失的 FSA；PRA 監管銀行、保險及其他大型金融機構，FCA 則監控金融市場的運作。

2. PRA 與 FCA 及 FPC 共同構成英國金融監管體系，PRA 負責銀行的「審慎監理」，FCA 則負責消費者保護與行為監理，FPC 負責宏觀審慎監理（Macroprudential Regulation），專注於系統性風險監控，並可調整逆週期資本緩衝（Countercyclical Capital Buffer, CCyB）等工具，以提升金融系統的韌性。三個機構透過資訊共享及平行評估，形成協調一致的監管框架。

3. FCA 的成果導向監管原則：FCA 將監管重點從「形式合規」轉向「成果導向」，特別是要求企業關注其對待客戶的實質成果。這項原則鼓勵金融機構從根本上提升服務品質和道德標準，而非僅止於滿足形式上的規定。

(二) 英國監管的全面性與前瞻性思維：

1. 宏觀經濟、社會、政治、科技和地緣戰略發展共同塑造了英國監管藍圖，並導致監管碎片化加劇，突顯監管當局在制定政策時，不僅僅侷限於短期目標的達成，更重要的是考量長期優先事項和廣泛的風險視角。

2. 英國監管機構長期關注的重點領域，包括企業文化、公司治理、系統與控制、風險文化、金融穩定性、金融犯罪、消費者保護和營運韌性。其對企業文化、治理、風險文化、金融穩定、金融犯罪、消費者保護和營運韌性等「長期關注領域」的持續強調，揭示了金融穩健的基石是內在的健全，而非僅限於量化指標。

3. 闡述建立抵禦外部威脅的韌性、實現良好客戶成果及在變動環境中風險管理的重要性。

四、ESG 風險管理與實務

(一) 本課程透過 BSI 的專家分享，說明了國際 ESG 及淨零標準的發展與實務應用，讓我們能理解 ESG 已不再是未來趨勢，而是當下金融與企業不可分割的一部分。課程內容兼具理論與實務，特別是介紹針對金融機構專門設計的淨零轉型標準，這套標準能協助金融業在風險管理與轉型推動中更為系統化，提升決策品質與永續競爭力，對於稽核人員來說，也能掌握轉型計畫所應涵蓋的監督機制與治理架構。

(二) ESG 及永續金融標準的全球趨勢與推動力

各類監管機構、投資者及社會大眾對 ESG 資訊揭露需求不斷提升，產生多重且複雜的報告架構。英國政府積極推動淨零轉型，制定強制性轉型計畫要求，BSI 憑其國家標準機構優勢，整合多方制定 ISO 標準。

渣打銀行展示如何將淨零排放目標具體嵌入客戶生命週期中，並開發了詳細的融資排放計算方法，例如透過客戶企業價值與其碳排放量來決定融資排放。這種量化且整合性的方法，提供金融機構規劃和管理氣候影響的實踐路徑。

(三) ISO ESG 實施原則與淨零金融機構轉型標準的架構

ESG Implementation Principles（IWA 48）提供通用語言及高階原則，協助企業導入永續實務、ISO 32212 標準聚焦金融機構，強調轉型規劃流程的系統性和連續性，而非僅揭露結果。標準強調環境（減緩與適應）、社會及治理三大面向及文化與溝通的整合，透過循環動態流程涵蓋風險與機會評估、具體目標設定、融入決策及產品設計、全面溝通以及績效回顧更新。

(四) 標準制定的治理與共識形成：

透過全球約 170 國家的利益關係者共識制定，包容各國國情與市場差異，強調標準的原則導向與彈性，避免因過於嚴苛影響全球適用度。具備定期覆核機制以因應市場與政策快速演變，兼顧內部稽核及第三方獨立驗證，確保執行之嚴謹性與公信力。

(五) 金融機構的獨特角色與轉型生態系整合：

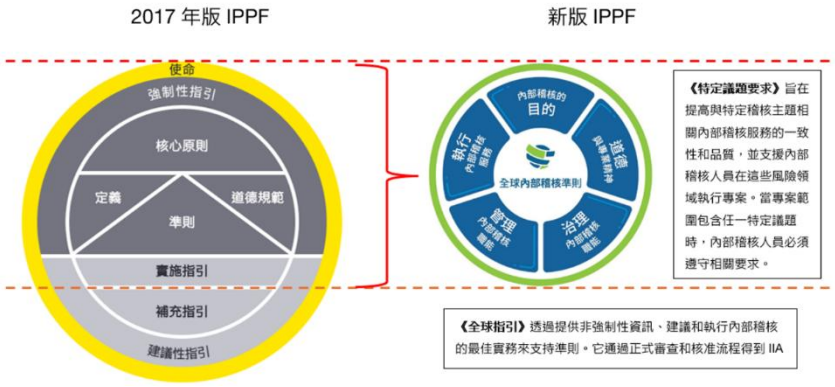
金融機構既是風險承擔者也是風險塑造者，透過融資活動影響實體經濟轉型。強調金融機構需與企業客戶、監管機構及政策制定者密切互動，合力推動轉型。認可碳權使用的

必要性與風險，並正嘗試建立透明且受約束的使用規範，防止過度依賴碳權而非真實減碳情形。

五、全球內部稽核準則

(一) 全球內部稽核準則的重要更新

1. 新版 IPPF 包含了《全球內部稽核準則》、《特定議題要求》及《全球指引》，將原先框架中《任務》、強制性指引中的《核心原則》、《定義》、《職業道德規範》、《國際內部稽核職業準則》、以及建議性指引中的《實施指引》彙整融合為《全球內部稽核準則》，簡化了整體框架。



資料來源：安永 2025.2.5 內部稽核品質評核因應新版 IPPF 之實務做法

2. 特定議題要求

透過為特定風險議題設定最低基準，為內部稽核人員提供明確的期望，涵蓋常見的高風險領域（如資通安全），不包含新興風險（如人工智慧）。對於確信服務（Assurance services）而言，遵循「特定議題要求」屬於強制性；對於諮詢服務（Advisory services）而言，則是建議性的指導。當議題符合以下條件之一時，即適用「特定議題要求」：A.該議題為內部稽核計畫中的查核專案、B.在執行查核專案時發現該議題、C.該議題為內部稽核計畫外之查核專案需求。

3. 各領域的挑戰與實務洞察（英國和愛爾蘭）

(1)領域一：內部稽核的目的，強調深度洞察和前瞻遠見。鼓勵內部稽核人員與利害關係人互動，使稽核工作與策略方向保持一致。除了透過確信服務提供洞察力之外，還要預見未來可能發生的情況以及組織如何應對潛在的未來風險和新興風險，稽核人員應思考如何在稽核計畫和工作程式中實現深度洞察和前瞻遠見。

(2)領域二：道德和專業精神，強調專業勇氣。在稽核團隊中倡導開放的文化和陳報機制。稽核人員必須秉持誠實和專業勇氣執行日常工作，公開所有關鍵事實，並根據需要適時向上陳報。面臨之主要挑戰為組織如何支持內部稽核人員暢所欲言並進行專業討論？內部稽核人員如何理解組織對他們在專業勇氣上的期望？組織如何監督和評估內部稽核人員所展現的專業勇氣？如何培養道德文化等。

(3)領域三：治理內部稽核職能，引入董事會、審計委員會和高階管理層的強制性要求，關注董事會、審計委員會、高階管理層及總稽核間各方之關係和資源支援。渠等透過核准內部稽核職能和績效目標、計畫、預算等具體作法來表現其對內部稽核之支持。

(4)領域四：管理內部稽核職能，引入內部稽核策略的概念，區分稽核策略與稽核計畫之差別。強調內部稽核策略的重要性，內部稽核職能由合規性查核調整為風險性查核，並將績效衡量標準與內部稽核策略及目標掛鉤，以達成組織目標。有關諮詢服務的績效衡量方式如何量化為當前的挑戰。

(5)領域五：執行內部稽核服務，強調利害關係人的參與、根本原因分析（Root Cause Analysis, RCA）和撰寫 SMART 建議，即以具備智慧性 smart、可衡量性 measurable、可行性 achievable、實用性 realistic 及時效性 time bound 的方式來撰寫建議事項。在規劃有效的稽核專案方面，應於制定稽核計畫時，確保已將利害關係人意見納入，並善用特定議題要求來評估現有的控制設計，著重於根本原因的分析。所面臨的挑戰為應如何評估稽核人員所提建議的品質。

4. 展望未來

(1)報告與溝通：董事會及審計委員會對內部稽核的參與程度不斷提高，透過定期的報告與雙向溝通，相互了解彼此的策略、期望及作法，達到策略夥伴的目標，提高稽核工作效能。

(2)稽核策略與績效衡量：稽核計畫需與組織長期發展策略（如數位轉型、永續發展、國際化等）連結才能達成目標，績效衡量標準亦應與內部稽核策略及目標掛鉤。傳統的稽核績效衡量偏重稽核專案數量、缺失數量等，未來將朝向內部稽核對高階管理層制定決策之影響力，與管理階層溝通效果、改善建議的採納率、風險降低成效、董事會信任度、對公司價值的貢獻度、外部品質評核結果等面向，兼具質化與量化指標發展。

(3)促進根本原因分析：稽核報告重點除了指出缺失外，更應著重於為什麼會發生，分析流程、制度或文化上等更深層的原因分析，協助不同單位共同檢討問題根源，透過分析共通性問題形成組織學習及改善。

(4)持續教育與參與：稽核人員應當與時俱進，除了傳統會計、資訊、法規遵循、營運流程等專業之外，針對網路安全、數據分析檢測、ESG 及 AI 等跨領域知識需求日益增加，透過參與訓練相關研討內容，持續精進專業，將有助於提供組織建議時，協助提升營運效率與創造價值。

六、人工智慧在金融犯罪預防的應用

(一) 匯豐銀行（HSBC）成立金融犯罪部門專注於金融犯罪防制措施及提升管理金融犯罪效率，本次課程主要介紹 HSBC 內部動態風險評估模型的核心基礎、架構、運作以及如何在營運過程中更精準及有效率協助判斷需要人工審查的客戶，減少假警示，提供簡化的金融犯罪防制框架並向主管機關提報更有價值的資訊，DRA 除運用於金融犯罪防制外，亦可運用於商業銀行帳戶審查。

(二) 動態風險評估（Dynamic Risk Assessment，簡稱 DRA）

1. DRA 是一種金融犯罪風險偵測模型，透過機器學習來預測客戶洗錢的可能性，摒棄傳統規則導向交易監控，以數據為驅動的特徵集，支援複雜的預測分析，並觸發調查。

2. 交易監控處理的指引包含五個原則：

(1)減少不必要的控制以免降低效率。

(2)不應過度要求客戶提供資訊以避免影響業務流程。

(3)聚焦真正的風險。

(4)提供更簡化的金融犯罪防制框架。

(5)向執法機關或相關主管機關提交更有價值的資訊。

3. DRA 反饋循環，用機器學習把人工作業的專業判斷抽取為特徵與標籤，讓系統不僅「複製」經驗，更能從結果中學習。

4. 網路分析與情境監控：重視「實體解析」（Entity Resolution）觀念，客戶可能同時以不同名稱、帳號或裝置出現，須整合跨交易、跨來源的片段資訊，運用更強的連結分析連起交易脈絡。整合內外部數據，即時交叉比對，提供更完整之風險輪廓。

(三) AI 在金融犯罪偵測與預防方面的應用

1. 生成式人工智慧開發深偽技術、語音模擬與人工影像等創造出新的詐騙方式，透過機器學習來優化人工智慧模型提升偵測能力並減少誤報。

2. 英國廠商 2024 年 10 月推出 Ask Sliver 詐騙檢測工具，客戶將可疑訊息截圖傳送系統，該項服務能夠即時分析簡訊、電子郵件、社群媒體內容之妥適性，並提供警示。

3. 稽核方法：模型部署前進行審查確保充分理解模型的運作方式與風險管理，模型部署後持續監控及其效能驗證。管理金融犯罪以風險為導向，識別對金融機構造成威脅並優先處理的高風險事件。

(四) 在英國，對 AI 的關注主要集中在治理機制，特別是確保組織在 AI 策略與導入方面的治理架構是健全的，包括是否設立了 AI 委員會、是否有決策機制來判斷 AI 應該嵌入組織哪些部分，以及對 AI 相關計畫的監督機制等。

(五) 對於內部稽核在 AI 領域的查核，國際內部稽核協會（IIA）雖然針對高風險議題制定強制性特定議題要求（Topical Requirements），然而目前並沒有針對 AI 制定專門的特定議題要求，AI 領域是目前大家非常關注的焦點，AI 的特定議題要求未來一定會出現，但未來幾年內還不會實施。

參、心得與建議

本次的研習課程安排的都是新興的熱門議題，包括英國對外國銀行金融監理法規、ESG、永續經營、資安風險、全球內部稽核準則、稽核數位轉型、以及人工智慧在金融犯罪上的應用等，本行雖然未在歐洲地區設立海外分支機構，但先進國家在金融監理的趨勢及要求，仍值得我們參考學習，並做為本行設立於其他國家/地區海外分行管理之借鏡，在新興科技蓬勃發展、各類風險與治理挑戰持續升高的環境下，如何善用新興科技進行內部稽核數位轉型，以期能更全面、即時、有效地規劃與執行稽核作業，並結合組織目標提升稽核的整體價值，是內部稽核積極創新與數位轉型的重要目標。以下分享本次研習心得及建議如下：

一、各國金融監理機關對營運韌性的重視程度提升，要求組織在面臨突發事件（如系統中斷、災害、網路攻擊、疫情、供應鏈中斷等）時，能夠持續提供關鍵服務、快速回復運作並降低影響，有別於過往的災害復原或業務持續營運等計畫，營運韌性更著重於服務不中斷、降低中斷成本與復原時間、強化企業形象與市場信任、提升風險預警與決策敏捷度、永續經營等全方位能力，因此組織需清楚識別關鍵業務、強化風險應對、建立持續運作機制與韌性文化，才能在多變的環境中穩健經營。

二、數位化帶來的便利及效率，但往往也成為犯罪人士利用的工具，深度偽造（deepfake）的技術也讓詐欺手段更難以用肉眼或傳統規則辨識，若金融業未能在流程、技術與組織等面向同時進行多層防護，恐帶來無法衡量的損失及聲譽風險，因此在邁向數位化時，除了利用多因子驗證、深偽檢測模型、數位簽章等技術層面外，仍需同時運用雙人複核、強化 KYC 作業及第三方供應商管理等流程，以降低網路威脅攻擊機率。

三、AI 發展趨勢已勢不可檔，如何善用 AI 未來將成為未來金融業致勝關鍵，銀行業應有短中長期規劃，全面盤點日常工作，透過 AI 之運用減少重複性人力作業，諸如公文撰寫、智能客服、產品行銷、申報主管機關報表彙整、財報分析、客戶資料蒐集、資料統計、交易監控、自動偵錯及風險管理等，以減省成本、提高效能、降低錯誤率及提高人力運用效能。

四、對跨國銀行來說，面對不同監理的規範與推陳出新的法規，內部稽核難以即時掌握各國監理的要求與同時符合各國監理的期望，以台資銀行為例，第二道防線的法遵主管多於當地聘僱專業人才，但第三道防線仍多以總行內部稽核單位人員查核為主，總行內部稽核單位在人力有限，以及台灣的內稽實務尚未與國際接軌的情況下，難以同時滿足各海外分行所在國的法規與監理要求，因此需積極與各海外單位的法遵/業務主管密切合作，定期掌握當地監理動態與政策變化。遇到同業裁罰案例或外部法規存在重大差異時，應優先聚焦於合規議題，例如洗錢防制、供應商管理等各國監理機關高

度關注的重點領域。對於監理要求差異顯著的情形，則需彈性調整稽核策略（如委外查核），從在地法規與實務出發，確保符合當地監理標準，提升合規效果與風險管控。

五、在 AI 技術持續進步，傳統以事後查核的稽核的工作正逐步被自動化工具取代，因此內部稽核角色必須轉型升級，從事後查核走到業務前端，參與策略與業務發展，透過風險辨識與分析，提供前瞻性、建設性的建議與回饋，朝向成為組織顧問的目標邁進，提升稽核的價值。

六、面對新興風險及多變的監理環境，內部稽核團隊必須持續提升跨領域專業能力，不僅要深化金融與風險管理專業知識，還需掌握 AI 技術應用、數據分析能力、以及 ESG 和組織行為等新興領域的理解，培養稽核人員的多元技能，並可輔助稽核人員取得國際專業認證，如國際內部稽核師（Certified Internal Audtor, CIA）、國際電腦稽核師（Certified Information Systems Auditor, CISA）、國際風險管理確認師（Certification in Risk Management Assurance, CRMA）等，增加國際競爭力與國際觀，並透過內部跨部門輪調與實務經驗累積，以持續提升稽核人員專業能力。

七、全球對 ESG 的重視程度，趨使台灣地區金融業必須逐步調整以配合國家 2050 淨零轉型，接軌國際訂定國家自訂貢獻目標，銀行業亦透過制定相關規範及實際行動來達成永續發政策，包含碳排放盤查、綠色採購與供應鏈管理、提供永續金融商品與服務、照顧員工福祉與發展、落實勞動相關法令、設置申訴與溝通管道、參與社會公益、重視金融消費者保護、設立永續發展委員會、明定高階管理階責任、參考「全球報告倡議組織」（Global Reporting Initiative, GRI）、「永續會計準則委員會」（Sustainability Accounting Standards Board, SASB）、「氣候相關財務揭露」（Task Force on Climate-related Financial Disclosures, TCFD）等強化永續報告書的揭露。除組織之外，個人亦可透過隨手關燈、改用環保杯、自備購物袋及環保餐具、搭乘大眾交通工具、購買節能標章商品、做好資源回收、支持弱勢團體、參加公益活動、維持並關心自身及家人健康等方法支持 ESG，貢獻一己之力。