出國報告（出國類別：其他）

2023 年金融檢查與稽核研修班

服務機關：臺灣銀行董事會稽核處
姓名職稱：徐秋蓉　助理稽核
派赴國家：澳洲
出國期間：2023.11.4. ~2023.11.11.
報告日期：2024.1.11.

摘　要

中華民國銀行公會與台灣金融研訓院本次特於澳洲雪梨舉辦 2023 年「金融檢查與稽核研修班」，希望藉由澳洲金融監理機構及澳洲同業銀行間經驗分享，及外部稽核之跨國交流，導入國際經驗與澳洲實務趨勢，提升臺灣金融業對於風險之因應能力、進而促進本國金融監理與稽核制度與國際接軌。

今年度活動主軸為「國際金融監理趨勢、內部稽核數位轉型、資訊安全、舞弊稽核及永續發展」，透過機構考察形式，與澳洲金融監理署（The Australian Prudential Regulation Authority, APRA）、跨國銀行（澳盛銀行 ANZ Bank、澳洲聯邦銀行 CommonWealth Bank）、國際知名會計師事務所（KPMG、PwC 等擔任澳洲金融機構之外部稽核）及 Fidelity National Information Services（FIS）和 S&P Global 等知名機構進行交流與學習，探討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。

目　次

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，幫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，中華民國銀行公會與台灣金融研訓院本次特於澳洲雪梨舉辦2023年「金融檢查與稽核研修班」，並由金管會檢查局張局長親自帶團，希望透過國內外主管機關及銀行稽核主管經驗分享，了解金融業新挑戰及因應戰略，提升本國稽核品質及法遵文化，加速內稽轉型，特邀請當地資深金融專家共同探討以下重要議題：

★ APRA對於銀行公司治理、風險管理、法令遵循與內部稽核之最新期待

★ 監管科技(Reg Tech)之最新趨勢、實際應用經驗分享與面對之挑戰

★ 2023年澳洲各銀行辦理CPS 234 Tripartite資訊安全獨立測試缺失及風險

★ 如何應用數位科技，落實風險導向稽核、分享新型稽核數位化工具與AI提升查核品質

★ 澳洲政府2023年~2030年網路安全戰略

★ 澳洲金融同業與外部稽核之氣候風險管理、詐欺風險管理策略

貳、行程

一、參訪行程

本次參訪期間為 112 年 11 月 4 日至 11 日，由金管會檢查局張局長子浩擔任團長，率領檢查局鄭稽核昭鈴，及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，與台灣金融研訓院工作人員及銀行同業共 16 員，共計參訪七個機構，列表如下：

日期	參訪機構	討論議題	會面人員
Day 1~2 11/4~5 下午		抵達澳洲雪梨	
Day 3 11/6 (一) 上午	APRA 澳洲金融監理署	從澳洲金融監理機構觀點，談強化銀行治理與風險管理 (Strengthening Bank Governance and Risk Management: Insights from Australian Financial Regulators)	➢Alison Bliss, General Manager, Cross Industry Insights ➢Katie Melville, Head of Government and Remuneration ➢Graham Ellis, Risk Specialist, Operational Resilience ➢Shoma Banerjee, Manager, Remuneration ➢Abhey Bains, Risk Specialist, Risk Culture
Day 3 11/6 (一) 下午	S&P Global 標準普爾全球	銀行業氣候風險管理 (Climate Risk Management for Banking Sector)	➢Michael Salvatico, Head of Asia, Pacific, Middle East & Africa ESG Solutions
Day 4 11/7 (二) 上午	Fidelity National Information Services (FIS)	稽核與新興風險 (Auditing and the Emergent Risk)	➢Michael Ahn, Head of Business Solution, APAC - Capital Market
Day 4 11/7 (二) 下午	ANZ 澳盛銀行	從銀行內部稽核觀點，談銀行業永續經營 (Driving Sustainable Banking: Insights for Bank Internal Auditors)	➢Mani Dhamodaram, Director – Corporate Centre, ANZ Internal Audit

Day 5 11/8 (三) 下午	CBA 澳洲聯邦銀行	啟動內部稽核數位轉型 (Driving Digital Transformation in Internal Audit)	➢Yeonee Law, General Manager, Business Banking, Deputy CEO, Advice & Insurance ➢Kathy Condos, Chief Operating Officer, Group Audit and Assurance ➢Niren Naidoo, General Manager Retail Banking Services, Chief Operations Office
Day 6 11/9 (四) 上午	PwC Australia	數位時代的詐欺風險管理(Strengthening Fraud Risk Management in Digital Age: Insights for Bank Internal Auditors)	➢Jane, He, Partner
Day 6 11/9 (四) 下午	KPMG Australia	網路觀察見解 (Cyber Insights)	➢Stuart Jones, Cyber Director
Day 7 11/10 (五) 上午	飯店	《小組心得分享》 《澳洲臺資銀行代表座談會》	➢合作金庫銀行雪梨分行洪祥洋協理 ➢兆豐商銀雪梨分行王慶宗經理 ➢華南銀行雪梨分行楊世彬經理 ➢臺灣銀行雪梨分行金元虎經理
Day 7 11/10 (五) 下午		返台	

二、參訪內容介紹

（一）參訪澳洲審慎監理署

2023.11.06

- 參訪機構：Australian Prudential Regulation Authority (APRA)
- 研討主題：從澳洲金融監理機構觀點，談強化銀行治理與風險管理(Strengthening

Bank Governance and Risk Management: Insights from Australian Financial Regulators)

一、內容概要

本次演講邀請 APRA 分享四大風險議題，包含公司治理(Governance)、風險文化(Culture)、薪酬制度(Remuneration)、問責制度(Accountability)等面向，並對包括 Cyber Risk 管理、CPS234 資訊安全第三方獨立驗證(Tripartite)等議題深入探討。

二、內容說明

1. GCRA 概述

澳洲審慎監理署(APRA)分享近年監理方向在於致力推動銀行文化轉型，希望推動良好治理、風險文化、薪酬制度與問責制度(以下統稱 GCRA)，提升機構安全及營運韌性。APRA 表示，探究金融體系風險事件之根源，在於業者輕忽 GCRA，未能識別和減輕 GCRA 問題的弱點可能會破壞受監管機構的財務和運營彈性，因此力推相關政策引領業者遵循為其監理重點。具體而言，APRA 期望促使金融機構建立強健董事會、高效決策流程與內部監督機制，營造重視風險之組織文化及形成一致價值體系，輔以著重風險策略和業績目標相稱之薪酬制度，與導入責任地圖及責任聲明書做法，要求高階管理人員明確承擔業務風險及結果之責任，確保機構達成長期穩健經營之目標。

在利率和通膨上升、房地產價格下跌和地緣政治持續不確定性的環境下，APRA 2023 年的優先事項為維持金融體系的韌性、提高整個金融體系的網路韌性，以確保受監管機構能夠迅速應對當今的風險以及即將到來的新挑戰，使銀行存款人、保險保單持有人和養老金成員利益，均獲得保障。為了改善澳洲金融機構、保險和退休金產業的機構的風險和治理文化，並強化董事和高階主管責任和問責框架，APRA 新推行「澳洲金融問責制度(Financial Accountability Regime, FAR)」。澳洲金融問責制度 (FAR)將取代2018年開始實施的銀行高階經理人問責制度(Banking Executive Accountability Regime, BEAR)，由APRA和澳洲證券和投資委員會(ASIC)共同管理，預計於2024年3月15日適用於授權存款機構(ADI)及其授權非經營性控股公司(NOHC)，另自2025年3月15日起適用於保險機構、其持牌NOHC和退休金受託人。

2. GCRA 自我評估

APRA 為有效推動 GCRA，分階段實施 GCRA 自我評估問卷，同時審視修訂相關監管規範，如 APRA 審慎監理標準 CPS 510 Governance、CPS 220 Risk management、CPS511 Remuneration，及為加強董事和高階主管責任訂定高階經理人問責制度(BEAR)和預計推動之澳洲金融問責制度 (FAR)等。針對問卷調查，APRA 分享 2022 年 11 月所公布之 18 家金融機構(ADIs)問卷結果，其中就機構高階管理層與基層員工對風險文化認知構面說明以下發現：

(1)機構雖持續改善風險文化，但仍有改進空間；

(2)高階管理人評估對風險管理有效性及投入程度已經足夠，惟相較風管人員及法遵人員，卻嫌樂觀；

(3)高階管理人認為風險胃納審慎保守，惟與基層人員認知有所差距。

有鑑於前項調查凸顯組織階層認知差異，APRA 鼓勵提升員工挑戰高階主管盲點之空間，並應強化揭弊及員工保護機制，以形塑從上到下一致之風險文化。

3. CPS 511 薪酬制度

APRA 就影響風險文化構面另提及新制定之 CPS 511 法規。CPS 511 將自 2025 年 6 月生效，要求受監管機構每年公開揭露薪酬制度框架、薪酬制度設計、公司治理及其結果，且要求須提供額外量化資訊，包括薪酬議定所考量之實質非財務指標項目與權重(風險管理、合規、客訴、監管結果等指標)。此外，金融機構應執行較長之獎金授予期間，避免員工受短期績效驅動而從事過度暴險之不當行為。

4. CPS234 資訊安全 Cybersecurity

隨著資訊及網路發展，金融機構運用數位科技提供服務之同時也面臨嚴峻資安風險。APRA 制定 CPS 234 規範，要求金融機構強化資訊安全框架、識別與分類資訊資產、確保第三方合規、系統安全保護、資安事件應變管理、資安事件通報等，以抵禦網路攻擊威脅，提升營運韌性。

為檢視受監管機構是否符合 CPS 234 資訊安全標準，APRA 分階段要求機構實施外部第三方獨立評估(Tripartite)。APRA 於第一輪評估之主要發現包括：

(1) 機構對關鍵和機敏性資訊資產的識別和分類不完整：

資訊資產包括軟體、硬體和數據都具有很大的價值和風險。APRA 觀察到，在識別和分類資訊資產方面，各行各業的成熟度各不相同。如果沒有適當的識別和分類，機構可能很難確定適當的資訊安全控制措施，以保護關鍵和敏感數據免遭未經授權的訪問或披露。

常見的差距包括：

(a) 資訊資產分類政策和方法尚未完全確立，也沒有明確界定哪些資產應被視為關鍵和/或敏感資產的標準；

(b) 資產登記清冊中的資訊沒有按照機構自身政策的要求由資產擁有者定期審查和更新，導致資訊不完整和不準確；

(c) 第三方管理的資產未得到充分辨識和分類，在某些情況下甚至根本沒有被識別。

為了解決這些差距，各機構必須確保：

(a) 在定義資產分類策略和標準時，考慮安全危害對資產的潛在影響

(b) 利用資訊資產資料庫，如配置管理資料庫（CMDB），促進資產登記

(c) 確保資訊資產繼承其組成元件的最高關鍵性和敏感度等級。

(2) 未能充分評估第三方供應商之資訊安全能力：

對第三方服務提供者運營的資訊安全控制，是一大挑戰。這是一個令人擔憂的問題，因為越來越多的機構依賴服務提供者來管理重要的系統。

常見的差距包括：

(a) 第三方資訊安全控制評估計劃範圍有限，或者在某些情況下不存在；

(b) 控制設計和運行有效性通常僅基於第三方的自我評估，而沒有通過額外的獨立測試進行驗證；

(c) 沒有保留控制測試證據來證實測試結論；

(d) 測試的性質和頻率與第三方管理的資訊資產的重要性和敏感性不一致。

為了解決這些差距，機構通常會：

(a) 瞭解哪些資訊資產由第三方管理，並使用它來確定測試所需的嚴格程度

(b) 瞭解第三方的控制措施

(c) 通過訪談、調查、控制測試、認證、合同審查、證明、轉介和獨立保證評估相結合的方式，測試第三方控制的有效性

(d) 確保已具備及時解決發現缺失能力。

(3) 對控制之定義及測試計畫之執行未臻妥適：

受 APRA 監管的實體必須通過系統的測試計劃來測試其資訊安全控制的有效性。第一期的調查結果顯示，在許多情況下，各實體的測試計劃不完整、不一致、缺乏獨立性，並且沒有為管理層和董事會提供足夠的保證。

常見的差距包括：

(a) 資訊控制保障計劃和計劃未到位或對關鍵控制措施的覆蓋範圍不足，例如：使用者訪問審查、物理安全控制測試、遺失數據防護控制

(b) 測試的性質和頻率往往與資訊資產的關鍵性和敏感性不相稱

(c) 測試不是由功能獨立的測試人員執行的

(d) 測試程式和成功標準缺乏一致性

(e) 為確定資訊安全控制的有效性而評估的證據不會被保留。

為了解決這些差距，機構通常會：

(a) 採用多種測試方法

(b) 定義明確的成功標準（包括何時需要重新測試）

(c) 由具有適當技能和職能獨立的專家進行測試，他們對正在驗證的控制措施不負有操作責任。

(4) 未定期審視並測試應變計畫

受 APRA 監管的實體必須制定計劃，以應對其認為可能發生的資訊安全事件。從評估中發現，資訊安全事件回應計劃不完整，缺乏定期測試和審查。

常見的差距包括：

(a) 事件回應計劃沒有到位，沒有定期審查和/或測試

(b) 事件管理政策和流程沒有明確定義第三方的角色和責任

(c) 事件回應 playbook 的合理中斷方案有限

為了解決這些差距，機構必須確保其事件回應計劃（包括由第三方運營的計劃）至少每年進行一次測試，以確保它們仍然適合目的。這些計劃將：

(a) 涵蓋各種可能的中斷方案，包括：惡意軟體感染（包括勒索軟體）、數據洩露 、洩露員工或客戶資訊、駭客攻擊面向互聯網的平台等

(b) 有足夠的詳細資訊，以說明最大限度地減少所需的決策量，並明確資訊安全事件期間的角色和職責。

(5) 對資安管理之內部稽核有限

受 APRA 監管的實體的內部稽核活動必須包括對資訊安全控制的有效性的審查，包括由第三方維護的控制。評估結果表明，整個行業對第三方資訊安全控制的內部稽核評估有限。

常見的差距包括：

(a) 通過內部稽核對第三方運營的資訊安全控制措施進行有限的審查

(b) 在某些情況下，執行控制測試的內部稽核人員缺乏必要的資訊安全技能

為了彌補這些差距，機構的內部稽核團隊應該：

(a) 針對資訊安全危害影響重大且依賴其他控制測試的能力較低的稽核領域

(b) 審查其他地區和第三方進行的測試的範圍和品質，以確定可以依賴該測試的程度

(c) 向董事會報告任何已發現的重大缺陷或缺乏任何保證。

(6) 未及時通報 APRA 重大事件與控制弱點

必須將每個實體網路安全系統中的重大事件和控制弱點通知 APRA。評估發現，確定和定義這些報告給 APRA 的過程往往不一致、不明確，在某些情況下甚至根本沒有到位。

常見的差距包括：

(a) APRA 通知要求未納入機構之政策中

(b) 與關鍵第三方簽訂的合同不包含向 APRA 報告重大事件和控制弱點的要求

(c) 未明確定義何為重大和應通報事件以及未明確定義控制弱項的標準

(d) 未建立即時通報的機制或未依規定執行

機構必須識別並向 APRA 報告重大資訊安全事件和控制弱點，並將受益於：

(a) 制定明確的治理流程，將事件和控制薄弱環節上報給相關治理機構，並及時通知 APRA

(b) 利用各種機制識別重大控制弱點，包括控制測試、保證活動、資訊安全事件、軟體和硬體供應商的漏洞通知，以及第三方和關聯方的其他形式的通知。

（二）參訪標準普爾全球公司 S&P Global

2023.11.06

- 參訪機構：S&P Global
- 研討主題：銀行業氣候風險管理 (Climate Risk Management for Banking Sector)

一、內容概要

1. 重要的永續發展情報。
2. 氣候風險信用分析對金融業風險的重要性
3. S&P 建議

二、內容說明

1. 重要的永續發展情報

(1) 以 ESG 作為所有利害關係人的風險抵減及價值驅動器：

- 股東：關心投資的長期價值
- 資產管理者:幫股東管理資金，關心 ESG 議題
- 債權人：關注永續可能影響公司表現
- 顧客：千禧世代顧客願意支持永續產品
- 員工：具備永續策略的公司較能吸引優秀人才
- 監管機關：監管機關對於 ESG 相關規定激增，且關注於永續報告的揭露與透明度。

(2) 融資碳排挑戰-範疇三

- 碳排的計算包含範疇一:直接碳排、範疇二:間接碳排、範疇三:包括組織之外的一切，銀行最大的碳排來源來自範疇三的授信資產組合。
- 金融業衡量融資碳排最大的挑戰在於資料的取得

(3) 氣候變遷風險：依據美國聯邦準備銀行芝加哥分行的研究報告，氣候變遷引發的風險可概分為實體風險（physical risk）、轉型風險（transition risk）與責任風險（liability risk）三大類型。

- 實體風險：實體風險是指極端氣候事件（如暴風雨、暴風雪、洪水、乾旱和相關的野火及熱浪），可能對房屋、基礎設施和企業供應鏈造成破壞，使相關企業或個人蒙受財務損失，從而無法履行交易或償還銀行貸款，亦令金融保險機構承擔損失或支出，可能造成銀行資產直接損失、授信企業戶擔保品嚴重損失、授信戶供應鏈斷鏈間接損失。實體風險衡量可以透過先衡量風險暴險程度，並將其轉化為財務數字，開始討論這些風

險的具體情況，也越來越多企業把氣候戰略列為重要議題於董事會議程中討論。銀行資產直接損失、授信企業戶擔保品嚴重損失、授信戶供應鏈斷鏈間接損失。

- 轉型風險：轉型風險泛指公共政策、法規的修訂逐漸將抑制氣候變遷納入考量，進而為企業帶來一定的風險。例如傳統企業因新環保法規推高生產和配銷成本，或來自環保團體抗爭的挑戰、新環保技術投資的抉擇與壓力，可能造成法規趨嚴之違規成本大增、授信企業戶低碳轉型過程不順利致影響債權、風險揭露不足或揭露不實致股東遭受重大損失提出訴訟、投入轉型不力致銀行形象聲譽受損、投資部位標的之企業低碳轉型過程不順利，可能影響其評等及評價。依據最新的目標，全球的減碳目標已經落後 72%，此為風險升高的強烈訊息，需要將這些資訊納入分析中，包括未來碳價等可能的影響。
- 責任風險，則是指遭受氣候變遷損失的當事人，透過訴訟或保險索賠等方式，從他們認為該為此事負責的人手中追回損失時可能產生的風險，較常見的案例是與氣候變化相關的集體訴訟與對保險公司的索賠等。例如 2018 年 7 月美國羅德島州政府對幾家石油公司提出訴訟，指責它們造成的氣候變遷效應，導致該州基礎設施及沿海社區遭到破壞。對這些石油公司來說，這是州政府尋求其為氣候變遷衍生成本負責的責任風險。客戶或公司因氣候變遷相關風險而可能遭受的損失尋求賠償時，可能造成：訴訟導致業務中斷、訴訟導致罰款等影響。

(4) 監管環境：針對永續發展的監管不是即將到來，而是已經到來，在紐西蘭、歐洲及印度等國家之監管機構，已經開始要求必須辦理永續發展報告的申報，台灣目前雖然還未有相關的申報要求，但應該在不久的將來會跟上國際腳步。針對正在發生中的氣候風險法規，未來公司都需要做出更多的回應，從創新轉向合規和監管的趨勢。另外，內部稽核亦需持續關注相關法規的發展。

2. 氣候風險信用分析對金融風險的重要性

(1) 氣候風險相關議題：由於「氣候風險的衡量」對現代企業的永續經營已產生關鍵影響。為因應此一趨勢，TCFD 為國際經濟合作論壇 G20 要求旗下的金融穩定委員會（Financial Stability Board, FSB）於 2015 年 9 月召開會議，由公營和民營產業部門代表參加，一同商討金融產業應如何考量氣候相關議題，於 2015 年 12 月成立氣候相關財務揭露工作小組（簡稱工作小組），於 2017 年 6 月正式發佈「氣候相關財務揭露」（Task Force on Climate-related

Financial Disclosures, 簡稱 TCFD)，要求企業藉由「治理」、「策略」、「風險管理」及「指標與目標」四個核心要素，來有效管理氣候變遷的風險與機會，引導企業投資者和管理者聚焦相關議題，並提供可靠的財務基礎資訊供利害關係人參考與衡量。

(2) S&P 介紹了氣候信用分析工具，這個工具是與聯合國環境計劃財務倡議合作開發的，它提供了行業特定模型、用戶特定調整和與財務數據的整合。已經有包括主要銀行和監管機構在內的眾多機構採用它來評估氣候風險並調整財務指標和信用評級。由於它是基於情境和財務數據進行壓力測試，從而使組織能夠評估氣候調整的違約概率和信用評級，讓組織能夠適應不斷變化的氣候風險環境。

3. S&P 建議：

(1) 氣候風險的議題，不僅僅是一個金融議題，也是全球各國需要一起面對的問題。金融業需要運用其於金融中介的影響力，協助個人和企業適應氣候變化及面對其帶來的威脅，並成為國家和社會穩定的力量，讓個人和企業於持續前進的過程中考慮氣候變化的金融影響，避免造成的損失。

(2) 在衡量新興風險中最挑戰的仍然是資料和技術，需要有全面性的數據分析，方能評估組織所面對氣候變化之實體風險和轉型風險，並擬定氣候戰略目標。

(3) 各國監管機關針對氣候風險議題，陸續制訂監管政策或監管報告要求，以提升金融業的營運韌性。目前台灣主管機關針對氣候風險的揭露雖尚未有相關監管報告，但可預見不久將來亦將會有相關監管報告。對於有較多海外據點的銀行，因所處的國家不同，相關的監管規定亦有所不同，總行需與海外分行合作了解當地規定，並提供相應的支援，未來金融業於因應新興風險之遵法成本勢將與日俱增。

(4) 未來需要主管機關對於氣候相關議題，及早與國際接軌制訂相關規定，並與各國主管機關和金融業合作，並進一步做到數據共享。內部稽核也需要持續保持學習，將氣候風險納入稽核計畫中，針對氣候風險之數據資料、信用風險評估方法論及計算進行確認，了解業務單位氣候風險戰略目標及於因應氣候風險所採取的相關因應措施，確保銀行動態因應持續演進發展中的永續議題及新興風險，保持銀行競爭力。

(5) 金融業於面對不確定性高的新興風險，我們應該採取的行動就是作好充分準備、冷靜分析環境與風險變化，並且及早著手擬定應對方案與隨時因應

調整，「Start Earlier」是我們迎戰未知且快速變化的金融環境與風險挑戰之最佳行動。

（三）參訪 Fidelity National Information Services (FIS)

2023.11.07

- 參訪機構: FIS, Fidelity National Information Services
- 研討主題: 稽核與新興風險 (Auditing and the Emergent Risk)

一、內容概要

FIS 主要就稽核作業與新興風險等相關議題進行分享，包含三道防線介紹、氣候風險、新興風險等主題，分述如下：

二、內容說明

1. 三道防線

(1) 管理風險最佳方式即為承擔風險，惟須考量以下限制：

(a) 承擔之風險已定義於風險胃納聲明並由相關管理委員會或董事會核准。

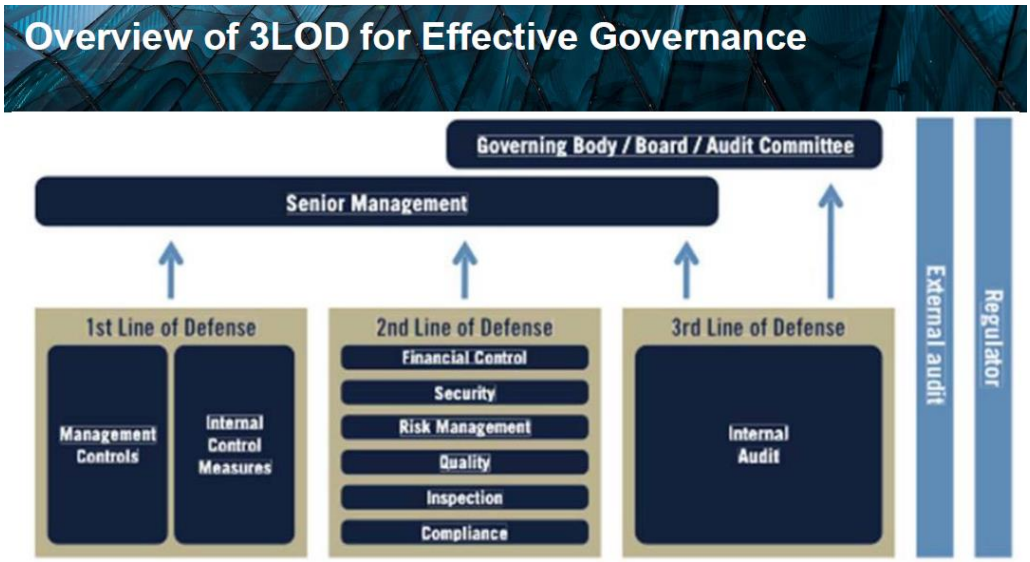
(b) 承擔之風險經由流動性或資本等工具之運用已為適當之抵銷。

(c) 風險應依銀行政策持續監控與管理。

(d) 風險管理架構應訂定承擔、監控和管理風險之總體目標指引。

(e) 建議採用三道防線以明確區隔風險承擔者(第一道防線)、風險管理者(第二道防線)及稽核(第三道防線)。

(2) 三道防線需要每條防線都具備足夠的知識、技能與訊息，並了解各自在經營環境中的獨立目標。



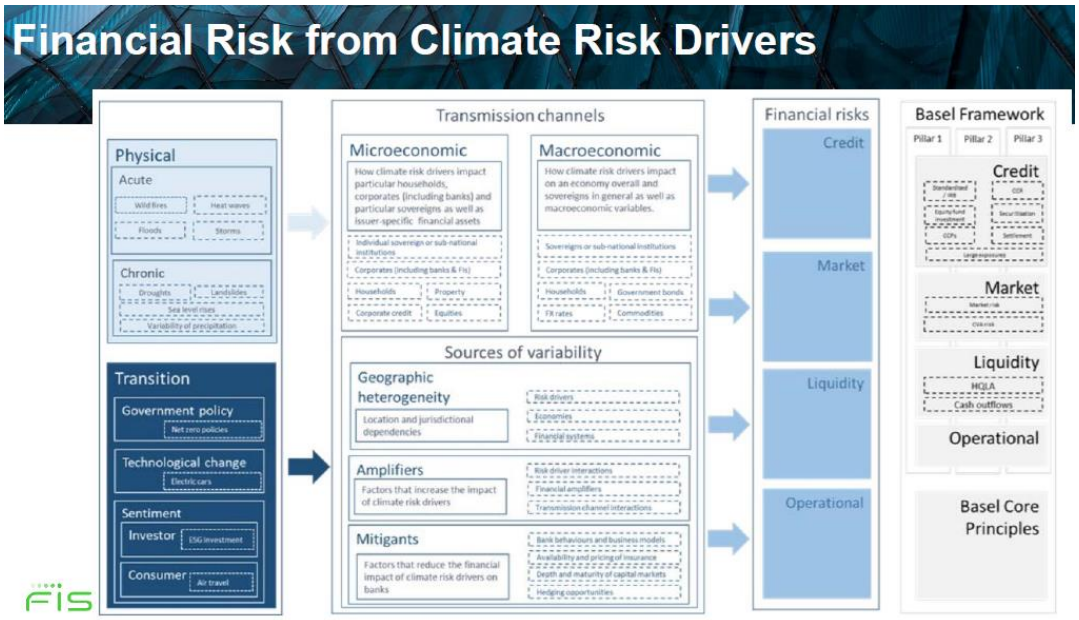
2.氣候風險

(1)氣候風險驅動所帶來的財務風險：

(a) 氣候風險可分為因氣候變遷或極端氣候造成衝擊之「實體風險」與為達成低碳經濟目標之「轉型風險」。

(b) 氣候變遷影響總體經濟表現，亦衝擊家戶或個別企業，直接或間接影響金融機構所承做之業務。

(c) 經濟活動影響金融機構之財務風險因子包含：信用風險、市場風險、流動性風險及作業風險等。



(2)建置氣候風險相關管理架構、模型或情境分析等，可參酌巴塞爾銀行監理委員會(Basel Committee on Banking Supervision, BCBS)風險治理建議、氣

候相關財務揭露工作小組(Task Force on Climate-Related Financial Disclosures, TCFD)之資訊揭露建議等。

(3) 數據資料是計算氣候風險最重要的因子，惟目前台灣銀行業的客戶資料完整性尚待加強。

解決方案：

●重新找客戶索取所需資訊，惟可能需耗費相當的人力、時間與資源；

●尋求資料提供之廠商協助，惟台灣中小型企業眾多，資料提供之廠商除大型企業數據資料庫外，能否提供完整的中小型企業廠商資料將是一大挑戰。

3.新興風險：

永續相關的新興風險，除了氣候風險外，還包括能源轉型、能源安全、資訊安全風險、聲譽風險及金融市場應對低碳替代能源解決方案需求增長的調整，永續相關的議題在金融服務業日益重要。業務面越來越多的數位運用，新興風險的挑戰持續增加，不論是風險衡量的方法和技術持續發展，其中最挑戰的是數據資料的不易取得，金融業於面對永續相關風險需要透過全面的數據分析，制訂戰略目標，以應對其帶來的挑戰與機會。

（四）參訪澳盛銀行 **ANZ**

2023.11.07

- **參訪機構:** Australia and New Zealand Banking Group Limited (ANZ)
- 研討主題：從銀行內部稽核觀點, 談銀行業永續經營 (Driving Sustainable Banking: Insights for Bank Internal Auditors)

一、內容概要

ANZ 分享內部稽核對氣候變化和永續性方面扮演的角色和應負的責任。主講者以氣候變遷風險為主題，除強調內部稽核持續教育之必要性外，並說明國際永續準則與框架、溫室氣體排放量之計算、應對實體風險、轉型風險與責任風險等議題。而為確保有效應對氣候變遷風險，內部稽核應瞭解機構運營策略及風險胃納，以有效評估風管效能。惟，內稽過程所採用數據品質與模型攸關執行成效，數據資料取得不易亦是內部稽核須面對之重要課題。

二、內容說明

1. 內部稽核角色與責任

(1) 教育訓練：內部稽核須積極持續參與教育訓練，以了解與氣候變遷與可持續性相關之專業術語、標準和框架。例如：全球報告倡議(GRI)與 Sustainability Accounting Standards Board (SASB) 標準、責任投資原則(PRI)、IFRS、可持續性評級(如 DJSI)和排名等，以提升內部稽核對氣候變遷和 ESG 議題之理解。

(2) 瞭解組織業務運營：內部稽核應瞭解組織核心業務環境與運營，監理機構期望、機構 ESG 戰略，以及與氣候相關之風險與機會等，以確保機構業務與其戰略目標保持一致。

(3) 提供獨立確認：內部稽核應瞭解機構範疇一、範疇二、範疇三(Scope1~3)溫室氣體排放主要來源、溫排計算方式(如 PCAF 指引及標準)、溫排對組織之影響；另設定情境分析及壓力測試評估風險，以多種面向分析提供獨立確認。

2. 對與氣候風險相關之產品與服務執行內部稽核

(1) 識別氣候相關風險：識別與機構相關之氣候風險，包括實體風險(如極端天氣之破壞)、轉型風險(如政策、技術變化或市場變革)、以及法律責任風險(如氣候訴訟)，並評估風險所產生之影響與潛在後果。

(2) 監控、風管與陳報：瞭解機構監控與陳報風險之關鍵指標、機構目標設定、內部政策程序及流程等構面，以掌握氣候風險管理完整機制。此外，內部稽核亦須擷取及儲存運用相關數據，以追蹤風險管理成果，評估機構 ESG 績效並陳報利害關係人。

(3) 情境分析與壓力測試：內部稽核應以長短天期氣候變化設定情境，以量化數據及模型，分析不同氣候狀態對機構本身與其核心業務之潛在影響，並進行壓力測試，以評估氣候變遷對其投融資部門可能造成之損失。

3. 數據重要性

(1) 瞭解數據：稽核需掌握數據來源與可靠度，以及數據擷取方式或數據生成原則等，確保數據品質及採用適當性，惟此係稽核目前面對之一大挑戰。

(2) 監理要求及新興標準：數據正確性與完整性奠定情境分析之關鍵基礎。內部稽核除應考量現行監理數據，亦應掌握於不斷更動法規環境所衍生之新興標準要求，以完整納入機構 ESG 評估面向。2023 年 6 月 1 日，歐洲議會通過了歐盟「企業永續盡職調查指令」，成員國應將人權和環境影響納入公

司治理的規則。公司將必須鑑別並在必要時防止、終止或減輕其活動對人權和環境的負面影響，該指令要求公司必須實施一項轉型計畫，致力將全球暖化控制在 1.5℃ 之內，對於員工人數超過 1000 人之企業，為了加強董事的責任，須將氣候轉型計畫績效連結高階主管獎酬制度。

4. 揭露策略與承諾

氣候變遷之風險評估須建立於適當之查核範圍(audit universe)，且應定期檢視涵蓋層面，並以三道防線之各個視角，執行整合性查核。同時，內部稽核應致力於確保機構充分揭露其 ESG 資訊，且該項資訊應以準確與可靠之數據為基礎，以滿足內外部利害關係人之期待。

（五）參訪澳洲聯邦銀行 CBA

2023.11.08

- 參訪機構：CBA (Commonwealth Bank of Australia)
- 研討主題：啟動內部稽核數位轉型 (Driving Digital Transformation in Internal Audit)

一、內容概要

銀行公會於 111 年 10 月公布「本國銀行建置內部稽核數位化查核機制指引」，金管會 111 年 11 月函請銀行公會配合國內、外內部稽核數位化情形及本國銀行需求，適時就銀行業內部稽核數位機制予以精進。本次安排與 CBA 進行參訪交流，請 CBA 分享如何推動內部稽核數位化轉型。CBA 員工約五萬人，稽核團隊 (Group Audit and Assurance, GA&A)約 250 人，佔比約 0.5%；CBA 分享該銀行為何積極推動數位轉型、實際運作情形、轉型之關鍵成功因素，以及運用新興科技對稽核人員的影響等四個議題進行說明。

二、內容說明

1. CBA 稽核團隊積極推動數位轉型原因

(1) 近年來銀行業積極推動業務轉型，提供數位化服務，客戶非臨櫃交易比例增加。隨著環境的變化和競爭威脅，CBA 體認到僅以傳統稽核方式顯然不足以跟進該行積極推動業務數位化發展演變，因此稽核亦需同步進行數位化轉型。

(2) 稽核在查核過程中都會碰到數據，也因此 CBA 注重提升稽核數據分析能力

及運用 AI 的技能，期許稽核人員應具備高附加價值之判斷的能力。

2. CBA 數位化轉型實際運作情形

(1) 過去三年，因關鍵風險及技術的出現，致 CBA 在應用分析方面投入大量研發，查核過程中，導入如何利用數據分析提昇查核效率。

(2) CBA 稽核團隊數位轉型，以每三年為一個循環，團隊中大約 30%具專精數位能力，60~70%則有運用資料分析的能力。另 CBA 也設定未來三年目標，目前約 20%稽核人員使用人工智慧技術，未來將提高至 60%。

(3) CBA 於內部網站平台提供模型和工具建置稽核流程，所採用的稽核數位化運用工具包含使用 Python、Process Mining、R 及 H2O.ai (Partnership)等工具開發模組。這些工具讓 CBA 從傳統的隨機抽樣，升級為對出現問題的全部交易進行測試，且不需花費大量時間規劃及收集資訊，達到精進查核工作效果，並透過持續場外監控，找出較高風險之領域進行加強查核。

(4) CBA 分享運用 AI 模型的案例：以詐貸案件為例，當客戶申請貸款時，會涉及稅務部門的收入報表，若依傳統方式查核，僅能就申貸文件抽樣查核，但若使用 AI 模型則可掃描文件並自動尋找異常，據以發現更多的冒貸申請，提高查核品質。

3. 推動數據化轉型之關鍵成功因素

(1) 同仁心態的改變與主管容錯的雅量在數位轉型的過程中同等重要。除了稽核作業最基本的確認功能以外，在邁向數位轉型的過程中，同仁可以更有意識的去思考在查程中如何引入數位工具或數據分析，讓整個查核更有效率。然而，新的查核想法、數位工具或技術導入未必總能達到預期的效果，主管能否理解同仁想要創新、改變的初衷，而坦然接納結果不如預期的可能性，將左右數位轉型能否順利推動。

(2) 資料(包含資料的取得與資料的完整性)是稽核數位化的關鍵因素，而這仰賴利益關係人(第一、二道防線)的支持；與利益關係人維持良好互動，有助於資料或資訊的取得、彼此專業知識的交流及新研發工具的試用等。

(3) 董事會及高階管理層的支持：

(a) 數位轉型需要大量的資金及資源投入，需獲得董事會及高階管理層的支持，方能讓轉型計畫順利推動與執行。

(b) CBA 稽核團隊取得董事會支持的方法為：選取三個重要的風險議題全

力投入數位分析，向董事會及高階管理層展現成果，取得經營階層的肯定。

4. 運用新興科技對稽核人員的影響

AI 所運用或分析的資料是「人」提供的，藉由科技的輔助，未來查核可能是就整個母體進行檢視而非僅是抽樣；而運用數位工具所產生的結果仍需要稽核人員進行專業判斷，這正是稽核人員的核心價值所在。

（六）參訪 PwC

2023.11.09

- 參訪機構：PwC
- 研討主題：數位時代的詐欺風險管理(Strengthening Fraud Risk Management in Digital Age: Insights for Bank Internal Auditors)

一、內容概要

1. 關注數位時代的詐欺風險
2. 數位時代打擊詐欺風險的好作法
3. 內部稽核的角色

二、內容說明

1. 關注數位時代的詐欺風險
   (1) PwC 每 2 年一次針對全球經濟犯罪和防範調查，2022 年針對 2300 家組織進行調查結果顯示：
      - 62%的受訪者在 24 個月內經歷過詐欺、貪汙或其他經濟犯罪（全球平均為 46%）。
      - 詐欺者有 40%是外部詐欺，31%為內部詐欺，26%內外勾結詐欺，而外部詐欺的第一名是駭客，其次是客戶被詐騙。
      - 經歷詐欺的組織中，約 40%經歷與數位平台相關之詐欺。
   (2) 詐欺案例和故事，不斷的出現在澳洲媒體，例如:NAB 前執行長的重要幕僚，透過其好友的活動管理公司，共同詐騙 NAB，損失約 9 百萬美元。另一個案例則是一對低收入的夫妻，因為身分被盜，在旅遊期間透過其 7 張信用卡被盜刷損失約 37 萬美元等案例。
   (3) 就統計資訊來看，銀行只有支付實際詐騙損失 2%，不論政府或社會大眾的期待，銀行在防止詐騙中應扮演更積極角色。

(4) 依照澳洲競爭及消費者委員會(ACCC)統計，2022 年詐騙損失達 31 億澳幣，較前一年成長 79%，主要來自投資有關的詐騙約 15 億澳幣。

(5) 澳洲政府和金融機構正在聯合採取行動，透過財政支持和積極措施打擊網路詐騙並保護澳洲公民。例如：澳洲銀行業推出詐欺報告交換 (FRX) 平台，可迅速採取行動阻止資金轉移給詐欺者。

2. 數位時代打擊詐欺風險的好作法

(1) 從 PwC 的全球經濟犯罪和防範調查中，32%組織沒有專門的資源，63%沒有正式風險評估，26%沒有紀律性的回應，這也顯示儘管威脅等級有所提高，但澳洲組織可能沒有做好充分準備來預防、發現和應對詐欺事件。

(2) 詐欺行為越來越複雜，詐欺者日益精練，組織缺乏資源、培訓和工具來跟上數位環境中快速發展的詐欺活動。內部稽核可以於年度稽核計劃思考以下面向：

- 是否進行詐欺風險評估？詐欺控制有效嗎？
- 是否建立了嚴格的身份驗證和認證流程？
- 治理和監控是否補充了現有的詐欺控制措施？
- 目前是否採取了預防措施，例如：自動阻止高風險詐騙活動？
- 員工和客戶是否了解詐欺威脅並接受過有關詐欺威脅的教育？
- 是否對第三方進行了適當的盡職調查？
- 是否實施了統一的詐欺偵測工具集，即詐欺分析？
- 是否有針對詐欺的升級、分類和回應的適當流程？

3. 內部稽核的角色

(1) 內部稽核可以運用其第三道的定位和經驗，透過以下面向於詐欺風險發揮稽核價值：

- 對組織提供支持和挑戰。
- 協調組織不同部門之間的投入。
- 評估宏觀經濟環境對組織特定領域之壓力。
- 針對詐欺風險的來源進行確信。
- 支持組織調查方法並對事件報告提供有效的回應。
- 支持使用科技作為打擊詐欺的工具。

(2) 內部稽核的最佳實踐：

- 提供敏捷的確信和洞察力
- 扮演重要角色，要求董事會和執行管理階層在最重要的領域建立韌

性。

- 與二線協作，建立透明的風險和確信的架構，確保根因、洞察和文化等共享，各自扮演好自己的角色。
- 了解科技和自動化的新趨勢，於組織運用技術發展業務機會時，適時提供建議及確認，並更廣泛管理風險。
- 幫助企業領導者應對日益的需求、審查及公布的資訊等所帶來的機會和挑戰，例如：ESG、風險管理、員工福祉等。

（七）參訪 KPMG Sydney Office

2023.11.09

- 參訪機構：KPMG Sydney Office
- 研討主題：網路觀察見解 (Cyber Insights)

一、內容概要

1. 資安議題責任層級應提升到董事會
2. 預擬網路事件發生之因應對策
3. 對 KPMG 提問與回答

二、內容說明

1. 資安議題責任層級應提升到董事會

本次課程 KPMG 分享資安議題(Cyber Insights)，特別強調董事會(Boards)及執行長(Executive)的職責及應有之監督作為，可謂見資安重要性。由於網路安全威脅日益廣泛，影響金融機構運作及民眾權益亦日益嚴重，如處理不當，將有可能傷筋動骨影響金融機構營運，不可不慎，如公私部門個資外洩、勒索病毒肆虐及引發關注的銀行遭駭事件。

董事會及執行長對資安議題的行動方案，包含 Raise Cyber awareness(提高網路意識) 、Challenge management(挑戰管理階層)、Ensure sufficient time at board(確保董事會有足夠時間)、Enable management(授權管理層)、Enable continuous enhancement(持續精進)；此一做法，將資安議題責任層級拉高到董事會，因董事會有權對資源分配及管理授權做最佳安排，爰對資安議題監督、防範及落實將顯有助益。

除了關注銀行內部之網路安全外，尚須注意供應鏈風險，因為數位化程度愈高、銀行愈無法自行完成所有資訊作業，代表越來越高的資訊供應商風險。

2.預擬網路事件發生之因應對策

預擬網路事件發生之應對：在網路事件發生時，必須預擬因應對策，包含事件最高領導者指派、組織回應團隊、營運不中斷計畫審視與運作、與第三方供應商如何合作、對主管機關通報義務、如何做正確的決定、網路保險覆蓋及其缺口、如何處理贖金要求等。

在網路世代下須審慎的正視網路風險管理以強化營運韌性、監管合規要求、持續有效的控制措施，於此目標下有下列持續性工作需到位:

- 管理職能必須三道防線均到位，不能只依賴內部稽核
- 系統性測試驗證有其必要性
- 內部稽核必須獨立審查控制措施
- 第三方或第四方必須考慮

透過主管機關要求資訊長(Chief Information Officer, CIO)之設置及要求董事會對資訊安全的積極參與，可強化銀行對資安之重視並提高銀行營運韌性。

讓組織從上而下形塑一致的文化(Culture)與心態(Mindset)，是建構組織韌性的關鍵要素，「網路安全與資訊安全人人有責」意識的建立，可推進組織資安文化及網路風險管理文化之形成，而有效且持續不斷的教育訓練，則是讓組織的網路風險管理能力能與時俱進的加速器，在評核設計與控制有效性時，併同考量教育訓練有效性，以及是否訓為所用、因材施教，亦是應加以落實之評核的工作。

3. 對 KPMG 提問與回答

【提問 1】開放銀行面臨兩大威脅，一是金融欺詐，二是未經同意使用 PII（個人識別資訊）。除了 ISO 27001 規範之外，是否有任何方法或監管政策來審查我們的銀行安全架構以強化所有威脅？

【答】：對於任何業務風險或威脅，企業如何透過適當的控制進行回應都有一系列的複雜性。

☑0 級 - 量身訂作或臨時的控制措施。

☑ 1 級- 底線：安全產業控制架構（例如 ISO 27001 和 2013 年美國國家標準技術研究院(NIST)根據現有的標準與網路安全架構指南）可視為基本安全控制，應對其有效性（通過/失敗或成熟度）進行質疑。

☑ 2 級：更高階的業務安全框架由治理、風險和合規框架支持，其中包括對關鍵業務功能和資訊資產的網路威脅評估以及這些安全控制。依賴質化風險評估，常常設計情境，以期與策略風險框架一致。

☑ 3 級：透過蒐集可能性和威脅、實際業務成本和模擬損失模型的將資安風險量化。

(1)基於歷史資料建模的特定網路控制的攻擊鏈和威脅場景攻擊路徑的攻擊步驟和防禦有效性的可能性分析。

(2)根據專門評估的間接和直接成本，報告網路風險以及預期的財務價值損失。

(3)確定降低網路風險的主要能力。

【提問 2】能否分享一下澳洲透過內部稽核部門的具體策略或行動計畫，成功加強或提升內部稽核在網路安全風險管理中的價值的最佳的實例？上述實例的內部稽核人員是如何達成的？

【答】持續改進，同時維護控制措施有效性的監控。

- 跨越第一道防線、第二道防線、第三道防線的整合測試框架
- 對控制措施保有自動且持續的監控
- 使用者行為分析 - 先進或領先的控制實務
- 數據分析
- 展望未來 - 透過使用 AI 改變 IA

【提問 3】客戶、三道防線、股東，不同主體可能各有不同的觀點，如何確保各利害關係人之間相互協作，高效增強網路安全韌性？能否分享澳洲的實務？

【答】維持下列各方的連繫

- 企業、監管機構、政府、論壇/參與、高級金融管理師、政府網路委員會之間的合作夥伴關係

- 澳洲政府 2023-2030 年澳洲網路安全戰略將納入核心政策領域
  (1) 加強和協調監管框架：考慮制定新的網路安全法案，將產業和政府的特定網路立法義務和標準結合起來；考慮是否有必要進一步製定 SOCI 法案，例如，將客戶資料和「系統」納入關鍵資產的定義中 。
  (2) 加強澳洲的國際網路安全戰略：以澳洲國際網路和關鍵技術參與策略為基礎，加強國際網路領導力；專注於提高整個地區的網路彈性。
  (3) 確保政府系統安全：在最佳實踐標準、評估、透明度、報告和一致激勵措施的推動下，制定政府可遵循的框架；加強跨部門和機構的支持、問責和領導機制。

- 澳洲政府 2030 年可能採取行動的領域：
  (1)改善網路威脅共享和攔截的公私機制：透過公私夥伴關係加強網路安全威脅共享和攔截；審議與資訊共享、取得、情報解密和現有監管框架有關的問題。
  (2)支持澳洲的網路安全勞動力和技能管道：考慮需要採取哪些步驟來建立澳洲的網路勞動力以及該戰略如何支持此類機制。
  (3)應對重大網路事件的國家框架：制定重大網路事件後的事件管理和協調、事件後審查和後果管理框架；分享經驗教訓，幫助組織做更好的準備。
  (4)社區意識和受害者支持：考慮採取舉措，支持進一步投資於網路安全的社區意識和技能建設，包括中小企業。
  (5)投資網路安全生態系統：探索澳洲如何創造一個吸引網路安全和其他關鍵技術投資的環境，以建立國家能力。
  (6)設計和維持新技術的安全性：如何為可能影響網路安全的新興技術（如量子和人工智慧/機器學習）制定面向未來的策略。

【提問 4】澳洲金融機構提供的開放銀行服務是否有對消費者權益產生不利影響的案例？您建議的稽核重點是什麼？

【答】澳洲發生了多起涉及 PII（個人識別資訊）和財務資訊等眾所囑目(備受關注)的安全事件，導致違反隱私法規。隨著對稽核和改善方案以及稽核計劃的重新審視，內部稽核受到越來越多的關注。

- 積極主動的資訊安全計畫需要具有前瞻性和挑戰性的管理，以不斷改進當前的控制；成熟度評估、操作有效性之控制測試、違規回應計畫和測試、第三方和第四方風險管理、網路和營運韌性。
- 發生網路安全事件並非不可能，您的組織如何因應才是重點。

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 ESG、氣候風險管理、永續經營、資安、稽核數位轉型、以及詐欺風險管理等。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報告如下：

一、 台灣內部稽核實務在資安議題遇到的挑戰與瓶頸：

1. 資訊發展快速時代，雲端、AI 運用日益普及，對金融機構資訊安全形成挑戰，銀行業不斷提升數位化程度，面臨資安稽核人才不足，職能不易與時俱進，資訊人才市場需求高，稽核業務不易爭取到資訊人才。
2. 網路監控腳步落後，資安風險暴露。
3. 資安示警不易快速跟進網路安全威脅。
4. 地緣政治不穩定性及日新月異、不斷變化的網路威脅技術，讓網路韌性之建構，如沒有三道防線協力合作，建立機構本身的網路韌性，以及透過政府力量執行國家資通安全防護、演練與稽核業務及通訊傳播基礎設施防護，難竟全功。
5. 網路駭客無國界，銀行的產業屬性，成為全球網路犯罪及駭客攻擊的重要標的，讓有效預防、即時偵測，以及災難復原等機制，須不斷更新，並面臨挑戰。

二、 缺乏 Data，須儘速找到解決之道：

本次參訪之絕大部分機構，不約而同提及數據(Data)為最大問題與挑戰。確實，過去我國金融業者就氣候風險議題並未主動蒐集 Data，致無足夠資料以估計銀行所貸放、所投資之企業若發生氣候風險，銀行可能遭受之潛在損失(如：無法償還貸款、投資標的折價等)。然而資料蒐集除有賴時間累積，亦須具備辨識資料需求及明確定義之能力。即使試圖購買外部 Data，亦須先確定市面已有類似資料庫之管道；此外，如何驗證外購資料品質不

無疑慮。因此，儘早開始蒐集資料(Start Earlier)、取得資料，方能儘早突破瓶頸，創造優勢。

三、 提升數位投資，增進數據管理技術

瞭解並善用數據為風險控管及內部稽核之基礎，本次參訪之金融同業已導入數位技術、資料科學家及大數據分析工具，有效蒐集、管理和分析 ESG 相關數據。國際金融同業數位發展歷程及技術實踐足供我國借鏡，尤應增進數位投資、強調數據治理(Data Governance)並改善數據處理流程，以提高數據品質與可靠性。

四、 台灣主管機關的進程

氣候風險和詐欺風險是近年來台灣主管機關關注的重點，自 2023 年 6 月起銀行業也需要依 TCFD 進行相關揭露，主管機關也推出一版台版的氣候風險壓力測試，金管會檢查局張局長也在 2023 年 10 月份論壇中強調防制詐騙已是年度檢查重點，還會透過專案檢查加強查核，並特別分享一些金融機構在阻詐上需要提高警覺的樣態，希望透過公私協力合作，把防制詐騙工作做得更好。本次研修班更由金管會檢查局張局長親自帶團，展現台灣主管機關與國際接軌的決心。

五、 氣候風險和詐欺風險的議題，不僅僅是一個金融議題，也是全球各國需要一起面對的問題。金融業需要運用其於金融中介的影響力，協助個人和企業適應氣候變化及面對詐欺威脅，並成為國家和社會穩定的力量，讓個人和企業於持續前進的過程中考慮氣候變化的金融影響，避免詐欺所造成的損失。

六、 在衡量新興風險中最挑戰的仍然是資料和技術，需要有全面性的數據分析，方能評估組織所面對氣候變化之實體風險和轉型風險，並擬定氣候戰略目標，或是了解詐欺風險的主要來源，進一步運用技術並透過資訊分享，運用新技術打擊詐欺活動。

七、 各國監管機關針對氣候風險或詐欺風險等議題，陸續制訂監管政策或監管報告要求，以提升金融業的營運韌性。目前台灣主管機關針對氣候風險的揭露雖尚未有相關監管報告，但可預見不久將來亦將會有相關監管報告。對於有較多海外據點的銀行，因所處的國家不同，相關的監管規定亦有所不同，總行需與海外分行合作了解當地規定，並提供相應的支援，未來金融業於因應

新興風險之法規成本勢將與日俱增。

八、 未來需要主管機關對於氣候相關議題，及早與國際接軌制訂相關規定，並與各國主管機關和金融業合作，並進一步做到數據共享。在詐欺預防上，也須主管機關透過政府力量，促成金融業的合作改革及持續分享欺詐的手法，協助金融業不斷適應新威脅，通過共同努力和保持警惕，才可以增強我們對欺詐的防禦，從而保護我們金融機構以及客戶對金融機構的信賴。

九、 內部稽核也需要持續保持學習，將氣候風險和詐欺風險納入稽核計畫中，針對氣候風險之數據資料、信用風險評估方法論及計算進行確信，了解業務單位氣候風險戰略目標及於因應氣候風險所採取的相關因應措施，針對詐欺風險之評估控制程序、確認身分驗證及認證流程、自動阻詐偵測機制、第三方的盡職調查及詐欺風險分析等進行確信，確保銀行動態因應持續演進發展中的永續議題及新興風險，保持銀行競爭力。