

出國報告(出國類別：國際會議)

參加 2025 年國際內部稽核協會國際研討會 暨訪問加拿大審計組織出國報告



服務機關：審計部

姓名職稱：張簡任審計兼組長甘霖、陳審計珮禎

派赴國家：加拿大

出國期間：114 年 7 月 12 至 20 日

報告日期：114 年 10 月 7 日

摘要

2025 年國際內部稽核協會(The Institute of Internal Auditors, IIA)國際研討會(International Conference)於 114 年 7 月 14 日至 16 日假加拿大多倫多會議中心舉行，超過 2,600 位來自超過 120 個國家的稽核、風險管理與治理專業人士共同參與，會議主題為「擁抱改變、提升標準，以精進內部稽核專業」(Advancing Internal Audit as We Embrace Change and Elevate Standards)，聚焦探討在生成式人工智慧、永續發展、網路安全及法規更新快速演變的環境下，內部稽核如何調整角色定位，兼顧監督、顧問與價值創造功能，會議現場提供 63 種語言的即時翻譯。

審計部為實踐專業與創新等核心價值，持續薦送審計人員參與國內外專業組織、機構或先進國家舉辦之年會、研討會或研習，希及時掌握國際專業脈動，適時推動審計制度與技術方法革新，厚植審計人員專業培力，提升審計監督、洞察及前瞻功能，以遂行法定職掌並對人民福祉產生正面影響力。本次遴派簡任審計兼組長張甘霖、審計陳珮禎等 2 人參與本次會議並拜訪加拿大審計與課責基金會 (CAAF)，透過與國際內部稽核專業人士交流、彙整專題演講及個別研討會之精要，及蒐集各議題相關文獻資料與審計機關發展現況等，撰擬完成本出國報告，其中策進建議如下：

- 一、參考國際審計社群評估國家氣候行動作法，加強查核政府因應氣候變遷相關作為，並賡續關注 INTOSAI 環境審計工作小組 (WGEA) 專案成果，協助政府因應氣候變遷的挑戰。
- 二、賡續強化績效審計考核面向，加強推動公平性審計，並運用根本原因分析，瞭解根因於組織文化的缺失，針對問題癥結研提改善建議，協助促成政府良善治理。
- 三、賡續深化國際合作與人員培訓，以在 AI 時代與全球變局下，接軌國際審計專業趨勢，並確保審計人員與時俱進，具備未來所需關鍵能力。
- 四、參考國際研討會專家分享導入 AI 應用之經驗與建議，持續提升審計數位轉型能量。
- 五、參考國際之作法，以前瞻思維評估潛在風險，確保政府建置 AI 系統在設計、建置與營運過程中均符合法規、倫理與社會期待。
- 六、參考國際研討會資安場次重點，加強查核行政機關資安治理與韌性建設。

目錄

壹、前言	1
貳、參加研討會及訪問加拿大審計組織過程	2
參、專題研討	4
一、 下一個文藝復興 (The Next Renaissance)	4
二、 重新思考風險：內部稽核在面臨交叉威脅的世界中不斷演變的角色 (Risk, Reimagined: Internal Audit's Evolving Role in a World of Interconnected Threats)	7
三、 在前所未有的時代推動轉型變革 (Driving Transformative Change in Unprecedented Times)	11
四、 蛻變：查核從不可能到現實的轉型 (Metamorphosis: Auditing the Transformation of the Impossible into Reality)	14
五、 全球審計轉型：人工智慧、監管與內部稽核的未來 (Global Audit Transformation AI, Regulation, and the Future of Internal Audit)	17
六、 資安威脅新局勢 (The New Cyberthreat Landscape)	20
肆、同步場次	24
一、永續相關議題	24
(一)CEESG：以強大控制環境重新定義環境、社會與治理 (CS2-5 CEESG: Redefining ESG with a Strong Control Environment)	24
(二)最大化內部稽核對組織永續性的影響 (CS4-5 Maximizing Internal Audit's Impact on Organizational Sustainability)	28
二、道德審計相關議題	31
(一)內部稽核在強化組織文化中的角色 (C3-5 The Role of Internal Audit in Enhancing Organizational Culture)	31
(二)解鎖確信：將行為風險與整合性人與流程稽核 (IPPA) 及雄心模型 (Ambition Model) 整合 (C3-2 Unlocking Assurance: Integrating Behavioral risks with IPPA and the Ambition Model)	34
(三)舞弊與鑑識矩陣 (CS3-7 Fraud and the Forensic Matrix)	37
(四)舞弊調查：如何執行 (CS5-2 Fraud Investigations: A How to Guide)	39
三、未來稽核相關議題	41
(一)未來導向的內部稽核領導力：全球稽核長的觀點 (CS5-7 Future Proofing Internal Audit Leadership: Perspectives of Global Chief Audit Executives)	41

(二)引領未來：新世代稽核人才的吸引與留任策略 (CS5-1 Engaging Tomorrow: Strategies For Attracting and Retaining The Next-Gen Auditors)	44
四、能力建置相關議題	47
激發潛力及邁向卓越：新版內部稽核職能框架 (CS1-1 Unlocking Potential and Elevating Excellence: A New Competency Framework to Promote Achievement)	47
五、人工智慧、資訊安全之議題	50
(一)提升公部門內部稽核－主計長觀點 (CS1-6 Advancing Internal Audit in the Public Sector-Perspectives from Comptroller Generals)	50
(二)次世代稽核人員：在人工智慧浪潮中生存 (CS1-8 NxtGenAuditor: Surviving the AI Impact)	52
(三)超越效率：稽核自動化的策略力量 (CS2-1 Beyond Efficiency: The Strategic Power of Audit Automation)	54
(四)法律框架中之人工智慧：平衡創新、倫理與全球合規 (C2-4 AI in the Legal landscape: Balancing Innovation, Ethics, and Global Compliance)	56
(五)生成式 AI 時代下的網路安全治理 (C3-1 Cybersecurity Governance in a Gen AI Era: 30 Questions the Board and Audit Committee Should Ask)	59
(六)AI 與 IA：如何有效應對同一體兩面的挑戰 (C4-1 AI and IA: How to Effectively Address Both Sides of One Coin)	61
(七)透過代理式 AI 強化內部稽核的未來準備 (C4-4 Future-Proofing Internal Audit With Agentic AI Solutions)	65
(八)AI 與內部稽核：創新來自更智能之文件互動 (C5-5 AI Meets Internal Audit: Innovating Through Smarter Document Interaction)	67
(九)駭入人性：超越科技的社交工程策略 (C5-8 Hacking the Human: Social engineering Tactics That Outwit Technology)	69
伍、參訪加拿大審計與課責基金會紀要	71
一、簡介	71
二、參訪過程及討論議題	71
(一)國際合作	72
(二)績效審計	73
(三)永續發展目標審計	77
(四)組織文化審計	79

(五)性別、權益、多元性與包容性審計（Gender Equity, Diversity, and Inclusion, GEDI）	80
(六)AI 與科技在審計中的應用	81
(七)培訓課程與方法	82
陸、研習心得與建議意見	83
一、參考國際審計社群評估國家氣候行動作法，加強查核政府因應氣候變遷相關作為，並賡續關注 INTOSAI 環境審計工作小組（WGEA）專案成果，協助政府因應氣候變遷的挑戰	83
二、賡續強化績效審計考核面向，加強推動公平性審計，並運用根本原因分析，瞭解根因於組織文化的缺失，針對問題癥結研提改善建議，協助促成政府良善治理	87
三、賡續深化國際合作與人員培訓，以在 AI 時代與全球變局下，接軌國際審計專業趨勢，並確保審計人員與時俱進，具備未來所需關鍵能力	89
四、參考國際研討會專家分享導入 AI 應用之經驗與建議，持續提升審計數位轉型能量	91
五、參考國際之作法，以前瞻思維評估潛在風險，確保政府建置 AI 系統在設計、建置與營運過程中均符合法規、倫理與社會期待	93
六、參考國際研討會資安場次重點，加強查核行政機關資安治理與韌性建設	94
附錄 1 會議議程	96
附錄 2 董事會與稽核委員會應檢視的 30 個關鍵提問	102
附錄 3 公部門組織文化審計（Auditing Organizational Culture in the Public Sector）	103

壹、前言

2025 年國際內部稽核協會(The Institute of Internal Auditors, IIA)國際研討會(International Conference)於 114 年 7 月 14 日至 16 日假加拿大多倫多會議中心(Metro Toronto Convention Centre, 圖 1)舉行，超過 2,600 位來自超過 120 個國家的稽核、風險管理與治理專業人士共

同參與，會議主題為「擁抱改變、提升標準，以精進內部稽核專業」

(Advancing Internal Audit as We Embrace Change and Elevate Standards)，聚焦探討在生成式人工智慧、永續

發展、網路安全及法規更新快速演變的環境下，內部稽核如何調整角色定位，兼顧監督、顧問與價值創造功能，會議現場提供 63 種語言的即時翻譯。

圖 1 多倫多會議中心



資料來源：多倫多會議中心網站。

加拿大審計與課責基金會(Canadian Audit and Accountability Foundation, CAAF, 圖 2)位於加拿大首都渥太華(Ottawa)，為非營利專業機構，致力於促進並強化加拿大及國際間公共部門的審計、監督與課責機制，主要透過研究、教育與知識分享推動公共治理品質的提升。

審計部近年來強化審計監督、洞

察及前瞻功能，為業務發展需要及掌握國際稽核實務發展脈動，推動審計制度與技術方法革新，厚植審計人員專業培力，以遂行法定職掌並對人民生活福祉產生正面影響力，爰遴派簡任審計兼組長張甘霖、審計陳珮禎等 2 人參與本次會議並拜訪 CAAF。

圖 2 CAAF 辦公室

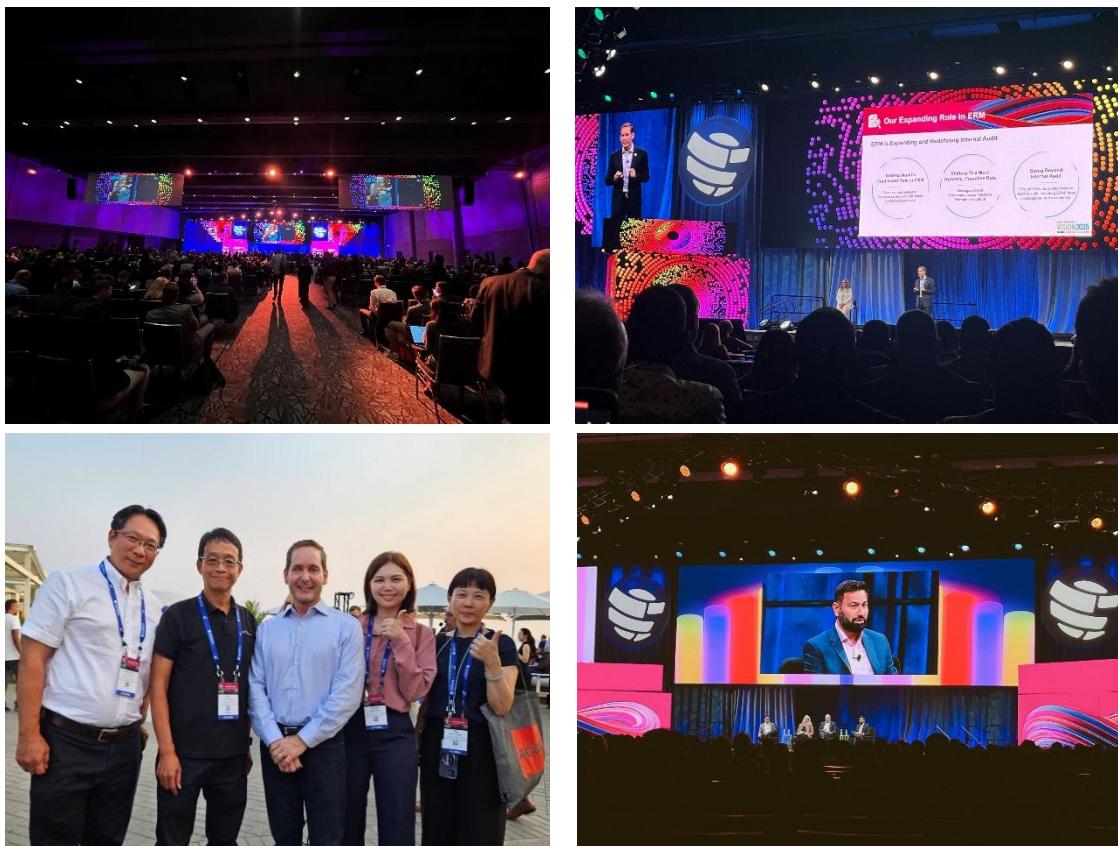


資料來源：自行拍攝。

貳、參加研討會及訪問加拿大審計組織過程

本次研討會於 114 年 7 月 14 日開幕，上午有 2 場專題研討，分別由前 OpenAI 市場推廣負責人 Zack Kass 分享「下一個文藝復興」、IIA 2024 至 2025 年理事會主席 Theresa Grafenstine 女士及 IIA 總裁與執行長 Anthony Pugliese 先生主講「重新思考風險：內部稽核在面臨交叉威脅的世界中不斷演變的角色」，解析當前全球風險交織情勢下內部稽核角色的轉型，並說明 IIA 新戰略藍圖，強調專業標準與能力架構的再定義；下午為 1 場次同步研討會，主題涵蓋能力框架、企業治理、系統實施、網路安全、公部門內部稽核與 AI 影響等面向，當日最後一場專題研討由前 Ingka/IKEA 首席永續長 Pia Heidenmark Cook 女士主講氣候變遷議題「在前所未有的時代推動轉型變革」。晚間，大會於多倫多安大略湖畔著名的 Rebel Nightclub 舉辦文化交流晚宴及聯誼活動，與會者於此欣賞音樂與多媒體表演，並與各國內部稽核專業人士交流，體驗加拿大當地文化與多元藝術氛圍，為首日研討活動畫下熱鬧且具文化意象的句點。(圖 3)

圖 3 會場花絮

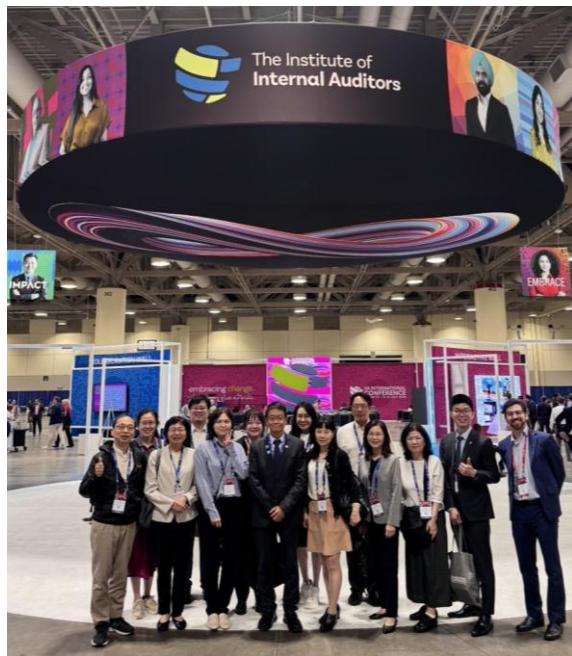


資料來源：自行拍攝。

研討會第二天由前 GE 西班牙與葡萄牙總裁 Isabel Aguilera 主講「蛻變：查核從不可能到現實的轉型」，強調全球趨勢加速風險變化，稽核應以前瞻性視角引領組織轉型，隨後共 2 場次同步論壇，聚焦於稽核自動化、AI 與法遵、聲譽風險及 ESG 等核心議題，壓軸場為論壇形式，由 Justin Greenberger 擔任主持人，與談人為 Bupa 公司內部稽核部門分析主管 Sachin Kapoor、Davy 公司內部稽核主管 Chris Cowley、Constellium 公司內部稽核副總裁 Karen Albert，就「全球審計轉型：人工智慧、監管與內部稽核的未來」議題分享觀點。另本次研討會國內參與人員包括中華民國內部稽核協會、臺灣集中保管結算所、財金資訊股份有限公司、臺灣證交易所、長榮航空公司、中華民國證券櫃檯買賣中心、臺灣期貨交易所、中華電信股份有限公司、台灣中油股份有限公司、台灣電力公司、中國信託金控及審計部等 12 個機關團體、13 名會員代表與會(圖 4)。研討會最後一日，先是 2 場次同步論壇，聚焦於內部稽核的角色與變革、AI 運用、稽核專業人才、舞弊等核心議題。壓軸閉幕會議，由前美國國家安全局(NSA)高階主管，現任摩根士丹利財富管理部門的資安總監 Rachel Wilson 主講「資安威脅新局勢」，聚焦新興資安威脅與企業韌性，提醒審計人員在高度數位化環境下需結合資安治理與風險管理思維，為本屆研討會劃下圓滿句點（會議議程整理如附錄 1，主要場次摘要於參、專題研討及肆、同步場次）。

結束為期三日的研討會日程後，另前往加拿大首都渥太華拜訪加拿大審計與課責基金會，由該基金會專業發展部門副總裁 Sharon Clark 女士、國際發展計畫副總裁 Caroline Jorgensen 女士負責接待，參訪前經擬具四大面向、14 項討論問題送 CAAF 參考，其中部分問題並由受訪者轉洽加拿大審計長公署（OAG）相關人員提供意見。

圖 4 我國與會人員合影



資料來源：自行拍攝。

參、專題研討

一、下一個文藝復興（The Next Renaissance）

本場專題研討由未來學家、全球 AI 顧問、前 OpenAI 市場推廣負責人 Zack Kass 先生（圖 5）主講，主要探討人工智慧（AI）技術的發展與其普及性、AI 對人類社會的多元影響與挑戰，以及因應 AI 時代如何準備等核心議題。

（一）AI 技術的發展與其普及性

AI 技術從過往的統計機器學習模型，演進至現今以神經網路為基礎的 Transformer 架構，此突破性進展促使 AI 能力自 2017 年以來呈現爆炸性成長，甚至達優於人類智力的水準。過去 AI 應用尚可以視覺化呈現，但伴隨 AI 能處理文字生成文字、圖像、影片、語音，乃至於 2024 年 6 月在數學奧林匹亞競賽中擊敗人類的複雜任務，顯見單純的視覺展示已不足以全面描繪 AI 可達成的能力程度。

AI 能力正以每 7 個月翻倍的速度快速發展，遠超摩爾定律¹的預測，顯示其在簡化複雜任務上的強大潛力，並已進入模型自我學習的遞迴²循環階段。更關鍵的是，儘管 AI 訓

練成本可能較高，但其運行（推理）成本正經歷前所未有的急速下降，未來將進入「無限制智慧

（Unmetered

圖 5 未來學家 Zack Kass 先生



資料來源：IIA 網站。

圖 6 未來將進入無限制智慧的時代



資料來源：2025 年 IIA 國際研討會。

¹ 摩爾定律指出，機器每 4 年成本降低一半，速度提高 1 倍。

² 遞迴，又譯為遞歸，在數學與電腦科學中，是指在函數的定義中使用函數自身的方法。另遞迴一詞常用於描述以自相似方法重複事物的過程。

intelligence」³的時代（圖 6），且如同歷史上關鍵資源（如水、電力及網際網路等）由稀缺轉為普及且經濟實惠的發展歷程，AI 的發展將帶來顯著的經濟效益。這項趨勢也顯示未來 AI 將更有效率，模型將逐步商品化，且技術更為普及，進而使更多人能夠使用 AI。

（二）AI 對人類社會的多元影響與挑戰

講者描繪 AI 融入生活的「增強型應用」、「自主代理」及「自然語言作業系統」等 3 個階段（圖 7），並指出機器將由協助轉為主動執行任務，最終並由攜帶式裝備（手機、筆記型電腦）轉變為穿戴式裝備，並由需要學習機器如何工作，轉變為機器知道我們如何工作，澈底革新人機互動與網路基礎結構，並對社會與個人體驗產生深遠的影響。然而，AI 的普及也伴隨多重社會挑戰，講者提出「低智商理論」，警世部分人口可能因缺乏批判性思考而智力退化，尤其於 Z 世代中正發生一種奇怪的模式，其似乎是第一個有許多人沒有比上一代更聰明的世代，然而，此世代的天才人均數量似乎增加近一個標準差，因處於 AI 時代，智商對成功與否的影響正在減少，而個人內在的動機才是決定成功的關鍵因素，因此，Z 世代透過自學就有機會達到專業的程度。講者觀察到此世代的人，有些具備學者般的特質，20 歲以下的大師與超級大師比 40 歲以上的人更多，Palantir（美國知名軟體分析公司）更已

圖 7 人工智慧革命的整合階段



資料來源：2025 年 IIA 國際研討會。

³ 無限制智慧（Unmetered intelligence）為一種人工智慧的典範模式，其以持續可用且無限可擴展的公用事業形式提供服務。如同電力或網路等基礎設施，無限制智慧無處不在，不受單次使用限制或分段供應制約，其使人工智慧能直接嵌入系統、環境與流程，往往催化產業與組織的轉型。此框架有別於傳統受限或孤立的人工智慧部署模式，而將智能整合於整個基礎建設中。

取消對所有新員工的本科學歷要求。又講者提出「去人性化理論」，擔憂虛擬世界導致成癮與孤立，故強調回歸實體社區的重要性。此外，AI 賦予「低資源惡意行為者」更大危害潛力，如金融犯罪，促使政策制定者須加強監管。更關鍵的是，AI 帶來的不是單純的失業，而是「工作身分認同危機」，因頻繁變革將衝擊個人目的感，個人須由工作中找到目的與身分認同（如歸屬感）。

儘管 AI 普及帶來多重社會挑戰，但其能拓展人類潛能，顯著提升生產力，加速科學突破（如生命科學領域的癌症治療、HIV 研究），並使商品與服務成本下降，優質生活資源普及，惟此情況亦可能導致大規模通貨緊縮效應。又 AI 將釋放人類更多自由時間，鼓勵個人探索工作之外的生命意義，重建親友與社群連結。

（三）因應 AI 時代如何準備

講者強調，面對 AI 時代，首先，須將「適應性」與「終身學習」作為核心策略，學習「如何學習」將成為關鍵技能，培養對知識的狂熱追求遠比專注於特定學科更重要，因 AI 將使許多專業知識快速商品化，但學習能力卻不會。其次，應著重發展 AI 無法取代的「人性化特質」，儘管 AI 將大量自動化重複性工作，但人類的適應力、好奇心、勇氣、同理心、智慧與幽默等特質將更顯珍貴，疫情期間的遠距實驗證明，實體人際互動仍具不可取代性，AI 將促使人類重新探索何謂「人性」，並更關注互動品質甚於知識層面。

最後，講者提及其觀察到 AI 趨勢對稽核工作的重要影響，首先，稽核助理過去所做的繁重工作，已有自動化的變革，再者，未來需要審計的數量將呈寒武紀式的大爆發，雖然 AI 工具可自動化稽核的基本工作，但全球化與複雜性增加將導致稽核需求激增，並使稽核人員由執行者轉變為提供治理洞察意見的策略顧問。此外，稽核專業職涯的線性發展可能因 AI 而改變，未來將有越來越多的年輕人跳過學徒期成為高級稽核員。而在如何敦促組織與監管機關採納 AI 方面，講者認為真正的問題在於不使用 AI 的網路安全威脅，因不使用攻擊者正在使用的工具，就會造成巨大的不對稱，因此，要竭力向政府強調將 AI 視為打擊不良行為的工具，而非助長不良行為的工具。

二、重新思考風險：內部稽核在面臨交叉威脅的世界中不斷演變的角色（Risk, Reimagined: Internal Audit's Evolving Role in a World of Interconnected Threats）

本場專題研討
由 IIA 2024 至 2025
年理事會主席
Theresa Grafenstine 女士（圖 8）及 IIA 總裁與執行長 Anthony Pugliese 先生（圖 9）主講，主要探討風險

圖 8 IIA 2024 至 2025 年
理事會主席 Theresa
Grafenstine 女士



資料來源：IIA 網站。

圖 9 IIA 總裁與執行
長 Anthony
Pugliese 先生



資料來源：IIA 網站。

樣貌的轉變、內部稽核於企業風險管理（ERM）中擴展的角色、科技於內部稽核與 ERM 中的角色，以及趨動內部稽核的未來發展等核心議題。講者指出，當前風險環境的變化雖然帶來挑戰，但也為稽核專業提供展現其價值的重要機會。

（一）風險樣貌的轉變

當前的風險樣貌已發生巨大轉變，安永（EY）的一項調查指出，董事會、高階主管及審計委員會主席最憂心的風險包括人才、組織聲譽、地緣政治緊張、法規變動及數位變革等，世界級董事會定到不可預測，組織正應對複雜且相互連結的威脅。

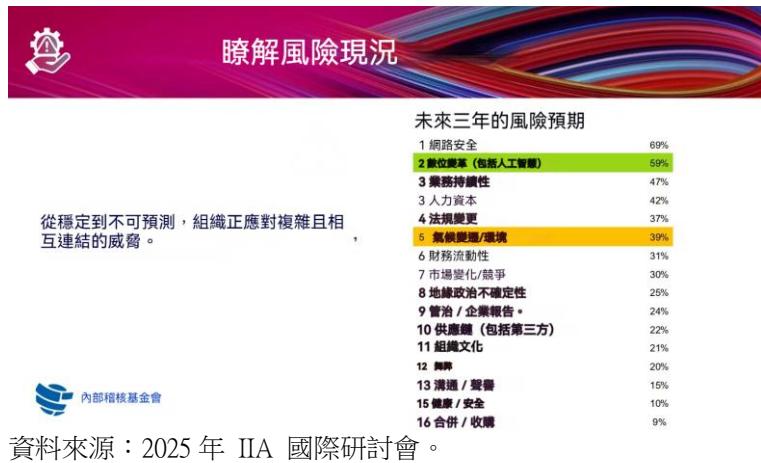
圖 10 風險聚焦報告列示年度風險



資料來源：2025 年 IIA 國際研討會。

事會及具有前瞻性的高階主管團隊會將 ERM 融入到營運的各個層面。前揭風險與 IIA 風險聚焦調查之結果雷同，依據 IIA 2025 年風險聚焦報告（Risk in Focus 2025），網路安全持續被視為首要風險（圖 10），而數位變革（包含 AI）的風險預期在未來三年將大幅攀升 20 個百分點（圖 11），現今的風險樣貌已不再是線性、孤立且緩慢移動的風險（如遵循、財務控制及營運風險），而是演變為快速、流動且緊密交叉的複雜威脅（如

圖 11 風險聚焦報告列示未來 3 年風險



資料來源：2025 年 IIA 國際研討會。

網路安全、組織聲譽、AI 與自動化、環境、社會與治理及道德規範、地緣政治動盪、第三方風險、企業文化）。

又世界經濟論壇 2025 年全球風險報告（The Global Risks Report 2025）揭示，不實資訊與 AI 的負面影響等新興全球風險也日益突顯，這些外部威脅不僅影響政府，也同樣衝擊各產業與組織。講者強調，虛假資訊類的風險主要是源於信任度下降所造成的影響，其以冰山為喻指出，許多風險隱藏在水面下，其相互關聯性會產生一階、二階甚至三階的連鎖效應，稽核人員必須理解風險匯集的結果，而非孤立看待，如須理解協力廠商風險與網路風險可能如何結合，目前網路威脅最盛行的方式之一即為網路威脅行為者將惡意軟體注入公司信任的供應商，進而要脅公司達成其要求。在全球對制度信任度普遍下降的趨勢下，內部稽核可藉由提供獨立確信（assurance）減少信任落差，此為稽核專業的機會，也是存在的意義。

(二)內部稽核於 ERM 中擴展的角色

為因應劇變的風險環境，內部稽核的角色正由傳統的觀察者與評估者，轉變為更具動態性、主動性的策略夥伴，亦即「策略副駕駛」(Strategic Co-Pilot)，其要將稽核工作對焦組織策略，即時提供洞察性意見，並提供持續性確信與前瞻性建議，由被動監督轉向主動協作，並將稽核融入決策與價值創造過程。此外，稽核人員的職責是辨識風險，而非管理或承擔風險，稽核人員需要提供審計委員會、董事會及其他利害關係人有關風險的獨立性洞見。數據顯示，已有 33% 的稽核長 (CAE) 同時負責 ERM 職能，相較於 10 年前的個位數，此為驚人的轉變。這種角色的擴展，主要是為應對如疫情後供應鏈網路攻擊激增 300%，或氣候變遷導致業務中斷等複雜風險。而此趨勢也使傳統的「三道防線模型」界線變得模糊，促使 IIA 成立新的委員會研究此現象，並為稽核人員提供支援。另講者特別以歷史為鑑指出，IIA 在 1960 年代曾忽視 IT 的重要性，其後促成 ISACA (國際電腦稽核協會) 的成立，而為避免重蹈覆轍，IIA 如今須正視並引領稽核與 ERM 職能融合的趨勢。最後，講者強調稽核人員要對 ERM 框架的發展提供建議，並運用對風險的洞見擬訂查核計畫，以及於維持獨立性之前提下，透過促進風險討論與教育增加內部稽核人員的價值。

(三)科技於內部稽核與 ERM 中的角色

依據 IIA 「內部稽核：2035 願景報告」(Internal Audit: Vision 2035) 的調查結果，83% 的受訪者認為虛假資訊與錯誤資訊將成為未來全球首要風險，講者以歐洲一家生物科技公司的產品因網路謠言而遭抵制的實際案例，說明不實資訊的破壞力；另 78% 的受訪者同意存在組織過度依賴新技術而減少人為參與的風險。針對生成式 AI，講者引用 IT 技術智庫 Gartner 的「炒作週期」(hype cycle)，說明 AI 正從期望值的頂峰，走向更為務實的「幻滅低谷」(trough)

of disillusionment)，面對此一趨勢，內部稽核的角色至關重要，稽核部門不能成為阻礙創新的「否決辦公室」(office of no)，因為在競爭對手擁抱新技術時，「不採取行動」本身就是一種巨大的風險。

鑑於目前仍有高達 86%的企業尚未試行運用 AI，此為內部稽核提供龐大的機會，其可運用專業協助組織安全、有效地導入新技術。又講者強調 AI 治理為組織策略上的優先要務，並建議稽核人員探索 AI 治理框架（如 RSM 公司的 AI 治理框架），並強調稽核人員不必成為演算法專家，只需要瞭解好的治理樣貌，並運用熟稔風險及控制的專業知能，針對偏見、一致性、數據隱私等面向，向管理階層提出正確的問題，評估組織是否已建立適當的控制措施。同時，稽核人員也需關注全球不同的監管趨勢，例如歐盟嚴格的 AI 法案，以因應其對稽核標準與方法可能產生的影響。最後，講者強調內部稽核人員要擁抱科技，在創新與監督間取得平衡，並持續提升自身的科技素養，以因應科技驅動變革的時代。

(四) 趨動內部稽核的未來發展

高達 89%的專業人士與利害關係人均認為內部稽核專業將在未來迎來重大變革，為此，IIA 正積極採取行動，引領專業的未來發展。首先是與時俱進更新全球內部稽核專業實務架構 (IPPF) 與相關準則，並針對網路安全、第三方風險與組織行為等議題發布主題式要求，確保指引能應對當代風險；其次，IIA 已發布新的「內部稽核職能框架」，以定義稽核人員所需具備的技能，並為職涯發展提供指引；最後，為確保專業人才的永續發展，IIA 正透過全球學生會議、實習計畫、導師制度及新的「內部稽核學術聯盟」等方式，強化人才管道的建構。此外，IIA 持續更新其核心證照（如 CIA、CRMA），確保其內容隨不斷演變的風險環境調整，以支持專業人員的終身成長。

三、在前所未有的時代推動轉型變革（Driving Transformative Change in Unprecedented Times）

本場專題研討由氣候變遷議題的全球領袖人物、多家企業董事會成員、高級顧問、前 Ingka/IKEA 首席永續長 Pia Heidenmark Cook 女士（圖 12）主講，主要探討永續轉型的原因與必要性「為何（Why）」、永續轉型的內涵與行動「內涵（What）」及永續轉型的實踐方法與稽核角色「如何（How）」等核心議題。

圖 12 前 Ingka/IKEA 首席永續長 Pia Heidenmark Cook 女士



（一）永續轉型的原因與必要性（Why）

講者首先闡述，AI 及氣候變遷是影響我們生活的兩大趨勢，其中 AI 雖在資料運算、模型建構及精準農業方面為氣候變遷提供解決方案，但其數據中心的能源消耗亦帶來新的環境挑戰。又以當前日益惡化的全球情勢強調永續轉型的必要性，舉如當前刻正發生技術戰爭或經濟及政治戰爭，全球地緣政治形勢異常動盪，武裝衝突數量已達二戰以來新高（目前有 92 場武裝衝突），且全球民主化進程倒退，僅 12% 的人口生活在真正的民主國家，另在經濟層面上，儘管 AI 有望帶來豐裕與生產成本下降的願景，但當前生活成本卻顯著攀升，食物、能源、住房日益昂貴，導致如歐洲已有高達 20% 的勞動人口面臨「在職貧窮」的困境，且依據世界經濟論壇每年發布的風險報告，環境災難已不再是世界經濟論壇認為的 10 年遠景，而是在未來一兩年內，就會對經濟造成損害。此外，當前氣候變遷、生物多樣性喪失及水資源短缺等多重環境議題正產生一種複合式的「雞尾酒效應」，使全球正迅速逼近引爆點（tipping points），全球 99% 的人口生活在空氣污染超標的地區，洪水、熱浪、風暴日益頻繁與猛烈，例如在英國，曾經每 50 年發生一次的風暴現在每 5 年

發生一次。鑑此，永續發展及應對氣候變遷相當重要。

講者提醒，當前採取行動應對氣候變遷的成本約占全球 GDP 的 1 至 2%，而不作為的代價（如生產力下降、由於氣候變遷、洪水、高溫導致的供應鏈中斷等）則可能高達全球 GDP 的 10 至 20%，此情形凸顯傳統「地平線悲劇」（tragedy of horizons）思維的短視，須正視前瞻未來風險的重要性。

(二) 永續轉型的內涵與行動（What）

永續轉型的具體內涵涵蓋個人角色與企業行動兩個層面。講者指出，每個人都能在 4 個領域作出貢獻，分別是：作為公民（透過投票與社區參與）、所有者（檢視自己的退休金投資流向）、消費者（反思消費需求與選擇）以及員工（在工作崗位上推動改變）。正如珍・古德（Jane Goodall）的名言：「你的所作所為會帶來改變，而你必須決定你想帶來哪種改變。」在企業層面，永續轉型充滿各種專業術語與框架，但講者以 IKEA 的經驗為例，聚焦兩大關鍵行動領域：循環經濟（Circularity）與氣候行動（Climate Action）。循環經濟的核心是打破傳統「開採—製造—丟棄」的線性模式，轉向儘可能延長產品與材料的生命週期，IKEA 的做法是為每項產品建立包含永續性原則的計分卡，每款產品都根據這些原則進行評分，並積極探索二手市場、產品回收、再生材料利用等商業模式；而在氣候行動方面，企業需全面檢視從自身營運、供應鏈到最終產品的整個價值鏈，IKEA 的策略是不僅提升自身的能源使用效率或協助供應商轉用再生能源，更直接投資於風能與太陽能發電場，實際擁有並營運這些設施，以確保能源自主與安全。

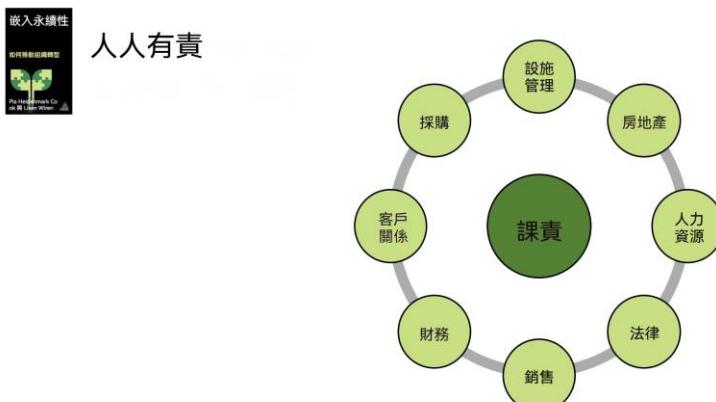
(三) 永續轉型的實踐方法與稽核角色（How）

領導力與稽核專業在企業系統性推動永續轉型的過程中，扮演著關鍵的角色。講者提出一個包含「四大支柱」（企圖心、當責與能力、主動性與敏捷性、倡議）與「七大步驟」（圖 13）的實踐框架，由理解外部環境到最終的

溝通與倡議，為企業提供清晰的行動藍圖。又永續轉型並非單一部門的責任，而是需要融入所有業務功能中，如採購部門對供應

鏈的影響至關重要。然而，僅有流程與制度是不夠的，更需要「領導力」來驅動變革，領導者須提供清晰的願景，並親身實踐，與團隊溝通永續目標的重要性，將個人的永續關懷連結至工作職責（圖 14）。在此過程中，內部稽核人員扮演著不可或缺的角色，其擅長風險盤點、盡職調查及流程理解，尤其是在執行「重大性議題矩陣（Materiality Matrix）」評估時，能協助企業聚焦於真正有影響力的議題。講者強調，稽核人員的任務是「勇於提出那些沒人敢問的困難問題」，以確保公司走在正確的道路上，協助企業長遠發展。

圖 13 實踐永續轉型的 7 大步驟



資料來源：2025 年 IIA 國際研討會。

圖 14 領導者心態



資料來源：2025 年 IIA 國際研討會。

四、蛻變：查核從不可能到現實的轉型(Metamorphosis: Auditing the Transformation of the Impossible into Reality)

由曾任 GE 西班牙與葡萄牙總裁、Google 伊比利半島區董事總經理、NH Hotels 營運長，以及 Dell 電腦西班牙、義大利與葡萄牙區執行長 Isabel Aguilera，分享稽核需進行「蛻變」，擇要分述如次：

(一) 觀點 1：稽核角色將延續，但必須發展出類投資者特質

在快速科技發展與自動化浪潮下，雖然大量工作將被改變甚至取代，但稽核功能不會消失，反而會變得更加重要。原因在於，隨著企業不斷擴張並衍生新風險，社會各界更需要稽核提供獨立與專業的保證。未來的稽核不僅要檢驗合規，還要審視資料完整性、演算法偏誤及治理架構，同時將 ESG、非財務資訊、舞弊與倫理納入範疇，稽核的責任因此更加廣泛而深刻。這也意味著稽核人員需具備跨領域能力，能像投資人般理解價值創造，像風險專家與心理學家般洞察人性，並結合創新思維與數據分析能力，成為能與管理階層對話的策略顧問。科技雖然改變了工作的型態，但同時也讓稽核得以從事過去難以涉入的領域，轉型成真正能為企業增值的功能。因此，稽核的角色將不僅持續存在，還會隨著時代需求而不斷提升重要性，成為組織信任、治理與永續發展不可或缺的核心支柱。

(二) 觀點 2：商業與技術固然重要，但培養人文素養與軟性能力更為關鍵

商業敏銳度與產業知識是未來稽核人員的核心能力，唯有深入理解商業模式如何創造價值與獲利，掌握價值鏈、產品與服務的市場定位，研究競爭者策略及產業生態系的併購動向，才能精準評估風險並提升與資訊、財務、人力資源及營運單位的跨部門合作。稽核人員需具備財務與策略素養，獲取營運洞察，不僅辨識風險，更要質詢營運流程，理解預算編製，透過實地訪查掌握實況，並在追蹤市場趨勢與競爭動向中培養批判思維與商業意識，提出與企業價值創造緊密連結的問題。人文素養與軟性能力是稽核人員從稱職

邁向卓越的關鍵，未來稽核需從傳統監督者轉為績效推動者，應具備系統思維，不僅檢查合規性，更關注企業是否以有效率且合乎倫理的方式達成目標，提供前瞻性價值，運用設計思考與被稽核單位協作。此外，稽核應檢視文化、信任、聲譽與倫理等無形資產，因這些隱性因素常決定企業成敗。稽核人員需成為故事講述者，將數據與事實轉為引人入勝的敘事，使報告不僅被理解，更能推動行動，影響決策，驅動組織前行。

(三) 觀點 3：未來最優秀的稽核人員，不再只是傳統的監督者

未來最優秀的稽核人員，將同時是分析師與顧問、技術專家與翻譯者、守護者與引導者、敘事者與策略家，甚至是能預測未來的先行者。透過側向思維 (lateral thinking)，稽核將成為一個更具動態性、創造力與策略性的功能。講者認為稽核人員需要具備人文能力，包括以下幾點：

- **批判性思維與判斷力**：現實世界往往不是非黑即白，因此必須具備良好的判斷力。
- **溝通技巧**：能夠根據不同的受眾，設計出最適合的報告形式，這是發揮影響力的關鍵。
- **情緒智商**：稽核人員經常需要傳達不愉快或嚴峻的訊息，傳達方式可能決定能否建立或摧毀信任，而信任是稽核成功的根本。
- **影響力與關係經營**：與利害關係人建立連結，激發行動力。
- **適應力與好奇心**：組織必須進化，而稽核則需要走得更快，提前預防可能發生的問題。
- **道德勇氣與誠信**：倫理是稽核工作的基礎，也是我們存在的核心價值。

以上能力無法僅靠個人單打獨鬥來發揮，必須與其他部門合作，像是資訊、人資、業務部門等，都是潛在的合作夥伴。因此，稽核人員需要培養「理解人」的能力，能夠觀察團隊氛圍、員工的恐懼、態度與情感，這些判斷將直接影響工作成果。

稽核人員懂科技語言、理解新興商業模式、以專業方式進行數據分析、

面對新型風險並因應最新法規，還要具備前瞻視野。同時也必須展現軟性能力，例如靈活性、同理心、前瞻性，提供真正能提升生產力與專業的支持。這種軟硬技能之結合，講者稱為「蛻變」(Metamorphosis)。

(四) 觀點 4：重新塑造稽核功能與事務所的商業模式

稽核事務所同樣面臨重大挑戰與轉型，許多事務所已經開始投資人工智能，將其應用於部分作業自動化。如果 AI 能即時稽核所有交易，那是否還需要基層員工進行人工抽樣？答案顯然是否定的。這意味著，事務所的人力規模勢必縮減。因此，單靠自動化遠遠不夠。事務所必須進一步推動轉型，重新設計（re-architect）運作模式，例如：

- 建立可信賴的 AI 系統，確保透明與合規。
- 由「銷售工時」轉型為「銷售成果與平台存取」，改變營收模式。
- 建構 ERP、稽核人員與監管機關之間的中介系統。
- 推動人才再造，協助員工轉型為具備商業洞察、技術能力與人文素養的新型專業人才。
- 建立新指標，監控轉型成效，例如：收入組合變化、利潤率演變、稽核周期縮短、錯誤率下降，以及員工生產力提升等。

最重要的是，事務所必須培育並引導員工，讓他們具備全新的專業形象與價值定位，才能在這場結構性變革中生存並成長。

(五) 小結

新的稽核模式，將以全面掌握數據為核心。未來的稽核人員將能存取所有資料，這將是一個極具力量的位置。同時，我們也必須理解新法規，並將其轉譯為具體且量身訂製的商業機會，提供資源與建議以支持組織的發展。對於大型事務所而言，AI 帶來的挑戰不僅是減少人力，更是利潤結構的根本變化。隨著「按工時計費」模式逐步消失，營收可能面臨短缺，或必須透過重大整合來維持規模。最終，勝出的將是那些能把 AI 從「工具」轉化為「平臺」的事務所。

五、 全球審計轉型：人工智慧、監管與內部稽核的未來(Global Audit Transformation AI, Regulation, and the Future of Internal Audit)

由 Justin Greenberger 擔任主持人，並邀請到 Bupa 公司內部稽核部門分析主管 Sachin Kapoor、Davy 公司內部稽核主管 Chris Cowley 、Constellium 公司內部稽核副總裁 Karen Albert 共同就內部稽核挑戰與轉型，分享各自觀點，擇要分述如次：

(一) 內部稽核在全球環境下面臨的主要挑戰

Karen 指出，美國與歐盟在監管上的差異加深了跨國稽核的複雜性，尤其 AI 相關規範的不確定性，使企業難以規劃長遠策略。Chris 則強調金融服務業為高度監管產業，歐盟 AI 法案雖會限制應用速度，但同時也是安全邊界，確保合乎倫理，他擔心 AI 導入過慢會錯失競爭優勢，因此積極推動 AI 落地，但仍需在安全與效率間取得平衡。Sachin 則以技術專業背景指出，科技進展速度遠超過企業的導入步調，先研究，接著試行，再建立治理，最後才擴大實施的傳統流程，往往在完成前就已錯失時機，另外還有一個挑戰是「信任與可解釋性」，他指出曾閱讀一篇國際調查，結果顯示逾半數人對 AI 抱持不信任或不確定態度。整體來看，內部稽核同時面臨法規不一致、技術迭代快速、以及信任缺口三大挑戰，如何兼顧合規、安全與競爭力，成為未來必須持續思考的課題。

(二) AI 導入內部稽核的實踐經驗

現場透過 slido 請參與會議人員即時投票「在全球營運與轉型的背景下，你的內部稽核部門目前最大的挑戰是什麼？」在現場約 650 名與會者的投票中，內部稽核當前最大的挑戰被認為是「跟上並採用新技術（如 AI）」(比率約 45%，圖 15)。Chris 分享自身經驗，他三年前接手部門時，團隊規模有限，雖然公司已有各類科技工具，但多數未被有效利用。因此，他將 AI 工具放在營運、法規遵循及資訊安全領域，並成功將過往仰賴外部顧問的成本減半。實務應用建議從日常工作著手，例如會議紀錄自動摘要、產製風險與控制矩

陣、報告草稿等，雖任務簡單，卻能逐步累積經驗，擴展新用途。Chris 強調，唯有親自嘗試才能真正理解 AI 價值，並要求自己以身作則，持續在董事會與高層展示成果，即便有失敗案例也視為學習契機。如今，他的團隊已能在規劃、執行與報告各階段普遍運用 AI，顯著改變工作模式。主持人則點出兩大要素：一是保持對市場與技術趨勢的掌握，二是透過實際案例驗證價值，同時需建立監管防護措施，確保應用安全。

圖 15 現場 slido 投票結果截圖



資料來源：出國人員自行截圖。

(三)AI 對內部稽核運作的影響

Sachin 認為 AI 應用可分 3 層：1. 使用現成工具，如 Copilot 或 Audit Board AI，將大量非結構化文字轉換為有價值之建議意見；2. 發展客製化解決方案，例如設計專屬 Chatbot 協助新人快速熟悉，或利用 OpenAI 產製稽核計畫書與報告草稿；3. 進階分析能力，結合機器學習、預測模型與偏差分析，AI 不僅能偵測控制缺口，更能幫助找出根本原因。Karen 則指出，傳統製造業導入 AI 不易，高層與基層接受度有限，他強調「整合性風險管理平台」的重要性，能集中呈現重大風險、控制措施與緩解策略，不僅財務報表更包含營運控制，對跨部門共享與協作相當重要，另外他認為「變革管理」是推廣 AI 之關鍵，工具本身的變動(如 ChatGPT、Copilot 的版本更新)，可能對舊有提示詞產生的結果大不相同，意味著需要對工具的迭代進行管理與測試，否則可能出現預期外的偏差。Chris 則強調 AI 必須成為日常習慣，並認為稽核展示 AI 的成功應用可帶動全公司數位轉型。未來目標是整合內部控制三道防線，串聯風險平台、第三方管理平台、合規平台等，讓董事會與高層清楚掌握全局，並透過 AI 自動彙整與比較資訊，提升決策價值。

(四)透過培訓體系推動 AI 與數據能力養成

Sachin 指出，未來稽核人員不僅需具備專業稽核技能，還必須掌握數據分析與 AI 能力。為避免過度依賴資料科學家，他在 Bupa 推動成立內部「分析學院」，採分級訓練，從白帶到黑帶逐步提升。白帶為具備基本分析與 AI 應用能力；綠帶與藍帶能與數據科學家協作，掌握更進階技術；黑帶則可獨立開發解決方案，熟悉業務且善用 AI 的核心人才。

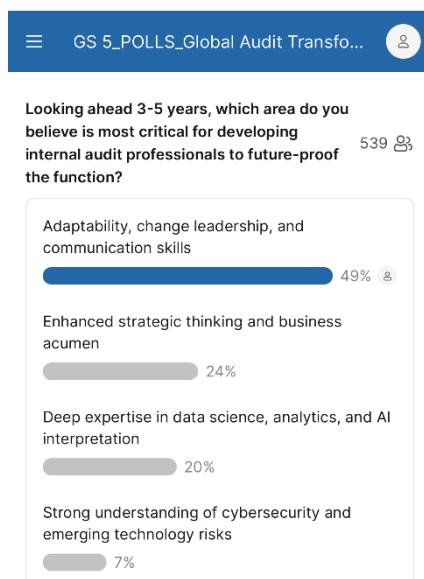
(五)稽核 AI

Karen 強調應從治理政策著手，先檢視 AI 治理架構的設計與落實，再到實際應用層面，無論是資料分析或合約審閱，都必須保留人類覆核並檢查來源。Chris 則指出，核心仍是「假設一驗證」的原則，先界定 AI 應達成的目標，再測試其輸出是否符合預期，若出現落差則進行調整，與傳統 IT 控制測試邏輯並無差異。Sachin 補充，應將 AI 視為一個「人」來審視，釐清其使用的資料、背後邏輯與產出依據，並建立完整的稽核追溯鏈，如此才能辨識相關風險並確認控制措施是否健全。

(六)未來三到五年最需要培養的關鍵能力

在現場約 530 名與會者的投票中，近半數（49%）認為未來內部稽核人員最需要培養的能力是適應力、變革領導力與溝通技巧（圖 16），顯示軟實力被視為因應快速變化的關鍵。Chris 強調不同世代間應互相學習，制定 AI 策略若只靠一群 50 歲左右的高階主管關起門來討論，絕對沒有效果，必須納入不同年齡層與專業背景的人員，以確保思維多元。他並提醒未來稽核人員可能過度依賴 AI 而忽視批判思維，因此仍需訓練獨立判斷。

圖 16 現場 slido 投票結果截圖



資料來源：出國人員自行截圖。

六、 資安威脅新局勢 (The New Cyberthreat Landscape)

由前美國國家安全局(NSA)高階主管，現任摩根士丹利財富管理部門的資安總監 Rachel Wilson 分享她對新興威脅的獨特見解，以及組織與領導者應如何因應的建議。講者認為現在所面對的挑戰比以往任何時候都要嚴峻，就其投身資安、資料保護與詐欺防制超過 25 年的經驗中，從未見過這樣險惡的環境。現行風險來源包括：國家級行為者、快速崛起的網路犯罪集團，以及人工智慧的廣泛應用，使得組織的第一、第二與第三道防線，都必須在難以想像的高壓下應對極為嚴重的後果。擇要分述如次：

(一) 國家級行為者－北韓網路攻擊戰略

北韓將駭客行為視為國家戰略的重要支柱，透過入侵銀行與金融機構竊取資金，形同把駭客行動變成一種「國家 GDP」來源。政府投入了高度資源培訓駭客，據估計，目前有大約一萬兩千名北韓人專職從事駭客工作，重要戰果如「孟加拉中央銀行案」，北韓駭客成功入侵該國央行，竊取將近 1 億美元。更驚險的是，他們原本要竊走接近 10 億美元，只因為在轉帳指令中出現拼字錯誤致交易未能完全成功，這顯示他們的能力已經到達極高水準。而且這並不是單一事件，光是在過去三年，全球已有 27 個國家公開指控北韓駭客入侵其央行或重要金融體系，聯合國也發布報告指出，累計損失超過 30 億美元。近年來，北韓更將目標擴展至加密貨幣領域。例如，Bybit 平台因北韓攻擊損失十五億美元，Coinbase 也曾遭到入侵，損失高達兩億美元。

(二) 國家級行為者－伊朗網路威脅

過去三年裡，伊朗成為講者最擔心的網路行為者之一，與北韓不同，伊朗駭客的目的並非單純為了金錢，而是因為他們深知「網路」是一種非對稱武器。想像一下，建造一艘航空母艦需要十年以上、數億美元的投入；研發核武更是困難重重。但對伊朗而言，只需要在德黑蘭某棟大樓地下室安置 40 名駭客，就能對全球產生極大破壞力。2012 至 2014 年間，伊朗駭客曾一波接一波攻擊銀行業，從華爾街、倫敦金融到香港，多地的金融機構皆遭遇大規

模阻斷服務攻擊，這些行動並非出於單純犯罪，而是對經濟制裁、軍事行動與網路反制措施的報復。觀察當前中東戰爭可以發現，哈瑪斯、真主黨、胡塞武裝等組織背後，不論在精神或金援上，都依賴伊朗作為支撐。因此，他們的網路攻擊不僅是區域性的報復行動，更是持續針對全球產業的威脅。

(三) 網路犯罪集團崛起與 AI 加劇風險

網路犯罪集團不是針對特定目標發動攻擊，而是以「誰脆弱就攻擊誰」為準則。他們的行動完全機會主義，不論對象是大企業、醫院、學校，甚至地方政府或非營利組織，只要能找到破口進入系統，就設法將其貨幣化。若將全球的網路犯罪活動合併計算，駭客收益足以構成全球第三大經濟體。光是去年，網路犯罪收入就達到約 11 兆美元。為何這股力量能在短時間內急速壯大？原因在於 AI 普及，過去駭客必須擁有電腦科學學位、具備國家級工具、受過專業訓練。如今有 ChatGPT 或 Gemini 並搭配教學影片，就能迅速掌握所需技術，門檻的降低讓攻擊數量、速度與規模以驚人速度倍增。目前，我們觀察到大約七成的惡意網路流量，來自這些犯罪集團。他們的攻擊不僅鎖定企業，也波及到每個人的日常生活—家庭、宗教場所、非營利機構、學校、醫院與地方政府，無一倖免。這正是當前環境最顯著的變化。

(四) 今年 3 R：Russia、Ransomware、Resilience

1. 俄羅斯（Russia）

俄羅斯在俄烏戰爭期間展現了強大的網路攻擊能力，並非如外界所想並未全力出手。事實上，俄羅斯的網軍已積極發動攻擊，以美國金融業為例，戰爭爆發前的幾個月內，美國各大銀行每日新開帳戶中約有三至四成屬於詐騙帳戶；但隨著戰爭臨近，詐騙帳戶比例急速攀升，一度高達九成五。銀行不得不暫停線上開戶流程，改為要求民眾親自到分行辦理，以確保客戶身份真實。經調查後被證實是俄羅斯策劃的國家級行動，意在阻斷數百萬烏克蘭難民將資金安全轉移至西方金融體系。俄羅斯將戰略設計隱身於全球犯罪活動的噪音中，讓外界難以追究其責任，並透過漸進式施壓達成既定目標。對

於稽核人員而言，此案例提醒我們必須重新思考：當表面看似是一般犯罪行為時，背後是否潛藏著國家級的意圖與威脅。

2. 勒索軟體（Ransomware）

去年網路犯罪高達 11 兆美元收入，大部分來自勒索軟體，平均每次勒索要求超過 200 萬美元，駭客組織規模龐大、遍布全球，行動高度商品化，幾乎堪比世界五百強企業。現在的勒索攻擊多採「三重勒索」模式：首先竊取組織的關鍵資料，接著癱瘓系統並要求贖金，最後再威脅公開或販賣資料，甚至演變為長期的「勒索即服務」。許多機構被迫在這種連環壓力下不斷支付，甚至像美國巴爾的摩市一樣，將勒索軟體支付費用納入年度預算。

3. 韌性（Resilience）

面對這樣的環境，唯一能保護我們的就是提升組織的韌性。這包括確保所有系統隨時更新與修補漏洞、定期進行桌上演練、明確界定高層在危機中的角色與倫理立場，以及最關鍵的一點：驗證備份策略是否真正有效。因為在駭客攻擊發生時，能否迅速復原，將決定一個組織能否存活。

(五) 強化韌性具體建議

在韌性方面，最重要的原則就是「預防勝於治療」。各位稽核人員應該不斷督促第一線團隊，思考在遭遇重大資安事件時能否即時應變。因此，韌性建設需要各位持續施壓、持續檢視，確保組織在面臨「網路黑天」時能夠站得住腳。

1. 補丁與更新

維護資訊安全的基本工作，軟體公司釋出更新檔時，對駭客而言是一份「寶藏地圖」，透過反向分析內容，尋找並利用漏洞攻擊未更新的用戶。因此，組織應確保所有系統即時更新，以降低攻擊風險。

2. 桌上演練

組織須定期模擬勒索軟體等網路攻擊場景，讓高階主管與跨部門成員清楚各自責任，並提前討論關鍵問題，例如：公司是否會支付贖金？是否願意

被挾持？這些決策涉及倫理與公司價值。

3. 備份驗證

許多資訊部門會拍胸脯保證已依循「3-2-1 備份原則」三份資料、兩地存放、一份離線。作為稽核人員要問的是：這套備份策略最後一次測試是什麼時候？測試過程是否真能在四小時內復原？不要在週末測試，因為週末會很順利，要在週二早晨工作繁忙時測試，才能檢視真實的應變能力。若未經驗證，備份計畫很可能只是一紙空談。

(六) 保護範圍延伸至客戶與民眾

內部稽核團隊近來也提高了對講者的期待，他們認為資安不僅要保護公司與員工，還必須把防護範圍延伸到客戶與投資人，確保客戶不會因為誤信詐騙而蒙受損失，也要能辨識出客戶何時正處於壓力或被操控之下。這意味著，在教育與偵測上的要求必須更進一步。講者分享一位客戶真實事件，她上週接到一通電話，誤以為是微軟打來，講者提醒各位，微軟永遠不會主動打電話給你。更何況這位客戶使用的是 MacBook，微軟更不可能主動提供技術支援，但她仍然深信不疑，結果讓詐騙者在她的電腦上安裝惡意程式，能記錄鍵盤輸入、擷取螢幕畫面，並在她操作時蒐集所有銀行、證券帳號與密碼。對方甚至假裝要「確認修復成功」，要求她逐一登入各種金融帳戶，結果所有資料全被竊走。雖然我們的偵測系統及時發現了異常，但在後續溝通中，她坦承自己十年來一直使用相同的密碼。更糟糕的是，她打算僅僅加上一個驚嘆號，當作「升級版密碼」，來抵抗駭客。這就是我們所面臨的真實挑戰：再先進的防護，也敵不過用戶缺乏警覺與基本的資安習慣。

(七) 小結

講者強調，身為組織的第一、第二、第三道防線，責任不僅是守住公司內部，也要協助外部利害關係人提升防護能力。整體而言，網路威脅已進入前所未有的危險時代，稽核與風險管理專業者必須成為推動安全與韌性的關鍵力量。

肆、同步場次

一、永續相關議題

(一)CEESG：以強大控制環境重新定義環境、社會與治理（CS2-5

CEESG: Redefining ESG with a Strong Control Environment)

本場次由風險與公司治理專家 Ali Rehman 博士（圖 17）主講，主要探討當前 ESG 實踐的困境、控制環境為 ESG 成功的基石，以及內部稽核在 ESG 浪潮中的關鍵角色與整合框架等核心議題。講者強調「控制先行，ESG 才得以永續」（Control First, ESG Next），亦即闡述 ESG 目標的實現，須奠基於一個健全且有效的控制環境。

圖 17 風險與公司治理專家 Ali Rehman 博士



資料來源：IIA 網站。

1. 當前 ESG 實踐的困境—治理失靈與舞弊風險

講者首先定義「永續性」（Sustainability），意指「滿足當代需求，且不損害後代滿足其需求的能力」。此概念最早由聯合國於 1983 年提出，並在 1987 年「我們共同的未來」（Our Common Future）的報告中正式定調。而 ESG 則是一套評估與報導永續性相關績效的標準或指標，其源自於金融與公司治理領域，旨在提供衡量永續性的工具。從歷史脈絡來看，全球對永續性的關注是自 1983 年聯合國世界環境與發展委員會的成立開始，歷經 2000 年的千禧年發展目標（MDGs），至 2004 年「ESG」一詞首次被官方正式使用，最終 2015 年發展出現在廣為人知的 17 項聯合國永續發展目標（SDGs），這 17 項 SDGs 可分別對應至 ESG 的三個面向，形成 ESG 實踐的全球性框架（圖 18）。

儘管 SDGs 為一個全面的框架，但講者指出其存在顯著失衡，17 項目標若分解對應至 ESG 三大面向，與社會面向直接相關者有 8 項，與環境面向直接相關者有 6 項，而與治理直接相關者僅有 3 項，講者強調，這種對治理的

輕忽是當前 ESG 推動的核心困境，因幾乎所有重大的資產挪用與財報舞弊案件，其根源都來自於治理的根本性失靈。根據舞弊三角理論，薄弱的治理結構會直接導致控制環境弱化，進而為舞弊創造「機會」，這些治理缺失導致各種類型的舞弊，包括以福斯汽車廢氣排放測試造假案為代表的「漂綠」（Greenwashing）、與賄賂與不實財報相關的治理舞弊，以及各類社會相關詐騙。講者更以台塑集團為例，說明該集團因污染與工安問題屢次被處以高額罰款，凸顯即便組織已遵循法規，若缺乏健全的治理，仍無法阻止危害的發生。

圖 18 UN SDGs 對應 ESG



資料來源：2025 年 IIA 國際研討會。

2. 控制環境為 ESG 成功的基石—五大原則與整合策略

為解決 ESG 實踐的困境，講者強調，成功實踐 ESG 的關鍵在於健全的控制環境（Control Environment, CE）。控制環境是組織為實現其目標、管理風險及遵循法規而制定的一套由價值觀、態度、政策與程序所構成的框架，其良窳主要由高階管理層與董事會所設定的「高層基調」（tone at the top）決定，

強大的控制環境可促使組織遵循最佳道德實務。講者進一步闡明，治理是控制環境賴以建立的基礎，透過積極的董事會監督、領導及明確的課責架構實現的有效治理、確立高層基調，可直接塑造控制環境。治理不僅影響控制環境，更「定義」控制環境，一個薄弱的治理結構必然導致一個破碎或無力的控制環境，進而增加舞弊、違規與營運失敗的風險。講者提出一個健全的控制環境包含：對道德與誠信的承諾—要求高層以身作則；董事會的獨立性—確保董事會能獨立於管理階層，有效履行監督職責；組織的治理結構—建立清晰的報告線，並明確定義角色與職責；適任的人才—不僅要聘用，更要留住合適的人，與培養具備 ESG 相關能力的員工；課責制度—要建立明確的機制，確保董事會與管理階層對其行為與決策負責等 5 大核心原則。

組織應建立一個健全的控制環境，並將控制環境與 ESG 進行雙向整合，以強化永續作為的成效。首先，應將控制環境的考量嵌入 ESG 的政策與程序中，具體做法包括針對企業污染物使用、再生能源、多元共融政策、供應鏈風險等 ESG 相關領域，建立有效的內部控制；其次，應在評估控制環境時評估控制措施解決 ESG 風險的設計及實施效果，例如，評估內部控制設計與執行是否足以應對環境事件，確保決策中已考量社會及道德因素。透過此種整合，組織能夠有效提升風險管理、強化對日益增加之 ESG 法規的遵循性，並與投資者、客戶及員工等利害關係人建立信任。

3. 內部稽核在 ESG 浪潮中的關鍵角色與整合框架

內部稽核在 ESG 與控制環境整合的過程中，扮演著不可或缺的關鍵角色。內部稽核透過獨立、客觀的確信與諮詢服務，可有效評估並改善組織的治理、風險管理及控制流程。內部稽核的職能與控制環境的五大原則緊密相連，例如稽核人員能評估組織的道德誠信文化、組織結構的有效性，以及針對董事會高階管理層進行課責審計 (accountability audit)，並提出意見。在 ESG

實踐上，內部稽核能透過多種方式作出貢獻，包括：為 ESG 報告的準確性提供確信服務、辨識與評估 ESG 相關風險、確保組織遵循 ESG 相關法規，並藉由獨立的評估強化利害關係人對 ESG 資訊的信任。

為協助稽核人員執行任務，講者提供一份針對溫室氣體排放（範疇一至三）的詳細檢查表，並首次公開整合性的「控制環境—環境、社會與治理—內部稽核框架」（CE-ESG and IA Framework）（圖 19），該框架將控制環境的五大原則與 ESG 加以整合，並列出內部稽核所應扮演的角色，為組織提供一個清晰的行動藍圖。例如，在「誠信與道德」原則下，整合 ESG 的重點在於考量攸關 ESG 的行為準則及防止漂綠的控制措施，內部稽核則應負責稽核有關 ESG 的道德議題與報告的誠信度。最後，講者再次強調，若無一個健全有效的控制環境，ESG 目標將無法實現，對稽核人員而言，「環境」一詞永遠始於「控制環境」，又雖然 ESG 強調國家 GDP，但也強調環境影響，關鍵在於 ESG 的關鍵組成要素是環境，而在談論環境時，正確的術語應該是氣候（climate），惟有用詞準確，治理才得以準確。

圖 19 控制環境—環境、社會與治理—內部稽核框架



CE 原則	ESG 整合	內部稽核角色
1. 誠信與道德	行為準則中的 ESG，漂綠控制	審核ESG倫理與報告完整性
2. 董事會監督	ESG 委員會，董事會 ESG 教育	ESG 確信報告提交董事會
3. 組織結構	明確定義ESG職責，跨部門ESG治理	審核ESG權責及報告流程
4. 能力	ESG 培訓與能力建設	審核ESG技能落差，評估能力準備度
5. 講責	將ESG 指標與補償連結	調查ESG偏差，審核績效激勵措施

多倫多 2025 年 7 月 14-16 日

資料來源：2025 年 IIA 國際研討會。

(二)最大化內部稽核對組織永續性的影響（CS4-5 Maximizing Internal Audit’s Impact on Organizational Sustainability）

本場次由熟稔稽核與風險管理實務的產業主管 Grant Ostler 先生（圖 20）與 Graeme Fleming 先生（圖 21）主講，主要探討當前內部稽核面臨的多元挑戰、內部稽核在永續報導內部控制（Internal Controls over Sustainability Reporting, ICSR）的角色，以及運用 AI 提升稽核生產力與留住人才等核心議題。

圖 20 產業主管 Grant Ostler 先生



資料來源：IIA 網站。

圖 21 產業主管 Graeme Fleming 先生



資料來源：IIA 網站。

1. 當前內部稽核面臨的挑戰

當前內部稽核人員正處於一個劇烈變動的時代，其面臨來自地緣政治不穩定、經濟波動（如關稅與潛在衰退）、法規變化及科技發展（如 AI 與勒索軟體攻擊）等多重的壓力，組織對稽核部門「事半功倍（do more with less）」的要求，以及吸引與留住專業人才的挑戰。在此背景下，永續性議題雖在全球法規層面呈現變動的狀態⁴，並為企業帶來更複雜的合規挑戰。然而，不論監管機關的態度如何，市場本身已做出反應，消費者（特別是年輕世代）、投資者與金融機構越來越傾向於依據企業的永續性表現，做出消費、投資或借貸的決策。缺乏永續性作為的企業將面臨失去市場、難以吸引年輕人才，甚至無法取得優惠融資條件的風險，進而衝擊其長期經營的能力。

⁴如美國聯邦層級的氣候規則有所放緩，但美國加州等多個州則訂有相關法規，歐盟亦實施「企業永續報導指令」（Corporate Sustainability Reporting Directive, CSRD）。

2. 內部稽核在永續報導內部控制（ICSR）的角色

面對永續報告的需求，內部稽核應扮演協助組織建立有效「永續報導內部控制」（ICSR）的關鍵角色，組織並應由過去推動「財務報告內部控制」（Internal Control over Financial Reporting, ICFR）的經驗中學習，避免重蹈由下而上、耗費大量資源卻效益不彰的情形，而應採取由上而下（top-down）、以重大性為基礎的風險導向方法。這意味著稽核工作應始於對組織使命與目標

圖 22 借鏡 ICFR 的經驗



資料來源：2025 年 IIA 國際研討會。

的理解，並以此為據，辨識與永續相關的重大風險。在控制措施方面，應追求預防性與偵測性控制的平衡，並儘可能將控制措施「內建」於流程中，而非事後「外加」（圖 22）。又由於永續性數據通常來源分散、多為非結構化資料，且多數過去未經稽核驗證，因此，稽核人員的早期介入至關重要。講者以一個實際案例說明，某企業的永續報告部分數據存在無有效支持文件或重大錯誤的情況，其支持文件竟只是一張寫著「Bob」名字的便利貼。因此，內部稽核人員應瞭解業務流程的內容及背後的原因，並體認控制措施不僅是為合規而實施，而應被視為協助企業營運、管理風險與實現目標的良好實務，

此外，應根據企業所處的行業與地理區域評估風險，協助管理階層管理風險。

3. 運用 AI 提升稽核生產力與留住人才

AI 為提升生產力（圖 23）與留住人才等挑戰提供強大的解決方案，其能協助稽核人員擴展風險視野、快速分析大量非結構化數據，並簡化文件編製工作。例如，稽核人員可利用 AI 將會議紀錄自動轉製為流程敘述、風險與控制矩陣（RCM）及流程圖，進而減少重複性的工作，將時間投入更具價值的諮詢活動。同時，隨著組織廣泛導入 AI，內部稽核在推動 AI 治理方面扮演著不可或缺的顧問角色，內部稽核人員須確保 AI 的使用安全、合規並與組織目標保持一致。此外，科技的導入與人才留任間存在直接關聯，現代員工（尤其是職涯尚處於早期的年輕世代）渴望從事有意義、具挑戰性且能學習成長的工作，並重視工作與生活的平衡，透過將例行性、較無需人工判斷的工作自動化，稽核部門不僅能提升效率，更能使團隊成員專注於解決複雜問題、運用數據分析提供洞見，並發展 AI 等新興科技的專業技能，而此正符合現代人才的職涯期望，且可有效提升團隊的敬業度與留任率。

圖 23 運用 AI 提升生產力



二、道德審計相關議題

(一)內部稽核在強化組織文化中的角色 (C3-5 The Role of Internal Audit in Enhancing Organizational Culture)

本場次由組織治理與內部稽核專家 Seita Almandeel 博士（圖 24）主講，依組織文化的策略重要性與其無形特質、系統化實施文化稽核的實務作法等核心議題，分享其在沙烏地阿拉伯最高審計機關（General Court of Audit, Saudi Arabia）領導團隊執行文化稽核的實務經驗與洞見。

1. 組織文化的策略重要性與其無形特質

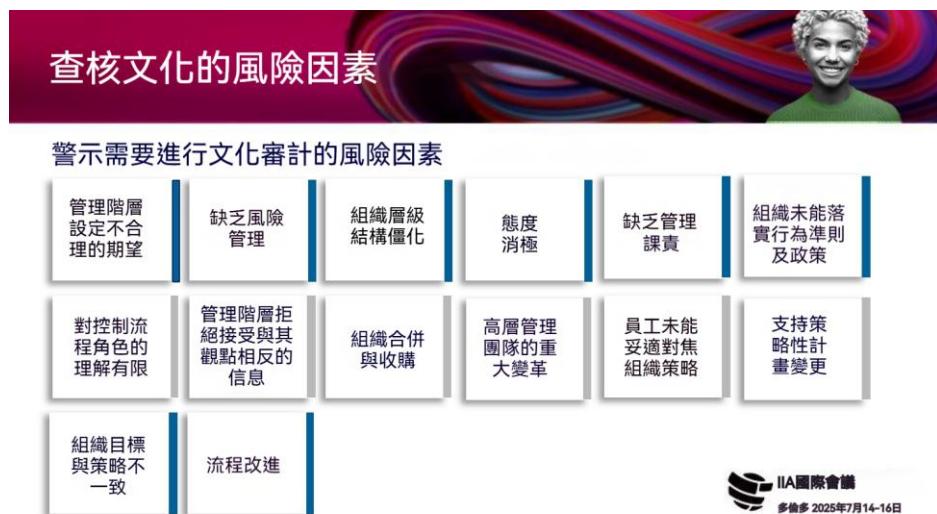
組織文化是組織成功的基石，然因其為組織中所有個體無形的信念系統、價值觀、規範與偏好，本質上難以定義，這種無形的特性使文化的評估充滿挑戰性。儘管如此，組織文化的重要性不容忽視，其對企業的策略性決策、營運等都有很大的影響，且為影響組織變革適應能力及其與利害關係人關係的決定性因素。又文化始於領導階層，一個正向、健康的組織文化特徵包含來自高層的積極基調、清晰的溝通、開放的對話、高度的員工參與度，以及與核心價值觀一致的激勵措施等，此種文化能有效促進變革管理、支持策略性決策、提升企業競爭力，並確保組織願景與策略間的一致性。影響組織文化的風險因子涵蓋多個層面，主要的態樣包括：管理階層因不瞭解團隊能力與組織潛力而設定不切實際的期望；缺乏針對營運的風險管理；員工對內部控制與程序理解有限，進而產生不當行為；管理階層拒絕接受與其意見相左的資訊；以及組織目標與策略未能一致等（圖 25），此外，員工展現退縮、不參與等負面態度，亦是重要的文化風險指標。內部稽核人員需要探究這些文化風險背後的原因，找出控制措施執行不當之處，並向管理階層提出建議，以確保員工的工作方式與組織策略需求取得一致。

圖 24 組織治理與內部稽核專家 Seita Almandeel 博士



資料來源：IIA 網站。

圖 25 主要的文化風險態樣



資料來源：2025 年 IIA 國際研討會。

2. 系統化實施文化稽核的實務作法

(1) 框架與方法論：內部稽核須運用結構化的框架，始得有效評估文化。

IIA 提出整合式⁵、目標式⁶與由上而下式 (top-down)⁷等 3 種稽核方法，講者建議首次進行文化稽核時，應採全面「由上而下」的方法，由高階管理者乃至於基層員工，全面檢視整個組織，以建立查核團隊的專業能力與對組織文化的基礎認知，並於次年依據前一年度的稽核結果，採用目標式或整合式方法進行查核。文化稽核的整個生命週期包含查核前準備、查核規劃、實地查核與報導等階段，其中查核前準備是最耗時也最關鍵的步驟，在此階段，稽核團隊需要投入大量時間研究並建立一個適合自身組織的文化模型。講者分享其團隊運用安永 (EY) 模型⁸（包含目標與價值觀、領導力、人員能力、員工間資訊與想法的交流、績效與獎酬、科技的運用、權責與角色定位、員工賴以執行工作所需設備與資源、業務流程、工作環境等 10 項文化支柱，(圖 26) 作為文化審計的衡量標的，成功將文化此一抽象概念進行量化的評估，另運用丹尼森 (Denison) 模型⁹，於正式進行文化稽核前，

⁵ 將文化風險因素納入所有查核工作，此方法在所有查核工作中考量文化風險因素。

⁶ 針對關鍵流程與控制措施中與文化相關的特定領域進行測試。

⁷ 此方法係對組織內所有與文化相關的活動全面進行審計。

⁸ 專注於組織內部營運相關的具體文化要素。

⁹ 用於評估組織文化的成熟度，並檢視其與外部挑戰的策略契合度。

完成組織的文化成熟度評估，以作為後續稽核工作的基礎。

(2) 資料蒐集、風險辨識與報導：在執行文化稽核時，應採用質化與量化並行的多元方法蒐集資料，以獲得全面且深入的觀點。講者團隊透過問卷調查、訪談及焦點小組蒐集資料，例如針對非管理職的全體員工進行匿名問卷調查；對中階主管舉辦焦點團體訪談；與副首長等高階主管進行一對一訪談等，其經驗顯示此種分層蒐集資料的策略極為有效，不僅能廣泛蒐集量化數據，更能透過訪談深入瞭解員工的真實感受與經驗。而稽核的價值在於交叉比對來自不同層級與不同方法的資料，以辨識其中的「差距」或「矛盾」。例如，當高階主管在訪談中描述的領導風格，與其團隊成員在問卷中反映的感受截然不同時，顯示存在潛在的文化風險，稽核人員會將這些辨識出的風險，連同其對應的文化支柱、控制措施與稽核程序，詳細記錄於「風險與控制矩陣」(RCM) 中，作為實地查核的基礎。最終，稽核報告不僅應呈現各文化支柱的成熟度水準，並須整合問卷、焦點團體與訪談的發現，提出具體的稽核發現與改善建議，並明確指出應負責執行的權責單位。這項工作充滿挑戰，例如資料的敏感性可能導致員工回應率偏低，且文化議題的權責歸屬往往橫跨多個部門，但內部稽核可透過系統性的方法，協助組織營造一個更健康的組織文化。

圖 26 10 項文化審計支柱



資料來源：2025 年 IIA 國際研討會。

(二)解鎖確信：將行為風險與整合性人與流程稽核（IPPA）及雄心模型（Ambition Model）整合（C3-2 Unlocking Assurance: Integrating Behavioral risks with IPPA and the Ambition Model）

本場次由 IIA 荷蘭分會的 Danny

Francken 先生(圖 27)

與 Peter Hartog 先生

(圖 28)共同主講，

主要探討整合性人

與流程稽核

(Integrated People

and Processes Auditing, IPPA) 的概念與重要性、IPPA 的應用方法與實務操作，
以及 IPPA 的導入與稽核部門的策略發展等核心議題。

1. IPPA 的概念與重要性

IPPA 是一套專為稽核設計的工具，其明確列示組織內文化與行為的重點，提供與稽核對象態度、行為與文化有關的具體資訊，進而使稽核人員可對關鍵的人員與流程組合進行周延的評估。傳統上，許多稽核人員認為因缺乏標準與衡量方法，且由訪談中取得的資料恐被視為不具可靠性，因此，評估行為是不可能的。然而，鑑於幾乎所有事件的根本原因都與人類行為有關，因此，文化與行為的重要性不容忽視。Google 研究證明，心理安全感 (Psychological Safety) 是高效團隊最關鍵的要素，此顯示行為等軟性控制 (soft controls) 對組織成效有直接且重大的影響。IPPA 工具箱包含超過 80 種行為面向 (圖 29)，並將這些抽象概念轉化為具體的評估標準、訪談問題與觀察方案，可克服前述的稽核障礙，協助稽核人員將行為面向有效納入稽核工作。

圖 27 IIA 荷蘭分會 Danny Francken 先生



資料來源：IIA 網站。

圖 28 IIA 荷蘭分會 Peter Hartog 先生



資料來源：IIA 網站。

圖 29 IPPA 80 種行為面向



資料來源：2025 年 IIA 國際研討會。

2. IPPA 的應用方法與實務操作

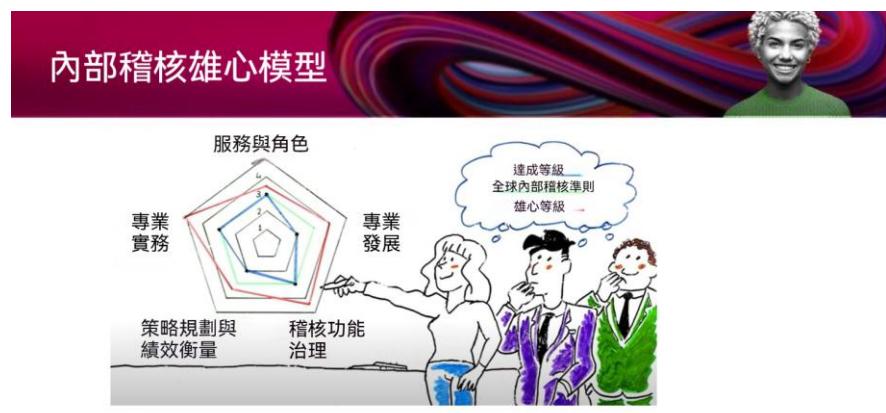
應用 IPPA 的方式有 3 種，最常見的應用是在稽核開始時辨識行為風險與關鍵行為，其他方式包括用於稽核結束時進行根本原因分析，或專門稽核組織的核心價值觀。講者以第一種最常見的應用方式為例，說明 IPPA 應用於稽核準備階段與審計對象相關行為風險的辨識，以銀行接受新客戶為例，其作業涉及多個步驟，稽核人員要定義關鍵人員與流程組合，在客戶身分驗證流程中，銀行人員可能存在因工作壓力大而導致草率行事的行為風險，稽核人員可利用 IPPA 工具，由資料庫中選出與此風險相關的行為面向（如員工的準確性與主管給予回饋的能力），並擇選其中最關鍵的幾個項目進行評估；下一步是將這些選定的行為面向具體化，運用 IPPA 提供的評估標準與結構化的訪談問題蒐集資訊。而資料蒐集的來源主要為訪談與觀察，其中訪談採用基於 STARR 面談框架（情境、任務、行動、結果、反思）的半結構化提問法，而觀察則可透過互動過程分析（Interaction Process Analysis, IPA）等工具進行系統性記錄，又為確保結論的可靠性，建議同時使用訪談與觀察兩種方法，以達成「方法三角驗證」(method triangulation)；在撰寫報告時，應提供豐富且詳

細的「深入描述」(thick description)，具體描述情境與行為，並避免過度概括或評價性的詞語，以客觀呈現行為風險。

3. IPPA 的導入與稽核部門的策略發展

導入 IPPA 可採取的方式有 2 種，其一是執行獨立專案，對團隊進行如何使用工具的培訓並直接應用；另一方式則是將其作為稽核部門更宏觀之策略發展的一環，後者可藉助 IIA 荷蘭分會發展的內部稽核雄心模型(Internal Audit Ambition Model)加以實現。該模型是一個為稽核長設計的自我評估模型，旨在協助稽核團隊評估其在專業實務、服務與角色、策略規劃與績效衡量、稽核功能治理、專業發展等 5 個面向（圖 30）上的表現水準，並設定未來發展的目標。其將稽核職能的成熟度分為 5 個等級，其中第 3 級代表符合全球內部稽核準則，而第 4 、 5 級則代表超越準則的更高企圖心。透過此模型，稽核部門可建立一個清晰的精進藍圖，不僅是年度計畫與預算的基礎，也是與董事會、審計委員會等利害關係人溝通的有效工具，另透過整合該模型提供的策略框架與 IPPA 提供的具體操作工具，可提升其在行為與文化等軟性控制領域的稽核能力，進而實現稽核部門的策略性發展目標。

圖 30 內部稽核雄心模型



IIA Maria 與內部稽核雄心模型



資料來源：2025 年 IIA 國際研討會。

(三)舞弊與鑑識矩陣（CS3-7 Fraud and the Forensic Matrix）

本場次由鑑識會計顧問公司 G.L. German Forensic Accounting, LLC 的 Gary L. German 先生（圖 31）主講，主要探討舞弊的普遍性與傳統稽核的侷限、鑑識會計的推論性思維模式，以及運用「鑑識矩陣」（Forensic Matrix）系統化發掘舞弊等核心議題，深入剖析舞弊的本質與查核挑戰。

1. 舞弊的普遍性與傳統稽核的侷限

舞弊的定義往往是模糊的，其判定也常取決於時間、地點、人物與情境，充滿灰色地帶。儘管定義困難，舞弊的規模卻十分驚人，根據國際舞弊稽核師協會（ACFE）的估計，組織每年因舞弊損失 5% 的營收，且超過 85% 的企業每年都受舞弊影響。然而，舞弊案件卻鮮少被起訴，其原因可能包括：執法部門面臨資源不足與優先順序的考量；企業可能基於成本效益、維持競爭力，甚至業務需求而容忍、縱容或要求舞弊行為；個人道德因素考量如同情心、擔心負面聲譽或達成私下歸還協議等，也降低起訴意願。在此背景下，儘管 80% 的公司將外部稽核列為首要反舞弊措施，但實際上僅有 3% 的舞弊是由外部稽核發現的，超過 52% 的舞弊都是偶然被發現的。依據講者的實務經驗，外部稽核之所以難以發現舞弊，主要是因三大結構性限制，首先，必須存在舞弊，舞弊交易在龐大的合法交易中占比極小，且線索微弱；其次，必須尋找舞弊，而執行大部分外勤工作的年輕稽核人員經驗有限，且在壓力下可能不敢多問；再者，必須堅持到找出舞弊為止，稽核成本高昂，存在著講求效率、避免麻煩等因素，導致稽核人員缺乏動機與資源堅持找出舞弊。

2. 鑑識會計的推論性思維模式

講者強調，聰明人往往因為專注於尋找預期的答案，而陷入「隧道視野」，反而忽略周遭的異常跡象。因此，舞弊查核需要「跳出框架思考」（out of the

圖 31 鑑識會計專家
Gary L. German 先生



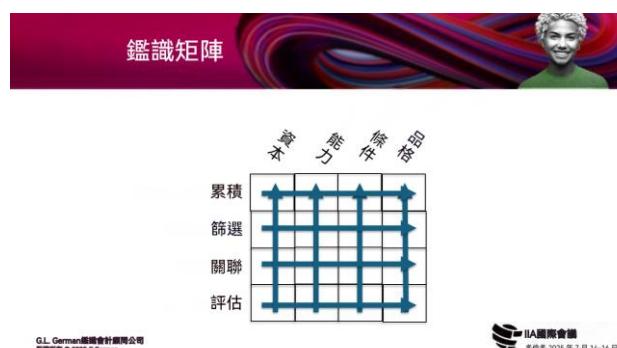
資料來源：IIA 網站。

box thinking)，運用「推論性思考」(inferential thinking)，亦即基於證據與先備知識 (prior knowledge)，而非僅依賴觀察得出結論的推理過程。講者將其稱為「非常識的常識運用」，並主張在調查初期應避免帶有任何先入為主的觀念，因調查人員往往不知道舞弊發生之處，甚至不知道其以何種形式存在。以保險理賠案為例，案例背景為某公司因火災導致電腦浸水，公司人員宣稱所有資料遺失並索賠 80 萬美元的業務中斷損失，然而，講者在下載該公司資料時，推斷出這些資料其實一直都儲存在雲端，並未遺失，進而揭穿整個騙局，顯見結論並非來自直接觀察，而是來自對證據背後邏輯的連結與推理。

3. 運用鑑識矩陣系統化發掘舞弊

講者提出其核心查核工具為「鑑識矩陣」(Forensic Matrix) (圖 32)，此方法論整合客觀的分析流程與主觀的情境影響因素，其中客觀分析流程包含 4 個步驟，首先是「累積」(Accumulate)，建立可獲取資訊的全貌，來源包括財務報表、稅務資料、銀行紀錄，乃至於網路、社群媒體與相關人員；其次是「篩選」(Select)，依據查核目標，聚焦於相關、重複出現或異常突出的項目，重點在於判斷在特定情境下「什麼是攸關的」；第三步是「關聯」(Relate)，透過建立對「正常」樣貌的理解，辨識趨勢、模式中的矛盾與不尋常之處，例如交叉比對財報、稅報與銀行對帳單間的邏輯關係；最後一步是「評估」(Evaluate)，判斷分析結果的邏輯性、是否能提供支持性證據，並決定是否需要進一步查核。另融入 4 項主觀的影響因素，包括：「資本」(Capital)，即追蹤金錢流向；「能力」(Capacity)，即判斷績效是否超出合理範圍（例如好到不真實）；「條件」(Conditions)，即分析可能影響行為的內外部環境因素與誘因；以及「品格」(Character)，即評估對象的聲譽、態度等細微線索，以提供一個全面且深入的舞弊查核框架。

圖 32 鑑識矩陣



G.L. German 服務有限公司
版權所有 © 2025 G.L.German

IIA 國際會議
多倫多 2025 年 7 月 14-16 日

資料來源：2025 年 IIA 國際研討會。

(四)舞弊調查：如何執行 (CS5-2 Fraud Investigations: A How to Guide)

本場次由 SaskPower 公營事業內部稽核主管 Brenda Youle 女士（圖 33）主講，透過探討舞弊調查的系統化流程與挑戰及調查各階段的關鍵實務等核心議題，分享其團隊在多年舞弊調查實務中淬鍊出的方法。

1. 舞弊調查的系統化流程與挑戰

舞弊調查的結果可能對涉案員工的職涯造成嚴重衝擊，甚至進入司法程序，因此，建立一套標準化且可重複的流程至關重要。講者強調，其團隊將調查流程明確劃分為規劃、實地查核與報導等 3 個階段，並為每個階段擬訂詳細的執行步驟，然而，調查過程充滿挑戰，稽核人員常面臨時間緊迫、缺乏合作、資料不足，以及管理階層可能因信任涉案員工而對調查過程缺乏認同等壓力。此外，調查本身（特別是涉及職場不當行為的案件）常使團隊成員與受訪者感到不安與情緒耗竭，這對調查人員帶來極大的考驗（圖 34）。

圖 33 SaskPower 內部稽核主管 Brenda Youle 女士



資料來源：IIA 網站。

圖 34 舞弊調查的挑戰



資料來源：2025 年 IIA 國際研討會。

2. 調查各階段的關鍵實務

- (1) **規劃階段**：首要任務是評估可取得的資源、團隊技能及紀錄，並完成蒐集初步資訊、評估指控內容、決定調查範疇與目標，以及擬訂行動計畫等步驟。講者特別指出，任何調查都應由至少兩名稽核人員共同執行，藉由多元觀點進行腦力激盪、事實查核，以有效消除個人偏見，並分擔單一稽核人員承受的巨大壓力。
- (2) **實地查核階段**：此階段包括蒐集證據與文件、訪談證人與嫌疑人、分析財務資訊、更新指控摘要、定期溝通等步驟。講者提醒，不能輕信涉案人的片面之詞，例如舞弊金額往往比對方主動承認的金額多，稽核人員須進行獨立查證。又訪談是另一項關鍵，稽核人員須為受訪者可能說謊預作準備，在訪談前充分掌握資訊，以便即時挑戰不實陳述，例如，在某案例中，涉案員工謊稱無法使用 Apple Pay，調查人員透過直接與銀行確認，並調閱系統紀錄後，以客觀證據戳破其謊言。此外，執行調查時，應靈活運用數據分析、趨勢分析等工具，由看似正常的交易中找出異常模式。另講者透過 2 個截然不同的案例，闡述調查方法的應用，在工時與油資竊取案中，團隊結合車輛的自動定位系統數據與薪資系統的工時紀錄，透過大量數據比對，計算出員工浮報的工時與盜用的油量，最終成功促使涉案者被起訴；在職場霸凌案中，調查重點在於與 31 位相關人員進行深度訪談，蒐集大量非結構化證詞，此案凸顯建立信任、保護受訪者及應對高張力情緒的重要性。
- (3) **報導階段**：此階段包括草擬調查報告、溝通結果、分送報告、考量法律影響及與執法機關合作等步驟。無論案件類型，最終的調查報告都需要考慮其法律意涵與潛在讀者（如警察或法務），並詳加說明所有假設及查核發現的依據，以適當呈現調查結果。

三、未來稽核相關議題

(一)未來導向的內部稽核領導力：全球稽核長的觀點（CS5-7 Future Proofing Internal Audit Leadership: Perspectives of Global Chief Audit Executives）

本場次由 加拿大 RSM 顧問公司的 Tabish Gill 先生主持，並邀請 3 位來自全球頂尖銀行的稽核長擔任與談人，分別為加拿大帝國商業銀行（CIBC）的 Heather Kaine 女士、蒙特婁銀行（BMO）的 Helen Killoch 女士及多倫多道明銀行

（TD Bank）

的 Michelle
Myers 女士

（圖 35），共
同探討在當
前劇烈變動
的環境下，內
部稽核職能
因應未來的

準備、經濟動盪下內部稽核的調適作為、內部稽核回應利害關係人期望的作
法、內部稽核實務的轉型與創新，以及變革時代下的領導力等核心議題。

1. 內部稽核職能因應未來的準備

為應對未來挑戰，內部稽核職能正經歷一場由傳統「法規遵循檢查者」轉型為組織「策略夥伴」的重大變革。此轉型促使稽核部門須制定與組織整體策略及風險偏好相符的願景與藍圖。稽核的範疇不再侷限於檢查控制措施的執行，而是擴展至評估企業的營運韌性、瞭解人才策略，並利用數據分析偵測趨勢與辨識新興風險。為此，稽核團隊須具備好奇心與卓越的溝通技巧，

圖 35 主持人及與談人



資料來源：自行拍攝。

其不僅要能發現問題，更要具備有效向業務夥伴闡述其潛在影響與風險的能力。在科技應用方面，稽核流程由規劃到報導的各個階段都應導入 AI 等新技術，以保持敏捷性。又儘管講者不認為稽核部門應成為組織內採用 AI 的領頭羊，但其須與企業的發展步伐保持一致，例如目前稽核團隊正嘗試利用 AI 撰擬報告及驗證問題的測試範本。然而，在數據與分析領域，稽核部門藉由其可存取整個組織數據的獨特優勢，有可能成為持續監控與異常偵測的領導者。

2. 經濟動盪下內部稽核的調適作為

內部稽核職能面對當前經濟的不確定性，須保持高度的敏捷性，主動關注地緣政治與經濟環境的變化，並理解其對組織的具體衝擊。稽核部門須不斷調整其方法論與稽核計畫，以應對因應動盪而產生的業務流程變更（例如資金流動性計畫或產品定價策略的調整），並透過健全的持續監控計畫，深入瞭解業務單位如何協助客戶渡過難關，以及追蹤關鍵風險指標，如商業銀行的授信違約率或抵押品追繳狀況的變化。當辨識出風險升高的領域時，內部稽核人員可運用如「目標性審查」（targeted review）等工具，迅速介入並提供管理階層有關控制措施有效性的確信。此外，因應外部環境的複雜性，稽核部門需要透過簡化內部流程、導入新技術等方式提升效率，並將節省的時間與資源投入可創造更高價值的領域。

3. 內部稽核回應利害關係人期望的作法

隨著利害關係人期望的演進，稽核長的角色已由過去提供「後見之明」（hindsight）的傳統稽核，轉變為提供「洞見」（insight）與「遠見」（foresight）的策略顧問，不僅要評估現況，更要預見業務未來的走向與潛在風險。為達此目標，建立並維護與各方利害關係人的穩固關係，已成為稽核長的首要職責，而這有助於將稽核部門打造成值得信賴的顧問。內部稽核人員藉由其橫跨整個組織的獨特視角，可針對流程簡化、最佳實務等方面提供建議，或透

過早期介入（如在銀行審查新的策略時，由稽核團隊確保其控制環境在變革中維持穩定，並將潛在風險降至最低），以滿足多元利害關係人的期望。

4. 內部稽核實務的轉型與創新

講者提及稽核部門正在制定涵蓋未來 1、3、5 年的策略藍圖，並以此規劃所需的創新方向。前述「創新」的定義廣泛，不僅包含新技術的導入，更涵蓋任何能簡化流程、優化方法論及提升報告效率的新思維與新做法。又講者指出，其稽核部門為推動轉型，已成立如「策略轉型辦公室」等專責團隊，負責引導整個部門的變革之旅，並設定如在 5 年內實現年度稽核計畫流程自動化的宏大目標，而轉型促使效率提升所節省的資源，可再投資於創新活動。然而，創新不僅是專責團隊的任務，更重要的是培養一種「由下而上」的員工主導式創新文化 (citizen-led innovation)，鼓勵團隊中的每一個人提出改進想法，並透過如設立白板牆等簡單工具，使創新成為日常工作的一部分，而非額外的負擔。

5. 變革時代下的領導力

在當前快速變革的環境中，領導力要展現清晰 (clarity)、同理心 (empathy) 與適應性 (adaptability) 等 3 個核心特質。領導者須對團隊的願景與策略有清晰的闡述，同時，須以同理心傾聽團隊成員的觀點，在變革中成為支持的力量，此外，更要展現適應性，樂於接受回饋並隨時調整自身的方法與策略。然而，所有領導作為的基石在於「人才」，吸引、發展、留住並賦能頂尖人才是最重要的任務，而賦權是其中的關鍵，領導者不僅要鼓勵團隊成員勇於承擔與決策，更要透過簡化方法論、減少不必要的核准層級等實際行動，為其創造一個真正能夠負責與自主的環境。最後，領導者應鼓勵稽核人員保持好奇心、擁抱變化，並善用稽核單位獨有的跨職能洞察力，促成內部稽核的轉型。

(二)引領未來：新世代稽核人才的吸引與留任策略（CS5-1 Engaging Tomorrow: Strategies For Attracting and Retaining The Next-Gen Auditors）

本場次由加拿大政府內部稽核專案負責人 Perla Habchi 女士（圖 36）主講，主要探討稽核專業的變革與人才斷層危機、建立行銷策略與重塑招聘思維，以及透過文化與賦權留住新世代人才等核心議題。

1. 稽核專業的變革與人才斷層危機

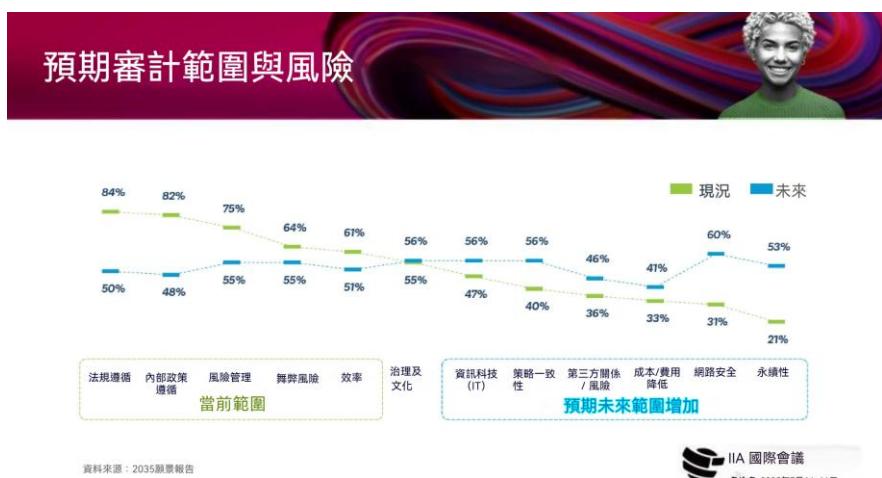
依據 IIA「內部稽核：2035 願景報告」的調查結果，超過一半的受訪者認為到 2035 年內部稽核人員的角色將會發生實質性或非常大的變化。隨著風險環境快速演變，未來的稽核範圍呈減少趨勢者包括：法規遵循、內部政策遵循、風險管理、舞弊風險及效率等領域，而呈現增加趨勢者則包括：網路安全、永續性、策略一致性、第三方風險、資訊科技及成本與費用降低等領域，另治理及文化領域則維持其屬重要稽核議題的趨勢（圖 37）。此外，由全球前五大風險的發展趨勢可見，2024 年前五大風險分別為網路安全、業務持續性、人力資本、

圖 36 加拿大政府內部稽核專案負責人 Perla Habchi 女士



資料來源：IIA 網站。

圖 37 未來審計範圍及風險



資料來源：2035願景報告
IIA 國際會議
多倫多-2025年7月14-16日

資料來源：2025 年 IIA 國際研討會。

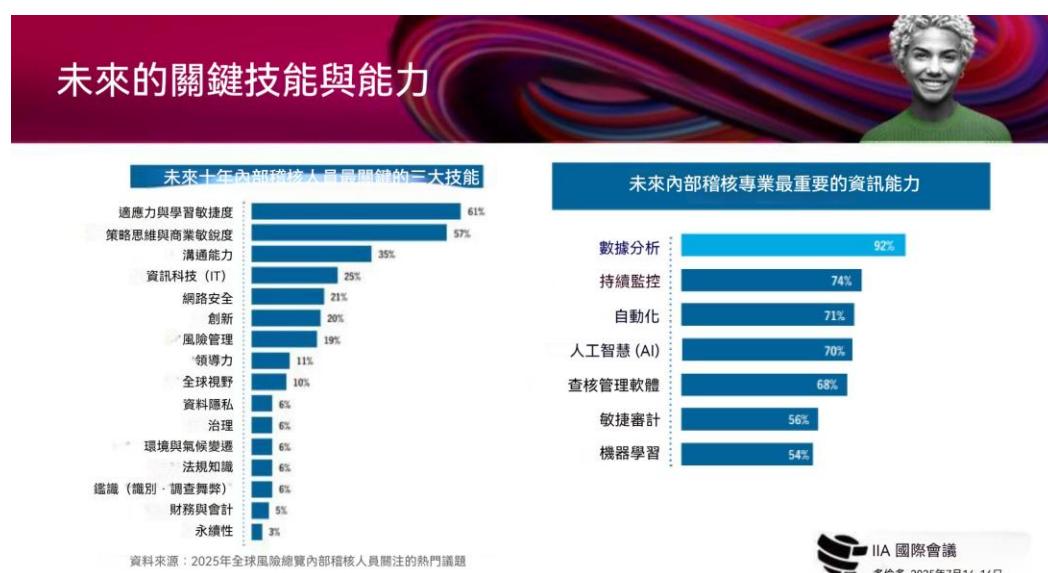
數位變革（含 AI）及法規變更，而由 2023 年至未來 3 年的變化趨勢可見，氣候變遷的風險排序由 2023 年第 14 名上升至 2024 年第 13 名，未來 3 年更上升至第 5 名，數位變革（含 AI）的風險排序則由第 5 名上升至第 4 名，未來 3 年則上升至第 2 名（圖 38）。講者並認為數位變革未來的風險排序將升至第 1 名，成為內部稽核人員要面臨的第一大風險，網路安全則將是第 2 名。

圖 38 未來審計範圍及風險



資料來源：2025 年 IIA 國際研討會。

圖 39 未來內部稽核人員的關鍵能力



資料來源：2025 年 IIA 國際研討會。

又傳統的遵循性查核已不足以應對挑戰，稽核人員被要求具備更廣泛的技能，如適應力與學習敏捷度、策略思維與商業敏銳度、溝通能力、資訊科技及網路安全等能力（圖 39）。然而，於此同時，稽核專業正面臨嚴峻的人才危機，且大量隸屬戰後嬰兒潮世代的資深稽核人員預計在未來十年內退休，此將留下龐大的職位空缺，因此，建立新世代的人才管道為稽核專業刻不容緩的任務。

2. 建立行銷策略與重塑招聘思維

內部稽核長期以來是個「最好保守的秘密」（best kept secret），此為造成人才管道薄弱的根本原因。大多數學生在大學時期對內部稽核一無所知，許多從業人員更是偶然踏入此領域。要扭轉此局面，稽核專業須採取主動、長期的策略性行銷。其中的關鍵是與學術界建立深厚的合作關係，稽核從業人員應主動走進校園，透過與職涯中心合作、進入課堂分享、舉辦座談會等方式，直接與學生互動。講者分享自身經驗，當其向學生詳細介紹內部稽核的職涯發展、工作生活平衡、差旅及薪酬等優點時，超過 7 成的學生表達高度的興趣，此證明只要有效傳遞資訊，內部稽核對年輕世代是極具吸引力的職業選項。此外，為應對未來的稽核需求，組織須擴展招聘的人才庫與背景，不再侷限於會計、財金背景，且因應數據分析、網路安全等稽核重點，應積極招募具備電腦科學乃至溝通專業等背景的人才，以打造一個具備多元技能互補的「夢幻團隊」；其次，須將實習計畫視為長期的策略性投資，而非短期的臨時人力，為實習生規劃有意義的學習路徑，並建立從實習銜接至正職的管道。

3. 透過文化與賦權留住新世代人才

成功吸引人才後，留任的關鍵在於創造正向且有意義的工作體驗。組織應致力於營造一個具協作、創新且富含情緒智商的文化，又有效的導師制度與入職計畫也相當重要，其能協助新進人員快速融入團隊，對年輕世代而言，最有力的激勵是賦予他們真正有意義且具影響力的工作，並讓他們看見自己的貢獻。講者以自身的實習經驗為例，當看到自己分析後寫下的一句話被完整納入最終稽核報告時，所得到的成就感成為其決心投身內部稽核專業的關鍵。

四、能力建置相關議題

激發潛力及邁向卓越：新版內部稽核職能框架（CS1-1 Unlocking Potential and Elevating Excellence: A New Competency Framework to Promote Achievement）

本場次由 IIA 專業準則負責人 David Petrisky 先生（圖 40）與 Palo Alto Networks 稽核長 Emre Alrpargun 先生（圖 41）共同主講，內容介紹 IIA 最新發布的內部稽核職能框架，並

探討準則遵循與框架的價值、新版職能框架的設計理念與核心架構，以及框架應用的實務作法等核心議題。

1. 準則遵循與框架的價值

IIA 於 2025 年 7 月發布新版內部稽核職能框架，其為協助稽核部門與人員具體實踐全球內部稽核準則要求的實用工具。該框架開發團隊於擬訂新的職能框架時，先行檢視全球內部稽核準則第三個領域「管理內部稽核職能」的 3.1 及 3.2，該 2 項要求提及與內部稽核實踐及與組織優先事項等相關的能力。基此，該框架設計 4 個層次的能力類別，並與準則中的概念直接對應，其中內部稽核、專業等 2 項與稽核實踐相關，而治理與風險管理、營運（領域知能）等 2 項與組織優先事項相關。又準則 3.2 強調持續維持與發展技能及取得專業認證的重要性，該框架透過建立 4 個熟練度級別（基礎、中級、高級、專家）將此概念具體化。此外，特別強調專業職能的重要性，此包含專案管理、應對衝突等軟技能，這些技能是內部稽核人員成為組織策略顧問、

圖 40 IIA 專業準則負責人 David Petrisky 先生



資料來源： II A 網站。

圖 41 Palo Alto Networks 稽核長 Emre Alrpargun 先生



資料來源： II A 網站。

提供卓越建議的關鍵，而此在 AI 快速發展的背景下尤為重要。另該框架對稽核長履行職責提供多方協助，其提供一套具體的工具，協助稽核長評估團隊當前的技能狀況，並規劃如何提升技能以滿足準則要求，並協助稽核長盤點團隊現有的技能，作出更明智的資源決策，也引入「職位角色概況」的概念，協助稽核長為不同職位，設定清晰且不同的能力期望，此外，框架的應用有助於支持稽核職能遵循相關準則的聲明，並協助稽核長達成品質評估的任務。

2. 新版職能框架的設計理念與核心架構

新版職能框架（圖 42）是一套連結全球內部稽核準則、個別稽核人員與組織需求三者的全面且可客製化工具。其核心架構由職能類別（Competency Categories）、熟練度級別（Proficiency Levels）與職級別期望（Job-Level Expectations）等三大要素組成。在職能類別方面，框架涵蓋內部稽核、專業職能、治理與風險管理，以及營運（領域知能）等 4 大領域。在熟練度水準方面，框架將能力由淺至深分為基礎、中級、高級與專家等 4 個等級，並提供具體的行為特徵描述，以減少評估時的模糊性與猜測，值得注意的是，若稽核人員的能力要由較低級別提升至高級別，不僅要予以培訓，更需要其在實

圖 42 內部稽核職能框架



資料來源：2025 年 IIA 國際研討會。

際工作中展現與應用相關技能。在職級別期望方面，提供基層稽核人員到稽核長，乃至於審計委員會成員等不同角色，各個層級所需能力的參考基準，有助於促使組織對內部稽核職位的要求符合市場人才供給狀況。

3. 框架應用的實務作法

為促進框架的實際應用，IIA 提供一套可操作的 Excel 範本，對個別稽核人員而言，該框架如同一個「職涯 GPS」，內部稽核人員可利用範本 A3 進行能力、培訓與發展、績效評估與晉升等面向的自我評估，並以此為基礎，與主管展開更具體、更有數據支持的職涯發展對話，此過程在結合主管回饋後，有助於客觀辨識能力落差、設定清晰的發展目標，並規劃個人化的培訓計畫，為晉升提供明確的路徑。另稽核長可透過範本 A4（圖 43）進行「集體職能評估」，取得一份完整的團隊技能盤點清單，以利擬訂策略與規劃資源配置，其能清晰揭示團隊現有能力與未來稽核專案所需技能間的落差，進而為聘用新人才、內部培訓或決定委外等決策提供依據。

圖 43 集體職能評估



- 集體能力評估
 - 過去及現在期間。
- 策略規劃
 - 下一階段的目標及策略計畫。
- 資源規劃
 - CAE 應採取提升技能或獲得足夠資源的行動。
- 向董事會及高層管理層報告
 - 總結集體能力評估結果及與策略相關的資源計畫，並記錄持續改進情形。
- 任務資源
 - 比較任務需求與個別評估 (A3)。



資料來源：2025 年 IIA 國際研討會。

五、 人工智慧、資訊安全之議題

(一) 提升公部門內部稽核－主計長觀點 (CS1-6 Advancing Internal Audit in the Public Sector-Perspectives from Comptroller Generals)

由 JC Singili 擔任主持人，並邀請到加拿大安大略省主計長 Beili Wong、新加坡主計長 Esther Wee 、加拿大主計長 Annie Boudreau 共同就內部稽核與組織目標之對齊等五個面向，擇要分述如次：

1. 內部稽核服務與公部門目標對齊之策略

Beili 指出「良好的治理」是讓內部稽核發揮戰略價值的關鍵，安大略省推動了一項改革，集中內部稽核資源並建立三級稽核委員會架構，將風險管理引入政府部門，連結政策、預算與支出，進而確保政策與服務能有效交付給民眾。透過這樣的整合，內部稽核是決策者的重要顧問。Esther 分享新加坡公部門內部稽核之作法，聚焦共享服務，由會計總署直接向小型機構提供內部稽核，同時任命跨部門首席內部稽核長來協調審計規劃、風險評估與人力管理，另強調公共部門的低風險容忍度，內部稽核需注重合規測試、成本效率與資產保障，以滿足納稅人對公共資源之期望。Annie 強調內部稽核應超越合規角色，成為提升效率與課責的策略夥伴，關鍵策略包括將稽核融入組織戰略、以風險為基礎擬定稽核計畫、定期與高層溝通，並善用數據發現異常與提升效率。最重要的是強化課責，確保稽核建議能真正落實，轉化為具體行動，進而提升政府治理效能與透明度。

2. 新興技術與創新實務的應用

Esther 分享審計方式的數位轉型，透過數據分析、RPA、Python 分析大量交易、採購數據找出異常，應用生成式 AI 檢索大量文件資訊、準備備忘錄或草擬報告，有助減少例行性工作。Annie 以加拿大聯邦預算要求橫向採購稽核為例，使用生成式 AI 整合風險分類、政策框架與以前年度稽核發現，有效縮短稽核期程，強調技術賦能團隊而非取代。Beili 則補充創新不僅限於技術，

更是一種心態。稽核人員應保持「客戶零號」的思維，先從自身流程著手，用於改善內部工作效率，再延伸至外部。他認為，真正的創新在於持續尋找更好的方法。

3. 有效溝通與視覺化工具

Esther 分享新加坡透過稽核系統蒐整所有稽核紀錄與報告，並建置儀表板，回顧控制缺失，並辨識常見風險領域，提供稽核委員會洞察系統性問題，強調內部稽核應提前瞻性意見，防止重複錯誤並改善治理。Beili 說明視覺化工具只是手段，最終目的仍是「提升影響力」，在安大略省，稽核團隊除了提出個別機關報告外，另針對共通主題，整理分享給其他公務機關，因為「最好的學習往往來自他人的錯誤與經驗」。而 Annie 則強調高階主管的支持與關注之重要性，直接影響稽核建議之落實程度。

4. 內部稽核之協作與專業發展

Beili 分享安大略省設立主計長學院，提供公部門財務人員、風險管理人員與稽核人員培訓與職涯發展，並強調跨界交流。Esther 透過功能領導角色發展橫向職能如財務與內部稽核，設立學院提供基礎、中階與領導課程，制定能力框架指導培訓路徑，建立內部稽核入口網站分享工具與指南，舉辦年度圓桌會議與集團首席內部稽核師網絡討論新興風險與專案，混合自下而上與自上而下方法，目標打造統一公共部門內部稽核以提供客觀洞察強化治理與政策成果。Annie 認為秉持「好奇心」是內部稽核人員不可或缺的素養，近年透過會計長、內部稽核長之領導層會議，促進合作與對談，知識共享，以提升專業服務。

5. 未來稽核人員的核心能力

Beili 認為是「好奇心與開放心態」，並強調軟技能的重要性；Annie 以一字「勇氣」可使稽核人員面對挑戰與推動改變；Esther 選擇「信任」，並分享早年經驗，指出主管在外部保護下屬讓她體會到信任是建立專業關係的關鍵。

(二) 次世代稽核人員：在人工智慧浪潮中生存 (CS1-8 NxtGenAuditor: Surviving the AI Impact)

由德國 Zappliance 執行長 Alexander Rühle 主講，探討 AI 對稽核專業的影響、新一代稽核人員需具備核心特質等，擇要分述如次：

1. 為衝擊做準備

講者強調 AI 已對稽核專業帶來轉變，許多稽核人員仍試圖逃避，這是過時的思維。如同微軟每 6 個月發布重大更新，持續重塑技術環境，稽核人員需轉變心態，積極為團隊轉型做好準備，成為「次世代稽核人員」(NxtGenAuditor)。講者鼓勵稽核人員可透過一面「鏡子」來反思自己的現狀，思考所處位置、期望達成的目標，或希望成為的樣貌，藉此正視 AI 帶來的機遇與挑戰，並擺脫既有觀念束縛。

2. 次世代稽核人員 3 個關鍵特質

(1) 人性思維 (Being human)：過去內部稽核角色為「觀察者、確信者、顧問」，而現在應將「幫助組織建立治理的信任」作為稽核任務，這是思維上的轉變。

(2) 精通科技 (Tech-savviness)：次世代稽核人員必須具備精通科技的特質，將 AI 視為工作與治理中不可或缺的夥伴。首先，需建立安全的試驗（沙盒）環境，鼓勵在日常工作中嘗試探索 AI 可能性與限制。其次，AI 應該被視為每一項決策和流程中的成員，稽核人員必須能解釋為何不使用 AI，而不是再去論證是否要使用。最後，把 AI 當作「人」來對待，明確指示、期望管理，培養長期合作的默契。

(3) 執行 (Execution)：次世代稽核人員要具備執行力，不能再依賴「獨立性」作為保護傘，而是要以「建立信任」為首要目標，勇於在治理風險產生時採取行動。必要時可暫時協助設計或測試解決方案，再移交給第一或第二線，重點在於確保信任而非僵化的角色界線。執行力係

將稽核成果視為自己的產品，並以客戶為中心，提供可落實的價值。過去內部稽核因不承擔責任而保有安全感，但這不再是生存之道。唯有展現行動力、責任感與能交付具體成效的能力，稽核人員才能在 AI 時代中突顯其專業價值。

3. 以實務案例給出行動建議

- (1) **案例 1—The Boys of Audit**：展現新世代稽核人員「玩中學」的精神，三位專業人士運用生成式 AI 創作音樂與影片，打破稽核嚴肅刻板印象，強調實驗過程重於成果完美。此案例凸顯稽核需具備人性、創意與執行力，並透過 AI 互動理解其潛力與限制，培養勇於嘗試與行銷專業的能力。最終，這樣的轉變有助於提升組織對治理的信任。
- (2) **案例 2—DIIR Working Group**：德國內部稽核研究所（DIIR）以小組實驗活動證明，AI 可顯著提升稽核專業協作與產出效率，透過即時轉錄、短時間完成創作成果，稽核人員不僅展現了溝通、同理與解決問題等人際技能。稽核應回到本質—用心「聆聽」與理解，並透過科技強化這一能力。同時，主管應提供「安全的 AI 試驗場域」，鼓勵團隊實驗與學習。未來稽核產出可能不再只是一份靜態報告，而應能根據需求轉換成播客、簡報或其他形式，實現真正以客戶為中心的服務，並強化治理信任。
- (3) **案例 3—使用 Triple AI 稽核手動分錄**：傳統稽核手動分錄需要分析龐大的交易數據，Triple AI 第一步由 Data AI 篩選可能存在風險的手動分錄，接著 Document AI 核對分錄與數位化原始憑證資訊是否一致、最後由人工專業判斷，稽核樣本從 160 萬筆縮減需人工檢查的 84 筆，大幅提升效率並降低誤判。展現次世代稽核人員應具備的人性思維（保持人類專業判斷）、科技敏感度（靈活運用 AI）、執行力（交付可落實的解決方案）。

(三) 超越效率：稽核自動化的策略力量 (CS2-1 Beyond Efficiency: The Strategic Power of Audit Automation)

由沙烏地阿拉伯 Elm 公司內部稽核 Abdulaziz Al Hidery、Saifeldin Ali，分享 Elm 公司內部稽核部門驅動公司數位轉型之經驗，擇要分述如次：

1. 內部稽核使命與轉型動機

五年前，Elm 內部稽核團隊透過各方建議與內部討論後，將「成為組織變革的關鍵代理人」設定為使命，旨在驅動公司轉型；首先須改變內部稽核自身，包括心態、方法、流程和稽核產出；傳統稽核作業係基於年度風險評估，排定稽核計畫並執行，提出稽核發現並追蹤，雖然有效但無法滿足快速變化之公司環境，因此轉向「即時稽核」。

2. 改變稽核頻率

為提升稽核頻率，以「完成一次傳統稽核後」為切入點，依據觀察與數據分析結果，擇選適合透過數位工具自動化且具高價值之稽核項目，改為季度稽核，彈性採用靈活稽核週期。根據經驗，將自動化稽核結果分為 3 類，以避免過多郵件通知干擾：

- (1) 直接觀察 (Direct Observation)：一旦測試結果異常，代表存在問題。
- (2) 警示訊號 (Red Flag)：結果顯示有潛在風險，需要稽核人員進一步調查。例如拆分採購單以規避授權規範，可能是異常，但仍需人工確認。
- (3) 洞見 (Insights)：屬於「值得瞭解」的資訊，但仍需要更多情境解釋，才能判斷是否重要。

3. 改變與管理階層溝通方式

推行自動化稽核後，最大挑戰是如何有效向管理階層傳達結果。直接通報稽核異常易引發反感，因此我們改變策略：先與支持單位合作建立信任，再優化報告內容，強調正面成果與整體確信，同時簡化呈現方式，改用一張投影片整合稽核重點，清楚標示異常與建議行動，便於追蹤，最終獲得管理階層認同並成為標準格式。

4. 導入 AI 應用案例

擇選自動化稽核的前提是「有沒有可用的結構化資料」，而「非結構化資料」之處理一直是稽核團隊稽核過程中最大的痛點，例如：合約文件以掃描 PDF 儲存不便使用（影像資料）、抽驗客服中心通話紀錄確認客訴處理是否有效（語音資料），只能人工檢查耗時易錯。AI 應用方式為語音轉文字、關鍵字提取（ex:部門名稱）、相似問題分群、生成結構化分析表，大幅縮減稽核人員時間，可針對關注案例深入檢視。另外，前面提及的警示訊號（Red Flag），我們也嘗試使用機器學習來協助，當稽核人員挑出 Red Flag 且調查後確實是異常，則將這筆資料標記為有異常，回饋給機器學習模型，希望透過 AI 完成第一層篩選；另稽核自動化過程失敗案例與調整（表 1）。

表 1 稽核自動化過程失敗點與解方

面向	失敗點	解方
領導思維	溝通不清晰，缺乏明確長期責任之界定。	目標清楚傳達、專注價值創造，並重視小成功之帶動。
人員	資料分析師缺乏稽核背景，稽核人員缺乏分析技能，溝通有障礙。	提升稽核人員的技能，並促進跨職能協作。
流程	稽核自動化工作是獨立進行，與其他稽核團隊的計畫脫節，導致自動化儀表板不符其他稽核團隊使用需求。	將連續稽核工作整合到稽核方法論中，使其成為稽核計畫的一部分。
技術	數位工具對一般稽核人員不友善，難以學習使用。	轉向使用更易於稽核人員學習和操作的工具。

資料來源：整理自 2025 年 IIA 國際研討會。

5. 小結

稽核自動化最大障礙是資料可用性與品質，然而完美乾淨的資料往往不存在，不可能等到資料「完全準備好」才開始，因此善用現有資料，並於報告中清楚揭露限制，例如備註「分析結果僅基於系統內可得資料，準確度約七至八成」。總結來說，有效推動數位稽核轉型的關鍵的方法就是：確立願景、爭取支持、強化能力、優化流程、擁抱新技術。

(四) 法律框架中之人工智慧：平衡創新、倫理與全球合規 (C2-4 AI in the Legal landscape: Balancing Innovation, Ethics, and Global Compliance)

講者 Imran Ahmad 是加拿大律師事務所資深合夥人，專長科技法律、資安、隱私與 AI。他指出 ChatGPT 推出後，有次與醫療產業客戶討論隱私與合規問題時，對方很快用 ChatGPT 生成法律建議，並請他(專業律師)確認，這反映一個現象，企業已將 AI 視為具效率與成本優勢的工具，不再完全仰賴傳統顧問，而會先透過 AI 獲得答案，AI 因此成為影響法律服務與醫療合規的新事實，專業人士需調整角色，兼顧效率與正確性，並意識到 AI 在市場滲透力。

1. AI 概論

AI 可簡單理解為三個要素：第一是「資料」，也就是蒐集的原始資訊；第二是「演算法」，像香腸製造機器般將資料運算；第三是「輸出結果」。資料品質與來源決定結果可靠性，但若資料不完整或偏頗，結果就會受到影響。例如法律領域中，美國判例量大，超過其他國家司法體系的案例，導致生成式 AI 的回覆偏向美國法。AI 可分為「狹義 AI」與「通用 AI」。狹義 AI（又稱弱 AI）只能處理特定任務，例如自駕車在同一條街道上反覆訓練能表現良好，但換到高速公路就可能失效。通用 AI（強 AI）則仍屬理論，理想上能模仿人類的廣泛認知。AI 技術的進展包含機器學習、深度學習與自然語言處理，例如臉部辨識、大型語言模型或語音助理等。

2. 法律問題與全球合規

許多企業與律師事務所已應用 AI 加速契約審查、合規檢查與資訊整理，提升生產力，企業客戶使用 AI 首要考量仍是「節省時間與金錢」。AI 伴隨之風險，首先，演算法可能反映或強化資料中的隱藏偏見，導致在貸款、招聘等決策上產生歧視，造成法律與倫理問題；其次，生成式 AI 存在「幻覺」風險，可能編造出看似合理但實際錯誤的答案，若被錯誤採信，後果不容忽視。舉例來說，曾有律師依賴 AI 尋找判例，並引用 AI 捏造的虛構案例，在法庭

上被揭穿並遭譴責，導致部分法院（如美國德州與加拿大聯邦法院）已要求律師提交文件必須經過正式來源認證。

自 ChatGPT 問世以來，全球 AI 監管歷經三個階段：初期的狂熱、隨後的恐慌，以及當前的監管需求。歐盟率先通過 EU AI Act，建立全面規範，涵蓋隱私以外的 AI 應用，被視為全球標竿；加拿大提出 C-27 法案與 AIDA 試圖跟進，但因國會解散而中止，僅部分省份如安大略、亞伯達有針對公共部門的規範；美國採取去中心化路線，聯邦不立法，由各州各自制定。這顯示全球 AI 法規處於多元與不確定狀態，未來各國將在「推動創新」與「避免風險」間尋找平衡。

3. 使用 AI 之控制措施

- (1) **盤點 AI 工具，依據接觸數據類型與敏感度判斷風險層級：**組織必須盤點並建立一份完整 AI 工具清單，確認工具是自行開發，還是向外購買，並釐清 AI 工具「接觸到哪些資料」，例如發票、員工個資所面臨的風險程度完全不同。
- (2) **建立 AI 導入框架：**AI 導入應避免零散，組織應設立跨部門小組共同建立框架，讓新 AI 技術能透過一套嚴謹流程進行審核，決定是否能導入，同時進行審查與追蹤。加拿大創新、科學與經濟發展部提出「先進生成人工智慧系統負責任開發與管理自願行為準則」，美國則有更完整的 NIST AI 風險管理框架，能協助組織評估風險並對應國際標準，框架化治理讓企業在推動創新與守法合規之間取得平衡，並成為未來法律防禦的重要依據。
- (3) **盡職調查：**AI 模型的訓練數據來源分為公開網路資料、合成資料與專屬資料，最大挑戰是 LLM 的不可逆特性，一旦數據被嵌入就難以刪除，若輸入錯誤或未授權資料，將難以補救。講者強調，組織導入 AI 工具時，必須將「資料來源與智慧財產權」列為首要盡職調查問題，確認廠商是否具備合法授權，否則將帶來重大的合規與訴訟風險。

4. 案例分享

以加拿大航空公司運用聊天機器人為例，乘客依聊天機器人指示申請喪親票價，卻因官方政策不同被拒，最終法院裁定航空公司必須承擔責任，聊天機器人回覆具法律效力（AI 工具的輸出必須視同企業行為）。此案突顯產品責任風險，即使有免責聲明，若資訊不清晰不足以保護消費者，企業仍需負責。因此建議納入審計與監督流程，透過 KPI 指標追蹤，如「出現多少次幻覺？」、「是否即時修正？」、「停機或故障頻率？」等，並依不同應用場景制定專屬監管方式。

又 OECD 早期提出資料保護的核心原則，包括公平、課責、透明，如今已成為 AI 立法的基石。這些原則正被各國納入隱私與 AI 監管中，藉此避免 AI 因資料偏差導致歧視。例如：在金融或招聘領域，若 AI 演算法因教育程度門檻而排除合格候選人，可能構成不公平差別待遇。加拿大先前提出的 AI 法案，就曾將此類系統列為「高風險」，必須嚴格監管。

至自駕車事故的責任歸屬極為複雜，若車輛全自動駕駛，車主多半僅為「被動乘客」，責任不大；若汽車硬體無瑕疵，重點會落在 AI 軟體；若軟體由製造商開發，責任可能由製造商承擔；若是第三方軟體，則可能由軟體公司負責，但仍視合約條款而定。實務上，事故發生後，受害者律師通常會「同時起訴所有相關方」，最後由法院判斷責任比例。此案例顯示 AI 技術導入後，法律責任更複雜，企業必須在產品設計與合約上提前釐清責任，以免陷入無止境的訴訟風險。

5. 小結

人工智慧應被視為一種「工具」，而非萬能解藥，它能提升效率、降低成本，但同時帶來偏見、幻覺、隱私與責任等風險。組織若要導入 AI，必須同時兼顧創新、合規與倫理。講者提醒組織應建立治理框架、強化跨部門合作、設立專責角色、持續監控與審計。AI 相關立法仍在演變，各國規範尚未統一，但若企業能先建立框架與最佳實務，未來即使法律落地，也能迅速調整而不需重建制度。

(五) 生成式 AI 時代下的網路安全治理 (C3-1 Cybersecurity Governance in a Gen AI Era: 30 Questions the Board and Audit Committee Should Ask)

講者 Tichaona Zororo 是企業 IT 治理、資安治理與稽核之專家，他指出資安稽核已成為稽核計畫的重要項目，但具備專業技能的人員仍極為有限。他認為資安應視為「商業議題」而非單純的「技術問題」，因為當發生攻擊時，真正承受衝擊的是業務運作與營運成果，而多數資安稽核報告仍以技術角度呈現，如漏洞數量，無法反應「風險層級」與「對業務的影響」等核心問題，致董事會難以判斷優先性與治理需求，因此，資安治理的首要挑戰，在於如何將技術性發現轉化為商業語言與治理決策，擇要分述如次：

1. 快速演變的威脅環境與治理

近期全球案例顯示資安事件已造成鉅額財務與營運損失，英國 M&S 遭攻擊損失逾 3 億英鎊，市值縮水 7.5 億英鎊，顯示治理不足的代價；南非 NHLS 攻擊事件則使公共醫療檢驗停擺數月，凸顯資安對公共服務穩定性的衝擊。另有 2024 年 7 月全球 900 萬台電腦「藍畫面」事件，雖非駭客攻擊，卻因變更管理不當導致大規模中斷，證明資安治理涵蓋內外部風險與流程控管。這些案例提醒董事會與審計機關必須將資安列為治理與合規核心，並以風險管理、稽核機制與資源配置確保韌性。

2024 年調查顯示資安已是全球首要風險，Uber 資安長因隱匿資安事件遭起訴，凸顯高階治理責任。生成式 AI 進一步推升攻擊手法，駭客運用深度偽造 (Deepfake)、網路釣魚簡訊 (Smishing)、語音釣魚 (Vishing)、AI 自動化及惡意 GPT 模型，讓非專業攻擊者亦能造成巨額損失，舉如中國企業 CFO 因 Deepfake 詐騙批准 2,000 萬元轉帳。新型威脅顯示資安不僅是合規議題，更是策略風險控管核心，需將 AI 駆動威脅納入治理架構、稽核計畫與合規檢查。

隨著威脅環境加劇，全球各地資安監管規範不斷強化。以美國為例，證券交易委員會 (SEC) 自 2023 年 7 月起規定，重大資安事件須於四個工作日

內揭露，透過 Form 8-K 報告事件細節，並在 Form 10-K 中揭露組織的資安策略、風險管理及治理架構。這意味著資安不再只是內部 IT 議題，而是直接與投資人資訊透明度、公司治理責任相連。

資安治理的本質是董事會與高階主管的責任，而非僅限於 CIO 或 CISO。其關鍵在於建立明確責任分工、設定風險胃納、制定全面資安策略並嵌入風險管理流程，並推動組織形成資安文化與多層次韌性。若董事會缺乏資安素養或未將資安列為治理核心，將導致策略缺口與重大風險。

2. 董事會應自我檢視的 30 個關鍵提問

講者指出，良好的資安治理有下列特徵，首先，董事會與高階主管需將資安列為固定議程，定期討論、審視並監督資安策略與執行情況。其次，應安排董事會與管理層接受資安教育與培訓，確保具備基礎數位素養與風險意識。此外，組織應定期舉辦資安事件模擬與演練，讓決策層與營運部門熟悉應變流程，確保發生攻擊時能迅速協調應對。董事會可透過 30 個核心提問強化資安治理，涵蓋政策與策略、風險胃納、資源配置、第三方風險及內稽能力（詳見附錄 2）。最終目標是建立組織韌性，讓資安成為支持業務持續與合規的核心力量，而非僅僅是被動防禦機制。

3. 個人資安防護要點

資安治理不僅屬於董事會與稽核範疇，也涉及個人的日常行為，建議採取多因子認證與強密碼管理，避免重複使用帳號與密碼，並保持系統與瀏覽器更新。同時應避免使用公共 Wi-Fi 處理敏感事務，並隨時鎖定設備螢幕。資訊安全方面，應謹慎處理陌生連結與附件，控制應用程式存取個資，並使用可信防毒軟體。財務交易宜使用專用電腦並定期檢查銀行帳號、信用評分與社群帳號，以降低詐騙風險。個人資安意識的提升與行為改進，不僅能保障自身資料與財務安全，也能強化組織整體資安韌性，成為合規與治理的重要基礎。

(六) AI 與 IA：如何有效應對同一體兩面的挑戰 (C4-1 AI and IA: How to Effectively Address Both Sides of One Coin)

主講者為加拿大皇家銀行創新、資料與分析副總裁 Kanika Vij、德國 Hugo Boss 首席稽核長 Oliver Petri，以及安永德國合夥人 Tobias Albrecht。三方分別代表高度監管的金融業、大眾消費品牌與全球審計公司，提供不同規模與監管情境下的觀點，擇要分述如次：

1. 內部稽核導入 AI 之動機

AI 涵蓋技術、模型、資料、隱私與合規等多重風險。稽核人員痛點為必須在有限的時間與資源下，快速理解新興風險，並在缺乏完整背景知識的情況下，確保稽核的一致性與品質；又被稽核單位也因外部環境快速變化，難以整合多份零散報告。Kanika 認為，AI 能協助稽核部門解決這些痛點，AI 可使稽核人員能更專注、迅速且清晰地處理海量資訊，提升工作效率與品質，也能為利害關係人提供更具洞察力、整合性的完整風險，而非片段的資訊。

2. AI 於稽核流程的應用機會

Kanika 指出，規劃階段可快速彙整法規、風險評估，協助聚焦高風險範圍；執行階段透過代理型 AI 按稽核人員設定測試步驟自動抽樣、測試與記錄，提高效率並確保一致性，仍需稽核人員覆核結果；報告階段 AI 可即時生成初稿、整合多份報告提供高層整體風險圖像。

Oliver 點出三個應用優勢，激發改變意願：透過 AI 工具快速產出優質結果，使團隊成員知道實用性，進而克服對新事物的抗拒。提升溝通效率：AI 預先摘要及翻譯文件，使稽核人員與受查單位溝通過程更流暢，有助於跨國團隊合作。輔助稽核規劃：依稽核人員角色提供完整提示，開發基於 Excel 生成式 AI 工具，可提供建立稽核方案。

3. 技術限制與風險

由於內部控制測試具有重複性與一致性，AI 工具能夠根據預設規則進行大量自動化處理，有效節省時間與資源，但 AI 缺乏情境理解，因此「人機協作」模式至關重要。稽核人員必須始終保持「人類參與流程」(Human-in-the-

Loop)，確保稽核的品質與最終判斷的準確性。為了確保 AI 模型的有效性，必須投資於文件管理系統，確保稽核資料的品質與可取得性，為 AI 應用打下穩固基礎。Kanika 強調金融機構須確保模型透明與可被稽核；Oliver 則指出大型語言模型雖可處理非結構化資料，但仍需審慎驗證，因輸出可能因模型與提示差異而出錯（幻覺）。

4. 稽核人工智慧系統（Auditing AI）

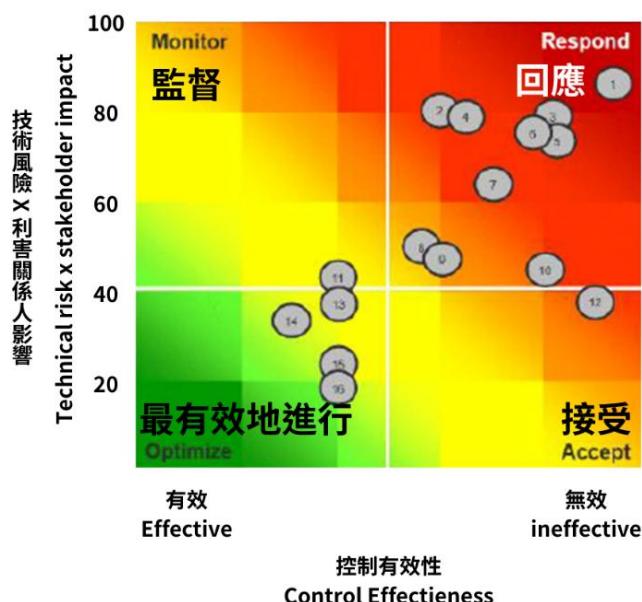
Tobias 提出稽核 AI 的第一步是全面盤點組織內 AI 應用並評估殘餘風險（圖 44），可參考公式考量技術風險與利害關係人影響，技術風險包含解決方案的目標、使用的技術與資料以及自動化程度；利害關係人影響則包含經濟、實體與法規層面。稽核 AI 的具體框架：先以風險熱區圖決定稽核優先順序，並從治理、風險管理、控制構面全面檢視（圖 45）。

圖 44 AI 殘餘風險評估公式

$$\text{AI Residual Risk} = \left[\text{Technical Risk} \times \text{Impact} \right] - \text{Control Effectiveness}$$

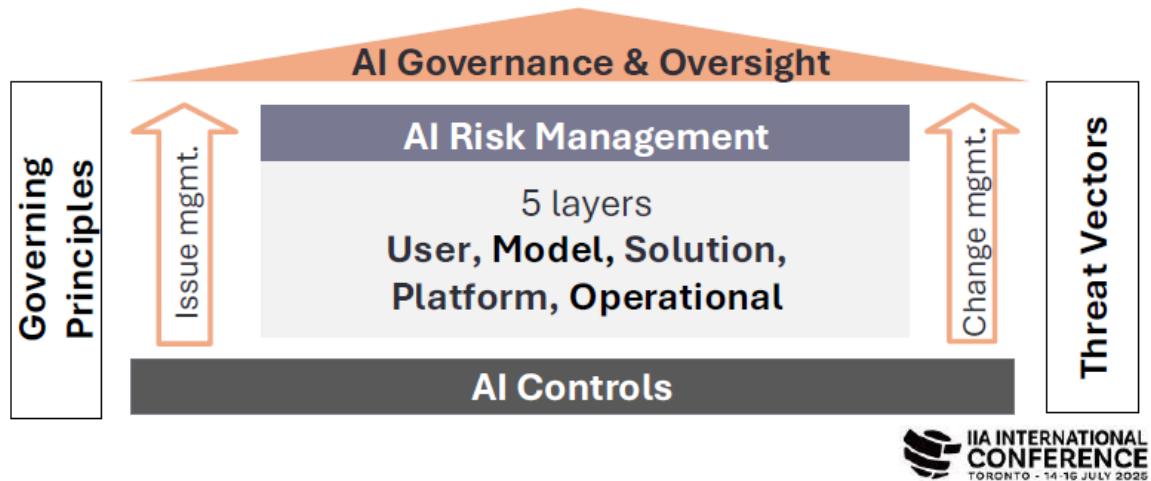
資料來源：2025 年 IIA 國際研討會。

圖 45 風險熱區圖



資料來源：2025 年 IIA 國際研討會。

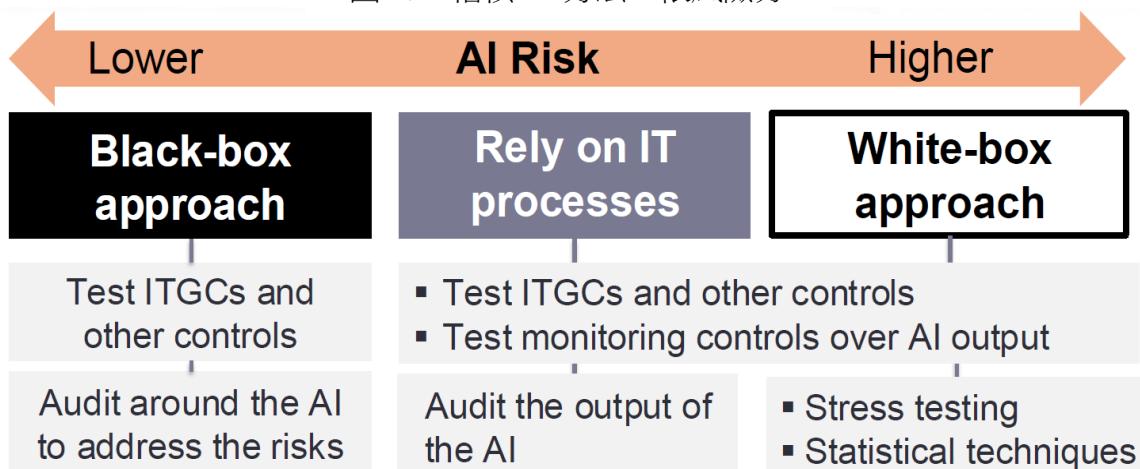
圖 46 稽核 AI 框架



資料來源：2025 年 IIA 國際研討會。

治理面，確認董事會與高階管理階層對 AI 建立明確的監督責任與決策架構，包含風險胃納、政策規範及與第三方廠商的角色分工；風險管理面，必須確保從使用者到模型的每一層都具備識別、評估、處理與監控機制，涵蓋使用者訓練、解決方案設計、平台資安及資料隱私保護，以便持續監督 AI 的表現與例外狀況；控制面，驗證內部控制有效性與持續運作，包括開發與維運人員的資格審查、完整的風險評估流程、資料治理與法規遵循，以及明確界定模型目標、邊界與偏差檢測機制，唯有三者協同運作並持續更新，才能確保 AI 系統在實務運用中符合法規、具備可稽核性並維持長期可靠的績效。(圖 46)

圖 47 稽核 AI 方法—依風險分



資料來源：2025 年 IIA 國際研討會。

稽核 AI 的方法按系統風險分為黑箱、灰箱與白箱三種層級(圖 47)，黑箱方法測試控制環境，忽略 AI 內部邏輯，於風險較低時採用；灰箱方法在測試控制環境基礎上，進一步監控 AI 的輸出品質並自行進行結果驗證，確保模型在持續運作過程中不會因資料或環境變化而產生偏差，適用於中等風險的系統；白箱方法除了測試控制環境與輸出，則要求深入演算法本身與資料處理邏輯，進行壓力測試、統計比對與跨模型交叉驗證，以確認模型決策的可靠度與公平性，這是高風險或關鍵性應用必須採取較高強度查核方式，而在實務上應根據系統的重要性與潛在影響選擇合適層級，並保留完整紀錄以確保稽核證據的可重現與法規遵循。

Oliver 分享團隊運用 AI 進行壓力測試與統計比對以驗證模型可靠度，並以服飾廣告為例，指出他們利用 AI 生成模特兒影像與影片，可依不同市場迅速更換膚色與背景，大幅降低攝影與設計成本，但同時帶來潛在的著作權侵害與公眾反彈風險，因此稽核程序必須檢視公司如何確保這些影像符合著作權與肖像權規範，以及如何與員工和外界溝通以避免因取代真人模特兒造成的勞動爭議與品牌損害；他又提到前任公司電商平台的「先買後付」服務，機器學習模型會評估客戶信用風險決定是否開放，稽核時刻意將性別與年齡等非模型變數納入分析以檢驗潛在偏差，雖結果僅顯示輕微差異，但這過程證明深入模型檢查對確保公平與合規至關重要。

5. 小結

Tobias 與 Kanika 強調 AI 的效率潛力需搭配稽核進步，培養質疑 AI 的人才並建立治理機制。Kanika 分享其銀行與本地公司合作，打造內部平台，確保資料不外流，依敏感等級設使用範圍，建立守則防外洩。針對 AI 輸出隨機性，Tobias 建議詳細記錄程序，交叉驗證結論，即使模型更新導致差異，完整文件可保稽核合規。最後，鼓勵以好奇心與批判思維用 AI 提升效率，強調 AI 是工具，需完善治理與風險管理，結合人類判斷與管控才能發揮其價值。

(七) 透過代理式 AI 強化內部稽核的未來準備 (C4-4 Future-Proofing Internal Audit With Agentic AI Solutions)

講者是柏林 Delivery Hero 科技公司之內部稽核 Liliana Staber 及 Zeyu Song，分享如何在稽核各階段導入科技，及示範自行開發的工具及其運作方式等，擇要分述如次：

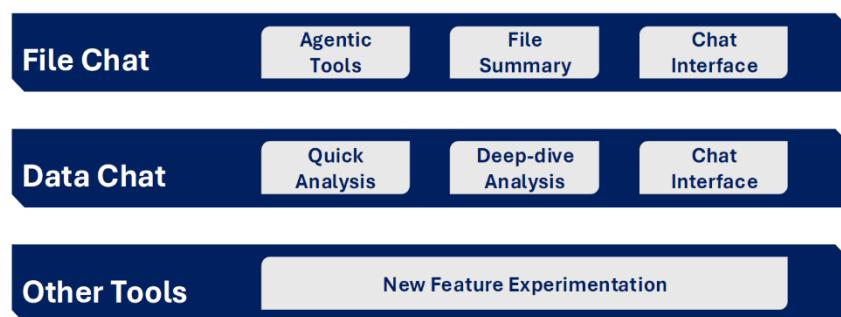
1. 自建 AI 工具的開發歷程

分為三個階段，**第一階段**是探索資料分析師隨同稽核團隊出差實地工作，親身體驗訪談與會議，並觀察稽核流程與需求，讓稽核與資料分析雙方可取得共識。**第二階段**是概念驗證，在工具中首先開發「文件對話」功能，使用者可上 PDF 或 Word 檔，系統即能自動摘要並進行互動問答，為稽核人員提供安全的試驗環境。**第三階段**是反覆迭代，定期召開工作坊與回饋會議，持續討論需求、改進功能，形成長期的循環開發模式，而非一次性的專案。

首次內部工作坊於 2024 年 12 月舉行，每年冬夏兩場，並於每季安排回饋會議，以確保開發方向符合實際需要。這些會議促進了雙方理解與共識，對工具的成熟度與實用性極為關鍵。目前工具主要具備三大核心功能(圖 48)：

- (1) **文件對話 (File Chat)**：作為知識庫，收錄歷史稽核報告與管理行動計畫，可快速摘要與翻譯文件，並進行互動問答。
- (2) **資料對話 (Data Chat)**：支援結構化資料分析，使用者可選擇快速統計或深度分析，系統能自動生成程式碼以供本地執行。

圖 48 自建 AI 工具三大核心功能



資料來源：2025 年 IIA 國際研討會。

(3) 實驗區（Other Tools）：測試與研發新功能的空間。

「Agentic(代理式)工具」可協助完成特定任務的功能模組，並交由 LLM 判斷是否在回應中啟用，以產生所需結果。這讓模型具備自主決定的能力，能依照提問選擇最適合的工具組合，內含 3 項主要功能：

(1) Google 搜尋：供模型在需要最新資訊時，能自行上網檢索並附上參考來源。

(2) 知識庫檢索：將歷次稽核發現及相關報告儲存在 Google Cloud，並與 Google Gemini 模型並透過企業合約串接 API（確保外部模型不會留存或訓練我們的內部資料），讓使用者可直接查詢過往議題與建議措施，系統會自動擷取關鍵字、比對文件並提供來源。

(3) 程式碼執行：與一般程式碼生成不同，允許模型撰寫 Python 程式，並在內建環境中實際執行。例如上傳一份文件清單後，只需提問「哪個部門被指派最多文件？」系統便會自行生成並運行程式，計算並輸出準確結果，甚至能偵測資料輸入錯誤，如部門名稱拼寫異常等。

稽核人員先以快速分析掌握資料概況並找出可疑權限組合，再透過深度分析自動產生程式碼進一步驗證；同時可利用知識庫查詢過往相似案例及建議的管理行動計畫，最後將所有資訊整合，由系統生成符合標準的觀察草稿，提升整體效率與品質。系統現行仍屬「輔助型」架構，AI 工具是整體流程的一部分，仍需人工監督與操作。但隨著技術成熟，模型將能在更高自主層級上決定任務步驟與工具組合，我們也積極探索多代理與流程協作框架，例如 LangChain 與 LangGraph，以支援更複雜的工作流程。

2. 小結

以漸進方式導入 AI 於稽核流程。從簡單可衡量的情境開始建立案例(重複性任務)；再透過探索、概念驗證與反覆迭代的三階段循環，持續蒐集使用者回饋確保符合實際需求；同時結合 AI 與非 AI 能力，可從知識庫搜尋、簡易程式碼生成等基礎功能著手；最後重視使用者體驗，透過定期工作坊與教育訓練加強跨部門溝通與實測，確保系統設計與操作貼近實際。

(八) AI 與內部稽核：創新來自更智能之文件互動 (C5-5 AI Meets Internal Audit: Innovating Through Smarter Document Interaction)

講者是來自美國 Crowe 會計與顧問公司合夥人 John Manilla，分享運用生成式 AI 以更聰明的方式與文件互動，擇要分述如次：

1. 文件智慧應用

生成式 AI 可在文件互動上帶來全新方式，例如：自動摘要、問題解答、文件比對、修訂標示、合規檢核、資料擷取、草擬新文件等。然而要獲得最佳成果，關鍵在於「提示詞（Prompt）」，問題問得越精準，答案越符合需求，以下是提示工程之技巧：

- (1) 系統提示/人格層級 (System Prompt / Personal Layer)：賦予 AI 專業背景，舉如「你是一名熟悉 IIA 標準的內部稽核專家」。
- (2) 查詢提示/使用者輸入 (Query Prompt / User input)：清楚描述需求，可簡可繁。
- (3) 格式提示/輸出結構 (Format Prompt / Output Structuring)：指定輸出型態，如段落、條列、表格，甚至可附上範例模板。
- (4) 互動式輸入 (Interactive Inputs)：生成式 AI 會詢問使用者一些問題，幫助細緻及精確的回應。

2. 工具與實務案例

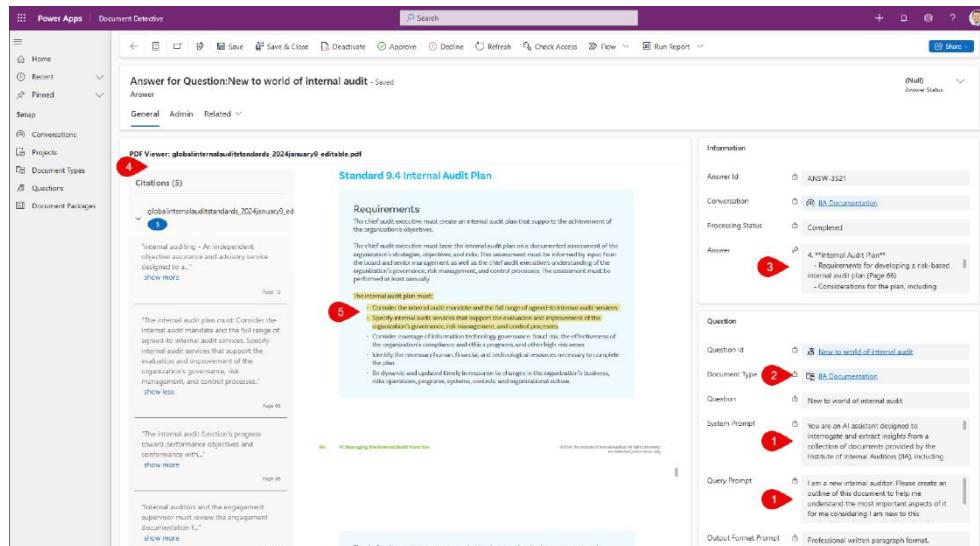
現場投票互動環節中，講者詢問與會者使用 AI 與文件互動的頻率，結果約有半數與會者每週至少使用一次，顯示此領域的關注度已相當高。近期 AI 產品與功能其實都圍繞相似概念，只是呈現方式不同。事實上，許多功能透過 ChatGPT Pro 或 Microsoft Copilot 就能先行嘗試，無須立即投入大量資金。另外講者分享「自建 PowerApp 串接 ChatGPT API」(圖 49)，係針對需大規模重複文件審查情境所開發之方案，透過這個介面，可定義並重複使用多組提示 (Prompt)，批次套用到大量文件。使用者可選擇每份文件個別分析，或將多份文件視為整體分析，並能直接輸出 Excel 或透過 API 傳送至其他系統，

最重要的價值在於其「可擴充性」與「可驗證性」：

- 產出結果皆附有來源引註，點擊即可跳轉至文件對應位置並以高亮度顯示，便於人工快速核對。
- 對需要多份長篇文件及多重問題的稽核任務，如貸款審查、補助審查等，可產出大量初步回答，節省時間，且保有人為審核的關鍵步驟。

講者並分享將這套 PowerApp 實際應用於反洗錢（BSA/AML）審查。美國銀行業須遵循「銀行保密法」及相關反洗錢規範，完整審查過程約需回答 500 個問題。專家將問題轉化為提示詞，並利用真實客戶資料進行測試與修正。最後，只要銀行提供 35 份相關政策與程序文件，我們便能一次性輸入系統，套用 500 個提示詞，大約二、三十分鐘即可產出初稿。稽核團隊不再需要從零開始，大幅節省時間與人力。

圖 49 PowerApp + ChatGPT API 與文件互動畫面截圖



資料來源：2025 年 IIA 國際研討會。

3. 運用 AI 進行文件分析的風險

講者指出，錯誤輸出（幻覺）、偏差、缺乏透明度、資料外洩皆是潛在風險。因應方式包括：保持人工複核、要求系統提供引註來源、使用符合合規標準的企業級解決方案、避免使用免費版本處理敏感文件（例如：客戶資料）、明確訂定組織政策，規範何時、何處可運用 AI，並建立驗證與治理流程。

(九) 駭入人性：超越科技的社交工程策略 (C5-8 Hacking the Human: Social engineering Tactics That Outwit Technology)

講者是偵測欺騙國際顧問公司執行長 Nejolla Korris，分享駭客常用的伎倆與心理操縱手法；瞭解社交工程不僅是為了竊取資訊，有時候也會誘導員工洩露特定部門或業務的細節；認識資安專家如何運用尖端技術偵測並阻止攻擊，進一步強化「人」的安全防線；學會如何將檢測人為脆弱性的措施納入組織防護中等，擇要分述如次：

1. 常見社交工程手法

「社交工程」本質是透過操縱或欺騙，取得系統、員工或資訊的存取權，不限於企業環境，個人也可能成為目標。

- (1) 尾隨進入 (Tailgating)：例如假扮送貨員、清潔人員或其他例行性角色，由於這些角色每天都會出現，且不會是同一個人，容易讓人誤以為他們具備進入權限。
- (2) 肩窺或偷聽 (Shoulder Surfing / Eavesdropping)：透過觀察他人操作或偷聽對話來取得資訊，這種手法容易發生在公共場合，例如電腦操作、ATM 提款或信用卡交易。
- (3) 網路釣魚或魚叉式攻擊 (Phishing/Spear Phishing)：最普遍社交工程手法，過惡意郵件或連結，誘使收件人點擊進而中毒，是駭客滲透的主要管道。另外，針對特定目標進行攻擊，透過社群媒體培養關係，建立信任（駭客的本質就是操縱人心），再發送精心設計的郵件，更容易中招。
- (4) 社群媒體滲透：社群媒體是社交工程師的「資訊寶庫」，無論隱私設定多嚴謹，駭客透過觀察公開資訊、偽裝身份並逐步建立信任，就能突破防護，須謹慎看待好友邀請與連結。
- (5) 心理操縱：權威、恐懼與急迫感、社會認同、建立情感連結、互惠、稀缺與從眾、漸進式承諾等。

(6) AI 與深偽技術：偽造聲音或影像以增加可信度。

2. 常見的心理操縱手法

- (1) 信任與權威：冒充可信任或具權威性的人物，例如上級主管、政府單位或知名機構，以此獲取目標信任。
- (2) 恐懼與急迫感：製造緊張或緊急情境，讓人來不及思考就迅速回應。
- (3) 社會認同：利用「大家都在做」的心態，誘使人跟隨群體行為。
- (4) 建立情感連結：透過長期互動或共同興趣培養關係，降低防備心。
- (5) 互惠心理：先提供小恩惠或免費資源，使對方覺得需要回報。
- (6) 稀缺與錯失恐懼：創造「機會有限」的氛圍，迫使人立刻行動。

3. 防範社交工程，建立組織對抗社交工程的韌性

在防範社交工程時，最重要原則：不要信任，而要驗證。懷疑精神是降低風險的最佳武器，單靠技術性解決方案並不足以全面防護。資訊安全不是IT部門的專屬責任，而是全體人員共同的義務。另外，社交工程培訓並非單一活動，而是需要長期規劃與持續更新。對內部稽核可切入觀察的方向有：

- (1) 將社交工程納入稽核範疇：檢視組織是否建立相關政策與流程。
- (2) 定期風險評估：找出組織在流程與人員管理上的潛在弱點。
- (3) 檢視教育訓練：確認培訓內容是否完整，並能因應最新威脅。
- (4) 測試防護成效：透過模擬或事件紀錄，分析攻擊模式與員工反應。
- (5) 推動責任文化：確保組織各層級都能理解並承擔資訊安全責任。

4. 小結

社交工程風險不斷演化，內部稽核應推動將其納入制度化管理，並透過全員訓練讓員工成為「資安守護者」。實體課程與線上模擬可增強警覺力，避免釣魚郵件與假冒連結得逞。核心原則是「保持懷疑，先查證再行動」，花幾分鐘驗證即可降低重大損失。高階主管雖繁忙，更應納入完整培訓，因其常為攻擊首要目標。唯有建立「不輕信、必驗證」文化，才能全面提升組織韌性與資安防護力。

伍、參訪加拿大審計與課責基金會紀要

一、簡介

加拿大審計與課責基金會（Canadian Audit and Accountability Foundation, CAAF）是一個致力於強化公部門審計與課責，並高度專注於績效審計專業領域的非營利組織（圖 50）。CAAF 雖為獨立於加拿大審計長公署（Office of the Auditor General of Canada, OAG）的機構，但其員工多曾任職於 OAG，因此具備豐富的實務經驗與專業。CAAF 的服務對象不僅涵蓋聯邦、省及市級政府的外部審計人員與內部稽核人員，亦包含國會的公共帳目委員會等關鍵監督機構，以提升審計報告的最終使用效益與課責循環的完整性，其透過包含專業訓練、研究與諮詢等服務，協助建構審計人員的核心能力。又為擴大審計工作的影響力，CAAF 特別強調與公民社會組織（CSO）及媒體的互動，以確保審計工作能真正回應公民需求，並對社會產生正面影響。

圖 50 CAAF 簡介



資料來源：CAAF 簡報。

二、參訪過程及討論議題

圖 51 出國人員與 Sharon Clark 女士合影



資料來源：出國人員自行拍攝。

本次參訪係由 CAAF 專業發展部門副總裁 Sharon Clark 女士及國際發展計畫副總裁 Caroline Jorgensen 女士負責接待（圖 51），參訪前經擬具四大面向、14 項討論問題送 CAAF 參考，其中部分問題並由受訪者轉洽 OAG 相關人員提供意見。又參訪過程經視討論情形調整問題內容及討論深度，謹將討論內容分類說明如下：

（一）國際合作

CAAF 自 1980 年成立迄今 45 年來，持續推動加拿大政府資助的國際發展計畫，該計畫協助其他國家審計人員至加拿大進行為期數個月的深度研習，並實際參與加拿大審計團隊的查核工作（現為完成四個月線上專案及五個月實體參與）；自實施以來，已有來自 54 個國家、288 位審計人員參與，其中許多學員已在其機關擔任績效審計工作的管理職務，此外，舉如曾協助盧安達的績效審計業務規模擴增一倍，並促使蓋亞那為其新興的石油與天然氣產業成立一個完全由結業學員組成的專責審計部門等，均為該計畫的成效。另 CAAF 於 2025 年啟動一項新的國際發展計畫—「包容性公共服務的治理、課責及透明度計畫」（Governance, Accountability, and Transparency for

Inclusive Public Services, GATIPS)，此計畫的期程為 4 年 (2025-2028)，參與對象為泰國、越南等 10 個國家最高審計機關的資深審計人員，並針對特定主題或專案計畫（如數據分析領域）獎助，此計畫的參與者須擬訂查核計畫，其查核項目並須符合重點關注領域（表 2），此外， CAAF 會提供參與者在地國的培訓課程，並強化導師指導與支持。另該計畫強調 CSO 的參與，由 CAAF 提供 CSO 參與的輔導與培訓，並協助參與的最高審計機關共同辨識需要邀請參與的 CSO，且要求參與的最高審計機關須至少與一個 CSO 合作。為利計畫的執行， CAAF 已更新培訓教材，強調性別平等、人權、弱勢群體等議題，以呼應此計畫聚焦的主題，也透過文化導向及性別平等等課程協助新進參與者快速適應。

表 2 GATIPS 重點關注領域

重點關注領域	說明
1.性別、多元性與多重身分	• CAAF 基於過去在性別主流化與性別平等審計方面的相關經驗，將與最高審計機關合作，瞭解不同身分認同者如何受到相同政策的影響，並將此納入考量。
2.包容性與參與度	• 創造多元聲音不僅被傾聽，更能積極形塑成果的空間。 • 優先推動 CSO 參與，並為最高審計機關提供相關培訓。
3.人權	• 每個人皆應享有的自由，不因背景或信仰而異。 • 引導最高審計機關履行其作為人權守護者的職責。
4.氣候變遷與環境	• 涵蓋災害管理與預防（氣候變遷）等議題，以及採礦與農業（環境）等相關議題。

資料來源： CAAF 簡報。

（二）績效審計

1. 選案標準與決策流程

加拿大審計長法賦予 OAG 相當大的自由裁量權，其可決定查核單一政府計畫或活動（如農藥監管）、涉及多個部門或機關的職責範疇（如文化遺產保護），或影響眾多部門的議題（如資訊安全），亦可能將有助於提升政府成效（如財務管理與控制）或備受國會議員及國民高度關注（如國家安全）的事項納列關鍵審計議題。在決定查核議題時， OAG 關注的重點為聯邦機關面臨最高風險的領

域，而高風險領域包括耗費納稅人巨額資金或一旦出現問題可能威脅加拿大人民健康與安全的領域。OAG 績效審計選案的核心方法為一套系統性且以風險為基礎（risk-based）的策略審計規劃流程。此流程通常提前數年展開，由各專業審計小組（如國防、衛生、資訊科技審計小組）每隔數年進行一次，過程本身猶如「迷你審計」（mini audit），審計人員會檢視過去的查核報告、訪談機關人員並蒐集文件，以評估風險並提出未來 3 至 5 年的審計議題清單。前揭風險的評估為策略審計規劃流程的核心，審計團隊會考量包括：議題的經濟、社會與環境影響；國會議員及 CSO 等利害關係人的關注度；計畫本身的特性（如目標清晰度、作業與資訊系統的複雜性、是否為新興或有重大變革的計畫）；財務規模的重大性；受查機關對過往審計建議的回應情形；公眾及媒體的關注程度等多重因素（表 3），以評估組織或領域活動的重要性及其相關風險，進而辨識對國會及加拿大國民最重要且相關的議題。又 OAG 的選案流程保有彈性，以因應如 COVID-19 疫情等突發重大事件，國會的審計要求亦是考量之一，其占比已從過去約 5% 顯著上升（目前至少 15%），近期的案例包括針對 ArriveCAN 應用程式超支問題的系列查核。至於擇選議題的決策，則是先由審計小組的主管人員開會討論，並於會中審視各小組所提出之議題，並排列優先順序，再交由審計長與高階主管組成的委員會共同決定。

另 CAAF 分享其績效審計課程教材納列用以判斷議題重要性的「MATCHES」原則，此為一個協助思考民眾關切點的實用架構，涵蓋重大性（Materiality）、課責性（Accountability）、透明度（Transparency）、遵循性（Compliance）、健康與文化資產（Health and Heritage）、所有的 E 原則（Everything）以及安全與保障（Safety and Security）等面向（表 4）。

表 3 風險因子

風險因子	說明
1. 經濟、社會和環境影響	<ul style="list-style-type: none"> 評估議題在經濟、社會與環境等面向的潛在衝擊。 影響大量人口或弱勢群體，或影響環境永續性的計畫、活動或過程可能被認為對組織更為重要。
2. 與利害關係人的相關性	<ul style="list-style-type: none"> 考量國會議員及 CSO 等利害關係人對特定議題的關切程度。 立法機關或其他管理機關、組織管理階層或公眾展現的興趣可

風險因子	說明
	能顯示該活動對利害關係人的重要性。
3.公眾與媒體能見度	<ul style="list-style-type: none"> 關注媒體報導或從其他管道浮現的組織問題。 考量來自公眾的電子郵件及信函。
4.組織目標與宗旨的多樣性、一致性及清晰度	<ul style="list-style-type: none"> 目標的多樣性或不一致會增加組織活動或專案未能充分考慮經濟、效率、效果、環境及永續發展等一項或多項原則的風險。 組織目標與宗旨定義不明確，可能會增加因員工不理解而無法實現的風險。
5.計畫本身的特性(執行複雜性及管理資訊與控制系統的複雜性及品質)	<ul style="list-style-type: none"> 計畫目標的清晰度、運作與資訊系統的複雜性，以及是否為新成立或有重大變革的計畫，其中新計畫通常伴隨較高風險，複雜的系統可能更難開發、強化與維護，倘管理資訊系統維護不善，可能無法實施適當的控制。 組織營運複雜性增加時，可能會存在無法有效、經濟實現其目標或無法充分考慮環境或永續性的風險。
6.環境或組織變革的影響	<ul style="list-style-type: none"> 組織環境或組織的變化可能會影響營運的持續性及員工對優先事項與流程的理解，進而增加組織無法實現目標的風險。 環境變化包括新的政府優先事項、重大預算修訂及法律變更等；組織變革包括領導階層變動、重組、新措施與員工流動等。
7.金額重大性及性質	<ul style="list-style-type: none"> 巨額、高交易量及交易複雜性可能為組織帶來更大的風險。
8.受查機關對查核結果的回應	<ul style="list-style-type: none"> 受查機關對過往查核建議的回應與改善情形。若其管理階層尚未做出足夠改善，以解決過去績效審計提出的重要問題，則可能更重要且風險更高。
9.組織結構	<ul style="list-style-type: none"> 預算、薪資發放、支出、人力資源管理及設施管理等關鍵活動的集中化與分散化會衍生相關的營運風險。
10.執行方式	<ul style="list-style-type: none"> 專案的執行方式可能為直接提供商品或服務，也可能是重分配收入或委外辦理，相關風險的大小可能因執行方式而異。

資料來源：整理自 CAAF 訪談內容及 OAG 績效審計手冊。

表 4 MATCHES 原則

判斷議題重要性的面向		說明
M	重大性 (Materiality)	主要指金錢。
A	課責性 (Accountability)	政府對稅金使用的責任。
T	透明度 (Transparency)	民眾有權知道政府作為。
C	遵循性 (Compliance)	法規遵循性。
H	健康與文化資產 (Health and Heritage)	如歷史建築的維護。
E	所有的 E 原則 (Everything)	包含 經濟 (economy)、效率 (efficiency)、效果 (effectiveness)、環境 (environment)、公平 (equity)、道德 (ethics)
S	安全與保障 (Safety and Security)	如民眾的健康與安全。

資料來源：整理自 CAAF 訪談內容。

2. 績效審計範疇

依據加拿大審計長法，OAG 的職權不僅是查核經費是否依國會撥款目的支用，更明確擴及經費支用是否兼顧經濟與效率（due regard to economy or efficiency）、是否建立衡量計畫效果（effectiveness）的妥適程序，以及是否考量對環境永續發展的影響。此外，審計長法指出，審計長應於其提交下議院的報告中，報告其認為具有重要性及下議院應予注意的所有事項。基於法律的廣泛授權，使績效審計得以查核「政府所做的任何事」（anything government does），無論是否直接涉及金錢，只要該事項涉及政府的承諾與行動，OAG 都可加以查核。

實務上，許多績效審計報告可能僅在前言段提及計畫總預算，而報告內文則完全不著重於金額，而是深入探討對民眾的影響、施政成果、組織文化、服務提供、尊重及課責等質化議題。諸如「職場尊重」、「軍中性騷擾」及「敘利亞難民安置」等議題，雖皆涉及經費支用，但其審計重點在於政府是否履行其政策承諾，並達成預期的社會效益。此種廣泛的職權使審計機關得以深入檢視政府治理的各個層面，超越傳統上著重於金額的範疇。

3. 績效審計方法論與利害關係人參與

由於績效審計涉及主觀性與專業判斷，遠比財務審計的數字或遵循審計的是非判斷更為複雜，CAAF 特別強調團隊合作、傾聽多元觀點及正視個人偏見的重要性，以減少因主觀判斷可能帶來的偏誤。在方法論上，特別重視根本原因分析（Root Cause Analysis），其開設專門課程教導審計人員探究問題的深層原因，以確保查核建議能對症下藥，而非僅處理表面症狀。同時，亦強調將複雜的查核發現精煉為關鍵訊息，並以淺顯易懂的文字（plain language）撰寫報告，以提升與國會及公眾的溝通效益。

利害關係人參與是提升績效審計品質與影響力的關鍵策略。在查核過程中，OAG 強調自選案及發展查核標準的最初階段即與受查機關互動，透過早期溝通

建立互信的基礎，以降低其在查核過程中的抗拒心理，並提升對最終查核建議的認同與執行意願。此外，OAG 設立由外部專家組成的諮詢委員會，成員包括學者、退休官員、產業代表及非政府組織（NGO）等。例如在查核鮭魚養殖相關案件時，委員會同時納入環保團體代表與產業團體代表，以獲取衡平的觀點。

（三）永續發展目標審計

依據加拿大審計長法，永續發展是一個不斷發展的概念，基於社會、經濟及環境問題的整合，其實現方式包括：環境與經濟的融合；保護加拿大人的健康；保護生態系；履行國際義務；促進公平；採取全面的規劃及決策方法，考慮到不同經濟選擇的環境與自然資源成本，以及不同環境與自然資源選擇的經濟成本；防止污染；以及尊重自然與後代子孫的需要。OAG 對政府落實永續發展相關作為的監督職權，明訂於加拿大審計長法中，該法為一部關於 OAG 及永續發展監督與報導的法案，其要求審計長查核資金支出未充分考慮其對環境影響的重大事項，並訂有「永續發展」專節，明訂環境及永續發展委員長（CESD）的職責，包括監測永續發展，並報告指定單位在永續發展方面的進展。

加拿大在 2015 年承諾實現聯合國永續發展目標（SDGs）後，OAG 曾回顧過去十年的審計報告，並將其與相關的 SDGs 進行對應，目前 OAG 實務上已在所有查核工作中考量 SDGs，其標準作業要求提交新的審計提案時，須說明其與哪一項 SDG 相關，以將 SDGs 系統性融入其審計實務，並由 CESD 依審計長法明訂的職責，監督與報導政府在永續發展方面的進展。OAG 2025 年已（或將）發布包括氣候變遷調適、瀕危物種的重要棲息地、海洋管理、陸域保護與保育區、海洋保護與保育區等有關環境與永續發展議題的報告，前揭查核議題都與特定的 SDGs 有關（表 5）。

在氣候變遷議題上，此議題已成為國家與國際層級的重要焦點，國際社會普遍承認氣候變遷已無法完全遏止，而應強化社會的應對與韌性，因此，國際審計趨勢正由過去的「減緩」（mitigation）逐漸轉向「調適」（adaptation），OAG 已積極參與 INTOSAI 環境審計工作小組（WGEA）氣候行動相關工作計畫，其

一為運用氣候掃描儀(ClimateScanner)評估加拿大政府的氣候行動，於2024年向國會提出「2024年加拿大淨零排放課責法案」查核報告；其二為參與INTOSAI專業發展組織(IDI)及WGEA主導的「氣候變遷調適行動」

表5 加拿大環境及永續發展委員長近期查核報告

序號	報告名稱	攸關 SDGs
已發布		
1	國家調適策略	13
2	瀕危物種的重要棲息地	14、15
3	海洋綜合管理	14
4	加拿大永續發展實施情形的經驗教訓	—
將於2025年發布		
1	陸域保護與保育區	15
2	海洋保護與保育區	14
3	部門推行永續發展策略的進展	—
4	淨零課責	13
5	原住民保護區與保育區	11、15
將於2026年發布		
1	應對氣候變遷	13
2	辨識洪水風險區域	13
3	應對禽流感	3

資料來源：整理自OAG官方網站(截至114年9月27日)，其中未發布報告攸關SDGs為出國人員自行辨識。

(Climate Change Adaptation Actions, CCAA)國際合作計畫。

另OAG訂有「環境與永續發展指南：將環境與永續發展考量融入直接參與工作」，指引查核團隊透過風險評估，發現組織、政策或計畫存在的重大環境與永續發展風險，併同其他業務風險考量後，決定是否納入查核策略，及評估查核議題是否存在環境與永續發展問題，並依據評估結果決定是否納入查核範圍。

受訪者指出，聯合國SDGs為「上天給績效審計人員的禮物」，此乃基於SDGs提供全球公認的目標(goals)、標的(targets)及指標(indicators)，且各國政府均已簽署承諾，此為績效審計提供現成且具高度正當性的查核標準。而有關OAG對各項SDG進展的評估情形，其目前尚無系統性循環查核17項SDGs的機制，此可能是因加拿大聯邦政府、省級與市級政府的各層級審計長角色有所不同，且許多與SDGs密切相關的重要領域(如醫療與教育)主要是由各省負責，目前亦尚無整合各級審計單位進行聯合審計的組織架構。因此，儘管OAG期望能涵蓋大部分目標，或至少使每項審計工作都與一項SDG連結，但並未有

逐一審核所有目標的計畫，而是透過定期追蹤評估 SDGs 進度的情形，使用此資訊監控趨勢、盤點過去有哪些 SDGs 已進行評估，並考慮未來應該著重的領域。在查核 SDG 14（海洋生態）上，OAG 近年來頻繁查核漁業相關議題，並公開 CESD 向國會提交的相關報告包括整合性海洋管理查核報告（2025 年）、監測海洋漁獲查核報告（2023 年）、保護瀕危水生物種查核報告（2022 年）等，此議題的擇選不僅是因其屬聯邦管轄範圍，更有其於歷史、經濟、社會與環境等層面上具重大性的考量。

(四)組織文化審計

CAAF 深刻體認不健全的組織文化 (unwritten rules) 往往是許多施政問題與違規行為的根本原因，早於 2020 年即發布「公部門組織文化審計」(Auditing Organizational Culture in the Public Sector) 研究報告（摘錄於本報告附錄 3），近期並推出一門關於組織文化審計的新課程。前揭研究報告指出，2008 年金融危機及一連串大型企業醜聞後，組織文化已不再被視為主觀、無形的議題，而是成為一個需要被管理與審計的公認風險領域，其介紹組織文化的意涵、審計文化的重要性，以及審計文化的方法論，其中方法論包括如何著手、辨識風險警訊 (red flags)、蒐集證據，以及報告敏感的查核發現等。而在組織文化審計的實務上，OAG 已成功執行「職場尊重」及「軍中性騷擾」等與組織文化高度相關的查核工作，又因其屬績效審計職權範圍，因此查核過程並未受到相較其他議題而言更多的阻力。又此類審計之所以能順利執行，關鍵在於其查核標準並非憑空創造，而是完全奠基於政府既有的法律、政策或公開承諾，且在所有績效審計中，OAG 都會在規劃階段與受查單位詳細討論所運用的標準。例如在「職場尊重」查核案例中，其查核標準是引用包括加拿大勞動法、人權法、財政委員會的公共部門價值與道德準則等逾 10 項法規與政策文件，透過將這些抽象的價值承諾轉化為具體的查核標準，賦予審計機關堅實的法理基礎，另「軍中性騷擾」的查核更為具代表性的案例，查核團隊於查核過程需面對階級分明且具

高度權威的軍方將領，但只要查核團隊堅持專業並提出明確證據，即便遭遇強大反彈，仍能產生深遠的影響力，並促成後續的改革。

(五)性別、權益、多元性與包容性審計 (Gender Equity, Diversity, and Inclusion, GEDI)

CAAFF 倡議在所有績效審計案件中應用「公平性視角」(equity lens)，亦即在查核任何政府施政時，都應主動檢視其是否對不同群體（如性別、弱勢、身心障礙或原住民族群）造成差異性影響，此一方法論亦反映在加拿大政府的對外政策上，聯邦政府

不會資助任何沒有考量性別要素的國際計畫，而這也成為 CAAFF 國際合作計畫的重點。為落實前揭方法論，OAG 內部設有性別、權益、多元與包容 (GEDI) 議題的內部專家，其被暱稱為「絕地武士」(Jedi)，提供多數查核案件諮詢意見，以確保 GEDI 觀點能融入查核規劃與執行工作，例如在查核礦業專案時，除環境衝擊外，也應納入對當

表 6 性平審計各階段考量事項

查核階段	考量事項
選案	<ol style="list-style-type: none">運用性別視角於擇定及定義查核議題(如：為何性別不平等對計畫或組織具重要性？)。審計人員可考量擇選適合進行性平審計的組織進行查核及評估組織對性平的重視程度。
規劃	<ol style="list-style-type: none">以性平角度評估所蒐集的領域知識。考慮查核團隊成員是否具備足夠性平知識以進行查核。考慮查核團隊是否需要專家支援，以規劃與執行查核工作。考慮查核可能的查核發現類型，以及增加查核報告影響力的方式。
執行	<ol style="list-style-type: none">執行性平審計的證據蒐集與分析技巧與一般績效審計相同，然而查核團隊可能須熟悉如基於性別的分析(gender-based analysis)、最佳實務比較、問卷調查、統計分析及根因分析等資料蒐集與分析技巧。將查核發現加以量化有助於增加查核的影響力。在可行的情況下，查核程序應包括估計性別落差、性別不平等的經濟成本或改正已發現不平等所能節省的費用。
報導	性平審計結果的報導與一般績效審計相同，然而須考量的風險如：媒體與民眾可能對性平程度有先入為主的看法，審計結果可能引起利害關係人的反彈及意料外後果，基此，審計報告及媒體溝通所傳遞的訊息須非常清楚。

資料來源：整理自 CAAFF 性平審計實務指南。

地社區女性可能造成的暴力風險等面向。受訪者建議，若審計機關內部缺乏此類專家，可考慮聘用外部顧問。

OAG 曾多次針對政府「性別分析+」(GBA+)政策的執行情形進行專案審計，檢視政府在制定公共政策前，是否已確實評估其對不同性別及具有多重身分認同（即「+」所代表的跨領域性）群體的潛在影響。CAAF 新推動的 GATIPS 國際合作計畫，更將「性別、多元與多重身分」及「包容性與參與度」列為核心主題領域。

又 CAAF 為協助各國最高審計機關辦理性平審計，於 2016 年發布性平審計實務指南 (Practice Guide to Auditing Gender Equality)，其引用聯合國婦女署對性別平等的定義，即女性與男性、女孩與男孩享有相同的權利、責任與機會，平等並非意指女性與男性將變得一樣，而是指女性與男性的權利、責任與機會不會取決於其身為女性或男性，女男平等不僅是人權議題，也是永續人本發展的前提。另在執行性平績效審計時，所依循的準則與流程（選案、規劃、執行、報導）與其他績效審計或內部稽核方法相同，但於查核各階段要注意考量運用性別視角等事項（表 6）。

(六)AI 與科技在審計中的應用

因應數位時代的挑戰，CAAF 已開發「資料分析與 AI」新課程，以全面提升審計人員的數位識能。此課程（表 7）涵蓋兩個核心面向：一是教導審計人員如何運用 AI 與資料分析工具（如 Excel、Python、Power BI）處理巨量資料、衡量計畫成效，甚至使用生成式 AI 輔助工作，例如撰寫報告摘要；二

表 7 資料分析與 AI 課程

大綱
1. 資料來源與類型的概述
2. 解決資料品質問題以確保準確性與完整性
3. 工具介紹：Excel、Python、Power BI 及如何選擇合適工具
4. 運用資料衡量成果、影響力與效率
5. 良好資料視覺化的強大效能
6. AI 概覽與審計人員應注意事項
7. 於審計工作中運用生成式 AI 工具
8. AI 應用的審計

資料來源： CAAF 簡報。

是探討如何查核政府機關對 AI 的應用情形。OAG 內部設有專責的資訊科技審計團隊，由具備專業技術背景的人員組成，負責執行網路安全、雲端個資保護等高技術性的查核工作。為確保機密性，審計機關在運用 AI 時，須使用內部專有版本，以避免將敏感的審計資料洩漏至公開的 AI 模型中，OAG 正在試行一個自有的 AI 系統，期望將其應用於審計生命週期的各個階段，但目前仍處於實驗階段，尚未全面推行。另加拿大政府甫於 2025 年 5 月任命加拿大眾議員 Evan Solomon 先生為首位 AI 部長（Minister of Artificial Intelligence and Digital Innovation），顯示其對 AI 治理的重視。

(七) 培訓課程與方法

CAAF 已開設基礎入門、學習工具與技術、職涯進階及深入審計主題等 4 大類、19 門培訓課程（表 8），其訓練課程的設計高度重視實務應用與互動性，確保審計人員能將所學直接應用於工作，並有廣泛的課程主題，包括績效審計基礎、根本原因分析、審計專案管理、性別平等、SDGs、組織文化及資料分析與 AI 應用等議題，兼顧傳統與前瞻審計需求，又其訓練模式極具彈性，涵蓋數十人的大型實體課程、小型的線上虛擬課程，乃至於可隨時學習的非同步自學課程，以及為客戶需求量身訂做的混合式課程，並發展出種子教師培訓（Train-the-Trainer）與查核團隊輔導等深度合作方案。其中依過去授課經驗顯示極為有效的關鍵策略是為最高審計機關的高階主管舉辦專題工作坊，以確保管理階層理解並支持其部屬所學的新技術與方法，避免改革因內部溝通問題而受阻，而此方法會依據不同國家的文化進行調整，例如在加勒比海地區，高階主管樂於與同仁一起受訓，但在越南則因層級文化而需分開辦理，具體展現 CAAF 對在地脈絡的尊重與適應性。

表 8 CAAF 培訓課程

課程名稱	提供方式	時數
一、基礎入門 (Start with the Basics)		
（一）審計新手訓練營 (Audit Boot Camp)	實體& 線上	16.5
（二）與受查單位互動 (Engaging the Auditee)	實體& 線上	10
（三）根本原因分析 (Root Cause Analysis)	實體& 線上	18
（四）績效審計設計與 3E 原則 (Performance Audit Design and	實體& 線上	7

the 3 Es)(新課程)		
二、學習工具與技術 (Learn Tools and Techniques)		
(一) 精煉查核發現 (Distilling Audit Findings)	實體& 線上	14
(二) 撰擬有效報告 (Effective Report Writing)	實體& 線上	16.5
(三) 證據蒐集與分析 (Evidence Collection and Analysis)	實體& 線上	19.5
(四) 審計人員訪談技巧 (Interviewing Skills for Auditors)	實體& 線上	14
(五) 資料分析與 AI (Data Analytics & AI) (新課程)	實體& 線上	12
(六) 精煉查核發現 (Distilling Audit Findings)(新課程)	實體& 線上	7
三、職涯進階 (Advance Your Career)		
(一) 新興領袖計畫 (Emerging Leaders Program)	實體	5 天
(二) 引導成功的審計工作(Leading Successful Audits)	實體& 線上	18
(三) 管理審計專案 (Managing Audit Projects)	實體& 線上	16.5
(四) 管理審計專案 (Managing Audit Projects) (新課程)	實體& 線上	7
(五) 審計品質管理 (Audit Quality Management) (新課程)	實體& 線上	4
四、深入審計主題 (Dive Deeper into Audit Topics)		
(一) 性別分析審計 (Auditing Gender-Based Analysis+, GBA+)	實體& 線上	6
(二) 永續發展目標審計 (Auditing Implementation of the SDGs)	實體& 線上	14
(三) 內部控制 (Internal Controls)	實體& 線上	14
(四) 組織文化審計 (Auditing Organizational Culture) (新課程)	實體& 線上	4

資料來源：整理自 CAAF 官方網站資料。

陸、研習心得與建議意見

一、參考國際審計社群評估國家氣候行動作法，加強查核政府因應氣候變遷相關作為，並繼續關注 INTOSAI 環境審計工作小組(WGEA)專案成果，協助政府因應氣候變遷的挑戰

聯合國政府間氣候變遷小組 (Intergovernmental Panel on Climate Change) 指出，極端天氣及氣候事件的增加已造成一些不可逆轉的影響。鑑此，國際上已有諸多最高審計機關體認到氣候變遷對其社會及經濟造成的風險，在 INTOSAI WGEA 近期的一項環境審計調查中，受訪者將氣候變遷調適列為 2024 至 2026 年查核工作的首要議題（圖 52），而氣候變遷也被 IDI 視為未來工作中的重要優先趨勢。又誠如本次會議講者所述，AI 及氣候變遷為影響我們生活的兩大趨勢，環境災難在未來一兩年內，就會對經濟造成損害，此外，當前氣候變遷、生物多樣性喪失及水資源短缺等多重環境議題已使全球逼近引爆點，隨著乾旱、洪水、水資源枯竭及海岸侵蝕日益普遍，政府採取相關

調適措施至關重要。

為積極推動國家氣候變遷因應事務統籌工作，行政院已於 112 年 4 月 26 日核定修正行政院國家永續發展委員會設置要點，明定「協調推動氣候變遷因應」為該委員會任務，增設副主任委員，由副院長擔任，督導氣候變遷與淨零轉型專案小組業務，以強化氣候治理運作；又考量聯合國生物多樣性 2030 年目標與策略框架涉及環境、經濟及社會等領域，於 114 年 7 月 25 日修正上開設置要點第 5 點，增設副執行長 1 名，由農業部副首長兼任，辦理生物多樣性議題之協調業務。審計部為積極回應 INTOSAI 有關各國最高審計機關應為達成 2030 永續發展議程作出有意義貢獻的倡議，及推動 SDGs 審計的國際潮流，多年來參考 INTOSAI 相關審計作業指引，及借鏡先進國家審計機關審計實務，檢視政府推動國家永續發展情形，99 至 103 年間以政府推動環境保護執行情形進行查核，104 年起擴展至永續發展相關議題，經檢視政府準備及實踐永續發展目標的情形，並就特定永續發展重要議題如政府推動氣候變遷調適執行情形、政府推動生物多樣性執行情形、政府推動溫室氣體減量情形等進行專案規劃與查核，前揭查核結果並以專章揭露於各該年度中央政府總決算審核報告。

又據 CAAF 受訪者指出，INTOSAI WGEA 為協助最高審計機關透過查核政府為適應氣候變遷所做的努力，進而作出具體貢獻，已推動氣候與生物多樣性專案(Climate & Biodiversity Hub)，該專案納列氣候掃描儀(ClimateScanner)

圖 52 2024 至 2026 年十大環境審計議題

2024至2026年最高審計機關規劃查核的環境議題及與2021年情況的比較



資料來源：INTOSAI WGEA 2024 年環境審計調查。

工具開發計畫及「氣候變遷調適行動」(Climate Change Adaptation Actions, CCAA) 國際合作計畫。經進一步蒐集氣候掃描儀的開發歷程及運用情形，該工具架構是由巴西審計法院等 18 個國家的最高審計機關、逾 70 名審計人員於 2022 年建構完成（圖 53），並提報 2022 年第 24 屆 INTOSAI 會員代表大會（INCOSAI）；又為推廣各國運用氣候掃描儀，計有逾 70 個最高審計機關代表參加 2024 年於紐約聯合國總部舉辦的全球呼籲活動，同年並舉辦 7 場研討會，培訓來自 141 個國家、逾 240 名審計人員。嗣經 61 個國家的最高審計

圖 53 氣候掃描儀



資料來源：巴西審計法院氣候掃描儀網頁。

機關依氣候掃描儀問卷完成各該國家氣候行動實施情形的評估，初步成果已於「聯合國氣候變遷綱要公約第 29 屆締約方大會」(COP 29) 發表（表 9），至全球整體性的評估結果將於 2025 年 10 月第 25 屆 INCOSAI 大會正式提出。

又依 CAAF 簡報，目前已有超過 100 個國家完成由巴西審計法院主導的氣候掃描器倡議工作，且 IDI 與 INTOSAI WGEA 刻正草擬「氣候變遷調適行動」最終報告。舉如 OAG 、德國審計院、紐西蘭審計長公署等最高審計機關均已運用氣候掃描器評估各該國家政府的氣候行動（表 10）。

鑑於 2022 年第 24 屆 INCOSAI 大會通過「里約宣言」(Rio Declaration)，

強調最高審計機關對緊急事件（含氣候變遷）的回應能力，並重申對 SDGs 的承諾等，又聯合國 2024 年 12 月 19 日第 79 屆大會通過 A/RES/79/231 決議，再次確認最高審計機關於強化公共行政效率、課責、效能及透明度的重要角色，並首次明確承認最高審計機關協助政府因應氣候變遷的重要角色，及鼓勵各國在適當及可行的情況下考量最高審計機關報告中與氣候有關的結論及建議。為持續協助政府因應氣候變遷，審計機關允宜加強查核政府因應氣候變遷相關作為，如可參考國際審計社群運用氣候掃描儀工具快速評估國家氣候行動的作法，評估政府的氣候行動，並持續關注 INTOSAI WGEA 氣候與生物多樣性專案成果，透過綜覽全球氣候行動執行情形，辨識我國氣候行動優勢與挑戰，協助政府因應氣候變遷的挑戰。

表 9 各國氣候行動初步評估成果

問卷對象	61 個國家的最高審計機關
評估方式	審計人員針對國家氣候變遷有關之治理（10 項）、公共政策（5 項）、融資（4 項）等面向共計 19 項評估項下之 2 至 4 個項目進行評分。
初步評估結果	<ol style="list-style-type: none"> 1. 大多數國家政府無法追蹤其用於氣候行動上之支出金額數字。 2. 最需要國際金援的國家獲取資金的能力很低。 3. 政府鼓勵私部門投資於氣候專案的策略缺乏追蹤機制及透明度。 4. 政府有已建立制度、法律、策略及氣候行動計畫，惟需要加強法律及計畫的監督。 5. 要建立更公平的氣候政策且不遺漏任何人，須將弱勢人口及群體納入決策過程。 6. 僅有制度、法律、策略及計畫是不夠的，政府需要確保地方政府有所行動，並監督行動的結果。 7. 大多數國家都有與國家減緩策略一致的部門計畫，惟政府須改善風險管理及氣候政策的監測與評估。

資料來源：整理自 INTOSAI WGEA 發布訊息。

表 10 最高審計機關運用氣候掃描儀示例

最高審計機關	運用情形
加拿大審計長公署	2024 年向國會提出「2024 年加拿大淨零排放課責法案」查核報告，查核過程運用氣候掃描儀評估政府減排計畫之進展。
德國審計院	2024 年參與氣候掃描儀專案，並運用氣候掃描儀評估德國政府因應氣候變遷實施的減緩與調適行動，以及國際氣候融資的情形，評估結果並透過致管理階層函（Management Letters）送交聯邦政府經濟事務及氣候行動部等機關。
紐西蘭審計長公署	2024 年運用氣候掃描儀評估政府應對氣候變遷的行動，評估結果作為辨識未來查核面向的參考，該署並鼓勵行政部門考慮評估報告中所辨識的優勢及劣勢，關注需要改進的領域。

資料來源：整理自各該機關網站資訊。

二、賡續強化績效審計考核面向，加強推動公平性審計，並運用根本原因分析，瞭解根因於組織文化的缺失，針對問題癥結研提改善建議，協助促成政府良善治理

依據 INTOSAI 專業聲明架構（INTOSAI Framework of Professional Pronouncements, IFPP）國際政府審計準則（ISSAI）第 300 號「績效審計之基本原則」（Performance Audit Principles），績效審計係對政府之施政、制度、營運、計畫、活動或組織之運作是否符合經濟性(Economy)、效率性(Efficiency)與效果性(Effectiveness)的原則（簡稱 3E 原則），及其是否尚有改善空間的審核。然隨政府審計所面臨內、外部環境持續變化，並為回應國際社會的倡議，先進國家最高審計機關辦理績效審計考核的面向已非侷限於傳統上的 3E 原則，如 OAG 已將環境列為第 4 個 E，加拿大審計長法並明確要求審計長查核資金支出未充分考慮其對環境影響的重大事項，且訂有「永續發展」專節，明訂環境及永續發展委員長（CESD）的職責；澳洲國家審計署已將道德列為第 4 個 E，OAG 亦已成功執行如「職場尊重」及「軍中性騷擾」等與組織文化高度相關的查核工作；英國國家審計署、巴西審計院則將公平列為第 4 個 E。

審計部近年來賡續加強推動績效審計，並因應國內外環境與情勢的發展，聚焦於攸關國家發展的策略性跨域關鍵審計議題，又為強化政府審計監督、洞察及前瞻的功能，積極完善審計機關組織架構，建立相關制度規章，加強推動諮詢專家學者、方案評估技術方法、發掘行政機關優良案例等，以提升績效審計的深度與廣度，在績效審計的考核面向上，除傳統績效審計 3E 面向的考核外，在環境面向，積極深化對國家永續發展之監督，經參酌 CAAF112 年 8 月發布查核永續發展目標之 10 個技巧（10 Tips for Auditing the Sustainable Development Goals）所揭示永續發展目標視角可納入大多數的審計工作，毋需單獨考量永續發展目標，而是將其納入現有的審計流程與方法等觀念，於關鍵審計議題查核規劃作業，由上而下引導審計工作對應臺灣永續發展核心目

標、具體目標及對應指標，以提升查核臺灣永續發展目標之覆蓋率，促成審計工作融入臺灣永續發展目標；在公平面向，有鑑於 INTOSAI 2024 年 11 月發布的「領航全球趨勢—對最高審計機關未來影響（2025—2040）」（Navigating Global Trends—Future Implications For Supreme Audit Institutions, 2025—2040）指出，不平等現象加劇為影響全球的重大趨勢之一（圖 54），面對當前全球面臨

圖 54 2025 至 2040 年全球趨勢



資料來源：INTOSAI 領航全球趨勢—對最高審計機關未來影響（2025—2040）。

所得分配不均、性別不平等、環境不平等、數位落差等問題，預估未來國家間及國家內部的不平等現象仍將持續加劇，審計部爰於 114 年初建構審計機關公平性審計推動架構，涵蓋審計機關加強推動公平性審計的 2 項策略、4 項具體作法，以及 2 項配套措施，復經透過培訓課程，提升審計人員公平性相關概念，並研擬指引使審計人員辦理公平性審計有所依循，引導審計人員關注政策或計畫的公平性面向，並對弱勢相關政策或計畫加強查核，未來 1 年並已規劃查核性別、醫療、教育、文化、社福等領域攸關機會平等與弱勢扶助的相關政策或計畫，冀能協助促成社會公義；在道德面向，經依審計法加強稽察各機關人員不法或不忠於職務的行為，並透過包括內審、外審合作，協助與督促強化政府財務控管作為；運用大數據查核相關資料篩選異常案件，

發掘高風險採購案；建置查詢系統警示控制點，發送異常案件預警；強化審計與廉政（政風）單位的聯繫，增進雙方溝通協作；以及聽取民眾陳情與建言，有效暢通雙向溝通管道等作法，預防與偵測貪腐或舞弊行為的發生。

又我國政府為回應人民的期待，甫於 114 年 9 月提出 4 大優先政策，聚焦經濟、民生、青年、弱勢等 4 大面向，並於立法院新會期推動 20 項相關法案，占新會期法案總數的比率高達 7 成。而審計部刻正積極推動公平性審計，其強調機會平等及弱勢扶助的本質，可具體回應政府當前施政重點，另誠如本次會議講者所述，幾乎所有事件的根本原因都與人類行為有關，文化與行為的重要性不容忽視，CAAF 受訪者亦指出，不健全的組織文化往往是許多施政問題與違規行為的根本原因，OAG 的報告更揭露聯邦政府的「文化問題」是導致 Phoenix 薪資系統失敗的因素之一。鑑此，為符合外界對審計機關強化績效審計、維護社會公義及預防與偵測貪腐或舞弊行為的期待，審計機關允宜繼續強化績效審計的考核面向，加強推動公平性審計，並運用根本原因分析，瞭解根因於組織文化的缺失，以針對問題癥結研提改善建議，協助促成政府良善治理。

三、賡續深化國際合作與人員培訓，以在 AI 時代與全球變局下，接軌國際審計專業趨勢，並確保審計人員與時俱進，具備未來所需關鍵能力

本次會議講者警示，當前地緣政治不穩定、數位變革、氣候變遷等多重威脅相互交織，導致風險樣貌發生巨大轉變，而此將促使審計專業功能與技能亟待轉型。誠如講者所述，AI 將使許多專業知識快速商品化，但學習能力卻不會，因此，學習「如何學習」將成為關鍵技能，又 AI 將大量自動化重複性工作，使人類的適應力、好奇心、勇氣、同理心、智慧與幽默等人性化特質更顯珍貴。再者，傳統的遵循性查核已不足以應對挑戰，稽核人員被要求具備更廣泛的技能，如適應力與學習敏捷度、策略思維與商業敏銳度、溝通

能力、資訊科技及網路安全等能力。新版的內部稽核職能框架則特別強調包含專案管理、應對衝突等軟技能的重要性，而這些是在 AI 時代下，稽核人員成為組織策略顧問、提供卓越建議的關鍵。鑑此，協助審計人員與時俱進，使其具備未來所需的關鍵能力，乃刻不容緩的任務。

本次受訪單位 CAAF 致力於透過研究、教育及知識分享，促進並強化國內外公部門的績效審計、監督與課責機制。為深化績效審計研究與培訓，其官網提供許多績效審計的理論與實務資源，受訪者分享 CAAF 已建置的「審計新訊」專區，該專區提供許多績效審計資訊與文件，其中「審計新訊資料庫」（圖 55）涵蓋全球 54 個司法管轄區的資料庫，並收錄逾 9,000 份績效審計報告及其他文件；績效審計指南清單則收錄 CAAF 於 2023 年發布的第 11 版

「績效審計指南清單—全球最新審計指引文件彙編」，前揭清單包括過去 10 年間全球最高審計機關發布的重要文件，並納

圖 55 審計新訊資料庫（展示版）

Title	Relevancy	Date	Audit Institution
An Auditor's Guide to the Performance Audit Process	High	January 2008	CANADA (GEN)
Office of the Auditor General of Alberta - Results analysis, financial statements and other performance information for the year ended March 31, 2008	Medium	June 2008	CANADA-Alberta
Performance Audit Manual	Medium	January 2007	INTOSAI
The Auditor-General's observations on the quality of performance reporting	Medium	January 2008	New Zealand
Guide to CCAF Principles of Performance Reporting	Medium	January 2007	CANADA-Taiwan/China
Year review of GAO (USA)	Medium	January 2008	INTOSAI
Peer review report - Denmark	Medium	January 2008	INTOSAI
Peer review report - European Union	Medium	December 2008	INTOSAI
Peer review report - Mexico	Medium	November 2008	INTOSAI
Peer review report - Netherlands	Medium	March 2007	INTOSAI
Peer review report - New Zealand	Medium	March 2008	INTOSAI
Peer review report - Norway	Medium	January 2008	INTOSAI

資料來源：CAAF 官網。

入 INTOSAI、IIA 及 CAAF 等組織發布的文件，內含最佳實務指南、背景資料、討論文件、檢核表及自我評估工具，共計收錄 28 個主題、199 份文件，有助於協助審計人員規劃與執行高品質的績效審計工作。此外，CAAF 官網尚提供實務指南、研究報告等資源，並會不時發布查核小技巧（如審計工作運用生成式 AI 的 6 大秘訣），每則專文均聚焦優良實務，並針對特定主題為績效審計人員提供實用建議，前揭 CAAF 發布的資源，如查核永續發展目標之 10 個技巧、性平審計實務指南等業經審計部參酌作為策進我國績效審計實務，以符合國際審計專業趨勢的參考。又 CAAF 已開設廣泛的課程主題，其

專業發展副總裁 Sharon Clark 女士長年投入於績效審計實務與培訓工作，並參與 INTOSAI 績效審計準則的訂定，審計部經審酌績效審計查核標準的揭露為外界關注重點之一，於 112 年邀請 Sharon Clark 女士擔任績效審計研習（進階班）講師，視訊講授「績效審計查核標準之探討」課程，協助審計人員掌握國際審計發展趨勢並向標竿實務學習。前揭課程並已上架「e 等公務園+學習平臺」審計數位學習專區供審計人員自主學習（圖 56）。本次參訪經洽詢受訪者未來再度合作的可能性，並獲正面支持與回應。

為促使審計人員與時俱

進，具備未來所需的關鍵能力，審計機關允宜將終身學習與適應力內化為審計文化，並賡續規劃如軟技能、數據分析、新興審計議題深度研習等多元化培訓課程，以及強化數位化自主學習的推動，此外，可評估再度邀請 CAAF 人員講授績效審計

圖 56 績效審計數位課程



資料來源：「e 等公務園+學習平臺」審計數位學習專區。

重要議題如根本原因分析或性平、文化審計等相關課程的可行性；另允宜賡續深化國際合作與交流，並視需要評估加入 CAAF 會員的可行性，以蒐集與運用國際審計研究資源。透過前揭營造終身學習文化、多元化培訓及深化國際交流合作等作法，確保審計人員在複雜多變的環境下得以具備未來所需的關鍵能力。

四、參考國際研討會專家分享導入 AI 應用之經驗與建議，持續提升審計數位轉型能量

本次會議中，人工智慧的應用成為最受關注的主題之一。專家們一致認為，AI 在稽核流程中具有明顯效益，在全球法規環境複雜且尚未明確之下，

未來 AI 實施必須兼顧創新與風險管理，經綜整講者導入 AI 之實務經驗與建議，主要重點包括：1.跨部門建立 AI 治理框架，可參考治理、風險管理、控制三層框架，治理層需有政策規範、界定責任等，風險管理層需涵蓋資料隱私、平台資安等，控制層需建立內控檢查、透明度等；2.盤點自行建置或外部購買的 AI 工具清單，並按所接觸資料進行風險分類，必要時須進行盡職調查（如資料是否經合法授權等），防止法律爭議；3.秉持「人類參與流程」（Human-in-the-Loop）之原則，確保輸出準確性，並管理 AI 工具之變更，持續測試避免偏差；4.建立「安全沙盒環境」，讓稽核人員能在低風險場域反覆試驗與學習，逐步累積經驗；5.定期召開工作坊與回饋會議，持續討論需求、改進功能，形成長期的循環開發模式。另研討會中亦有多位講者分享了 AI 在稽核領域的實務應用案例，顯示已逐漸從概念驗證走向實踐，包括自建 PowerApp 串接 ChatGPT API，進行會議摘要與報告草稿生成並保留提示與輸出軌跡；建立知識庫檢索，將歷次稽核發現儲存於 Google Cloud 並透過 Gemini API 查詢，系統自動擷取關鍵字、比對文件並提供來源，減少資訊斷裂等（表 11）。鑑於人工智能已成為推動審計（稽核）數位轉型的重要動能，審計部數位審計發展委員會設置要點於 114 年 5 月 23 日修正，新增 AI 審計應用推動小組，負責研議 AI 審計相關應用議題，及軟硬體設備資源與技術服務整備、人員培訓等事項，本次研討會綜整之制度與實務經驗可作為該小組未來推動 AI 審計應用的重要參考。

表 11 稽核領域的實務應用案例

應用面向	應用案例
文件與報告自動化	用 AI 自動摘要會議紀錄、產出風險控制矩陣、生成報告草稿
稽核規劃與測試	<ul style="list-style-type: none"> ● 開發基於 Excel 生成式 AI 工具，可提供建立稽核方案 ● 自建 PowerApp 串接 ChatGPT API：以低程式碼 PowerApp 建立查核/抽樣/回覆流程，後端串接 ChatGPT API 產出摘要、草稿與建議；內建提示模板(Prompt Library)、權限與稽核軌跡
知識庫檢索	將歷次稽核發現/報告、政策依據存放於 Google Cloud；以企業合約串接 Gemini API(保障不留存/不訓練企業資料)，啟用檢索增強(RAG)：自動抽取關鍵字、比對文件並回傳來源

應用面向	應用案例
資料分析與異常偵測	Triple AI：由 Data AI 篩選 → Document AI 比對 → 人工判斷，將 160 萬筆縮減至 84 筆需人工檢查
持續監控與自動化	Elm 公司：建立 AI 異常訊號(Red Flag)監測，並將結果回饋模型學習；改以即時/季度稽核
跨部門協作與文化推動	Oliver：用 AI 翻譯摘要改善跨國溝通；Elm：與支持單位合作簡化呈報方式
實驗與學習環境	推動「安全沙盒」試驗；案例「The Boys of Audit」以 AI 創意實驗取代追求完美

五、參考國際之作法，以前瞻思維評估潛在風險，確保政府建置 AI 系統在設計、建置與營運過程中均符合法規、倫理與社會期待

本次會議中，安永德國合夥人 Tobias Albrecht 提出「稽核 AI」具體框架與方法，首先全面盤點組織內 AI 應用，並依據技術風險（如目標、使用技術、資料來源、自動化程度）與利害關係人影響（經濟、實體、法規等）進行殘餘風險評估，透過「風險熱區圖」決定優先查核領域，並從治理、風險管理與控制三方面全面檢視，治理層可檢核董事會或高階管理階層對 AI 建立明確的監督責任與決策架構，包含風險胃納、政策規範及與第三方廠商的角色分工等；風險管理層可檢核使用者訓練、平台資安、資料隱私及解決方案設計；控制層可檢核內部控制的有效性與持續運作，包括開發人員資格審查、資料治理、與偏差檢測等。稽核方法建議依系統風險高低採取黑箱、灰箱與白箱查核，低風險以控制環境測試為主，中等風險需監控輸出品質並驗證結果，高風險則必須深入演算法與資料邏輯，進行壓力測試、統計比對及跨模型交叉驗證，並完整保存稽核紀錄，確保證據可重現。

歐盟個人資料保護委員會(European Data Protection Board, EDPB)於 2024 年 6 月 27 日公開一份「AI Auditing」專案文件，係由專家支援計畫 (Support Pool of Experts Programme) 項下委託 Gemma GALDON CLAVELL 博士研究，內容提出一套「端到端社會技術式演算法稽核 (E2EST/AA)」的方法學與詳細檢核清單，旨在協助各方在「人工智慧法案」(AI Act) 的脈絡下，理解並評

估資料保護的保障措施，可協助各國資料保護機關（DPA）藉由制定一套以檢核清單為形式的方法論，來對演算法進行稽核，並提出可提升透明度的工具。鑑於人工智慧在公共服務、決策支援及資料分析之應用愈加廣泛，審計機關允宜參考國際之作法，以前瞻思維評估潛在風險，確保政府建置 AI 系統在設計、建置與營運過程中均符合法規、倫理與社會期待。

六、參考國際研討會資安場次重點，加強查核行政機關資安治理與韌性建設

在生成式 AI 廣泛應用於公共治理與審計作業的背景下，資安風險的範疇已從技術層面延伸至治理、倫理與營運持續性。資安稽核專家 Tichaona 指出資安稽核已成為稽核計畫的重要項目，但具備專業技能的人員仍極為有限。又資安技術人員所產出的安全性檢測報告（弱點掃描、滲透測試），仍多以技術面呈現，如漏洞數量，無法反應「風險層級」與「對業務的影響」等核心問題，Tichaona 認為資安應視為「商業議題」，因為當發生攻擊時，真正承受衝擊的是業務運作與營運成果。另提供 30 個核心問題（詳見附錄 2），包括政策與策略、風險胃納、資源配置、第三方風險及內稽能力，可作為審計人員評核公部門資安之參考。

前美國國家安全局（NSA）高階主管 Rachel 指出，國家級行為者及犯罪集團的攻擊日益頻繁，AI 更降低了駭客技術門檻，全球約七成惡意流量源於犯罪組織，其勒索行動已具產業化規模，面對這樣的環境，唯一能保護我們的就是提升組織的韌性，包括確保所有系統隨時更新與修補漏洞、定期模擬勒索軟體等網路攻擊場景與高層應變訓練，以及最關鍵的一點：驗證備份策略是否真正有效，資安事件發生後，能否迅速復原，將決定一個組織能否存活。114 年 9 月 26 日南韓國家資訊資源管理院（NIRS）機房發生火災，造成雲端儲存平台「G-Drive」損毀，導致 647 個政府業務系統停擺，約 75 萬名公務員累積七年的 858TB 文件永久消失，顯示公共部門暴露出備援與離線

備份不足、災難復原計畫未落實等結構性問題。另外，偵測欺騙國際顧問公司執行長 Nejolla 指出，「人」是資安中最薄弱的一環，駭客已從技術滲透轉向心理操弄，透過釣魚郵件、偽裝邀請及社群媒體詐術滲透組織，因此建議將社交工程風險納入資安治理架構，促使各機關建立制度化教育訓練與模擬演練，使每位員工皆具「網路守護者」意識。**鑑於資安治理在 AI 時代的重要性與挑戰日益提升，審計機關允宜參考國際作法，採風險導向方式檢視政府機關資安防護成效，藉以提升整體政府資安韌性與危機應變效率。**

附錄 1 會議議程

時間 (Time)	主題 (Topic)	講者及職稱 (Speaker and Title)
2025-07-14		
8:20-8:40	Innovation Session: Beyond the AI Hype: Our ISO 42001 Certification Story	
9:00 AM - 10:15 AM ET	下一個文藝復興 (The Next Renaissance)	Zack Kass, 未來學家、ZK.AI Advisory 創始人、前 OpenAI 市場推廣負責人 (Futurist, Founder of ZK.AI Advisory, Former Head of Go To Market at OpenAI)
10:35 AM-10:55 AMET	Innovation Session: Bots, Boost, and Beyond: Reimagining Internal Audit with Generative AI	
11:15 AM - 12:05 PM ET	重新思考風險：內部稽核在面臨交叉威脅的世界中不斷演變的角色 (Risk, Reimagined: Internal Audit's Evolving Role in a World of Interconnected Threats)	Anthony J. Pugliese, IIA 總裁兼首席執行官 (President and CEO, The Institute of Internal Auditors)
1:45 PM - 2:45 PM ET	CS 1-1: 激發潛力及邁向卓越：新版內部稽核職能框架 (CS1-1 Unlocking Potential and Elevating Excellence: A New Competency Framework to Promote Achievement)	David Petriski, 專業標準總監 (Director, Standards and Guidance, IIA); Emre Alpargun, 副總裁兼首席審計執行官 (Vice President, Chief Audit Executive, Palo Alto Networks)
1:45 PM - 2:45 PM ET	CS 1-3:無企業治理的商業管理 - 會出什麼問題？ (Managing a Business without Corporate Governance - What Could Go Wrong?)	Christopher Schneck, IIA 奧地利首席執行官 (CEO, IIA Austria)
1:45 PM - 2:45 PM ET	CS 1-4:超越保證：內部稽核在系統實施中的策略角色 (Beyond Assurance: Internal Audit's Strategic Role in System Implementation)	Nausheen Ahmed, BRAC 大學內部稽核與合規負責人、IIA 孟加拉秘書長 (Head of Internal Audit and Compliance, BRAC University; Secretary General, IIA Bangladesh)
1:45 PM - 2:45 PM ET	CS 1-5:紅隊演練：內部稽核提供網絡安全保證的主動方法 (Red Teaming: A Proactive Approach for Internal Audit to Provide Cybersecurity Assurance)	Matthew Maglieri, 主動服務區域領導 (Regional Leader, Proactive Services, Mandiant); Neil Power, 內部稽核服務高級總監 (Senior Director, Internal Audit Services, Hydro One); Eddie Ng, 網絡安全高

時間 (Time)	主題 (Topic)	講者及職稱 (Speaker and Title)
		級總監 (Senior Director, Cybersecurity, Hydro One); Susan Papadopoulos, 內部稽核服務高級經理 (Senior Manager, Internal Audit Services, Hydro One)
1:45 PM - 2:45 PM ET	CS 1-6:提升公部門內部稽核－主計長觀點 (CS1-6 Advancing Internal Audit in the Public Sector-Perspectives from Comptroller Generals)	Annie Boudreau, 加拿大審計長 (Comptroller General, Canada); Beili Wong, 安大略審計長 (Comptroller General, Ontario); Esther Wee, 新加坡會計總長 (Accountant-General, Singapore); Jason Gilley, 內部稽核總監 (Director, Internal Audit, Ontario Lottery and Gaming)
1:45 PM - 2:45 PM ET	CS 1-7:按設計防詐：根據新全球標準融合審計、風險與分析 (Fraud Proof by Design: Converging Audit, Risk & Analytics Under the New Global Standards)	Brad Monterio, 學習、許可與銷售執行副總裁 (EVP, Learning, Licensing, and Sales, IIA); Andi McNeal, 副總裁 (Vice President, ACFE)
1:45 PM - 2:45 PM ET	CS 1-8:次世代稽核人員：在人工智慧浪潮中生存 (CS1-8 NxtGenAuditor: Surviving the AI Impact)	Alexander Ruehle, zapliance 首席執行官兼聯合創始人 (CEO & Co-Founder, zapliance)
3:30 PM - 4:00 PM ET	OPTIONAL SESSION 全球視角：解碼地緣政治與經濟趨勢 (Global Perspectives: Decoding Geopolitical and Economic Trends for the Future)	Janice Gross Stein, 蒙克全球事務學院創始主任 (Founding Director, Munk School of Global Affairs, University of Toronto)
4:15 PM - 5:15 PM ET	前所未有的時代推動轉型變革 (Driving Transformative Change in Unprecedented Times)	全球領袖人物、多家企業董事會成員、高級顧問、前 Ingka/IKEA 首席永續長 Pia Heidenmark Cook
2025-07-15		
9:00 AM - 10:15 AM ET	蛻變：查核從不可能到現實的轉型 (Metamorphosis: Auditing the Transformation of the Impossible into Reality)	GE 西班牙與葡萄牙總裁、Google 伊比利半島區董事總經理、NH Hotels 營運長，以及 Dell 電腦西班牙、義大利與葡萄牙區執行長 Isabel Aguilera
11:45 AM - 12:45 PM ET	CS 2-1:超越效率：稽核自動化的策略力量 (CS2-1 Beyond Efficiency:	Saifeldin Ali, 持續審計總經理 (Continuous Audit General Manager,

時間 (Time)	主題 (Topic)	講者及職稱 (Speaker and Title)
	The Strategic Power of Audit Automation)	Elm); Abdulaziz AlHidery, 首席審計官 (Chief Audit Officer, Elm)
11:45 AM - 12:45 PM ET	CS 2-3:漣漪效應：在社交媒體、AI 與傳染風險時代保護聲譽 (The Ripple Effect: Safeguarding Reputation in an Era of Social Media, Artificial Intelligence and Contagion Risk)	Dana Lawrence, 金融科技合規高級總監 (Sr. Director of Fintech Compliance, Pacific West Bank)
11:45 AM - 12:45 PM ET	CS 2-4:法律框架中之人工智慧：平衡創新、倫理與全球合規 (C2-4 AI in the Legal landscape: Balancing Innovation, Ethics, and Global Compliance)	Imran Ahmad, 技術與網絡安全隱私加拿大負責人 (Partner, Canadian Head of Technology, Norton Rose Fulbright Canada)
11:45 AM - 12:45 PM ET	CS2-5 CEESG：以強大控制環境重新定義環境、社會與治理 (CS2-5 CEESG: Redefining ESG with a Strong Control Environment)	Ali Rehman, 內部稽核總監 (Internal Audit Director, University of Central Asia)
11:45 AM - 12:45 PM ET	CS 2-6:強化內部稽核與審計委員會關係以優化風險管理 (Strengthening Internal Audit-Audit Committee Relationship to Optimize Risk Management)	Gordon Braun, 董事總經理 (Managing Director, Protiviti); Abim Kolawole, 首席審計執行官 (Chief Audit Executive, Northwestern Mutual)
11:45 AM - 12:45 PM ET	CS 2-7:品質評估挑戰與機遇 - 公開論壇 (Quality Assessment Challenges and Opportunities - Open Forum)	Warren Hersh, IIA 品質服務總監 (Director, IIA Quality Services); Keith Kahl, IIA 外部品質評估團隊顧問 (IIA EQA Team Lead Advisor); Marthin Grobler, 首席審計執行官 (Owner, Chief Audit Executive, IA Professionals)
11:45 AM - 12:45 PM ET	CS 2-8:內部稽核在促進金融服務業整合監督中的角色 (Internal Audit Role in Fostering Integrated Supervision Across Financial Services Industry)	Sophia Issabella Watimena, 審計委員會主席 (Chairwoman of Audit Board, Indonesia Financial Services Authority)
2:15 PM - 3:15 PM ET	CS 3-1:生成式 AI 時代下的網路安全治理 (C3-1 Cybersecurity Governance in a Gen AI Era: 30 Questions the Board and Audit Committee Should Ask)	Tichaona Zororo, 數位與網絡安全顧問總監 (Director Digital & Cybersecurity Advisory, EGIT)

時間 (Time)	主題 (Topic)	講者及職稱 (Speaker and Title)
2:15 PM - 3:15 PM ET	CS 3-2:解鎖確信：將行為風險與整合性人與流程稽核 (IPPA) 及雄心模型 (Ambition Model) 整合 (C3-2 Unlocking Assurance: Integrating Behavioral risks with IPPA and the Ambition Model)	Peter Hartog, 專業實務總監 (Director Professional Practices, IIA Netherlands); Danny Francken, 首席執行官 (CEO, IIA Netherlands)
2:15 PM - 3:15 PM ET	CS 3-4:未來不再如昔：以真誠導航利益相關者關係 (The Future Ain't What It Used To Be: Navigating Stakeholder Relationships With Authenticity)	Ursula Schmidt, 內部稽核與合規專業人士、IIA 盧森堡董事會成員 (Founder, Internal Audit & Compliance Professional, Schmidt Advisory)
2:15 PM - 3:15 PM ET	CS 3-5:內部稽核在強化組織文化中的角色 (C3-5 The Role of Internal Audit in Enhancing Organizational Culture)	Seita Almandeel, 內部稽核總監 (Supervisor General of Internal Audit, General Court of Audit)
2:15 PM - 3:15 PM ET	CS 3-6:區塊鏈商業模式、規範與風險管理 - 韓國案例研究 (Blockchain Business Models, Regulation, and Risk Management - The Korean Case Study)	David Dongki Lee, 合夥人 (Partner, Deloitte Consulting Korea); Seonghoon (Sean) Ju, 首席技術官 (Chief Technology Officer, CODE)
2:15 PM - 3:15 PM ET	CS 3-7:舞弊與鑑識矩陣 (CS3-7 Fraud and the Forensic Matrix)	Gary German, 負責人 (Principal, G.L. German Forensic Accounting, LLC)
2:15 PM - 3:15 PM ET	CS 3-8:整合風險管理：首席審計執行官作為變革催化劑 (Integrated Risk Management: The Chief Audit Executive as a Catalyst for Change)	Nancy Chase, 全球風險負責人 (Partner, Global Head of Risk, KPMG); Jamie Meziere, 首席審計執行官 (Chief Audit Executive, FedEx); Clarissa Crane, 風險與轉型執行官 (Risk and Transformation Executive, Former Shopify); John-Paul Font, 全球內部稽核與控制負責人 (Global Head of Internal Audit and Controls, KPMG)
4:15 PM - 5:15 PM ET	全球審計轉型：人工智慧、監管與內部稽核的未來(Global Audit Transformation AI, Regulation, and the Future of Internal Audit)	Bupa 公司內部稽核部門分析主管 Sachin Kapoor、Davy 公司內部稽核主管 Chris Cowley 、Constellium 公司內部稽核副總裁 Karen Albert
2025-07-16		

時間 (Time)	主題 (Topic)	講者及職稱 (Speaker and Title)
9:00 AM - 10:00 AM ET	CS 4-1:AI 與 IA：如何有效應對同一體兩面的挑戰 (C4-1 AI and IA: How to Effectively Address Both Sides of One Coin)	Tobias Albrecht, 合夥人 (Partner, EY Consulting); Kanika Vij, 數據與分析總監 (Director, Data & Analytics, Royal Bank of Canada); Oliver Petri, 內部稽核副總裁 (Vice President, Internal Audit, Hugo Boss AG)
9:00 AM - 10:00 AM ET	CS 4-2:增強課責與透明度：安大略內部稽核治理模型 (Enhancing Accountability and Transparency: Internal Audit Governance Model in Ontario)	Sanjeev Batra, 首席內部稽核師 (Chief Internal Auditor, Government of Ontario)
9:00 AM - 10:00 AM ET	CS 4-4:透過代理式 AI 強化內部稽核的未來準備 (C4-4 Future-Proofing Internal Audit With Agentic AI Solutions)	Zeyu (Levin) Song, 內部稽核分析專員 (Associate Analytics, Internal Audit, Delivery Hero); Liliana Staber, 內部稽核高級經理 (Senior Manager, Internal Audit, Delivery Hero)
9:00 AM - 10:00 AM ET	CS 4-5:最大化內部稽核對組織永續性的影響 (CS4-5 Maximizing Internal Audit's Impact on Organizational Sustainability)	Grant Ostler, GRC 行業負責人 (Industry Principal, GRC, Workiva)
9:00 AM - 10:00 AM ET	CS 4-6:當消化不良遇上酸性 (When Indigestion Meets Acidity)	Adil Buhariwalla, 內部稽核與風險諮詢高級合夥人 (Senior Partner, Internal Audit & Risk Consulting, UHY James)
9:00 AM - 10:00 AM ET	CS 4-7:內部稽核促進價值創造 (Internal Audit Contributing to Value Creation)	Kiyotaka Sasaki, 客座教授 (Visiting Professor, Hitotsubashi University)
9:00 AM - 10:00 AM ET	CS 4-8:從監督到洞見 - 提升內部稽核為可信策略顧問 (From Oversight to Insight - Elevating Internal Audit to a Trusted Strategic Advisor)	Rao Wandawasi, 審計服務總監 (Director, Audit Services, B C Lottery Corp.); Jug Lalli, 審計服務高級經理 (Senior Manager, Audit Services, B C Lottery Corp.)
10:15 AM - 11:15 AM ET	CS 5-1:引領未來：新世代稽核人才的吸引與留任策略 (CS5-1 Engaging Tomorrow: Strategies For Attracting and Retaining The Next-Gen Auditors)	Perla Habchi, 內部稽核項目負責人 (Internal Audit Project Leader, Government of Canada)

時間 (Time)	主題 (Topic)	講者及職稱 (Speaker and Title)
10:15 AM - 11:15 AM ET	CS 5-2:舞弊調查：如何執行 (CS5-2 Fraud Investigations: A How to Guide)	Brenda Youle, 內部稽核總監 (Director, Internal Audit, SaskPower)
10:15 AM - 11:15 AM ET	CS 5-3:與合規和企業風險管理有效對齊 (Creating Effective Alignment with Compliance and ERM)	Gerard Zack, 風險顧問 (Risk Advisor, RiskTrek LLC)
10:15 AM - 11:15 AM ET	CS 5-4:轉型領導在內部稽核中的應用：推動全球不確定性中的變革 (Transformational Leadership in Internal Audit: Driving Change in a Global Landscape of Uncertainty)	Renato Trisciuzzi, 商業顧問與導師 (Business Advisor and Mentor, Instituto Renato Trisciuzzi Ltda)
10:15 AM - 11:15 AM ET	CS 5-5:AI 與內部稽核：創新來自更智能之文件互動 (C5-5 AI Meets Internal Audit: Innovating Through Smarter Document Interaction)	John Manilla, 合夥人 (Partner, Crowe LLP)
10:15 AM - 11:15 AM ET	CS 5-7:未來導向的內部稽核領導力：全球稽核長的觀點 (CS5-7 Future Proofing Internal Audit Leadership: Perspectives of Global Chief Audit Executives)	Tabish Gill, 國家風險諮詢與金融服務行業負責人 (Partner, RSM); Michelle Myers, 全球首席審計師 (Senior Vice President & Global Chief Auditor, TD Bank); Heather Kaine, 執行副總裁兼首席審計師 (Executive Vice President & Chief Auditor, CIBC); Helen Killock
10:15 AM - 5:30 PM ET	CS 5-8:駭入人性：超越科技的社交工程策略 (C5-8 Hacking the Human: Social engineering Tactics That Outwit Technology)	Nejolla Korris, 首席執行官 (CEO, InterVeritas International)
11:30 AM - 12:30 PM ET	資安威脅新局勢 (The New Cyberthreat Landscape)	前美國國家安全局(NSA)高階主管，現任摩根士丹利財富管理部門的資安總監 Rachel Wilson

附錄 2 董事會與稽核委員會應檢視的 30 個關鍵提問

1. 組織是否具備經董事會批准的正式網路資安政策？
2. 組織是否具備經董事會批准、且與企業和業務優先事項保持一致的正式網路資安策略？
3. 資安是否為您的董事會、IT 治理或 IT 策略委員會及/或稽核與風險委員會的議程項目？
4. 董事會中是否具備網路資安專業知識的人員？
5. 董事會是否精通網路資安？
6. 組織是否具備網路資安事件應變計畫（CSIRP）？
7. CSIRP 是否與業務永續管理計畫（BCMP）和災難復原計畫（DRP）保持一致？
8. 是否已測試過 BCMP 和 DRP？
9. 董事會和高階主管是否已模擬過 CSIRP？
10. 是否具備韌性？
11. 董事會和高階主管是否定期收到網路資安事件與事件管理摘要報告？
12. 是否具備網路資安危機溝通計畫？
13. 組織是否維護一份準確、完整、最新、已分類且已歸類的資訊與技術資產清冊？
14. 組織是否正在使用不支援更新的作業系統？
15. 組織是否設有資訊安全長（CISO）？
16. CISO 向誰報告？
17. CISO 是否出席董事會會議？
18. 組織是否具備網路資安保險，且其保障是否足以彌補潛在損失？
19. 組織是否具備網路風險偏好，並將其運用於策略決策中？
20. 組織多久執行一次第三方網路資安風險評估、威脅與漏洞評估以及外部滲透測試？
21. 組織的五大網路資安風險為何？
22. 核心資產（端到端關鍵產品或營運和基礎設施）是否受到保護？
23. 是否已充分展望未來，以瞭解當前的技術投資將如何產生網路資安影響？
24. 網路風險是否在組織的風險管理框架中被明確識別？
25. 是否正在稽核網路資安？
26. 網路資安是否納入您的年度或三年稽核計畫或內部稽核策略中？
27. 內部稽核團隊中是否具備網路資安技能？
28. 內部稽核正在使用哪些網路資安稽核工具？
29. 是否設有網路資安營運中心（SOC）？
30. 已完成網路資安意識培訓的員工比例是多少？

附錄 3 公部門組織文化審計（Auditing Organizational Culture in the Public Sector）

一、前言

過去，審計組織文化被認為是主觀、不切實際且不適當的。然而，在 2008 年金融危機與一連串大型企業醜聞之後，組織文化已成為一個公認的風險領域，需要被管理、監督與審計。如今，審計文化已被許多專業協會視為一項新的要務。本報告旨在回答 3 個主要問題：什麼是組織文化？為什麼查核組織文化很重要？如何查核組織文化？

二、什麼是組織文化？

組織文化的定義多樣，但最簡單的說法是「我們在這裡做事的方式」(The way we do things around here)。其包含期望的文化（所說的）與實際的文化（所做的）等兩個元素：

(一) 期望的文化（所說的）：指組織的願景、使命、公開的價值觀、道德準則、內部政策等。

(二) 實際的文化（所做的）：指員工的實際行為、實踐、態度與思維模式。

在理想情況下，實際文化應與期望文化一致，但現實中，許多因素會造成兩者之間的差距，例如「高層的基調」(tone from the top)、高階管理層的行動、溝通方式、訓練計畫及獎勵制度等。高層領導在設定文化上扮演關鍵角色，但中層與基層員工同樣具有影響力，可能在組織內形成不同的次文化 (sub-cultures)。此外，組織文化並非靜態，其會隨著領導風格、策略方向與社會趨勢的變化而演變。

三、為什麼要查核組織文化？

許多知名的私部門企業醜聞（如安隆 Enron、福斯 Volkswagen）都顯示出陳述的價值觀與實際行為之間，存在巨大的鴻溝。這些事件促使內部稽核專業反思，並認識到文化在組織治理中的關鍵角色，且是一個需要定期審計的風險領域。這不僅適用於私部門，公部門同樣存在不道德行為與功能失調的文化問題。例如，加拿大審計長的

報告曾揭露，聯邦政府的「文化問題」是導致 Phoenix 薪資系統失敗的因素之一。

綜上，組織文化是決定組織績效、轉型計畫的成功與否，以及組織內舞弊、腐敗與其他不道德行為程度的關鍵因素。查核文化有助於公部門管理前揭風險，縮小期望與實際文化間的差距，預防計畫失敗、聲譽受損，並維護公眾信任。

四、如何查核組織文化？

(一) 審計人員應從何處著手以及查核什麼？

1.漸進式方法：建議審計人員初次接觸文化審計時應循序漸進。首先，可在常規審計中透過根本原因分析辨識潛在的文化因素；其後可在查核計畫中納入文化的特定面向；最終再進行全面的組織文化審計。

(1)在常規審計中融入文化考量：審計人員可以在常規審計中，開始思考是否有潛在的文化因素可以解釋其查核發現。透過使用根本原因分析 (root cause analysis) 工具，審計人員可辨識出這些因素，並將其記錄於查核報告中。例如，若審計人員觀察到網路安全弱點，透過根本原因分析可能會發現問題並非起源於技術因素，而是文化因素，例如因組織對風險的高度容忍或過度關注結果的文化所導致。

(2)在查核計畫中納入文化面向：即於查核計畫中規劃一個專門的章節檢視組織文化化的某個面向。

(3)執行全面的文化審計與總結報告：待審計團隊的能力與信心提升後，可考慮對組織文化進行一次全面的審計，並在累積多次查核文化面向的經驗後，產出一份對整個組織的文化議題提供橫向檢視的總結報告。

2.核心任務與風險辨識：文化審計的本質是判斷組織的實際文化是否符合其期望的文化。審計人員應特別關注揭示文化問題的警訊 (red flags)。如：

- 財務或安全控制措施經常被逾越。
- 未能落實行為準則，違規行為無相關後果。
- 不信任審計人員與監管機關，且執行其建議的紀錄不佳。

- 員工調查中表達高度不滿。
- 來自員工、客戶或公眾的高投訴率。
- 高員工流動率與缺勤率。
- 長期未解決的問題（例如，查核缺失一再重複出現）。
- 缺乏支持組織價值觀的行動或激勵措施。
- 績效獎勵與指標未能與組織的政策與價值觀保持一致。

3.選擇查核領域：為使查核標準更為精確，查核工作應聚焦於特定領域，例如協作文化、合規文化、網路安全文化、道德文化、平等文化、開放（透明）文化、風險文化、安全文化，以及高層基調等。

4.擬訂查核重點：在選定查核領域後，可運用加拿大環境與氣候變遷部審計與評估處所開發的 3 步驟模型擬訂查核重點，並納入查核計畫。

(1)第一步：理解期望的文化

審計人員須清楚地理解組織所設想的文化樣貌，以及組織如何向員工傳達這種文化，這些資訊將成為建構查核標準的基礎。

(2)第二步：檢視實際做法與流程的一致性

審計人員須檢視期望文化與組織實際做法、流程間的一致性，判斷預期的行為是否被獎勵、整合到流程中並被員工實踐。

(3)第三步：檢視監督流程與實踐

審計人員須檢視相關的監督流程與實踐，瞭解組織如何衡量、監督文化契合度，以及如何回應不當行為。

（二）審計人員如何蒐集證據？

審計人員應混合使用量化與質化工具如下：

1.蒐證技術：除訪談、調查、直接觀察、文件審查等傳統技術外，也可使用進階數據分析與文本分析等新興技術。

2.質化證據：訪談與焦點小組對於獲取敏感資訊非常有價值，但須注意高階主管的

看法可能過於理想化。

3.量化證據：匿名的員工調查可提供量化數據，以支持訪談中的觀察，但其結果也可能存在偏誤。

4.文件證據：可分析的文件包括道德準則、人力資源政策、高階主管會議紀錄等。

(三) 需要哪些技能？

雖然許多審計人員已具備所需技能，但文化審計特別強調下列事項：

1.設計與分析問卷的技能：由於文化審計常運用問卷調查，設計與分析問卷的技能顯然極具價值。

2.卓越的訪談與溝通技巧：由於文化議題常具主觀性及敏感性，特別是在與高階管理層訪談時，需要高超的技巧、機智與判斷力。

3.建立安全的訪談環境：使受訪者感到安全至關重要，審計人員須向受訪者保證其匿名性將受到保護。

4.專業知識與外部協助：審計人員可能需要接受特定領域的培訓，或在必要時聘請外部專家（如組織心理學家）。

(四) 審計人員如何報告敏感的文化觀察發現？

管理階層對於文化審計的查核發現可能採取防禦的心態，審計人員在撰寫報告前，應先與管理層溝通，並提供具體的觀察與範例，以支持觀點，又為使報告更為有效，審計人員應在報導負面發現與正面發現間取得平衡，例如彰顯模範行為或辨識最佳實務。

五、結論

多數審計人員於數年前並不認為查核組織文化是其職責的重要部分，但現在態度正在轉變。為能更熟練進行文化審計，審計單位自身的文化可能需要轉變為更善於追問「為什麼」，並深入挖掘缺失背後的文化根本原因。期望隨著時間、指引與經驗的累積，查核組織文化成為公部門審計的常規工作。