出國報告（出國類別：開會）

參加 2025 年全球審計、舞弊偵測及資訊科技大會

服務機關： 審計部

姓名職稱： 李副審計長順保、林科長東慶、鄭審計琰芳、林稽察文棟

派赴國家： 阿拉伯聯合大公國（阿布達比）

出國期間： 114 年 11 月 17 日至 11 月 22 日（共計 6 日）

報告日期： 115 年 2 月 2 日

摘要

本次出國奉派參加於阿拉伯聯合大公國阿布達比舉行之「2025 年全球審計、舞弊偵測及資訊科技大會」，該會議由國際內部稽核專業組織主辦，旨在回應人工智慧、數位科技及資料應用快速發展背景下，全球審計與稽核專業於舞弊防制、治理信任及組織韌性所面臨之新興風險與轉型挑戰。會議透過專題演講、實務案例及工具展示，探討審計專業由傳統事後查核，逐步轉向前瞻預警、策略支援及公共價值創造之發展方向，並就人工智慧治理、倫理規範及實務應用提出具體觀察與經驗分享，對我國推動智慧審計具重要參考價值。經綜整會議研討內容，謹提出以下五點具體建議：

一、深化審計願景對齊國際趨勢，以達成前瞻治理價值

會議中 IIA 全球主席於 Vision 2035 主題演講指出，未來審計專業須透過重新定位角色、強化能力基礎及擴大影響力，由缺失揭露者轉型為組織韌性與治理決策之重要夥伴。此一發展方向，與審計長所揭示之「智慧審計、永續審計、韌性審計及共臻善治」四大願景高度契合。未來推動重點，允宜持續深化巨量資料分析與風險導向方法之運用，並結合跨域協作機制，使審計成果能具體反映對政府韌性治理、永續政策推展及公共價值創造之實質貢獻。

二、留存 AI 運用軌跡強化審計透明，以達成可信成果

多場次研討指出，生成式 AI 與自動化工具廣泛應用後，若其分析過程欠缺透明與可追溯機制，易因模型偏誤、深偽技術或 AI 幻覺而放大治理風險。鑒於審計機關近年已廣泛運用 AI 輔助程式撰寫、資料蒐集及異常篩選，允宜將 AI 參與過程視為審計證據形成之一環，制度化留存重要問答紀錄、分析邏輯及人工修正說明，使審計結論形成具備完整軌跡，並展現審計機關於運用科技時之審慎態度與可問責性。

三、檢視本部現行 AI 治理規範，以確保倫理合規與實務一致

本次會議自治理與倫理角度，反覆強調 AI 應用須以人為最終判斷，並具備可被審計追溯之治理架構。我國人工智慧基本法已完成立法，確立政府機關使用 AI 應兼顧發展與安全之原則。就審計機關而言，允宜配合國內法制與國際趨勢，系統性檢視既有 AI 應用規定，涵蓋使用範圍界定、資料治理與安全控管、透明與可解釋要求、責任歸屬及人工覆核機制等面向，俾使制度設計與實務運作保持一致，持續鞏固審計專業公信力。

四、審慎評估 AI 工具適用情境，以強化輔助審計實務效益

會議介紹多項 AI 工具及其於審計與治理領域之應用案例，綜合評估後，生成式 AI 嵌入既有辦公環境之模式，尤以 Microsoft Copilot 整合 Microsoft 365 並支援文件審核、審計規劃及報告產製者，較符合審計機關以文字審核與分析為主之業務型態。後續允宜依實際使用經驗，持續蒐集對作業流程、效率及品質之影響，並就授權成本、維運負擔及擴充需求進行實證評估，作為調整應用範圍及資源配置之參考依據。

五、強化高層定調引導方向，以支持 AI 應用穩健推進

IIA 全球主席指出，組織推動新科技之關鍵，在於高層是否清楚定調方向並公開表達支持，使第一線人員得於明確框架下持續嘗試與修正。就審計機關實務而言，近年 AI 輔助審計已具多元實作基礎，允宜透過高階主管課程及案例說明，協助高層掌握整體推動現況與限制，並形成對可行與不可行應用情境之共通認知，使各單位得於一致定調下穩健累積經驗與成果，維持推動智慧審計之整體動能。

目錄

壹、目的

隨著全球數位轉型加速，人工智慧（Artificial Intelligence, AI）技術已廣泛滲透政府運作、企業經營及社會生活各層面。AI 於提升效率及精進決策之同時，亦衍生前所未有之挑戰，特別是在舞弊手法日益精進、網路攻擊趨於自動化，以及深度偽造技術（Deepfake）氾濫之背景下，傳統審計及舞弊偵測手段正面臨嚴峻考驗。

本屆「全球審計、舞弊偵測及資訊科技大會」即於前揭背景下召開。面對語音釣魚攻擊成長達 442%、勒索軟體高度武器化等威脅，審計機關與內部稽核部門亟需掌握新興科技，轉型為具備數位韌性之現代化確信提供者。此次會議旨在匯聚全球專家智慧，探討如何運用 AI 技術強化偵測能力，並同步因應 AI 所衍生之治理風險。參與本次會議之具體目的包括：

一、汲取新知：深入研析 AI 於審計及舞弊偵測領域之雙面應用，以及雲端治理、持續性控制監控（Continuous Controls Monitoring, CCM）及網路韌性等國際最新趨勢與實務案例。

二、標竿學習：借鏡各國審計機關及頂尖企業於數位審計、AI 治理及跨域協作（審計、舞弊偵測、資訊科技）方面之成功經驗與面臨挑戰，作為本部策進相關業務之參考。

三、拓展網絡：與全球審計及舞弊偵測專家建立聯繫，深化國際合作，並就跨境金融風險及數位資產監理等議題交換意見。

參與本次會議之目的，除在於掌握國際間最新舞弊偵測趨勢及 AI 審計工具外，亦著重於借鏡先進國家之治理框架（如 COBIT、NIST AI RMF 等）與實務經驗，作為我國推動審計數位轉型、強化資通安全管理法制落實，以及建構政府數位信任體系之重要參考。透過與國際同業之交流，期能建立跨國協作網絡，共同因應無國界之數位犯罪挑戰，並提升我國於國際審計領域之能見度與專業能量。

貳、參加會議過程

一、 主辦單位簡介

本次大會由三個國際級專業組織聯合主辦，凸顯現代審計監督必須跨越傳統界線，整合多元專業職能：

(一)阿拉伯聯合大公國內部稽核師協會（UAE Internal Auditors Association, UAE IIA）

阿拉伯聯合大公國內部稽核師協會（UAE IIA）成立於 1984 年，係中東地區最早成立之內部稽核專業組織之一。該協會隸屬國際內部稽核師協會（The Institute of Internal Auditors, IIA Global）全球網絡，致力推動內部稽核專業標準、精進從業人員能力，並促進公私部門治理及風險管理之現代化。UAE IIA 之成立，源於阿拉伯聯合大公國政府推動經濟多元化及治理現代化之政策背景。1970 年代石油危機後，海灣國家體認單一經濟結構之脆弱性，爰開始強化內部控制與審計機制，以確保公共資源之有效運用及透明問責，UAE IIA 即於此一脈絡下應運而生，成為推動該國審計專業化之重要力量。

歷經四十餘年發展，UAE IIA 已成為中東北非地區（MENA Region）具高度影響力之專業組織之一，不僅服務本國會員，亦積極參與區域及全球審計網絡建構，並多次舉辦具國際影響力之研討會與培訓活動。截至 2025 年，UAE IIA 擁有逾 2,000 名個人會員及 150 家機構會員，涵蓋政府審計機關、國有企業、跨國公司及金融機構，會員分布於阿布達比、杜拜、沙迦等主要酋長國，形成緊密之專業網絡。協會設有理事會（Board of Directors）、專業委員會（包括 IT 審計、舞弊偵測及治理等委員會）及區域分會。現任主席 Abdulkadir Ahmed Ali 先生於 2023 年就任，其任內推動治理中心（Governance Hub）、品質保證成熟度模型（QA Maturity Model）及內部稽核大使計畫（IA Ambassador Program）等三大策略倡議，展現前瞻之專業願景。

(二)國際舞弊偵測稽核師協會（Association of Certified Fraud Examiners, ACFE）

國際舞弊偵測稽核師協會（ACFE）成立於 1988 年，總部設於美國德州奧斯汀，為全球規模最大之舞弊偵測專業組織，於全球擁有逾95,000名會員，遍布160個國家及地區，會員背景涵蓋內部稽核師、會計師、鑑識會計專家、法務人員、執法機關及政府部門等多元領域。該協會之核心使命，在於降低全球職務舞弊（Occupational Fraud）發生率，並協助舞弊偵測專業人員發現及遏止舞弊行為。

ACFE 每兩年發布一次《職務舞弊報告：全球研究》（Report to the Nations），為全球舞弊偵測領域最具影響力之研究文獻。2024 年版（第 13 版）報告分析來自 138 個國家及地區共 1,921 件真實舞弊案例（調查期間為 2022 年 1 月至2023年9月），揭示舞弊案件總損失金額逾31億美元、中位數損失為145,000美元、22%案件之損失金額達100萬美元以上、舞弊案件平均持續期間為12個月，且 43%之舞弊案件係透過檢舉揭發，為次常見方式內部稽核之 3 倍以上；其中以資產挪用（Asset Misappropriation）為最常見之舞弊類型，占比達 89%，顯示相關風險之普遍性。

另ACFE所提供之CFE（Certified Fraud Examiner，國際舞弊稽核師）認證，係全球舞弊查核、控管及安全等專業領域中具高度指標性之認證資格，自 1988 年推出以來，已成為查弊及防弊專業人員之重要認定標準，持證人涵蓋企業內部稽核、政府執法機關、會計師事務所、金融機構及法務部門等多元領域。

(三)資訊系統稽核協會（Information Systems Audit and Control Association, ISACA）

資訊系統稽核協會（ISACA）成立於 1969 年，原名為「資訊系統稽核與控制協會」，隨著數位科技快速演進，現已發展為全球資訊治理、風險管理、資通安全、隱私及新興科技領域具高度影響力之專業組織，全球會員人數逾 185,000 名，遍布 180 餘國，並設有超過 225 個地區分會（Local Chapters），為 IS／IT 專業人員提供全方位之職涯支持。其核心專業領域包括 IT 治理（透過 COBIT 框架協助組織整合 IT 目標與業務策略目標，以實現價值創造、風險管理及資源最佳化）、資訊安全審計（建立系統化之稽核方法，以評估組織資訊系統之可用性、機密性及完整性）、風險管理（協助組織識別、評估及管理資訊系統相關風險）、資料隱私（推動隱私保護最佳實務及合規要求），以及新興科技（聚焦 AI、雲端及區塊鏈等新興科技之治理與審計）。

另 ISACA 提供多項業界高度認可之專業認證，涵蓋稽核、資通安全、風險、隱私及治理等領域，其中 CISA（Certified Information Systems Auditor，國際電腦稽核師）自 1978 年推出以來，已成為資訊系統、審計、控管、監督及評估等領域之全球成就標準，目前全球持證人數逾 46,000 人，認證內容涵蓋資訊系統稽核流程、IT 治理與管理、資訊系統之取得、開發與實施、資訊系統之營運與業務韌性，以及資訊資產保護等五大領域，並強調以風險導向（Risk-Based Approach）進行稽核規劃、執行及報告之能力。CISA 認證亦為我國「公開發行公司建立內部控制制度處理準則」所定內部稽核人員適任條件之一，並為數位發展部資通安全署認可之資通安全專業證照。

二、會議主題及議程

本屆會議首次將 AI 技術列為核心主軸，反映出全球審計專業對數位轉型的迫切需求，會議主題「Stronger Together: Elevating Assurance, Innovation & Fraud Prevention」（團結更強：提升確信、創新與預防舞弊），吸引超過 1,050 位來自 38 個國家的專業人士。

圖 1 本團團員與會合照

會議議程相關資料彙整如下：

■ 11 月 19 日（三）- 會議日（第一日）

時間	地點	內容
08:00-09:00	展覽區	登記與咖啡休息時間
09:00-09:10	主會場	開幕典禮暨致詞
09:10-09:50	主會場	在兆美元詐騙時代重建信任
09:50-10:30	主會場	AI 心靈術—如何讓不可能成為可能
10:30-11:00	主會場	咖啡休息與交流時段
11:00-11:50	主會場	稽核長的新使命：創新治理、網絡韌性與倫理風險領導
11:50-12:30	主會場	從創新到開發運用：人工智慧在資安領域的陰暗面
12:30-13:30	主會場	午餐與禱告時間
13:30-14:10	多個會廳	同步場次
宴會廳 1：網路風險稽核與資訊科技控制 宴會廳 2：當調查導致訴訟時 宴會廳 3：信任人工智慧—為什麼重要以及如何建立		
14:20-15:00	多個會廳	同步場次
宴會廳 1：爐邊談話/稽核角色轉型 宴會廳 2：超越熱烈討論：AI 跨部門實務應用 宴會廳 3：從洞察到確信—在內部稽核中部署 Microsoft Copilot		
15:00-15:40	多個會廳	同步場次
宴會廳 1（15:00-15:20）：現場展示與客戶成功案例-運用人工智慧驅動持續性控制監測(CCM) （15:20-15:40）：AI 驅動 CCM 自動化過程之挑戰與啟示 宴會廳 2：利用既有審計技術採用 AI 之策略與實踐 宴會廳 3：人工智慧對抗舞弊—終極貓捉老鼠遊戲		
16:00-18:00	交流時段	為參會者提供寶貴的社交機會，促進潛在合作與知識分享

■ 11 月 20 日（四）- 會議日（第二日）

時間	地點	內容
08:00-09:00	展覽區	登記與咖啡休息時間
09:00-09:10	主會場	贊助商暨品質保證感謝典禮
09:10-09:50	主會場	IIA 全球主席主題演講—成為未來 2026-2025
09:50-10:40	主會場	動盪中的領導之道：策略、治理與韌性
10:40-11:20	主會場	咖啡休息與交流時段
11:20-12:00	主會場	確保人工智慧倡議妥善治理之管理
12:00-12:50	主會場	專題討論-航空業內部稽核：應對頑固的顛簸
12:50-13:50	主會場	午餐與禱告時間
14:00-14:40	主會場	企業防舞弊指南：預防與偵測實務
14:40-15:30	主廳	結合審計、舞弊偵測與資訊科技優勢，打造韌性治理體系

參、會議探討議題

本次會議議程涵蓋 AI 治理、舞弊偵測、內部稽核轉型及組織韌性四大主軸，由阿拉伯聯合大公國內部稽核師協會（IIA UAE）主席 Abdulqader Obaid Ali 致開幕詞，邀集 IIA 全球主席 Stefano Comoti 及 ACFE 專家 John Edwards 等貴賓，及全球產官學界專家共同參與，進行深入研討。茲摘錄重點如次：

一、UAE IIA 主席開幕致詞：三大策略倡議的前瞻擘劃

IIA UAE 主席於致詞中首先回顧 UAE IIA 過去一年之重要成果，包含會員人數成長突破 2,000 人、辦理逾 50 場專業培訓活動，以及與多國審計機關建立合作關係。嗣後，正式宣布協會未來三大策略倡議，旨在引領中東北非地區審計專業之現代化發展。

第一項倡議為「治理中心」（Governance Hub），其設立背景係因應中東地區企業治理需求快速成長，尤以家族企業轉型為專業經營之過程中，對董事會治理及風險管理專業知識之需求尤為殷切，爰與國際董事協會（IOD）合作設立專責治理知識中心，開發線上治理資源平台，提供最佳實務案例及政策範本，並規劃董事認證培訓課程，涵蓋風險治理、倫理決策及策略監督等主題，俾提升高階管理層及董事會之治理專業能力，強化組織韌性，並促進區域治理標準與國際接軌。

第二項倡議為「品質保證成熟度模型」（QA Maturity Model），該模型係以IIA 全球品質保證與改進計畫（QAIP）框架為基礎，聚焦人員（專業能力及倫理操守）、流程（審計方法論標準化及風險評估機制）、績效（建議採納率及價值創造指標）及品質（內部品質審查及持續改進機制）等四大支柱。組織得透過線上自評工具進行成熟度評估，區分為五級（初始級、發展級、定義級、管理級及優化級），俾協助內部稽核部門進行基準比較（Benchmarking），識別改進機會，並作為爭取資源及高階支持之客觀依據。

第三項倡議為「內部稽核大使計畫」（IA Ambassador Program），透過導師制（Mentorship）及知識傳承，培育新世代審計領袖，並擴大內部稽核專業之社會影響力。該計畫遴選資深審計執行長（CAE）及專家擔任大使，每位大使負責指導3 至 5 名年輕審計人員，並定期前往大學、企業及政府機關進行專業倡議，以提升內部稽核之能見度；另每年舉辦「大使論壇」，表揚傑出貢獻者並分享成功案例，俾加速專業知識傳承，吸引優秀人才投入內部稽核領域，並強化專業社群之凝聚力。

表 1 UAE IIA 三大策略倡議總覽

倡議名稱	核心目標	主要內容	預期效益
治理中心(Governance Hub)	提升區域企業治理專業能力	• 與 IOD 合作建立知識中心 • 線上治理資源平台 • 董事認證培訓課程	• 強化董事會治理能力 • 促進治理標準國際接軌 • 支援家族企業專業化轉型
品質保證成熟度模型(QA Maturity Model)	建立稽核品質評估標準	• 四大支柱：人員、流程、績效、品質 • 五級成熟度分級 線上自評工具	• 協助稽核部門基準比較 • 識別改進機會 • 爭取資源與高階支持
內部稽核大使計畫(IA Ambassador Program)	培育新世代審計領袖	• 資深 CAE 擔任大使 • 1 對 3-5 導師制 • 年度大使論壇	• 加速專業知識傳承 • 吸引優秀人才 • 提升專業能見度

資料來源：整理自 UAE IIA 主席開幕致詞。

二、場次一：在兆美元舞弊時代重建信任（ Rebuilding Trust in The Era of Trillion-Dollar Fraud）

(一) 信任危機的三重維度與數位韌性新定義

在數位轉型加速及 AI 技術普及之背景下，如何於擁抱創新之同時，兼顧網路安全並重建數位信任，已成為全球審計與治理專業所面臨之核心挑戰。本場次由 Monica Verma 主講，憑藉其於 AI 倫理及網路安全領域之深厚背景，從技術、心理及社會三重視角，剖析 AI 對信任機制所造成之衝擊。

講者首先指出，隨生成式 AI 技術廣泛應用，「眼見為憑」之傳統信任基礎正同時面臨視覺、聽覺及認知等三個層面之嚴峻挑戰，其中以生物特徵驗證之脆弱性尤為顯著。銀行業普遍使用之語音身分識別系統，現已可透過僅 15 秒之音頻樣本遭 AI 複製，且成功率逾 90%；深度偽造技術亦可即時生成動態影像，繞過活體偵

測（Liveness Detection）機制，「眼見不再為憑，耳聽不再為真」（Seeing and hearing is no longer believing）已成為數位時代之新現實。相關數據顯示，語音釣魚（Vishing）攻擊年增長率高達 442%，且 2024 年英國發生之單一深偽（Deepfake）詐欺案件，損失即達 2,500 萬美元，顯示信任危機已非危言聳聽。

講者並以愛爾蘭總統選舉深偽攻擊事件為例說明，於 2024 年愛爾蘭總統選舉期間，一名候選人遭深度偽造影片攻擊，影片中其發表極端言論並攻擊對手，攻擊者係利用該候選人之公開演講影片訓練 AI 模型，生成高度逼真之假影片，並透過社群媒體快速擴散。雖競選團隊即時澄清，惟假訊息已造成支持度下滑約 8 個百分點，凸顯深偽攻擊對民主進程之重大威脅。該案例顯示，傳統「事後澄清」策略效果有限，組織亟需建立主動之深偽偵測及快速回應機制。

進一步而言，現代舞弊已演變為高度組織化之「舞弊即服務」（Fraud-as-a-Service）產業，攻擊者可輕易透過暗網取得自動化工具與個人資料，並運用機器人進行全天候之魚叉式網路釣魚，致使傳統防禦手段難以有效因應。Monica 指出，傳統網路安全（Cybersecurity）思維多著重於「預防入侵」，惟於 AI 時代，組織須轉向「韌性思維」，不再僅關注「是否會遭受攻擊」，而應聚焦「遭受攻擊後如何快速復原」，並建構「零信任架構」（Zero Trust Architecture），對各項存取請求進行持續驗證，而非依賴單一身分認證，同時於高風險決策（如大額轉帳及權限變更）中保留人為覆核機制，避免完全倚賴 AI 自動化。

（二）重建數位信任的四大支柱與審計實務啟示

面對前揭險峻情勢，講者提出重建數位信任之四大支柱：一、透明度（Transparency），係向使用者清楚說明 AI 系統之運作方式及所使用之數據；二、可解釋性（Explainability），係 AI 決策須具可供審計追蹤之能力，尤以涉及民眾權益事項為然；三、問責性（Accountability），係明確界定 AI 系統發生故障或誤判時之責任歸屬；四、韌性設計（Resilience by Design），係於系統設計階段即納入異常偵測、備援機制及人為介入節點。

講者並強調，組織須建構涵蓋技術、人員、流程、治理及合規等五大防禦支柱。在技術層面，應部署深偽偵測工具（如 Microsoft Video Authenticator），並落實多因子生物特徵驗證；在人員層面，則須透過社交工程演練，建立「質疑文化」，鼓勵員工對異常指令進行二次確認。此外，於治理層面，應落實透明化原則，公開揭露 AI 使用範圍，並建立倫理審查機制，俾確保組織於擁抱創新技術之同時，亦能有效控管新興風險，重建數位時代之信任基石。

表 2 數位信任四大支柱與組織防禦五大支柱

支柱類別	支柱名稱	核心要求	實務作法
數位信任四大支柱	透明度 (Transparency)	清楚說明 AI 系統運作方式與數據使用	• 公開 AI 演算法邏輯 • 揭露訓練數據來源 • 說明決策影響範圍
	可解釋性 (Explainability)	AI 決策必須能被審計追蹤	• 建立決策軌跡記錄 • 提供決策理由說明 • 支援人工覆核機制
	問責性 (Accountability)	明確定義責任歸屬	• 建立 AI 治理委員會 • 定義故障責任鏈 • 設立申訴管道
	韌性設計 (Resilience by Design)	系統設計階段即納入防禦機制	• 異常偵測機制 • 多重備援系統 • 人為介入點設計

支柱類別	支柱名稱	核心要求	實務作法
組織防禦五大支柱	技術層面	部署防禦工具與驗證機制	• 深偽偵測工具（如 Microsoft Video Authenticator） • 多因子生物特徵驗證 • 加密數位簽章
	人員層面	建立「質疑文化」	• 社交工程演練 • AI 識讀培訓 • 異常指令二次確認機制
	流程層面	強化驗證程序	• 多管道驗證機制 • 「冷靜期」制度 • 實體簽核要求
	治理層面	透明化與問責	• 公開 AI 使用範圍 • 建立倫理審查機制 • 定期治理評估
	合規層面	符合法規與標準	• 遵循 AI 倫理準則 • 符合隱私法規要求 • 建立合規查核機制

資料來源：整理自 Monica Verma 專題演講。

就審計實務啟示而言，首要在於信任機制之根本性轉變。傳統身分驗證方式（如語音及臉部辨識）已難以確保可靠性，「眼見為憑」之時代已告終結，審計人員須重新評估組織之驗證及授權控管機制，是否足以因應 AI 偽造所衍生之威脅。其次，係由防禦思維轉向韌性思維，組織應由「預防入侵」之既有思維，轉為「假設已遭入侵」之韌性導向，並建構快速偵測、回應及復原機制。

具體建議包括：審計應確認組織於高風險交易（如大額轉帳及權限變更）是否建置多管道驗證機制，而非僅倚賴單一生物特徵或影音證據；檢視組織是否採行零信任架構（Zero Trust Architecture），對各項存取請求進行持續驗證，而非依賴一次性身分認證；並協助組織建立 AI 倫理與治理框架，確保透明度、可解釋性、問責性及韌性設計等四大支柱之具體落實。

三、場次二：AI 心靈術互動工作坊（AI Mentalism－ How to make the impossible ... possible）

以下為 2025 年「全球審計、舞弊偵測及資訊科技大會」中，由瑞士心靈術師兼經濟學家克里斯蒂安·比紹夫（Christian Bischof）所呈現之「AI 心靈術」表演摘要：

（一）序幕：心靈與審計專題之共鳴

表演伊始，比紹夫即結合大會主題，引導觀眾進行「心靈暖身」。其列舉多項與審計及資訊科技相關之主題，包括網路風險（Cyber Risk）、法律索賠管理（Legal Claims Management）、人工智慧信任（Trust in AI）、持續性控制監控（CCM）、預測分析（Predictive Analytics）及舞弊預防（Fraud），並請現場二百餘名觀眾隨機自其中擇一感興趣之主題。比紹夫強調，該等選擇完全屬隨機且具保密性，即便其與在座觀眾相識，亦無從得知其內心所選。為進一步展現互動之隨機性，比紹夫邀請三位於座位下發現金箔糖果之觀眾起身，作為後續連結之代表；並另行挑選一位予人高度信賴感之觀眾阿里（Ali），將一只內含「驚喜」之神祕信封交由其保管，約定僅於表演最後之關鍵時刻始得揭曉。

（二）夢境冒險與 AI 虛擬化身之介入

隨後，比紹夫以拋接紙球方式選出一名觀眾 Azat，邀其共同構築一段「魔幻夢境」。在引導式想像中，雙方跨越國界，最終降落於世界上任一國家，該名觀眾最終選擇加拿大（Canada）。比紹夫接續揭示其「AI 心靈術師」之身分，並展示一具於網路流傳之「深偽虛擬化身」（Deep Fake Avatar）。該虛擬化身聲稱已掃描比紹夫全部魔術筆記，並可與其即時對話。比紹夫指出，面對日益精進之 AI 技術，人類與其對抗不如學習如何妥善運用，以創造實質價值。

（三）數位駭客：人類與 AI 之協作

表演進入高潮之一之「密碼破解」環節。現場觀眾受邀於筆記本上隨機書寫多組五至六位數之數字（如手機解鎖碼或信用卡驗證碼），並將該等數字加總形成一組秘密隨機總和。比紹夫先以人類感官進行推測，成功辨識該六位數密碼之首位數字為「2」。其後，餘下之破解任務交由虛擬化身執行。儘管過程中出現短暫之 AI 算力誤判（曾將末兩位數誤判為 38），惟於比紹夫要求化身「啟動超級能力」後，虛擬化身即準確報出完整六位數密碼「291077」，展現人類與 AI 協作所能達成之高度可能性。

（四）全場互動：預見未來之儀式

接續，比紹夫邀請全體觀眾共同參與一場關於「未來」之集體互動。每位觀眾自座位取出卡片，於其中一張書寫自身姓名作為「幸運卡」，並依循比紹夫引導，配合大會主題（如網路風險、法律管理、CCM 等）進行多次洗牌、翻轉及位置移動。儘管過程中包含與鄰座交換卡片等隨機變數，然於最終揭曉時，多數觀眾驚訝發現，留於手中之最後一張卡片，正係印有自身姓名者，象徵每位參與者皆掌握屬於自身之「未來選擇」

（五）最終揭曉：預言之實現

表演尾聲，比紹夫以紙球方式隨機選出顏色（黃色）及時鐘整點（3 點鐘），並請保管神祕信封之阿里揭曉內容。信封內為比紹夫於會前即完成之畫作，其內容精準對應觀眾於現場隨機選擇之「3 點鐘」，完成整場預言。最後，比紹夫嘗試感應最後一位觀眾對「大數據」（Big Data）之內心聯想，並以鼓舞人心之語作結，強調於科技快速演進且充滿不確定性之時代，更須保有對未來之想像與突破既有限制之勇氣。整體而言，該場表演猶如一套精密之審計程序，表面看似隨機且充滿變數，惟透過邏輯、技術與心智之交織運作，最終仍能導引至高度一致且令人震撼之結果。

四、場次三：稽核長的新使命：創新治理、網絡韌性與倫理風險領導（The CAE's New Mandate: Innovation Governance, Cyber Resilience & Ethical Risk Leadership）

本場次採專家座談形式，聚焦探討於 AI 與數位轉型快速演進之時代，稽核長（CAE）之使命是否於本質上產生改變，抑或係面臨嶄新挑戰。主持人於開場即提出核心問題指出，「眼見為憑、耳聽為真」向為審計人員執行業務之重要基礎，惟於深偽與 AI 普及之時代，該一基礎正面臨根本性挑戰，爰有必要審慎思索因應之道，以在不偏離 CAE 角色本質之前提下，展開相關討論。茲摘錄重點如次：

（一）信任與敏捷：創新環境中的稽核定位

Martin Schneider 以其於 Meta（前 Facebook）任職六年之實務經驗，分享內部稽核人員如何於創新驅動之環境中，同時扮演挑戰者與賦能者之角色。其強調，一切關鍵在於信任（It all comes down to trust）。內部稽核最重要之任務，在於取得董事會、高階管理層及執行團隊之信任，該等信任使審計人員得以「在決策現場」（be in the room when decisions are being made），成為策略形成過程之一環，並於公司策略研擬階段即能參與其中。

此一信任關係，使審計人員具備挑戰新技術之正當性，並得於決策形成時受邀提供意見，持續履行內部稽核之核心使命，即為高階管理層提供建議，協助組織以負責任且受控之方式推動創新，同時確保具備進行測試之能力與信任基礎。其並指出，「信任、取得權限、妥適執行工作」（Trust, access, and doing a good job）為三大關鍵要素。

為有效執行相關任務，審計人員須具備高度敏捷性，並於確信業務（assurance）與諮詢顧問（advisory）角色之間取得適當平衡，同時維持足夠彈

性，以因應組織創新節奏。爰此，內部稽核除須確保作業品質外，亦應扮演值得信賴之專業顧問角色。

（二）創新治理的適應性：從檢核表到風險思維

ISACA 專家 Bruno Horta Soares 自治理視角剖析審計如何賦能創新。其指出，創新並非僅止於簡報呈現，亦非單一工具之運用，真正關鍵在於思維方式之轉變。Bruno 強調，當開始以風險視角及非線性視角進行思考，即已具備持續創新之基礎，所追求者並非一次性「做創新」，而係能夠不斷延續之創新能力。

其並以歐盟 AI 法案為例說明，監管機構重點並非規範技術本身，而係聚焦於技術之使用案例，顯示監理思維已由傳統合規導向，轉為以風險及使用情境為核心之管理模式。Bruno 進一步回顧三次重要之思維轉變，包括：2002 年由紙本作業轉向 Excel（由會計重大性轉為流程風險）、2016 年 GDPR 時期（由規定性要求轉為風險對齊之控制機制），以及 AI 時代（由確定性系統轉向機率性演算法）。其並指出，倘仍僅依賴檢核表式之打勾作業，將可能淪為阻礙創新之因素。

（三）創新速度超越治理時的平衡之道

資訊稽核長 Robert Findlay 以「高階管理層如同欲打造獨木舟之孩童」為喻，說明組織導入 AI 時，往往未能周延考量其後果。其強調，審計須持續維持攸關性，並扮演「房間裡的成年人」，於參與過程中同步進行引導與教育，並適時提醒問責所在。其指出，欠缺治理之創新終將失敗，惟未能因應創新之治理亦將流於過時。

另就獨立性與參與度之平衡而言，Robert 表示，最具挑戰之處在於如何於不損及獨立性之前提下，適度嵌入專案運作。審計工作須於高度複雜之情境中，審慎拿捏自身定位，既維持專業獨立性，亦能即時提供具體且具價值之意見。

（四）IT 技能缺口、通才素養與 ESG 審計經驗

Bruno 指出，審計人員無須與受查對象競逐專業知識，其表示：「審計人員未必成為 AI 專家，惟仍可在未成為專家之前提下，進行 AI 之審計、管理與討論。」其關鍵在於能否提出適切問題，並理解回應內容。Martin 亦補充，Meta 團隊之內部稽核人員多屬通才（Generalist），具備分析能力、好奇心及毅力，而非侷限於特定領域之專家。通才並非獨立作業者，而係擔任連結不同專業之橋樑角色，其並指出，「需要引進更多通才，使其能與專家有效互動」。

Robert 則推薦《Range》一書，強調通才於高度專業化之環境中所具備之價值。另其分享實務經驗，說明其團隊曾投入三日於工廠現場拍攝電表照片，肇因於 ESG 數據未有明確負責單位，反使審計成為唯一掌握整體情況之團隊，並因此建立高度信任關係。其建議，審計人員不應畏懼新事物，應主動投入，發揮自身所長，包含瞭解流程、分析數據及持續追蹤事項。

（五）審計領袖必須立即培養的技能

座談會最後，主持人請各專家提出當前審計領袖亟須培養之關鍵能力。Robert Findlay 強調 IT 技能及業務語言表達能力，其指出，審計報告應以業務意涵加以說明，而非僅使用專業術語，亦即須具備將技術用語轉譯為業務語言之能力，方能使審計結論對報告使用者產生實質意義。Bruno 則著重於風險思維，強調應理解不確定性所伴隨之風險，而非僅依循風險檢核表進行判斷。Martin 亦呼應並提醒審計人員不必畏懼，其表示，即使未必較受查對象更熟稔其業務，亦毋須退卻，因審計人員最具優勢者在於掌握分析架構與風險管理能力，應善用該等專長，引導對話回歸至熟悉且可有效討論之領域。

五、場次四：從創新到開發運用：人工智慧在資安領域的陰暗面（ From Innovation to Exploitation: The Dark Side of AI in Cybersecurity）

AI 技術猶如雙面刃，於帶來效率提升與創新動能之同時，亦為犯罪者提供前所未有之強大工具。本場次由資深資訊安全專家 Ramona Ratiu 主講，揭露 AI 技術遭武器化之實際案例，並以具體數據及影像佐證，警示全球審計與風險管理專業須正視此一「AI 軍備競賽」所衍生之嚴峻現實，茲摘錄重點如次：

（一）核心論點：AI 必須被約束，不可自主決策

Ramona 於開場即提出一項具爭議性且極具關鍵性之觀點，指出「必須如同教導孩童般，為 AI 設定明確邊界，絕不可允許 AI 於無人類監督之前提下，自主作出重大決策。」其進一步說明，當前不少組織過度信賴 AI 之「理性」與「客觀性」，卻忽略 AI 本質係以歷史數據為基礎建構之統計模型，既可能承襲人類既有偏見，亦可能遭受惡意操縱。其並指出，AI 作為強大之欺騙工具，具備三項主要特性：一、低門檻，深偽生成工具已趨商品化，無須具備專業技術背景即可操作；二、高逼真，生成內容之真實度已達專家亦難以辨識之程度；三、快速擴散，透過社群媒體，假訊息得於短時間內迅速觸及數百萬人。

（二）深度偽造詐欺：真實案例與衝擊分析

於金融詐欺領域，Ramona 詳述兩起具代表性之重大案例。其一為 2023 年歐洲某能源公司遭詐欺轉帳 1,000 萬美元案件，該公司財務長接獲自稱「執行長」之緊急來電，要求立即將 1,000 萬美元匯至指定帳戶，以完成一項機密併購交易。詐欺者事前蒐集執行長公開演講影片訓練 AI 語音模型，透過 AI 生成之執行長語音進行電話指示，並同步傳送偽造之電子郵件與文件（其標誌及簽名均由 AI 生成），以強化指示之可信度，復以時間壓力（如「交易窗口僅剩 2 小時」）阻斷財務長進行

多重驗證。最終，財務長於無法即時聯繫執行長之情況下完成轉帳，數日後始發現受騙，惟資金已轉移至多個離岸帳戶而難以追回。該案例顯示，多媒體組合攻擊（語音、電子郵件及文件）顯著提升詐欺成功率，傳統「回電確認」作法已不足以因應。

另一起更為嚴重之案例，係 2024 年初香港某跨國公司發生之 2,500 萬美元深偽視訊會議詐騙案。該公司財務部門人員參與一場視訊會議，與會者包含「財務長」及多名「總部同事」。詐欺集團透過社交工程事前蒐集公司高層照片及語音樣本，運用深度偽造技術即時生成多位高層之動態影像與語音，於會議中由「財務長」指示員工分別執行 15 筆轉帳，累計金額達 2,500 萬美元；會議中之「同事」皆以符合其平日風格之語氣與用語附和，具高度說服力。事後該名員工回憶，雖注意到「財務長」之背景環境與平時辦公室略有差異，惟當下未生疑慮。該案震撼全球金融業界，並促使多數機構重新檢視視訊身分驗證之可靠性。

就防禦作法而言，建議包括：對於高風險決策，應採多管道驗證機制（如回撥至既有且已確認之電話號碼，或詢問僅當事人知悉之私密問題）；建立「雙人授權」機制，使單一人員無法獨立完成大額轉帳；並加強員工教育訓練，提升其辨識深偽影像細微特徵之能力（如眨眼頻率異常或光影不一致等）。

（三）語音釣魚與 AI 驅動的攻擊激增

依據資安公司發布之全球威脅報告，2024 年上半年語音釣魚攻擊較前一年同期成長 442%，其中逾八成案件係運用 AI 語音複製技術。AI 語音複製技術之易得性尤值關注，僅需約 15 秒之目標語音樣本，即可透過 Resemble.ai 等商用平台生成高度逼真之語音，且基礎版本多為免費，專業版月費約介於 50 至 200 美元間；

其生成語音已可複製情緒、口音及語速等細微特徵，致使辨識難度大幅提高。常見攻擊情境包括：「老闆」緊急指示（員工接獲自稱「主管」之電話，要求即時提供敏感資訊或執行特定操作）、「親友」求助（假冒親友聲音，聲稱遭遇緊急狀況而需金錢援助），以及「客戶」驗證（針對銀行電話客服系統之語音身分驗證機制發動攻擊，以竊取帳戶資訊）。

Ramona 並特別提及 2024 年羅馬尼亞總統選舉期間發生之深偽語音事件。選舉前夕，大量深偽語音訊息透過社群媒體迅速擴散，內容為候選人發表極端民族主義言論，雖競選團隊即時澄清，惟假訊息已對選情造成重大影響，引發選舉結果之高度爭議，最終由憲法法院裁定選舉無效並須重新舉行。該案係首次以「AI 假訊息」為由取消國家層級選舉，亦引發國際社會對 AI 治理議題之高度關注與迫切討論。

（四）勒索軟體與網路攻擊的 AI 化

於勒索軟體領域，關鍵數據顯示，89%之勒索軟體攻擊已整合 AI 或生成式 AI 技術，主要應用於：自動掃描並鎖定備份系統（傳統勒索軟體多僅攻擊主系統，AI 版本則優先破壞備份）、以 AI 撰寫具高度針對性之釣魚郵件以提升開信率與點擊率，以及依受害者財務狀況與支付意願動態調整勒索金額。其演進趨勢顯示，攻擊模式已由「雙重勒索」（資料加密加上威脅公開）進一步演變為「四重勒索」，包括：第一重以資料加密要求贖金；第二重威脅公開敏感資料；第三重對受害者客戶發動 DDoS 攻擊以施加間接壓力；第四重則直接聯繫受害者之客戶與合作夥伴，告知資料外洩情形以損害其商譽。

另 DDoS 攻擊之成長幅度亦相當驚人，2023 年至 2024 年間，Web DDoS 攻擊流量成長 549%，峰值達每秒 1,460 萬次請求。其背後之 AI 驅動因素包括：AI 優化攻擊模式以規避傳統防火牆規則、AI 協調殭屍網路（Botnet）以提升攻擊效率，

以及 AI 即時分析防禦反應並動態調整攻擊策略。隨著「網路犯罪即服務」（Cybercrime-as-a-Service）產業化發展，相關威脅更趨嚴峻。以「Rain Maker Lab」勒索軟體平台為例，其採訂閱制商業模式，月費 389 美元，即提供完整勒索軟體套件，服務內容涵蓋攻擊工具、加密演算法、匿名通訊管道、比特幣洗錢服務，並提供 24 小時全年無休之技術支援、攻擊成效分析及所謂「售後服務」（協助談判），大幅降低犯罪門檻，使未具技術背景者亦能發動高度複雜之攻擊。另依 IBM《2024 年資料洩露成本報告》，企業每發生一次資料洩露事件，平均損失高達 440 萬美元。

（五）其他新興 AI 威脅與防禦策略

於市場操縱風險方面，2023 年曾有一張由 AI 生成之「五角大廈爆炸」影像於社群媒體流傳，該影像發布後僅 4 分鐘內，美國股市即出現劇烈波動，道瓊指數一度下跌逾 100 點。由於影像逼真度極高，多家媒體於初期未能即時辨識為假訊息，致其快速擴散。另 LinkedIn 假冒招募舞弊亦日益猖獗，舞弊者利用 AI 生成之專業頭像與履歷，冒充知名企業招募人員，誘使求職者提供個人資料、銀行帳戶（聲稱作為薪資轉帳用途）或支付所謂「培訓費用」，LinkedIn 於 2024 年間已移除逾 10 萬個由 AI 生成之假帳號。

Ramona 於演講結尾強調，面對 AI 所帶來之威脅，「批判性思維」（Critical Thinking）為較任何技術工具更為關鍵之防線，其內涵包括：質疑表象（不輕信任何未經驗證之影音或文字訊息）、多管道驗證（透過不同通訊方式交叉確認重要指示）、持續學習（瞭解最新 AI 技術以識別其弱點），以及建立組織文化（鼓勵員工提出質疑，而非盲目服從權威）。

六、同步場次（宴會廳 1）

宴會廳 1 於 11 月 19 日下午舉辦三場連續專題，聚焦網路風險之快速演變，以及 AI 與自動化技術對控制環境與內部稽核角色所帶來之全面性衝擊。隨著攻擊手法橫跨惡意程式、深度偽造、雲端弱點及資料汙染等多重面向，企業亟需同步強化治理韌性，並由傳統之靜態查核模式，轉型為連續監控與智慧審計。於此脈絡下，稽核人員除須確保合規性外，亦應協助組織建構具前瞻性之風險管理能力，茲摘錄重點如次：

（一）第一場：網路風險稽核與資訊科技控制（Cyber Risk Audits & IT Controls）

本場次由 Elwalid Beddi（Protiviti 副總監）及 Sidhartha Jain（Protiviti 副總監兼 IT 審計創新負責人）主講，聚焦網路風險之快速演變，以及 AI 與自動化技術對控制環境與內部稽核角色所造成之全面性衝擊。講者指出，新興科技之導入往往伴隨攻擊面之擴張，組織所面臨之威脅已由傳統病毒及惡意程式，擴展至更為複雜之多重風險樣態，包括：AI 生成詐騙（運用生成式 AI 製作假發票、假合約或假授權文件，以規避既有驗證機制）、資料外洩（敏感資料因雲端設定不當、內部人員或供應鏈弱點而外洩）、雲端設定錯誤（雲端服務快速部署致存取控制設定不周，成為主要入侵途徑）、帳號劫持（透過釣魚、憑證竊取或社交工程取得合法帳號，進行橫向移動及權限提升）、零日攻擊（利用尚未公開之系統漏洞發動攻擊，致組織難以及時防禦），以及資料汙染（於 AI 模型訓練階段注入惡意資料，使模型產生偏誤或隱藏後門）。

議程重點強調三項關鍵轉變：一、由合規導向轉為韌性導向，隨網路威脅型態持續演進，稽核角色須由單純確保合規，轉向協助組織建構整體韌性能力；二、新技術伴隨新風險，AI 及資料應用日益增加，已對組織風險輪廓產生重大影響，須同步識別並回應新興網路風險；三、控制現代化具其必然性，既有 IT 控制多已不符現況，亟須重新設計以因應新型態威脅，自動化與數據分析將成為關鍵手段。為此，組織應採行現代化控制作法，包括零信任架構（對內外部使用者及系統一律不預設信任，每次存取皆須驗證與授權）、持續監控（運用自動化工具及 AI，即時監測系統活動、交易與使用者行為）、行為分析（建立正常行為基線，自動偵測偏離常態之異常活動），以及自動化事件回應（於威脅偵測時即時執行隔離、封鎖或告警等處置措施）。

會中並提出組織導入AI之四個轉型階段：第一階段為「Human-first」，AI作為輔助工具以提升個人工作效率；第二階段為「Human + Agents」，於團隊中導入AI代理人，自動完成部分作業；第三階段為「Human + Orchestrator Agent」，AI除輔助執行外，並可統籌及協調多項任務，由人員負責監督；第四階段為「Agents」，部門或流程得於 AI 高度自主運作下維持穩定，僅需最小化人工介入。惟 AI 導入同時亦衍生模型偏誤、資料隱私、演算法操控、模型汙染及深偽詐騙等風險，組織爰須建立明確之治理基礎。

本場次提出負責任 AI 之六大原則，包括透明性、公平性、問責性、隱私治理、系統韌性及以人為本，均應內嵌於專案執行與技術決策之中。另就完整 AI 治理架構而言，其十項支柱涵蓋政策、治理委員會、風險框架、使用案例盤點、第三方風險管理、法規要求、模型監測、技術防護、資料治理及人才能力等面向，作為組織推動AI應用與風險控管之重要依據。

（二）第二場：爐邊對談—稽核角色轉型（Fireside Chat/ From Policeman to Partner）

本場次由 Jihad Tayyara（EVOTEQ 執行長）及 Abdulqader Obaid Ali（IIA UAE 主席）主講。Jihad Tayyara 以其逾 28 年之科技產業經驗，分享於數位環境快速演進下，如何重新定位稽核角色，以及科技如何成為稽核治理中不可或缺之一環。其坦言，早年擔任科技主管時，曾將稽核視為「干擾者」，主因科技團隊面臨快速交付之壓力，而稽核部門要求完整文件及冗長審批流程，常被認為係「減速器」。惟隨組織治理觀念逐步成熟，其逐漸體認稽核之真正價值在於「陪伴與提醒」，而非「挑錯與阻擋」。倘稽核僅著眼於文件程序或零碎缺失，實難助益專案成功；反之，若稽核能於專案初期即理解企業策略、掌握技術脈絡，並提出具前瞻性之建議，即可成為協助團隊達成目標之重要夥伴。

講者進一步提出「由警察轉為策略夥伴」之心態轉變，指出稽核之核心功能已由事後糾舉，轉向前期洞察與共同促成成功。其認為，具高度價值之稽核應具備下列特質：一、早期介入，於專案規劃階段即參與，而非待專案完成後始行查核；二、理解策略，掌握企業策略與業務目標，並將風險管理與業務成功相互連結；三、技術理解，具備足夠科技知識，得以與 IT 團隊進行具實質意義之對話；四、前瞻性建議，著重於「如何做得更好」，而非僅指出「何處有誤」；五、陪伴與提醒，扮演值得信賴之顧問角色，於關鍵時點提示風險，協助團隊順利推進。

Jihad 並指出，科技之進展使稽核得以由「事後反應」邁向「預測與預防」。現今科技已使稽核能分析 100%之交易資料，而非僅仰賴抽樣；透過資料平台、即時分析及流程自動化，稽核得以更早辨識異常，並向管理階層提供具體洞見，使組織由被動因應轉為主動管理風險。其以「智慧進化歷程」形容稽核科技化之發展軌

跡，依序為基礎分析、流程自動化，進而至人工智慧輔助之洞察強化。其並將理想之稽核模式形容為「科技強化，人本驅動」，亦即科技提供速度與規模，稽核則提供方向與整體判斷。未來稽核人員須具備更高之科技素養、資料理解能力、跨部門溝通技巧及倫理判斷能力，能以科技為工具、以專業判斷為核心，與技術團隊共同確保風險獲得適當之辨識、管理與監督。

（三）第三場：

1. 現場展示與客戶成功案例-運用人工智慧驅動持續性控制監測[Demo & Customer Success-Driving Continuous Controls Monitoring (CCM) with AI]
2. AI 驅動稽核自動化過程之挑戰與啟示(Challenges and Learnings from an AI driven Audit Automation Journey)

本場次分為兩部分進行實務分享。第一部分（15:00－15:20）由 TRPGLOBAL 及 MODON 公司人員現場展示 AI 驅動之持續性控制監控（Continuous Controls Monitoring, CCM）；第二部分（15:20－15:40）則由 AD Ports 及 Aldar 集團之稽核主管，分享「AI 驅動稽核自動化過程之挑戰與啟示」。於當前以數據為核心之治理環境下，內部稽核正由傳統之週期性審查，逐步轉型為結合自動化與人工智慧之持續保證（Continuous Assurance），並探討雲端 AI 代理如何賦權 IT 審計及 IT 治理主管，以降低風險並強化資料安全。

講者指出，內部稽核角色正由「發現錯誤」轉向「協助成功」。傳統稽核模式多於業務流程完成後始介入，易形成阻力與誤解；惟在 AI 及 CCM 支援下，稽核得以前移介入流程，及早協助識別風險並提出預警，使稽核成為管理階層可信賴之

顧問。Aldar 集團稽核主管 Haider Najim 強調，「連續改善心態」（Continuous Improvement Mindset）係推動稽核轉型之關鍵，須同時理解業務策略、掌握技術變化，並快速迭代工具，方能使科技真正創造稽核價值。AD Ports 集團稽核主管 Sayan Deb Chatterjee 亦指出，AI 之核心價值在於「釋放稽核人力」，使稽核得以專注於高判斷性、跨部門協作及策略層級議題，而非耗費於大量重複性查核作業。就 CCM 實務導入而言，講者一致認為資料品質不足及資料分散（如混合雲端與地端系統並存）為最大挑戰。倘企業資料未標準化、系統未有效整合，即使導入先進 AI 工具，亦難以發揮預期成效。其次，業務使用者之理解落差亦為重要障礙，許多使用者難以理解 ERP 權限設定、角色代碼等技術性描述，亦無法即時判讀異常訊號，導致初期推動阻力較大。爰 AI 自動化之成功，關鍵在於使業務單位能清楚理解「異常所代表之意涵」及「應採取之行動」。此外，跨部門協作與信任建立亦屬關鍵因素。倘管理階層認為自動化增加作業負擔，或業務單位仍將稽核視為「警察」，均將影響導入進度。基此，兩位講者均建議採行「快速見效」（Quick Wins）策略，先自低複雜度、高風險且可快速產生成效之項目著手，藉以建立信任，再逐步擴大應用範圍。

AI 驅動之 CCM 使 100%交易資料分析成為可能，稽核不再依賴抽樣，而係透過異常模式之自動偵測（如採購至付款流程、三方對帳、職務分離、例外交易等）進行監控。AD Ports 並分享實務案例指出，在採購至付款（P2P）流程中，企業可將約 80%符合標準流程之交易自動化處理，僅將稽核資源聚焦於約 20%之例外樣態，顯著提升效率與命中率。同時，CCM 可自動彙整異常權限、異常交易及例外流

程，並持續回饋至風險矩陣，使稽核由「年度一次」之查核模式，轉型為「持續監控」機制。

講者最後強調，AI 驅動之 CCM 並非單一工具導入，而係一項長期轉型工程，其成功關鍵包括：採行「小步快跑、快速見效」方式逐步建立信任、確保跨部門合作與資料治理同步精進、以稽核之專業判斷補足科技之限制並維持人為監督，以及將稽核角色定位為「策略夥伴」，而非僅止於發現錯誤之查核者。誠如講者所言：「AI 係工具，轉型係心態；CCM 係方向，價值在於稽核角色之升級。」

七、同步場次（宴會廳 2）

宴會廳 2 於 11 月 19 日下午舉辦三場連續專題，匯集法務會計、治理風險合規（GRC）及 AI 應用三大領域專家，分享實務經驗與轉型路徑，摘錄重點如次：

（一）第一場：當調查導致訴訟（When an Investigation Leads to a Claim）

本場次由 Chris Clements（Deloitte 法務會計合夥人）擔任主講人。講者具備處理舞弊、火災、帳目偽造，甚至重大刑事案件與火山事故調查之豐富經驗，指出企業於法律風險情境中，既可能為訴訟之發起方（受害者），亦可能成為被告，爰理解風險來源、建置有效控制措施，並促進跨部門協作，為組織治理之關鍵。講者說明，調查進而引發訴訟之常見情境包括：一、資產挪用（Asset Misappropriation），屬最常見之舞弊類型，範圍自工廠設備、車輛、高價庫存，至智慧財產權竊取（如可口可樂配方）不等；二、企業併購糾紛，併購後整合過程中，因庫存評價差異或系統整合問題而產生爭議；三、舞弊性併購，賣方透過粉飾帳目操縱財務數據，隱匿庫存過期或虛增營收，情節嚴重者可能升高為刑事訴訟；

四、賄賂與貪腐，屬全球性且高度隱蔽之風險，常發生於帳外交易，難以即時偵測，講者並舉例英國前首相 David Cameron 曾收受價值約 2 萬美元之馬匹，以說明貪腐樣態之多元性。講者提出具啟發性之觀點指出，在特定情境下，約 80%至 95%之人員皆可能產生舞弊或不當行為。其以情境測試說明：若桌上放置 1,000 美元且被查獲機率達 99%，幾乎無人會取走；惟若金額高達 1 億美元且被查獲機率僅 0.0001%，或係為救治重病之子女，則即便一向誠實之人，亦可能產生動搖。其結論為，企業治理不可僅仰賴員工之道德操守，而須透過完善之控制措施以「移除誘惑」。舞弊與訴訟事件對組織之衝擊，主要於三個層面：一、財務影響，包括鉅額罰款與賠償責任；二、營運影響，訴訟程序往往分散高階管理層之注意力，例如福斯汽車排放門事件引發之集體訴訟；三、聲譽影響，屬最難回復之損失，如 Perrier 氣泡水因生產線污染停產三週，短時間內即喪失其全球市場主導地位。就法律訴訟管理而言，講者強調三項關鍵要素：一、跨部門協作，由財務團隊評估訴訟之經濟價值，避免耗費鉅額成本追討實質價值有限之索賠；二、依據 IAS 37 妥善評估或有負債與或有資產；三、適切運用法律特權（Legal Privilege），以避免關鍵資訊於不當時機過早揭露。其並引述特殊案例說明，如假市場舞弊（透過遊說政府強制計程車司機接受培訓，創造原本不存在之市場需求），以及汽車租賃公司因員工腦瘤導致殘值計算錯誤之非故意行為，強調訴訟對象之判斷應回歸實質受益者或保險機制。

講者最後指出，內部稽核應扮演組織之最後一道防線，確保所有重大法律暴險均能於早期即被識別並妥善管理，並協助建立周延之危機管理計畫，以「隨時準備好」（Be Prepared）之態度，因應不可預期之法律與舞弊風險。

（二）第二場：超越熱烈討論：AI 跨部門實務應用（Beyond the Hype: Real-World AI Across Functions）

本場次由UNIQUS顧問公司合夥人Nagaraj Uchil（公司治理、風險管理與法規遵循諮詢）擔任主持人，由UNIQUS顧問公司合夥人Wouter van Gelderen (會計諮詢)、Tarandeep Bindra（技術諮詢）、及SecurityScorecard公司銷售總監Will Gray共同討論。

講者指出，AI已非僅止於理論探討，根據2025年調查數據顯示，約62%的組織正處於試驗AI代理（AI agents）或推向企業級應用的階段。在受監管嚴格的金融服務業中，更有高達 68%的企業將 AI 應用於風險管理與法規遵循視為首要任務。就實際效益而言，導入AI的組織在效率上提升了40%，準確度提升30%，成本節約達20%。特別是在內部稽核領域，AI的應用正在重塑確信服務（Assurance Redefined），約39%的內部稽核部門已採用AI，預計未來12 個月內將有額外41%的組織跟進。講者強調，AI不會取代稽核人員，但善用AI的稽核人員將取代那些不使用者。

講者分享實務AI代理應用案例：例如在內部控制測試中，AI代理能在數秒內檢查大量控制文件，判斷設計與執行之有效性，大幅縮短傳統人工抽樣所需的時間，並將查核範圍從「抽樣」擴大至「全查（100% testing）」。另一實務案例為費用報銷的舞弊偵測。透過 AI 模型進行異常偵測分析，雖然目前準確度尚未達完美，約 75%-78%的結果準確，仍需人工複核，但能有效識別出重複付款、違反政策門檻及異常供應商等風險，使稽核從「回顧式」轉向「預測性」與「預防性」。此外，在法規遵循與文件管理上，AI 能協助自動摘要、分類與比對主數據（Master Data），提升數據一致性。

面臨的新興風險包括：影子 AI（Shadow AI，未經授權的 AI 使用量預計快速上升，帶來資安隱憂）、偏見與可解釋性（公眾對 AI 信任度與偏見問題日益受關注）、法規就緒度（如歐盟 AI 法案已於 2024 年 8 月生效）、AI 賦能的舞弊（利用合成身分、深偽技術及生成式工具進行的舞弊行為增加防禦難度）。講者強調，AI 作為投資約需 2 至 3 年才能看到具體成效，組織應選擇實際可行的用例、向董事會與審計委員會展示成果、並制定 2 至 3 年的發展計畫。ROI 衡量的最大挑戰在於預防性效益（避免的成本、洩漏、舞弊等）難以量化，建議在導入 AI 前先建立良好的基線衡量。

（三）第三場：利用既有審計技術採用 AI 之策略與實踐（Leverage your Legacy Audit tech in adopting AI）

本場次由 Aurex 執行長 Shantosh Sridhar 主講。講者指出，其於兩年前首次於 IIA 會議中談論 AI 時，尚屬唯一聚焦該議題之講者，迄今已累積超過 25 至 30 項 AI 部署實務經驗，得以提出更為成熟之觀察與洞見。

講者提出 AI 成熟度模型，區分為四個層級：一、Level 1（實驗性／試點階段）：以人工方式使用 ChatGPT 等工具撰寫報告或摘要，尚未與管理系統整合；二、Level 2（新興／有限採用）：AI 開始用於規劃及文件起草，並初步應用於異常偵測；三、Level 3（整合應用階段）：AI 導入整個審計週期，結合內外部資料進行 AI 輔助風險評估；四、Level 4（轉型／領先實踐）：審計角色進一步轉型為企業 AI 治理之策略顧問，AI 深度內嵌於審計與風險管理職能。

講者指出，目前多數組織仍集中於 Level 1 至 Level 2，Level 4 實務案例幾近不存在。就 AI 採用障礙而言，最大挑戰在於與既有系統及作業流程之整合，占

比達 47.75%。講者形容此情形為「零和遊戲」：雖藉由 ChatGPT 等工具自動化部分作業，惟因無法與管理系統串接，反而衍生額外之人工處理流程。即便暫不討論個人資料或內部文件外流風險，審計人員若逕行使用外部 AI 工具（如 Copilot）產製報告或備忘錄，管理階層亦難以掌握其是否符合組織內部政策與標準作業程序。此種應用模式不僅未能達成預期效率，反而增加人工驗證負擔與合規風險，使 AI 應用流於形式，難以創造實質價值。針對上述問題，講者提出「統一 AI 引擎」（Unified AI Engine）之解決方案，作為獨立層級串接所有 GRC、ERP、風險管理、合規管理及審計分析系統，透過 API 取得資料以執行 AI 應用，毋須更換既有系統。講者並於現場展示 Aurex AI Studio 之實際功能，包括：一、風險控制矩陣自動生成：連結歷史風險紀錄並接軌國際最佳實務，原需 1 至 1.5 個月之研究工作，可於數秒內完成；二、審計範圍備忘錄自動起草：AI 可理解組織既有文件模板並依循格式產製草稿；三、工作底稿自動生成：上傳證據後約 2 分鐘內完成完整工作底稿，涵蓋步驟、問題、觀察及結論。就導入路徑而言，講者歸納四項步驟：一、評估（Assess）：盤點現行審計及技術環境、資料準備度，並識別 AI 使用案例及效益；二、規劃（Plan）：取得管理階層支持，完成預算與基礎設施規劃；三、部署（Deploy）：整合資料來源，建構統一生態系；四、賦能（Enable）：教育團隊 AI 使用案例，辦理技術研討活動，推動採用與文化轉型。

另就常見挑戰之因應作法，講者說明：針對「幻覺」問題，應透過持續微調模型並維持資料品質加以改善；針對技術準備度不足，宜採用具擴充性之基礎設施託管；針對安全性風險，須建立資料目錄分類及角色存取控制（RBAC）；針對人才

技能落差，則應定期辦理 AI 識讀及提示工程相關訓練。講者最後強調，AI 僅為賦能工具，演算法與訓練資料之正確性與適切性，仍須由人員持續維護與把關。

八、同步場次（宴會廳 3）

宴會廳 3 於 11 月 19 日下午舉辦三場連續專題，針對 AI 專案的高失敗率與治理缺失、AI 驅動的內部稽核轉型及 AI 舞弊偵測實務提出解決方案，摘錄重點如次：

（一）第一場：信任人工智慧－為什麼重要及如何建立（Trust in AI - Why It Matters and How to Build It）

本場次由 PwC AI 聯盟英國負責人 Felicity Copeland 主講。講者自述為「AI 成癮者」，高度依賴 ChatGPT 輔助日常工作，並形容若失去 ChatGPT，「彷彿失去一隻手臂」。其由 AI 技術演進談起，說明人工智慧自 1956 年達特茅斯會議提出概念以來，歷經傳統 AI（專家系統、規則引擎）、機器學習（自資料中學習模式）、深度學習（神經網路），發展至 2020 年代之生成式 AI（如 ChatGPT、Gemini、Claude 等大型語言模型）。尤值得注意者為，ChatGPT 僅用 2 個月即達成 1 億使用者，相較 TikTok 需 9 個月、Instagram 需 2.5 年、Facebook 需 4.5 年，顯示生成式 AI 具前所未有之採用速度與影響力，茲摘錄重點如次：

講者引用 PwC 全球 CEO 調查結果指出，56%之 CEO 觀察到員工因生成式 AI 而提升工作效率，34%認為 AI 有助於提升獲利能力，42%則認為若未進行根本性改革，企業於 10 年內恐難以存續。惟阻礙 AI 採用之三大障礙包括：一、技能與文化落差（47%），員工不理解 AI 之本質，亦不知如何於日常工作中運用；二、技術投資風險（26%），MIT 研究顯示 95%之 AI 概念驗證（PoC）專案未能成功；三、

信任問題（29%），包括對 AI 輸出品質之疑慮及對資料安全之擔憂。講者強調：「此不僅為技能差距，更係文化差距。」

講者進一步提出「AI 成功策略三步驟金字塔」架構，並指出多數組織直接跳至第三步（轉型專案），係導致 95% PoC 失敗之主因。正確推動順序應為：第一步，建立 AI 啟用勞動力，使員工理解、信任並具備使用 AI 之能力，此為創新及發掘實際用例之基礎，目標係使員工對 AI 之信任程度如同使用 Microsoft Word 或 Excel；第二步，自動化後勤流程，依據前述步驟所辨識之高價值用例進行流程自動化，優先聚焦內部效率；第三步，轉型客戶體驗，於前兩步基礎穩固後，運用 AI 推動營收成長及市場差異化。講者並以英國某律師事務所為例，該所向全體律師及後勤人員提供 ChatGPT Enterprise 並辦理培訓後，員工自行建立多項 Custom GPT 以支援特定任務，管理階層再由高頻使用之工具中識別最具投資價值之自動化項目，成功建構「由下而上」之 AI 啟用勞動力模式。

在 AI 工具選擇方面，講者說明三類 AI 架構及其風險矩陣：一、供應商嵌入式解決方案（如 Microsoft Copilot），AI 涵蓋整體資料環境，存取權限廣泛，具較高風險，可能導致敏感資訊外洩；二、獨立企業級平台（如ChatGPT Enterprise、Gemini Enterprise），由使用者主動上傳資料操作，屬中度風險；三、領域專用 AI（如 Harvey 法律 AI、Bloomberg GPT 金融 AI），因預先於特定領域訓練，風險相對較低。哈佛商學院研究顯示，使用生成式 AI 可使工作品質提升 40%、任務完成率提升 12%，惟前提為必須維持人員於流程中反覆檢核與修正。

針對 AI 特有之倫理風險，講者詳述公平性、透明性、隱私性及安全性等倫理審查流程，並建議組織建立風險評估矩陣，依 AI 系統影響程度與發生機率進行分

級管理。其以三星禁止員工使用公共版 ChatGPT 為例，說明資料安全風險：員工將程式碼、會議紀錄等輸入公共版 ChatGPT，導致資料外洩，且公共版資料將用於模型訓練，而企業版則完全隔離不納入訓練。講者特別強調「人類參與流程」（Human-in-the-Loop）之必要性，並舉澳洲政府報告因 AI 捏造參考文獻未經查核、媒體刊出含有提示語之 AI 生成文章等案例，警示盲目信任 AI 輸出之風險。

就內部稽核角色而言，講者認為於 AI 治理中應扮演五項功能：一、顧問角色，協助管理階層設計 AI 治理架構；二、保證角色，驗證 AI 系統控制之有效性；三、教育者角色，提升組織對 AI 風險之認知；四、監督者角色，持續監控 AI 使用情形；五、創新推動者角色，主動探索審計 AI 應用並以身作則。內部稽核應定期評估治理架構之有效性與合規性，並向董事會報告 AI 治理成熟度及精進建議。

（二）第二場：從洞察到確信：在內部稽核中部署 Microsoft Copilot（From Insight to Assurance: Deploying Microsoft Copilot in Internal Audit）

本場次由 BDO 公司合夥人 Ashish Gupta 主講。隨著組織加速數位轉型進程，內部稽核功能須由傳統之事後審查，逐步轉型為即時洞察與前瞻性確信。本場次聚焦 Microsoft Copilot 如何嵌入 Microsoft 365、Dynamics 365 及 Power Platform，賦能內部稽核團隊提升效率、準確性與洞察力。透過策略說明結合現場展示，講者說明 Copilot 於風險導向審計規劃、自動化證據蒐集、複雜資料摘要分析，以及於熟悉之 Microsoft 工具環境中產製前瞻性洞見等應用情境。本場次旨在協助領導階層清楚理解如何於審計環境中負責任地導入 AI，兼顧創新與治理、資料隱私與確信標準。

講者首先說明 Microsoft Copilot 之整合架構優勢。Copilot 深度嵌入 Microsoft 365 生態系，可直接於 Word、Excel、Outlook、Teams 及 Power BI 等審計人員既有工具中運作，無須另行學習新介面。「原地作業」之設計有效降低導入門檻，使審計人員得於既有工作流程中自然運用 AI 輔助。Copilot 並可透過 Microsoft Graph 存取組織資料，整合電子郵件、文件、會議紀錄及業務系統等資訊，提供更完整之審計分析情境。

於審計實務應用方面，講者展示四項核心案例：一、風險導向審計規劃，Copilot 可分析歷年審計報告、風險評估資料及相關會議紀錄，自動辨識新興風險議題並提出審計重點建議，協助制定更精準之年度查核計畫；二、自動化證據蒐集，透過 Copilot 於 Excel 及 Power BI 之功能，得自多元資料來源擷取交易資料，執行異常偵測分析並標示需進一步檢視項目，大幅減少人工處理時間；三、複雜文件之摘要與分析，Copilot 可快速摘要冗長合約、政策文件或法規異動內容，萃取關鍵條款與要求，協助審計人員迅速掌握查核重點；四、前瞻性洞察意見產製，透過分析歷年審計發現事項及缺失態樣，Copilot 可預測潛在風險區塊並提出改善建議。

另就治理與資料安全面向，講者特別強調 Copilot 之使用須賦予廣泛資料存取權限，組織於導入前應完善權限管理機制，確保 AI 僅能存取經審計人員授權之資訊。建議作法包括：建立明確之資料分類與標示機制、設定角色存取控制（RBAC）、定期檢視 AI 存取紀錄，以及建置敏感資訊自動偵測與攔截機制。講者指出，Copilot 之優勢來自其對組織資料之整合存取，惟同時亦伴隨風險，審計單位應審慎訂定使用規範，確保組織內部負責任地運用 AI。

在導入策略方面，講者建議採取分階段推動方式：第一階段（試點），選定 1 至 2 項審計專案進行試用，以累積經驗並辨識關鍵問題；第二階段（擴展），將成功經驗推廣至其他專案，並建立最佳實務指引；第三階段（深化），進一步發展如持續性監控等進階應用。最後，講者強調，成功導入之關鍵不在於技術本身，而在於組織心態之轉變，須由將 AI 視為威脅，轉為視其為賦能工具，並由擔憂被取代，轉向思考如何運用 AI 創造更高價值。

（三）第三場：終極貓捉老鼠遊戲—AI 對抗舞弊（AI vs. Fraud: The Ultimate Cat and Mouse Game）

本場次由 Baker Tilly UAE 合夥人 Nadeem Maniar 及 Baker Tilly UAE 內部稽核長 Reefat Maniar 主講。講者指出，舞弊已非過往型態，對抗舞弊之方式亦隨之轉變。本場次引導與會者深入理解人工智慧介入金融犯罪後所形成之快速變化環境，議題已不再僅止於事後損害偵測，而係關於如何預測、預防，並持續保持領先。本場次剖析 AI 如何改變舞弊偵測之遊戲規則、其仍面臨之限制與挑戰，以及人類洞察於其中仍不可取代之關鍵角色。關鍵啟示包括：舞弊手法演化之新觀點及 AI 因應方式、過度仰賴 AI 所衍生之風險（如假陽性、資料偏誤及對抗式攻擊），以及未來發展重點在於人機協作，而非彼此取代。

講者以「湯姆貓與傑利鼠」作為比喻，說明舞弊偵測之演化競賽。AI 偵測系統如同湯姆貓，透過學習歷史資料以識別異常模式；舞弊者則如傑利鼠，於掌握偵測邏輯後即調整手法規避查核，形成持續對抗之循環。現今更進一步演化為 AI 製作舞弊工具，以對抗 AI 偵測系統之新局面。講者透過六項實務案例，具體說明 AI 與人類協作之必要性：管理層凌駕控制案例顯示，AI 可迅速搜尋全球資料庫並

繪製關聯圖譜，惟動機理解與治理缺口辨識仍須仰賴人員訪談；偽造學歷案例凸顯「認證不等於驗證」（Attestation is NOT Verification），AI 雖可批次查詢教育資料庫，惟最終仍須直接向學校查證，且於資訊矛盾時須由人類進行批判性判斷；循環金流迷宮案例（涉案金額約 2 億美元）顯示，AI 能精確描繪複雜交易網絡，惟商業邏輯判斷、情境理解及法律責任認定仍有賴人類專業；幽靈員工案例（金額逾 50 萬美元）中，AI 可進行薪資資料異常分析與帳戶關聯比對，惟實地查核與確認仍須由人員執行。

講者另以 Amazon 招聘 AI 系統系統性排除女性候選人之案例，說明 AI 之根本性限制，包括資料偏誤（複製既有歧視模式）、情境理解不足（無法掌握文化與組織特性）、動機盲點（無法理解人類行為背後之原因）、倫理判斷缺乏（無法進行價值衡量），以及可解釋性不足（深度學習之黑箱特性）。講者並提出人機協作之建議比例：資料蒐集階段 AI 80%、人類 20%；初步分析階段 AI 70%、人類 30%；深度調查階段 AI 30%、人類 70%；證據評估階段 AI 20%、人類 80%；最終決策階段則應完全由人類負責。

講者強調，AI 所提供之答案「可能不正確」，惟若未保持批判性思維即予以採信，將衍生重大風險。AI 應負責資料處理與異常識別等高負荷工作，人類則須專注於專業懷疑、情境理解、動機分析、倫理判斷及最終決策之專業判斷，二者相互補充，缺一不可。

九、場次五：IIA 全球主席演講—成為未來（IIA Global Chair Theme – Be The Future 2025-2026）

本場次由 IIA 全球主席 Stefano Cometti 發表主題演講，闡述其 2025-2026 年度主席主題「Be The Future」（成為未來）及 IIA 最新發布的「Vision 2035: A

North Star」策略願景。主席開場即引用一段振奮人心的名言：「每一個強大的組織，都站在其內部稽核團隊的靜默力量之上」（Every strong organization stands on the quiet strength of its internal audit team），彰顯內部稽核團隊對於協助組織成功的核心價值。隨著風險環境劇變、科技進化及新興威脅湧現，內部稽核師必須做好準備，以清晰視野與前瞻思維引領組織前進。內部稽核不僅是贏得信賴的專業，更關乎擁抱使命感。本場次探討內部稽核當前面臨的關鍵時刻、未來十年的挑戰，以及IIA如何塑造未來並賦能審計專業迎接下一階段的發展。

（一）當前風險情勢與審計資源錯置之警訊

講者首先指出，全球組織正處於高度不確定與快速變動之環境，惟多數內部稽核資源配置仍未與實際風險變化同步調整。依據 IIA 相關調查結果顯示，經濟環境變動、人才吸引與留任等風險，於風險重要性排序中名列前茅，然實際審計投入卻相對不足；反之，部分風險評等已相對下降之議題，仍持續獲得較高審計資源配置。講者強調，此一落差顯示內部稽核仍過度依賴既有風險框架與歷史經驗，未能即時校準關注焦點。在全球局勢快速變化下，內部稽核不僅須調整「查核什麼」，更須重新思考「為何而查」，以確保有限資源能真正對應組織當前與未來之關鍵風險。

（二）專業角色之誤解與轉型必要性：由被動回應邁向主動影響

講者坦言，內部稽核長期面臨「價值被低估或誤解」之結構性問題。IIA Vision 2035 相關研究顯示，近半數受訪者仍將內部稽核定位為「警察」或「查核清單執行者」，此一刻板印象不僅弱化專業影響力，亦限制稽核參與策略性對話之空間。講者指出，問題並非內部稽核缺乏價值，而係價值未被有效展現。未來內部稽

核須由「證明自身價值」轉向「實際發揮影響力」，從事後回應既成事實，轉為以前瞻視角介入重大決策。此一轉型並非放棄獨立性或核心價值，而係改變角色呈現方式，透過更主動、具方向性之作為，成為組織可信賴之意見來源。

講者並以自身參與併購案件之經驗說明早期介入之價值。其於併購初期即提出關鍵營運與技術相容性問題，促使管理階層進一步進行商業層面盡職調查，最終避免可能導致重大失敗之交易。該案例具體展現內部稽核於決策前端即能發揮之風險預警與價值創造功能。

（三）Vision 2035 之三大核心轉向：重新定位、能力提升與影響力擴展

面對 AI、自動化與營運模式快速變革，講者指出內部稽核必須進行根本性轉向，Vision 2035 即為此一轉型之北極星，其核心包括三項主軸。1.重新定位角色（Reframe the Role）：內部稽核不再僅為缺失揭露者，而應成為「組織韌性之建構者」，協助設計能抵禦不確定風險之制度與流程，從被動觀察者轉為積極參與塑造未來之關鍵角色；2.能力提升（Elevate）：除傳統稽核專業外，審計人員須同步強化數位素養、資料分析能力、AI 應用理解及業務洞察力，並具備以清楚、具策略意涵之語言，向董事會與高階管理階層溝通風險與影響之能力。簡報中並指出，採用 AI 之審計單位，在辨識重大資安風險之能力上，明顯優於未採用者，顯示科技已成為維持專業攸關性之必要條件；3.擴大影響力（Expand Influence）：審計功能須由合規導向，進一步轉型為策略夥伴，於專案設計與重大決策初期即介入，提供具前瞻性之風險觀點與建議，協助組織在不確定環境中作出更佳判斷。

（四）動盪環境下之五項行動原則與能力實踐

講者於演講尾聲提出內部稽核人員可立即採行之五項具體行動，作為「成為未來」之實踐路徑：1.於每項查核中提出策略性問題，跳脫單純檢核表思維；2.主動掌握議程，不待邀請即將關鍵議題帶入決策對話；3.勇於改變現狀，將創新視為內部稽核之策略責任；4.重新形塑審計之全球定位，使其成為各產業與地區建立信任與韌性之核心力量；5.由防禦轉向進取，聚焦 AI、ESG 及組織文化等未來關鍵議題，主動提出問責與建議。講者並強調，內部稽核領袖須擁抱新科技、建立允許試錯之文化，並與風險管理、資安等單位形成協作生態系。最後以「Be the Future」作結，指出未來並非等待而來，而係由內部稽核主動塑造；未來十年將為審計專業之關鍵轉折期，唯有積極轉型者，方能於 AI 時代持續發揮不可取代之影響力

表 3 IIA Vision 2035 三大策略支柱與實踐路徑

支柱	核心理念	轉型目標	所需能力	實踐路徑
重新定位 (Reframe The Role)	從「缺失查核者」到「韌性建構者」	・組織韌性的建構者 ・未來的塑造者 ・價值創造的夥伴	・策略思維 ・風險洞察 ・前瞻視野	・轉變審計目標設定 ・重新定義成功指標 ・建立韌性評估框架
能力提升 (Elevate)	從「傳統稽核」到「全方位專家」	・精通數位技術 ・深化業務洞察 ・強化溝通影響力	・數據分析與 AI 應用 ・深刻業務理解 ・數據故事述說能力 ・向董事會報告技巧	・技術能力培訓 ・業務輪調計畫 ・溝通技巧工作坊 ・持續學習機制
擴大影響力 (Expand)	從「被動合規」到「策略夥伴」	・引領變革的夥伴 ・早期介入專案 ・擴大價值貢獻	・專案管理 ・變革領導 ・跨域協作 ・影響力建立	・早期介入機制 ・與管理層建立夥伴關係 ・參與策略規劃 ・創新試點專案

資料來源：整理自 IIA 全球主席演講內容。

十、場次六：動盪中的領導之道：策略、治理與韌性（Leading Through Turbulence: Strategy, Governance and Resilience）

本場次為專家座談形式，由 Mohamed Dukandar、Joanne Traice、Sumanta Mallik 及 Ross Pry 共同與談，聚焦於動盪與高度不確定環境下，組織如何透過有效領導、健全治理及韌性建構，引領團隊因應複合風險挑戰。討論重點涵蓋領導心態、危機應變、治理架構、新興科技風險及跨職能協作等關鍵面向。

（一）動盪時代之領導特質與心態調適

與談專家一致指出，領導者於不確定情境下所展現之心態，將直接形塑組織整體的「情緒基調」。若領導者表現焦慮與遲疑，團隊易陷入恐慌；反之，領導者若能保持冷靜並清楚傳達方向，即可穩定組織運作。專家強調，現代領導並非建立於「全知全能」，而係在資訊尚未完全掌握（例如僅掌握約八成事實）時，仍能作出具方向性的判斷，並承認自身未知之處，信任並授權專業團隊共同推進組織願景。此外，「可被看見的領導力」與「道德文化的示範」尤為關鍵。高階主管若能親自參與風險意識活動、支持並獎勵勇於發聲（speak up）之行為，將有助於建立誠信、當責與透明的組織文化，並降低風險被隱匿之可能。

（二）危機管理與溝通策略之實務原則

針對危機情境下的即時應變，與談者提出可操作之 SPACE 模型，作為領導與管理之行動框架：S（Situation）：快速釐清現況與已知事實；P

（Priorities）：設定明確且有限的優先順序；A（Actions）：聚焦於最具影響力的關鍵行動；C（Communication）：對內對外進行清楚、一致且即時的溝通；E（Empathy）：以同理心關注人員所受之實際衝擊。此一模式有助於避免組織在混亂中失焦，並強化指揮體系與角色分工。專家亦指出，危機往往成為數位化與流程簡化的催化劑，組織應善用契機，移除不必要之官僚層級，以提升決策速度與回應能力。在溝通層面，面對不利或負面訊息，宜直接且誠實說明，而非過度修飾。同時，建議刻意保留「暫停空間」，例如在回覆關鍵郵件或作出重大決策前，先進行短暫冷靜與視角轉換，以降低情緒化判斷風險。

（三）治理架構強化與組織韌性建構

專家指出，組織韌性之基礎，來自平時即建立明確且可運作之治理架構。董事會應透過設定清楚的風險基調（tone at the top）、分層負責機制及專責委員會（如風險委員會、重大交易委員會），確保資訊於危機時能迅速且一致地向上傳遞。此外，與談者強調，平時即取得董事會對重大風險處理原則之共識，將有助於危機發生時依循既定參數快速行動，而非臨時爭論方向。在稽核與控制層面，導入持續性控制監控或「數位稽核員」概念，有助於縮短問題發現之時間落差；每次重大事件後，亦應進行獨立之事後檢討（post-crisis review），將經驗轉化為制度化流程，以提升下一次危機之回復速度與成本效益。

（四）新興科技風險與 AI 治理之審計觀點

面對 AI 與自動化快速擴散，與談專家一致認為，稽核部門不應僅被動回應，而應主動建立 AI 治理與稽核框架，針對未經授權使用之 AI（Shadow AI）進行盤點，並明確界定風險責任歸屬。相關作法可參考既有國際標準（如 NIST、ISO）發展組織內部之 AI 風險管理機制。專家亦提醒，過度依賴生成式 AI 可能對人才培育產生長期影響，包括批判性思考能力弱化等隱憂，組織於推動 AI 創新之同時，仍須維持人類判斷與專業懷疑。在資安實務上，與談者指出，儘管科技快速演進，防護核心仍回歸基本功，包括即時修補系統漏洞、持續進行釣魚郵件演練，以及確實測試災難復原計畫，而非僅停留於文件層次。另就中長期風險而言，量子運算對既有加密與資安架構之潛在衝擊，亦應納入前瞻性規劃。

（五）對審計實務之整體啟示

綜合本場次討論，動盪時代下之有效領導與治理，並非單一職能所能完成，而須仰賴領導團隊、稽核、合規及舞弊偵測等單位之高度協作。內部稽核於其中之角色，正由事後查核者，逐步轉型為韌性建構與危機應變之關鍵支點。未來審計實務除持續強化專業獨立性外，亦須深化對人性、科技與治理互動關係之理解，方能在不確定環境中，協助組織穩定前行並創造長期價值。

十一、場次七：確保人工智慧倡議妥善治理之管理（Ensuring Proper Governance Management over AI Initatives）

本場次由 ISACA 名人堂成員 Mark Thomas 主講。講者指出，人工智慧（Artificial Intelligence，AI）正深刻改變組織之營運模式，惟若缺乏妥適之治理與管理機制，AI 專案可能迅速由創新動能轉化為重大風險來源。無論係演算法偏頗、決策不透明，抑或法規遵循不足，均可能引發合規違失與聲譽損害，其風險不僅真實存在，且有日益加劇之趨勢。

講者強調，「數位信任」（Digital Trust）係數位經濟之關鍵基石，建立於四大支柱之上：1.資訊安全（Cybersecurity），係透過多層防禦架構與即時監控機制，防範資料與系統遭未經授權之存取、破壞或竊取；2.隱私保護（Privacy Protection），係確保個人資料之蒐集、處理及儲存符合 GDPR 等相關法規要求，並尊重資料主體之權利；3.倫理責任（Ethical Accountability），係要求 AI 系統於設計與使用過程中遵循倫理原則，避免偏見與歧視，並確保決策具可解釋性與可追溯性；4.系統韌性（System Resilience），係指組織於遭受攻擊或系統故障後，能迅速恢復運作，並自事件中持續精進防護與管理機制。

面對多元且繁複之國際規範環境，講者建議組織採行「整合式治理策略（Integrated Governance Strategy）」。其核心作法包括：以具法律強制力之歐盟《AI 法案》（EU AI Act）作為合規基線，該法案依風險程度將 AI 系統區分為不可接受風險、高風險、有限風險及最小風險四類，並對高風險系統施加嚴格管理要求；運用 ISO 42001 建立系統化之 AI 管理架構，明確規範政策、流程、角色與責任；並參採 NIST AI 風險管理框架（AI RMF） 進行實質風險評估，透過「治

理（Govern）、盤點（Map）、衡量（Measure）、管理（Manage）」四項功能，協助組織全面識別與控管 AI 風險。透過將前揭國際標準整合納入既有 COBIT 資訊科技治理體系，組織得以建立一套兼顧法規遵循與實務運作之 AI 治理機制，進而鞏固客戶及利害關係人之信任基礎。

講者最後特別指出，數位信任並非一次性建置成果，而係需長期經營之管理課題。組織宜建立「信任儀表板（Trust Dashboard）」，即時監測關鍵信任指標，包括資安事件發生頻率、隱私合規狀態、倫理審查完成情形及系統可用性等，並定期向董事會報告，俾確保高階管理層之關注與資源投入，落實數位信任之持續維繫與強化。

十二、場次八：專題討論-航空業內部稽核：應對頑固的顛簸（Panel Discussion -Airline Industry Internal Auditing－Tackling Tenacious Turbulence）

航空業正處於快速且持續變動之風險環境中，若論長期承受高度動盪風險之產業，航空業首當其衝。該產業面臨之挑戰涵蓋多元面向，包括公眾健康風險（如疫情衝擊）、技術發展（數位化與自動化）、地緣政治衝突（影響國際航線與制裁措施）、ESG 議題（減碳與環境永續壓力）、勞資關係（罷工風險與人力短缺）、監理法規（飛航安全與合規要求）、供應鏈（航材零件供應與維修能量）及基礎設施（機場擴建與現代化需求）等。前揭風險變化快速且頻繁，影響層面深遠，單一重大風險事件即可能對航空公司營運造成災難性衝擊。

在此情境下，傳統以風險登錄或每月風險報告為主之管理模式，已難以及時反映高度動態之經營環境。本場次由三位來自中東大型航空公司之稽核主管分享航空業內部稽核實務經驗，並由內部稽核與風險顧問公司資深合夥人 Adil

Buhariwalla 擔任主持人，邀集 Etihad Airways 稽核長 Andrew Fisher、Emirates Group 資深副總裁 Derek Blaney，以及 flydubai 內部稽核資深副總裁 Tom Mtine 共同與談，針對航空業於高度不確定環境下，內部稽核如何調整角色定位、強化風險即時辨識能力及支援組織決策韌性進行交流，茲摘錄重點如次：

（一）第三方風險管理應採分層治理而非單一稽核項目

Emirates Group 之 Derek Blaney 指出，該集團並未以單一「第三方風險管理」項目進行整體確信，而係將相關風險拆解為多個流程與控制層面加以審查。其治理架構涵蓋需求定義（業務需求是否明確）、供應商評估（採購程序是否就所有潛在供應商進行充分評估及盡職調查）、合約管理（是否納入審計權及具實質意義之服務水準協議）、供應商引入（資訊分享機制及系統存取控管方式）、持續監控（是否持續監督服務水準履行情形及供應商認證維持狀況）、資訊安全（資安單位是否監控供應商之系統存取行為）及業務連續性（相關計畫是否定期檢討與測試）等面向。透過前揭分層治理模式，稽核團隊得以深入測試各項流程控制之設計與執行情形，據以產出具分析價值之結果，並提供具體且可驗證之確信意見。

（二）稽核人才應兼具技術能力與跨領域軟實力

與談者普遍指出，稽核人員除須具備專業技術能力外，亦須同步強化談判技巧及溝通說服能力。Andrew Fisher 表示，審計報告倘無法有效向利害關係人清楚傳達並取得認同，即使查核發現具高度價值，仍難以轉化為實質改善行動；審計成果之影響力，關鍵在於是否能被理解、接受並採納。Derek Blaney 則強調兩項關鍵軟實力：其一，對學習之熱愛，航空業務高度複雜且變動快速，幾乎不存在重複之審計情境，稽核人員須持續吸收新知以因應環境變化；其二，對品質之不懈追求，無論係電子郵件、簡報或正式審計報告，均應以最高標準自我要求，未達最佳

品質即不應視為完成。在技術能力層面，Tom Mtine 建議，稽核團隊應積極引進具工程或其他技術背景之專業人才，以強化對高度技術性領域之理解與查核深度，回應航空產業日益複雜之風險與控制需求。

（三）AI 治理應聚焦輸入輸出監控而非演算法稽核

Andrew Fisher 引述 Google 稽核主管之觀點指出：「無法稽核演算法，如同無法稽核人類大腦之思考方式。」其說明，AI 稽核之重點不在於深入解析演算法內部邏輯，而應聚焦於三項核心面向：一、資料輸入之品質與適切性；二、輸出結果之合理性與可解釋性；三、於不同情境下執行壓力測試，以確認系統於極端或異常條件下之穩定性與風險表現。

Derek Blaney 補充指出，航空產業長期即仰賴高度複雜之演算法進行定價與需求預測，例如 Emirates 每年即需處理約 190 億筆需求相關要素。於此情境下，關鍵控制並非檢視演算法本身，而係建立完善之結果監控機制，透過設定合理之基線期望值，持續比對實際輸出結果，及早識別異常偏差並啟動因應措施。另與談者特別提醒「影子 IT」風險，即使組織已建立完整之 AI 治理架構，倘各部門自行開發或使用 AI 應用而未納入正式管理，仍可能導致資料外洩、模型偏誤或決策風險擴大。

Tom Mtine 強調，組織應建立明確之資料分類制度，例如區分關鍵資料、高度機密資料及公開資料，並依資料屬性訂定清楚規範，明定各類資料是否得輸入 AI 工具處理，作為防範 AI 應用風險之重要基礎控制措施。

（四）網路安全需從組織生態系統整體防護

與談者一致指出，網路安全已成為董事會最為關注之核心風險議題。

Andrew Fisher 表示，航空業因其營運特性，係多重駭客攻擊之高度價值目標，涵蓋忠誠度計畫、訂位系統（單次停機即可能造成每分鐘數百萬美元之營運損失）、飛航安全相關系統及大量旅客個人資料。又航空公司高度仰賴第三方服務供應商（如 GDS 系統、地勤公司等），爰必須將資安治理範圍擴及整體生態系統，確保端到端之安全控管。

Tom Mtine 分享 Flydubai 之實務作法，將網路威脅明確定位為「稽核議題」，而非僅屬 IT 技術問題，並由內部稽核單位主動與資安長密切協作，建立涵蓋法務、資訊安全及稽核之跨職能治理架構，以強化風險辨識、決策一致性及問責機制。

Derek Blaney 則強調，許多重大資安事件往往源自看似平凡之基礎控制缺失，例如修補程式更新延宕、存取權限管理不當或防火牆設定錯誤等。爰內部稽核應持續關注並測試此類基礎控制之有效性，而非僅聚焦於高階或新興技術風險。

另於持續監控議題上，Derek Blaney 提出具啟發性之觀點指出，倘內部稽核已完成高風險控制之識別（如重複付款）並協助建立監控機制，後續之持續監控責任，原則上應回歸業務單位（如財務部門）負責執行，而非由稽核單位長期承擔。此一作法有助於釐清第一道防線之責任歸屬，並使內部稽核專注於監督與確信角色，提升整體治理效能。

十三、場次九：企業防舞弊指南：預防與偵測實務（Fraud-Proofing the Enterprise: A Practical Guide to Prevention and Detection）

本場次由杜拜控股公司稽核長 Aldrian Sequeira 主講，全面概述企業如何預防與偵測舞弊，涵蓋建立舞弊偵測文化、實施內部控制、運用資訊安全技術以應對不斷演變的威脅等關鍵要素。

（一）舞弊風險升級的三大驅動因素

講者首先闡述當前組織面臨舞弊風險急速升高之原因。其一為技術濫用風險，AI 與自動化雖可提升生產力及效率，惟若遭不當或錯誤使用，易引發技術性破壞、組織運作失序及聲譽損害，舞弊者正刻意濫用連結工具、自動化技術及AI，對組織造成實質影響；其二為跨境複雜性，某一國家可被接受之商業習慣，於他國可能涉及文化差異，甚或構成違法行為，語言隔閡及法律差異（如合約爭議、調查程序所受法律限制）均進一步提高舞弊風險；其三為共謀勾結風險，當內部人員與外部人員勾結（如應付帳款人員與外包技術公司串通），或組織內多層級人員共謀（如財務、應付帳款及資訊科技部門聯合欺瞞公司），傳統之預防與偵測控制機制恐難以發揮效能。

（二）舞弊偵測策略的六大組成核心

講者詢問現場有多少組織設有正式之「舞弊偵測策略」（Anti-Fraud Strategy），約五成與會者舉手。其指出，即使組織未明確以舞弊偵測策略命名，下列組成要素多已分散存在於不同政策文件之中：1.行為準則（Code of Conduct），係舞弊偵測策略之起點，涵蓋公司使命、願景及價值觀，其中以「價值觀」最為關鍵，明確界定員工行為規範（可為及不可為）、專業行為期待及檢舉機制；講者強調，多數調查最終均回溯至行為準則，因受調查者常主張「不知不得如此為之」，而行為準則即為組織已明確告知之佐證，並可證明員工已完成相關訓練及簽署確認；2.領導層訊息（Leadership Message），多數組織皆宣示對舞弊

「零容忍」，惟關鍵在於是否落實執行，倫理行為是否自領導層向下貫徹至基層，抑或存在雙重標準；表現優良之組織特徵在於言行一致，領導層確實實踐其所宣示之價值觀；3.角色及責任矩陣（RACI Matrix），應明確規範舞弊事件中各項責任歸屬，包括調查、損失追回、訴訟處理、後續改善及向董事會報告等事項；許多組織仍存責任重疊或空白之模糊地帶，爰須清楚界定分工，並使董事會及審計風險委員會充分知悉；4.內部控制框架，係舞弊偵測策略之核心支柱，涵蓋預防性控制、偵測性控制、職責分離、製作者與檢查者分工、授權分層、調節核對及監控等機制，並須具備足夠強度，持續由內部稽核加以驗證；5.政策與程序，其中以人力資源紀律政策尤為重要，該政策應完整列示自疏忽至蓄意舞弊之各類違規態樣，並明確規範相對應之處置方式（如口頭警告、書面警告至解僱），以確保處理之一致性與公平性；6.舞弊風險評估及經驗學習，於檢視特定業務循環時，應以「舞弊者視角」思考可能之欺騙手法，完整列舉潛在舞弊模式，檢視既有控制措施是否足以有效降低相關風險，並透過測試確認控制措施之實質有效性。

（三）跨境舞弊調查實務啟示

講者透過多個匿名化之真實案例說明，在跨國、跨產業環境中，基本原則（如行為準則、內部控制及 RACI 矩陣）於舞弊偵測與調查中如何發揮關鍵作用。其強調，縱使 AI 與自動化工具日益重要，組織仍須先建立穩固之基礎，方能有效預防與偵測舞弊。核心意涵在於，舞弊防制毋須過度複雜之理論，而在於持續落實基本原則、形塑健全文化，並從實務經驗中精進改進。

十四、場次十：結合審計、舞弊偵測與資訊科技優勢，打造韌性治理體系（Combining Strengths of Audit, Anti-Fraud and IT for Resilient Governance）

本場次為專家座談形式，由四位來自審計、舞弊偵測及資訊科技領域的國際專家 Abdulqader Obaid Ali（IIA UAE 主席）、Jemila John（IIA UAE 策略長）、John D. Gill（ACFE 代表）、Chris Dimitriadis（ISACA 代表），展示審計、舞弊偵測與資訊科技之間的實務協作模式，並透過真實案例與經驗分享，提供強化組織韌性的可行策略。

（一）跨職能協作的迫切性

IIA UAE 策略長於開場即指出，過去三日會議反覆強調之主題包括威脅已非孤立存在、舞弊手法日益複雜，以及網路韌性與 AI 治理等議題，前揭挑戰顯示治理已不僅屬合規問題，而係需跨職能整合之策略性課題。IIA UAE 主席亦坦言，當前審計、風險管理及合規部門常各自運作，形成所謂「穀倉效應」（Silo）。其以 IIA 歷年辦理之 144 次品質確信審查（QA）經驗說明，早期（約五年前）多數組織中各職能確實獨立運作，惟近年來已逐漸意識整合之必要性並採取具體行動。整合之動力主要來自業務導向需求，因 CEO、審計委員會及董事會所需者，係統一且清晰之風險全貌，而非分別來自風險、合規及審計三個部門之三份報告；組織若欲真正與業務對接，必須以業務為核心整合確信活動。其並舉例指出，審計與風險管理職能因同以「風險」為起點，最常出現合併情形，惟真正之最佳實務，係將審計、風險及合規三者整合為單一確信生態系，向 CEO 提供一致之風險報告。至於舞弊偵測職能之定位則較為複雜，部分組織將其納入審計職能，主席個人認為舞弊偵測與

審計間仍應維持明確界線，惟亦承認整合趨勢已逐步形成。其最後強調，三大專業組織（IIA、ACFE 及 ISACA）之跨界合作，正係為使各領域專業人員回到組織後，能以一致目標服務業務需求，並共同促進組織成功。

（二）檢舉機制：舞弊偵測的首要管道

John D. Gill 援引 ACFE 自 2000 年起定期發布之《職業舞弊與濫用報告》（Report to the Nations），該報告每兩年發布一次（下一版預計於 2026 年 3 月發布），內容涵蓋舞弊手法、行為紅旗及損失成本等重要資訊，其中最關鍵之統計結果顯示，自 2000 年以來，舞弊案件之發現方式以「檢舉」為最主要來源，比例長期居冠，約占 40%，顯著高於內部稽核、外部審計或管理階層審查。尤為重要者在於，檢舉來源中約半數來自員工，另半數則來自客戶及供應商，顯示檢舉管道不應僅限於內部人員，而須對外部利害關係人開放。基此，組織有必要建置健全且易於使用之檢舉機制，且不宜侷限於傳統熱線電話形式。John 並分享其組織實務經驗，於 Microsoft Outlook 中設置一鍵回報可疑釣魚郵件或附件之功能，期盼舞弊檢舉亦能達到同樣便利。他指出，員工往往能察覺異常行為，例如主管收受異常高價禮品或頻繁旅遊等，心中雖產生「不尋常」之疑慮，惟常因不知如何處理，或擔憂誤舉將影響自身工作而裹足不前，爰組織須建立讓員工感到安全且受保障之檢舉機制，鼓勵其於發現異常時勇於通報。主持人補充說明，ACFE 相關報告猶如對企業重大失敗案例（如 Enron、WorldCom、印度 Satyam 及英國 Carillion）之事後檢討，揭示舞弊行為之徵兆，並提供檢舉機制設計之最佳實務參考。

（三）IT 治理框架：整合與共同語言建立

Chris Dimitriadis 指出，協作之核心在於「人」及「共同語言」。組織須建構更為堅實且具全方位訓練之專業人才隊伍，相關人員除應具備垂直專業能力，對網路安全、內部稽核或舞弊偵測等領域具深度理解外，亦須具備橫向理解與溝通能力，得以跨領域互動並使用彼此可理解之語言。當審計、風險、資安等不同職能分別向執行長報告時，因語言與觀點各異，即使最終服務目標一致，執行長仍難以整合形成清晰之整體風險圖像。是以，IT 治理在協助專業人員建立共同語言上具關鍵角色，並須結合適切訓練，使網路安全專業人員能以業務語言溝通，使內部稽核人員得以理解技術內涵，並使舞弊稽核人員亦能掌握跨領域知識。

他進一步警示，全球經濟高度仰賴科技運作，惟近一年已多次見證數位生態系統崩潰導致大規模停擺，無論其肇因為網路攻擊、品質缺失或人為錯誤，均對產業與國家造成重大衝擊，包括 CrowdStrike 事件對全球多國多產業之影響，以及 AWS、Microsoft 服務中斷，甚至前一日 Cloudflare 之故障，皆可視為「數位瘟疫」（Digital Pandemics）之警訊。

隨著 AI 因素加入，該技術不僅將改變審計、舞弊稽核與資安等專業職能，更將全面重塑各行各業；惟其網路安全面向尤具風險，大型語言模型及業務流程正遭「武器化」，被用以提升網路攻擊成功率、實施舞弊或突破內部稽核控制。回歸治理框架層面，Chris 指出，COBIT 係一項良好之治理架構，可適用於多個專業領域，並整合 ISO 標準及政府發布之最佳實務，形成具整合性之治理體系。其最終強調，「人」係一切之起點，唯有培育同時具備垂直專業深度與橫向整合能力之人才隊伍，方能真正落實跨職能協作，並強化組織韌性。

肆、研習心得與建議意見

基於兩日會議的深入研討，並綜整會議關鍵發現與國際趨勢，謹提出以下五點具體建議：

一、深化審計願景對齊國際趨勢，以達成前瞻治理價值

陳審計長於第二任任期已明確宣示「智慧審計、永續審計、韌性審計及共臻善治」四大願景，並以「落實監督、強化洞察及邁向前瞻」三大審計主軸，系統性推動政府審計轉型，其政策內涵涵蓋數位科技導入、永續發展查核、風險預警機制及行政協力治理等面向，使審計職能由傳統財務監督角色，逐步拓展為兼具顧問、預警及公共價值創造功能之現代政府審計體系。

本次會議中，IIA 全球主席於 Vision 2035 主題演講提出「重新定位、能力提升及擴大影響力」三大策略支柱，明確指出未來十年審計專業應由單純缺失查核者，轉型為組織韌性之建構者與策略夥伴，並強調透過數據分析、科技運用及跨域協作，強化審計對治理決策之實質影響力。

綜合觀之，審計長所揭示之四大願景，與 Vision 2035 所指引之國際審計發展方向高度契合。未來推動重點，允宜進一步聚焦於執行層次之深化與整合，包括於智慧審計及韌性審計架構下，持續強化以巨量資料分析及風險導向方法支撐審計目標設定，使審計成果能具體反映對政府韌性治理之貢獻；於永續審計推展過程中，結合關鍵審計議題發展機制，提升跨域及跨年度查核之系統性與前瞻性，確保永續政策執行情形得以持續追蹤與回饋；並於共臻善治願景下，賡續推動審計於政策及重大專案早期即行介入，透過跨機關協作與溝通影響力之強化，擴大審計機關促進政府良善治理及公共價值創造之整體效益。

二、留存 AI 運用軌跡強化審計透明，以達成可信成果

本次會議於「在兆美元舞弊時代重建信任」場次中指出，隨著生成式 AI 與自動化工具廣泛應用於分析、決策及內容生成領域，數位環境中之信任基礎已產生結構性變化，任何未經檢視即逕行採信之系統輸出，均可能因深偽技術、模型偏誤或 AI 幻覺而放大治理風險。講者強調，重建數位信任之關鍵，不在於是否使用 AI，而在於其設計是否具備透明、可解釋及可問責之特性，使 AI 之分析過程與判斷邏輯得以被追溯與檢視，並於關鍵判斷節點保留人工介入及最終責任歸屬，確保決策結果仍由人為專業承擔。

近年來，審計機關積極推動 AI 輔助審計，於程式撰寫、資料蒐集、異常篩選及調查規劃等面向，廣泛運用相關工具以提升分析深度與查核廣度，已成為智慧審計發展之重要基礎。惟在 AI 高度參與審計作業流程之情境下，如何妥適留存其參與過程，已成為確保審計結果可被信任之關鍵環節。

基於此，審計實務允宜將 AI 輔助過程視為審計證據形成之一環，透過制度化方式留存與 AI 互動之重要問答內容、分析邏輯及修正歷程，作為審計判斷之輔助佐證。具體而言，於運用 AI 協助擬定查核方向、設計分析程式或歸納調查重點時，得將關鍵問答紀錄、生成結果及人工調修說明，併同納入調查計畫或審計報告附件保存，使審計結論之形成過程具備完整軌跡，展現審計機關對 AI 運用採取透明、審慎且可問責之態度，俾於善用科技提升效能之同時，持續鞏固審計專業所仰賴之信任基礎與公共責任。

三、檢視本部現行 AI 治理規範，以確保倫理合規與實務一致

本次會議就人工智慧衍生之倫理規範與道德風險，於場次七「確保人工智慧倡議妥善治理與管理」、宴會廳 3 第一場「信任人工智慧—為什麼重要以及如何建立」及場次一「在兆美元舞弊時代重建信任」等場次中，分別自治理、倫理及風險控管角度進行完整論述，指出 AI 應用若欠缺透明、可解釋及可問責機制，易衍生偏誤、不透明決策及責任歸屬不明等風險，爰強調應建構可被審計追溯，且以人為最終判斷之治理架構，使 AI 應用得以在創新與信任間取得適當平衡。

另我國《人工智慧基本法》已於 114 年 12 月 23 日經立法院三讀通過，明定國家整體 AI 治理之基本原則與制度架構，確立以人為本，兼顧發展與安全之治理方向，並就政府機關使用 AI 所涉風險評估、治理責任、透明揭露及內部控管等事項，建構原則性規範，要求各機關依其業務特性訂定相應管理機制。

就審計機關實務而言，近年推動 AI 輔助審計已具相當成果，並訂有相關制度及作業規範以導引實務運作。惟隨國際 AI 治理趨勢日益明確，且國內法制正式成形，允宜適時參考本次會議所揭示之治理重點及人工智慧基本法之規範精神，系統性檢視既有 AI 應用規定內容，涵蓋使用範圍界定、資料治理與安全控管、透明與可解釋要求、責任歸屬及人工覆核機制等面向，俾使審計機關 AI 應用制度兼顧實務需求與法制要求，並持續鞏固其專業公信力與外界信賴。

四、審慎評估 AI 工具適用情境，以強化輔助審計實務效益

本次會議於多場次中介紹人工智慧工具於審計與治理領域之應用情境，包括以 ChatGPT 等生成式 AI 說明即時生成與推理能力、透過 ChatGPT、Gemini、Claude 及 Microsoft Copilot 比較不同 AI 類型之治理與風險控管考量，並以 Microsoft Copilot 嵌入 Microsoft 365 為例，說明其於文件彙整、審計規劃及報告產製等實務應用；另相關場次亦提及 Aurex AI Studio 及 TRPGLOBAL、MODON 等稽核或控制監測案例，並舉 Microsoft Video Authenticator 說明深偽詐欺風險之因應方向（其餘工具詳附表）。

綜合本次會議所示工具及應用情境，考量審計機關業務以文字審核、分析及報告產製為主，現階段較具導入條件者為生成式 AI 嵌入既有辦公環境之模式，尤以 Microsoft Copilot 整合 Microsoft 365 並支援 Word 等文件作業，與現行流程相符，且審計部資訊處已規劃於 115 年導入並購置授權，具備運作基礎。後續允宜依實際使用經驗，檢視其對作業流程、文件產製效率及工作品質之影響，並評估是否降低重複性文書負擔及提升分析彙整即時性。

另就資源配置而言，授權費用、使用規模及擴充需求對資訊預算影響甚鉅，允宜配合實際使用情形，逐步累積成本效益數據，作為擴大應用或調整授權配置之依據；並同步留存維運負擔、版本更新頻率、供應商政策變動影響及內部支援人力等管理資訊，據以進行實證評估，作為後續推廣、調整應用範圍或研議引入其他工具之決策參考。

表 4 會議各場介紹之 AI 工具及審計機關應用評估情形表

場次名稱	介紹之 AI 工具	審計機關應用評估情形
場次二：AI 心靈術互動工作坊（AI Mentalism Interactive Workshop）	ChatGPT、Claude、Gemini 等生成式 AI 模型	屬概念展示與能力說明性質，主要提供生成式 AI 基本能力與應用趨勢之認知，短期內尚無具體實務應用環境
宴會廳 3 第一場：信任人工智慧—為什麼重要以及如何建立（Trust in AI – Why It Matters and How to Build It）	ChatGPT、Gemini、Claude、Microsoft Copilot、ChatGPT Enterprise、Gemini Enterprise、Harvey、Bloomberg GPT	以不同 AI 類型及治理模式為說明重點，供政策研析與治理制度設計參考，短期內尚無直接實務應用條件
宴會廳 3 第二場：從洞察到保證—在內部稽核中部署 Microsoft Copilot（From Insight to Assurance: Deploying Microsoft Copilot in Internal Audit）	Microsoft Copilot（嵌入 Microsoft 365）	與審計機關以文字審核、分析及報告產製為主之業務型態高度契合，且審計部資訊處已規劃於 115 年導入，具近期實務應用條件
宴會廳 2 第三場：利用既有審計技術採用 AI 之策略與實踐（Leverage your Legacy Audit Tech in Adopting AI）	Aurex AI Studio（原生 AI 稽核平台）	屬高度客製化之企業型稽核平台，與審計機關制度及作業流程差異較大，作為中長期制度發展與技術趨勢參考
宴會廳 1 第三場：現場展示與客戶成功案例—運用人工智慧驅動持續性控制監測（Demo & Customer Success – Driving Continuous Controls Monitoring with AI）	TRPGLOBAL、MODON（AI 驅動 CCM 工具）	著重企業即時內部控制監測與營運管理需求，與政府審計業務屬性不同，短期內尚無應用環境
宴會廳 1 第三場：AI 驅動稽核自動化過程之挑戰與啟示（Challenges and Learnings from an AI-driven Audit Automation Journey）	AI 驅動稽核自動化與 CCM 導入案例（AD Ports、Aldar）	屬企業導入經驗分享，提供制度設計、導入風險及推動節奏之參考，作為中長期規劃觀察
場次一：在兆美元舞弊時代重建信任（Rebuilding Trust in the Era of Trillion-Dollar Fraud）	Microsoft Video Authenticator	屬深偽偵測專用工具，提供舞弊風險辨識與政策查核觀點，短期內尚無實務應用環境

五、強化高層定調引導方向，以支持 AI 應用穩健推進

本次會議場次五「IIA 全球主席演講—成為未來」中，IIA 全球主席指出，組織推動新科技及轉型行動，關鍵不在於初期即具備周延細節，而在於高層是否清楚定調方向、公開表達支持，並確保資源配置與行動方向一致，使第一線人員得以在明確方向下持續嘗試、修正及累積經驗。主席並強調，高層定調本身即具啟動效果，除可傳達組織對創新之明確態度外，亦有助於降低對新技術導入之不確定感，使相關行動得以循序推進，而非因過度觀望或遲疑而停滯。

就審計機關實務而言，近年 AI 輔助審計推動呈現多元發展態勢，各單位陸續嘗試不同應用情境，顯示組織整體已具備一定行動基礎與實作經驗。惟在 AI 技術與應用模式快速演進下，倘未能及時形成明確之高層定調與共同理解，實務推動過程中，易出現各單位自行摸索、推動節奏不一，或對可行與不可行界線認知不清之情形，進而影響整體推動一致性與資源運用效益。

基於此，建議於高階主管相關課程中，具體納入下列三項內容：一是透過實際案例，系統性說明目前審計機關已推動或規劃之 AI 應用情形，協助高層快速掌握整體推動現況、重點方向及階段性成果；二是就 AI 應用過程中已辨識之限制與侷限，整理為可供判斷之原則或提醒事項，作為高層於支持、調整或暫緩推動方向時之參考依據；三是引導高層就「可持續嘗試」與「宜放緩或調整」之應用情境形成共通認知與判斷基準，使審計人員於實務推進時，得以清楚理解支持界線與調整方向，俾在一致定調下穩健累積經驗與成果，維持組織推動 AI 應用之整體動能。

表 5 五項建議事項總覽

建議事項	核心目標	參考國際案例／標準	具體作法	預期效益
一、深化審計願景對齊國際趨勢	將既有四大審計願景具體落實於前瞻治理與組織韌性	IIA Vision 2035（Reframe、Elevate、Expand）	於智慧、永續及韌性審計推動過程中，調整審計目標設定與績效觀點，強化風險前瞻分析及跨域介入，並同步提升數據分析能力與溝通影響力	使審計成果更能反映對政府治理穩定性、政策韌性及公共價值之實質貢獻
二、留存 AI 運用軌跡強化成果可信	確保 AI 輔助審計結果具可解釋性與可問責性	Rebuilding Trust in the Era of Trillion-Dollar Fraud（數位信任相關論述）	將 AI 輔助過程視為審計證據形成之一環，留存重要問答內容、生成結果及人工調修歷程，併同納入調查計畫或審計報告附件保存	提升審計結論可信度，展現審計機關透明、審慎及可問責之專業形象
三、檢視 AI 治理規範體系	使既有 AI 應用制度符合國際趨勢與國內法制要求	Ensuring Proper Governance Management over AI Initiatives；Trust in AI – Why It Matters and How to Build It；我國《人工智慧基本法》	參考會議所揭示之治理重點及人工智慧基本法原則，系統性檢視現行 AI 應用規定，涵蓋使用範圍界定、資料治理與安全、責任歸屬及人工覆核等面向	確保審計機關 AI 應用制度兼顧實務需求與法制要求，持續鞏固外界信賴
四、審慎推動 AI 工具應用並進行部署後評估	確認 AI 工具於審計實務之實際效益與資源投入	Microsoft Copilot 於內部稽核之應用經驗（From Insight to Assurance）	於 Microsoft 365 環境部署後，評估其對文件產製效率、作業流程及工作品質之影響，並同步彙整授權費用、維運及管理成本，作為後續推廣或調整之依據	以實證資料支撐 AI 投資決策，避免資源配置失衡，提升整體推動效益
五、強化高層定調引導 AI 推進方向	在一致支持下推動 AI 應用穩健前進	IIA Global Chair Theme – Be The Future 2025 – 2026	於高階主管相關課程中，納入 AI 應用現況、推動經驗及需留意之少數限制，協助形成可前進且可校準之共同認知	提供明確支持訊號，提升組織行動一致性，降低推動不確定感，維持推進動能

陸、附錄

附錄一：會議議程（摘錄）

■ 11 月 19 日（三）- 會議日（第一日）

時間	議程	內容
08:00-09:00	展覽區	登記與咖啡休息時間
09:00-09:10	主會場	開幕典禮暨致詞
09:10-09:50	主會場	在兆美元詐騙時代重建信任
當人工智慧正從正反兩面徹底改變世界格局，當網路犯罪分子利用人工智慧濫用信任時，這將如何影響數位世界的詐欺行為？這不僅關乎遏止詐欺，更關乎在合成時代重建信任。您將深入理解人工智慧與網路犯罪的雙面現實，並獲得實用的防詐技巧與重建信任的具體方法。		
09:50-10:30	主會場	AI 心靈術—如何讓不可能成為可能
AI 心靈術—如何讓不可能成為可能。克里斯蒂安·比紹夫既是頂尖魔術師，亦是當代「歐洲最佳心靈術師」。同時身為傑出經濟學家，他曾在瑞士伯爾尼大學從事研究並教授戰略管理課程。他將心靈的魔力與人工智慧的可能性完美融合，創造出創新表演與尖端人工智慧帶來前所未有的體驗——它必將激勵我們突破不可能的界限。		
10:30-11:00	主會場	咖啡休息與交流時段
11:00-11:50	主會場	稽核長的新使命：創新治理、網絡韌性與倫理風險領導
關鍵要點： 1.內部稽核職能作為轉型與創新的戰略推動者 2.風險與保證領導力中的技能演進與全球協作 3.首席審計長如何因應創新、人工智慧與網路威脅調整治理架構 4.審計、轉型與營運風險間的戰略對接 5.全球觀點：道德審計、ESG 與內部稽核團隊技能提升 6.跨領域洞察：打造未來導向的內部稽核職能		
11:50-12:30	主會場	從創新到開發運用：人工智慧在資安領域的陰暗面

在當今快速演變的數位環境中，人工智慧既是創新的催化劑，亦是網路犯罪分子手中的強大武器。這場引人入勝的講座將深入探討 AI 的雙面性，揭示其如何重塑網路威脅格局，並放大現代攻擊的規模、速度與複雜程度。		
12:30-13:30	主會場	午餐與禱告時間
13:30-14:10	多個會廳	同步場次

宴會廳 1：網路風險稽核與資訊科技控制

瞭解網路風險稽核與資訊科技控制如何協同運作，以保護組織資產、確保合規性，並有效管理網路威脅。關鍵要點：

1. 從合規到韌性：隨著新型威脅態勢演變，網路風險的演進軌跡
2. 人工智慧與數據應用等新興技術的普及帶來影響：識別新型網路風險。
3. 現行 IT 管控機制已顯落伍，亟需重新設計以因應新型網路風險：自動化與數據分析技術或將成為關鍵解決方案

宴會廳 2：當調查導致訴訟時

此類訴訟往往複雜且對組織構成重大風險。本場次將探討上述情況的成因、管理此類訴訟的對策，以及如何把握機會減輕自身風險，內容涵蓋以下要點：

1. 風險評估與訴訟風險識別：參與原因：內部稽核人員需理解組織如何識別與評估訴訟所衍生的潛在風險。此舉尤為關鍵，可確保及早辨識所有重大法律風險，從而及時採取緩解措施並確保財務報告的準確性。
2. 法律訴訟管理之控制措施：為何參加：內部稽核人員應關注訴訟管理相關的控制措施，包括文件記錄、核准流程及追蹤機制。此項工作在處理多起訴訟及/或團體訴訟時尤為關鍵。有效的控制措施能降低訴訟負債陳述錯誤或遺漏的風險，並確保符合政策規範。

宴會廳 3：對人工智慧的信任 – 為什麼重要及如何建立

隨著阿聯酋和更廣泛地區的組織加速採用人工智慧，內部稽核師在確保負責任且充滿信心地部署這些技術方面發揮關鍵作用。本次會議探討了有效的人工智慧治理是什麼樣子，從了解人工智慧風險和控制，到設計和實施符合歐盟人工智慧法案和區域監管發展等新興標準的框架，再到人工智慧模型的驗證和測試。與會者將獲得有關如何：

1.了解為什麼負責任的採用對於可持續的 AI 成功至關重要。
2.調整 AI 治理規模，以適應組織的風險狀況和成熟度。
3.將 AI 相關風險整合到內部稽核計畫和風險評估中。
4.使用實用工具測試和驗證 AI 用例。
該討論將幫助首席審計主管和審計團隊加強對人工智能的監督，使組織能夠利用其潛力，同時保持信任、透明度和合規性。

宴會廳 4：動態資本項目審計

透過自動化儀表板強化建設專案監管——整合多元數據源開發並實施，實現建設專案持續監控、問題識別與決策效能提升決策效率。關鍵要點：

1.整合數據來源實現即時洞察：自動化儀表板匯集多元數據源，實現即時監控工程進度。此整合機制有助迅速識別延誤與預算超支等問題。
2.持續監控與預測分析：建立關鍵績效指標（KPI）與警示機制，可實現專案健康狀況的持續評估。預測分析技術能預見潛在問題，強化主動決策能力。

14:20-15:00	多個會廳	同步場次

宴會廳 1：爐邊談話（Fireside Chat）

本場次將圍繞兩大主題進行討論：

一、Jihad 以科技專家暨執行長之觀點

本部分將從 Jihad 身為科技專家與企業領導人的背景出發，探討其如何在科技與稽核治理之間建立橋樑，並說明內部稽核人員可從中汲取之啟示。主要訊息：

- 從「稽核警察」到「合作夥伴」
  探討稽核角色之演變——從過去僅負責執法與查核遵循，逐步轉型為協助決策、提供建議之可信賴夥伴。
- 從被動反應到主動預防
  說明數據與科技如何協助內部稽核由「事後查核」轉向「預測與預防」的角色，能及早辨識風險，並為組織創造實質價值。
- 大規模資料導向之保證機制（Data-Driven Assurance at Scale）
  科技使稽核得以分析百分之百交易資料，而非僅依樣本推估，從而提升精確度、洞見力與利害關係人信任。
- 智慧進化之歷程（Evolution of Intelligence）

說明從基礎分析、流程自動化到人工智慧（AI）之發展過程，展現智慧系統如何帶來更快速、更可靠之洞察。

- 人與流程仍為核心（Human + Process Still Matter）
  即便自動化普及，稽核人員仍具關鍵地位。未來焦點將轉向顧問角色，需具備更高之科技與數據素養，以協助決策者並確保倫理與成效兼顧。

二、EVOTEQ 於可追溯性與供應鏈透明化之實踐

此部分將介紹 EVOTEQ 在阿聯醫療供應鏈中，如何透過科技建立信任與透明化，為關鍵系統提供確信之具體案例。重點說明：

- 系統目前處理逾 120 億筆以上交易，展現其規模、可靠性與成熟度。
- 可防止偽造產品、管理藥品調撥與短缺，並促進更快速且精準之產品召回。
- 使製造商、經銷商、藥局與醫院間之流程完全透明，達成供應鏈端到端追蹤。
- 此技術不僅具監管功能，更能強化病患安全與整體系統韌性。
- 呼應阿聯王儲殿下所倡導之精神——以數據導向的保證機制帶來「安心與信任」。
- 展現 AI 與可追溯技術如何打造更安全、更智慧且更值得信賴之供應鏈。

結語：在面向未來十年的稽核工作中，最重要的心態與能力，乃在於持續學習、擁抱科技，並以前瞻思維結合人類判斷與智慧審慎應用新興工具。

宴會廳 2：超越熱烈討論：AI 跨部門實務應用（UNIQUS）

人工智慧已不再停留於理論探討或試行階段，而是成為審計、風險與合規團隊的核心助力。透過自動化、進階分析與預測能力，AI 正在重塑組織營運模式。其實務應用包括：自動化合規流程、動態政策制定、預測性風險識別及內控制度優化，帶來顯著的效率提升與風險管理改善。成功導入並擴展 AI 之組織，普遍重視基礎建設投資，如健全的資料治理、政策標準化，以及針對偏誤、透明度與模型可解釋性之持續監控。重點摘要：

1.AI 帶來可量化的價值

具體 AI 解決方案已可自動化文件審閱、合規報告、風險預測及控制缺口分析，大幅節省時間、減少人工操作並提升效能；部分評估與修正流程之效益甚至可達 60%。

2.基礎建設至關重要：有效 AI 仰賴成熟的 GRC 實務

成功導入 AI 需建立穩固的治理、風險與合規（GRC）基礎，包括一致的資料結構、嚴謹的治理架構及明確的責任分工。許多組織常低估此類投資的重要性，導致 AI 難以達成可擴展且永續之成果。

3.新風險需新控制策略

AI 帶來模型偏誤、可解釋性不足、法規複雜（如歐盟 AI 法案）及「影子 AI」（未受監管之 AI 使用）等新型風險，需建立不同於傳統資訊科技審計之全新稽核與風險管理框架。

宴會廳 3：從洞察到保證——在內部稽核中部署 Microsoft Copilot

隨著組織加速推動數位轉型進程， 內部稽核職能必須從傳統的事後審查轉型為即時洞察與前瞻性保證。 本場次將探討如何透過整合於 Microsoft 365、 Dynamics 365 及 PowerPlatform 的 Microsoft Copilot， 賦能內部稽核團隊提升效率、 精準度與洞察力。透過策略性指導與現場演示的結合， 本場次將展示 Copilot 如何協助風險導向的審計規劃、 自動化證據蒐集、彙整電子郵件與報告中的複雜數據， 並在熟悉的 Microsoft 工具中直接呈現預測性洞察。 領導者將清晰掌握如何在審計環境中負責任地採用人工智慧—在創新與治理、 數據隱私及道德保證標準之間取得平衡

宴會廳 4：防火牆與虛假帳冊——網路欺詐時代下之稽核挑戰

Dimitrios Petropoulos 為公司帶來了 30 多年的資訊科技經驗，專長於網路安全和資訊風險管理。在過去的 25 年裡，他專注於資訊安全，並曾在企業 IT 安全小組、顧問公司和解決方案提供者等各個行業領域工作。 最近在英國畢馬威會計師事務所任職，Petropoulos 擔任技術總監，為 C 級高管提供資訊安全策略、轉型和網路防禦方面的建議。 在網路團隊中，Petropoulos 領導了畢馬威的多項諮詢服務，包括：安全轉型、安全架構、雲端安全、DevSecOps 和基礎設施/應用程式安全。在加入四大公司之前，他是 HPE Enterprise Solutions（後來的 DXC Technology）網路業務負責人，專注於金融服務領域的客戶。在此之前，Petropoulos 在中東工作了十多年，擔任沙烏地阿拉伯 IT 安全培訓和解決方案的首席執行官，以及網絡解決方案提供商 ENCODE 的董事總經理，在那裡他建立了 GCC 子公司並領導了該部門的強勁增長。

15:00-15:40	多個會廳	同步場次

宴會廳 1（15:00-15:20）：現場展示與客戶成功案例-運用人工智慧驅動持續性控制監測

在數據氾濫與可操作洞察追求的時代，人工智慧驅動的客戶關係管理（CCM）為企業用戶提供創新解決方案，協助其迅速應對

可能威脅企業安全的複雜存取風險與異常交易。本次爐邊談話將透過現場演示，重點展示雲端安全人工智慧代理如何賦能資深 IT 稽核與 IT 治理主管降低風險並強化資料安全。關鍵要點：

1.人工智慧與自動化在持續性控制監控（CCM）的實機演示
2.企業面臨的內外部威脅如何浮現？
3.石油天然氣與房地產領域的兩家客戶如何監控內部威脅—客戶實踐案例

宴會廳 1（15:20-15:40）：AI 驅動 CCM 自動化過程之挑戰與啟示

在當今數據驅動的時代，內部稽核正從定期審查轉型為由自動化與人工智慧驅動的持續性保證。本次爐邊對談中，來自頂尖房地產與港口集團的稽核主管將分享其持續性控制管理（CCM）實踐歷程——如何運用自動化技術即時偵測風險與異常狀況。現場演示將聚焦於安全雲端驅動的人工智慧與 CCM 工具，如何革新稽核監督機制並強化企業韌性。關鍵要點：

1.持續控制監控（CCM）自動化工具實機演示
2.內部稽核職能面臨的挑戰
3.港口集團與房地產企業如何監控內部威脅

宴會廳 2：利用既有審計技術採用 AI 之策略與實踐

若您在審計與風險流程中運用人工智慧，卻無需更動現有系統，會是怎樣景象？在本場次中，我們將探討如何透過專為內部稽核與風險團隊打造的原生人工智慧平台—AurexAIStudio，讓您充分發揮人工智慧的價值，同時擺脫現有稽核與風險技術的限制。有別於傳統工具需深度整合或大幅變更系統，AurexAIStudio能充分運用現有技術驅動人工智慧應用場景，使您得以快速導入人工智慧，無需中斷現有的稽核、風險或治理、風險與合規（GRC）基礎架構。您將親眼見證這項次世代平台如何賦能審計團隊：

1.透過人工智慧而非程式碼，自動化處理重複性、手動操作及高度判斷性的任務
2.以指尖觸控之姿，即時分析結構化與非結構化數據
3.即時偵測新興風險並進行基準對照
4.推動更智慧的審計規劃、範圍界定與執行

宴會廳 3：人工智慧對抗舞弊—終極貓捉老鼠遊戲

舞弊手法已今非昔比，對抗舞弊的方式亦然。在這場引人入勝的講座中，納迪姆與瑞法特將帶您深入探索人工智慧與金融犯罪交鋒的快節奏世界。這已不僅關乎偵測，更涉及預測、預防與保持領先一步的策略。我們將剖析人工智慧如何重塑遊戲規則、其面臨的挑戰，以及人類洞察力為何仍不可取代。您將見證真實案例、獲得真知灼見，並在過程中收穫幾分驚喜。關鍵要點：

1.關於詐騙手法演變與人工智慧應對策略的新觀點。
2.過度依賴人工智慧的風險：誤判警報、數據偏見與敵對策略。
3.為何未來在於人機協作而非競爭。

宴會廳 4：海灣合作委員會地區新興舞弊型態：法規挑戰與實務啟示

隨著海灣合作委員會(GCC)地區數位轉型快速推進，舞弊行為類型亦趨多樣且複雜——從數位金融犯罪、資金駭客帳戶（Money Mule）舞弊，到跨境犯罪網絡，皆成為日益嚴峻之威脅。隨著舞弊手法演變，各國監理機關之要求亦同步提升，促使金融機構需調整其舞弊風險管理架構與合規策略。本場次將探討 GCC 最新舞弊趨勢，分析監理環境變化對金融機構因應措施之影響，並透過實際案例解析複雜舞弊事件之挑戰與對策。重點摘要：

1.掌握 GCC 主要及新興舞弊類型
包括線上舞弊、資金駭客帳戶（Money Mule）及跨境詐欺等，2 瞭解其對金融體系造成之衝擊。
2.解析最新監理發展之影響
認識 GCC 地區近期法規更新如何改變金融機構在舞弊風險管理與合規要求上的作法。
3.學習實務對策
探討如何調整防詐策略，以同時符合新興威脅及監理期望，建立更具前瞻性之防護體系。
4.借鏡實務案例
透過實際舞弊案件之分析，汲取經驗與最佳實務，強化主動防禦與風險預警能力。

■ 11 月 20 日（四）- 會議日（第二日）

時間	議程	內容
08:00-09:00	大廳展覽區	登記與咖啡休息時間
09:00-09:10	主會場	贊助商暨品質保證感謝典禮
09:10-09:50	主會場	IIA 全球主席主題演講—成為未來 2026-2025
誠邀您參與全球董事會主席（2025-2026 任期）斯特凡諾·科莫蒂的啟發性演講，探討其全球董事會主席主題：「成為未來」。隨著風險格局變遷與科技發展，隨著環境不斷演變，利害關係人的期望日益提升，內部稽核人員必須以清晰的視野與前瞻的洞見引領方向。這已不再是取得一席之地的問題，而是要懷抱使命感積極參與其中。本次講座中，史蒂法諾將探討內		

部稽核當前面臨的關鍵時刻、塑造未來的必要條件，以及國際內部稽核師協會（IIA）如何賦能專業領域迎接新挑戰。		
09:50-10:40	主會場	動盪中的領導之道：策略、治理與韌性
會議目標： 1.理解有效戰略領導力的特質與行為模式。 2.認識治理機制如何支持符合道德規範、透明且具韌性的決策過程。 3.探討高風險情境下領導團隊、稽核部門、合規單位與舞弊偵測團隊的跨職能協作模式。 4.識別塑造未來十年的新興風險與領導挑戰。 5.運用全球領袖洞見強化危機應變準備與治理架構。		
10:40-11:20	主會場	咖啡休息與交流時段
11:20-12:00	主會場	確保人工智慧倡議妥善治理之管理
人工智慧 (AI) 正在改變組織的營運方式，但若缺乏完善的治理與管理，AI 計畫可能會迅速從「創新泉源」轉變為「風險來源」。從算法偏見、決策不透明，到違反法規與商譽受損，這些挑戰不僅真實存在，且日益嚴峻。		
12:00-12:50	主會場	專題討論-航空業內部稽核：應對頑固的顛簸
航空業堪稱快速、突發性與瞬息萬變的風險格局。若論哪個產業始終飽受頑強風險漩渦的衝擊，航空業當屬其一。航空業面臨的風險成因不勝枚舉，包括政治、經濟、天氣、技術、衝突、化石燃料供應、環境、法規、供應鏈、流行病、競爭、自然災害、安全、安保、基礎設施等。這些風險多數具有突發性、快速變化、頻繁發生、難以預測、全天候運作且影響深遠的特質。上個月的風險登記冊，可能在下個月就過時失效。其中任何一項風險的單一爆發，都可能對航空公司的未來營運持續性造成毀滅性後果。		
12:50-13:50	主會場	午餐與禱告時間
14:00-14:40	主會場	企業防舞弊指南：預防與偵測實務
本課程是一份實用指南，全面概述企業如何預防與偵測舞弊行為。內容涵蓋完善舞弊偵測策略的核心要素，強調採取主動式、多層次防禦機制，而非被動應對。會議探討關鍵概念，例如建立強大的舞弊偵測文化、實施內部控制，以及運用資訊安全技術以應對不斷演變的威脅。本課程旨在為參與者提供知識與工具，建立抵禦內外部舞弊的韌性防禦體系。		
14:40-15:30	主廳	結合審計、舞弊偵測與資訊科技優勢，打造韌性治理體系

展示審計、舞弊偵測與資訊科技部門之間務實的實務合作，呈現建立韌性組織的可行策略。目標：
1.展示審計、舞弊偵測與資訊科技部門間的實務協作模式。
2.分享真實案例與經驗教訓。
3.提供強化組織韌性的可操作策略。
4.強調主動風險偵測與緩解的工具與框架。
5.透過互動式問題解決引導參與者深度參與。
聽眾關鍵收穫：
1.跨稽核、舞弊防制與資訊科技部門的協作，是打造韌性組織關鍵要素。
2.真實案例展示適用於現實環境的實用方法。
3.共享情報與聯合應對以提升風險管理效能。
4.持續學習與跨職能協作，培育韌性文化。

附錄二：參考資料與連結

國際組織

1. 國際內部稽核師協會（IIA）

   網址：https://www.theiia.org

   重點資源：Vision 2035、國際專業實務架構（IPPF）、全球內部稽核能力架構

2. 國際舞弊偵測稽核師協會（ACFE）

   網址：https://www.acfe.com

   重點資源：全球舞弊報告、舞弊偵測專業標準、CFE 認證

3. 資訊系統稽核協會（ISACA）

   網址：https://www.isaca.org

   重點資源：COBIT 2019、CISA/CISM 認證、數位信任框架

4. 國際最高審計機關組織（INTOSAI）

   網址：https://www.intosai.org

   重點資源：ISSAI 國際審計標準、IT 審計指引

AI 治理框架

5. 歐盟 AI 法案（EU AI Act）

網址：https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

重點：風險分級監理、高風險 AI 要求

6. 美國 NIST AI 風險管理框架

網址：https://www.nist.gov/itl/ai-risk-management-framework

重點：Govern-Map-Measure-Manage 四大功能

7. ISO/IEC 42001:2023

網址：https://www.iso.org/standard/81230.html

重點：AI 管理系統要求與指引

8. OECD AI 原則

網址：https://www.oecd.org/digital/artificial-intelligence

重點：五大原則（包容成長、人本價值、透明、穩健、問責）

審計工具與技術

9. ACL Analytics

網址：https://www.wegalvanize.com/acl

用途：資料分析、異常偵測、持續監控

10. IDEA（Interactive Data Extraction and Analysis）

網址：https://www.caseware.com/idea

用途：資料擷取、分析、審計自動化

11. Power BI（Microsoft）

網址：https://powerbi.microsoft.com

用途：資料視覺化、互動式儀表板

12.Tableau

網址：https://www.tableau.com

用途：進階資料視覺化與分析

Deepfake 偵測工具

13.Microsoft Video Authenticator

重點：影片真偽偵測

14.Intel FakeCatcher

重點：即時深偽偵測

15.Sensity AI

網址：https://sensity.ai

重點：深偽威脅情報平台

16.阿拉伯聯合大公國內部稽核師協會（UAE IIA）

網址：https://www.iia.org.ae

重點：中東地區審計專業組織

17.《2024 年全球舞弊報告》（ACFE）

重點：全球舞弊趨勢、偵測方式、損失統計

18.《Vision 2035：內部稽核的未來》（IIA）

重點：重新定義、提升能力、擴大影響力

19.《AI 治理：從原則到實務》（OECD）

重點：AI 治理框架、國際最佳實務

附錄三：本團團員與會識別證