出國報告（出國類別：國際會議）

參加舞弊防治與鑑識協會（ACFE）亞太區年會出國報告

服務機關：審計部

姓名職稱：陳建仲審計兼科長、蘇志祥審計員

派赴國家：新加坡

出國期間：中華民國 108 年 9 月 25 日至 27 日

報告日期：中華民國 108 年 12 月 13 日

摘要

舞弊防治與鑑識協會（Association of Certified Fraud Examiners, ACFE）是國際上公認最重要的反舞弊專業組織，且是反舞弊培訓及教育的主要提供者，本次亞太區年會於民國 108 年 9 月 25 日至 27 日假新加坡濱海灣金沙會議中心舉行，計有 255 名來自亞太地區各公私部門之舞弊防治人員參與。年會於 9 月 25 日下午開始， 由主辦單位安排「如何增進訪談技巧：舞弊稽核師及審計人員」之預備會議揭開序幕，並於 9 月 26 日至 27 日安排「運用區塊鏈科技防治支付舞弊及數位犯罪」、「亞太地區跨境調查」、「調查工作之多方交涉：如何達成客戶要求與期望，並維持專業誠信」、「瞭解舞弊者心態」、「領航而非追隨：採行國際反賄賂標準」、「運用資料分析及商業智能辨識利益衝突」、「新興資料分析及工具：風險與機會」、「公開資訊調查及現場調查的方法與工具：整合途徑」、「創設具防弊知能之組織」、「打擊網路詐欺：攻擊及因應措施」等 10 場專題演講，藉由與亞太地區舞弊稽核師之交流，增進舞弊調查、關鍵證據取得、舞弊偵測、預防及遏止制度之建立等專業能力。

本部為拓展審計人員國際視野，汲取舞弊防治相關專業新知，鼓勵同仁參與稽核專業研討活動，遴派 2 名審計人員參加本次年會。

茲綜整參加本次年會之心得，擬具建議意見如下：

一、參照 INTOSAI 莫斯科宣言，賡續強化審計人員資料分析技能、策略思考能力及軟實力，俾發揮審計前瞻功能及影響力，促進政府良善治理。

二、參酌洗錢防制顧客盡職調查作法，賡續加強蒐集及研析轄審機關非結構化資訊，俾落實風險導向之審計，提升選案查核成效。

三、因應監理科技發展，賡續強化本部 GBA 及審計機器人之自動化分析及示警功能，俾利提升查核成效，發揮審計監督及嚇阻功能。

四、落實聯合國及臺灣 SDGs 反貪腐目標，持續選派審計人員參加 ACFE 國際研討會及鼓勵取得專業證照，以精進相關查核專業技能，協助政府形塑廉能政

風。

五、因應工業 4.0 風潮，加強查核政府推動相關資通安全方案及資通安全管理法執行情形，適時研提相關前瞻及洞察意見，以協助維護我國整體資安環境，促進數位經濟發展。

目錄

圖目錄

壹、前言

舞弊防治與鑑識協會（Association of Certified Fraud Examiners, ACFE）為強化舞弊稽核師專業知能，增進其對舞弊型態及手法之認識，並提供平台以利會員交流，每年皆於亞太地區舉辦年會，亦作為舞弊稽核師教育訓練之一環。該協會於 2019 年 9 月 25 日至 27 日，假新加坡濱海灣金沙會議中心舉行年會，計有 255 人與會，以內部稽核、審計、法遵及財務等部門人員為主，亦不乏資訊人員及高階主管，其任職單位包括國際組織、各國政府機構、會計師事務所及私人公司等。ACFE 本次年會並未設定會議主題，惟揆諸各場次議題，資訊科技將成為未來防治舞弊之利器，重點領域為數據分析技術應用，而網路犯罪及其衍生之國際合作，則成為未來舞弊防治焦點。本部為鼓勵同仁精進舞弊防治相關智識，以及拓展國際視野，本次年會由第四廳陳審計兼科長建仲及蘇審計員志祥等 2 人與會。謹就本次參加年會過程、專題演講摘要、重要研討議題、研討心得及建議意見等，提出報告如次。

貳、參加年會過程

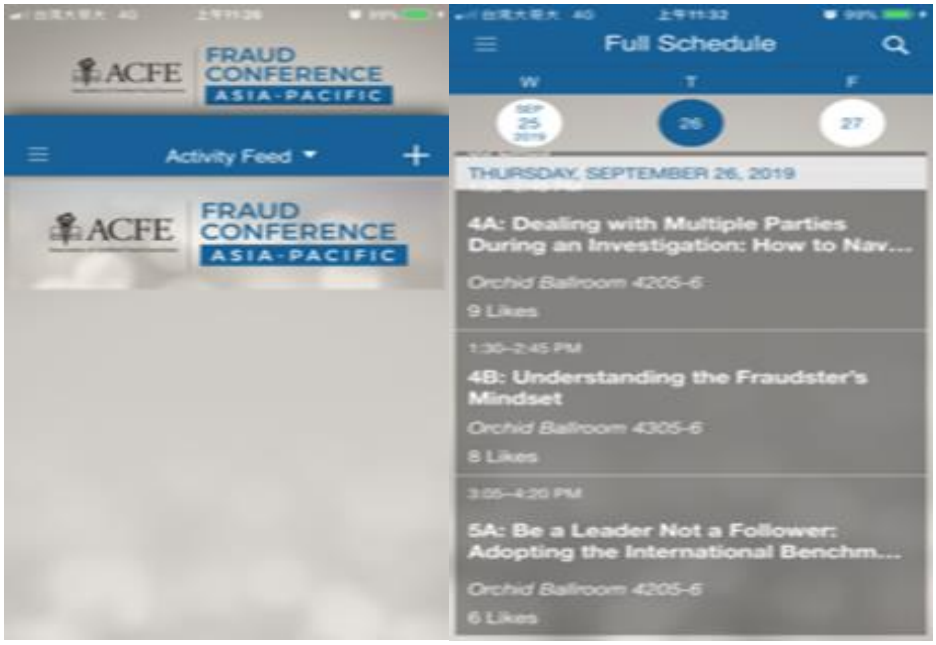
2019 年亞太地區舞弊防治年會於 9 月 26 日至 27 日，假新加坡濱海灣金沙會議中心舉行，主辦單位安排「運用區塊鏈科技防治支付舞弊及數位犯罪」、「亞太地區跨境調查」、「調查工作之多方交涉：如何達成客戶要求與期望，並維持專業誠信」、「瞭解舞弊者心態」、「領航而非追隨：採行國際反賄賂標準」、「運用資料分析及商業智能辨識利益衝突」、「新興資料分析及工具：風險與機會」、「公開資訊調查及現場調查之方法與工具：整合途徑」、「創設具防弊知能之組織」、「打擊網路詐欺：攻擊及因應措施」等 10 場專題演講，另主辦單位在正式會議開始前，於 25 日下午舉辦預備會議作為暖場，主題為「如何增進訪談技巧：舞弊稽核師及審計人員」，並於專題演講中穿插專題研討會。

各場專題演講主題

項次	專題演講主題	演講者
1	運用區塊鏈科技防治支付舞弊及數位犯罪	Andrew Koh
2	亞太地區跨境調查	Matthew Fleming
3	調查工作之多方交涉：如何達成客戶要求與期望，並維持專業誠信	Alexander Nasr
4	瞭解舞弊者心態	Annamaria Kurtovic
5	領航而非追隨：採行國際反賄賂標準	Tim Phillipps
6	運用資料分析及商業智能辨識利益衝突	Diana Ngo、Allanna Rigby
7	新興資料分析及工具：風險與機會	Saket Bhartia
8	公開資訊調查及現場調查之方法與工具：整合途徑	Abdallah Alomari
9	創設具防弊知能之組織	Shalinder Taneja
10	打擊網路詐欺：攻擊及因應措施	Parag Deodhar

為響應環保，相關會議資料在會前已公布於網路，供與會人員瀏覽，會場未提供相關書面資料，主辦單位並要求與會者事先下載手機應用程式（ACFE Events），提供議程、講者個人資料、上課地點等資訊，與會者亦可運用該 APP 上傳照片與心得，並可輸入各課程認證碼，以獲得進修時數。

圖 1　ACFE Events 手機 APP 截圖



參、預備會議及專題研討會

一、如何增進訪談技巧：舞弊稽核師及審計人員(Taking Your Interview Skills to the Next Level: Techniques for Fraud Examiners and Auditors)

本專題主講人羅伯．科克雷爾(Robert Cockerell) 係 KordaMentha 事務所之合夥人，該事務所提供專業諮詢、鑑識會計、房地產及投資等服務，其提及舞弊稽核師及審計人員可透過訪談相關人員取得資訊，惟因訪談品質及證詞可信程度不一，間有無法納為查核證據情事，爰應持續增進訪談技巧，以利調查作業遂行，研討重點

包括訪談規劃與執行、資訊蒐集方法、如何辨認謊言等，茲臚述如次：

圖 2　Robert Cockerell

(一)　訪談規劃與執行

調查(investigation)可定義成依據法律規定，為落實司法正義而尋找真相。調查階段包括歸納(induction)及演繹(deduction)等 2 階段，前者係蒐集資料，後者則係導出結論。訪談係蒐集調查證據重要方法之一，訪談成功重要因素包括：規劃、問題明確、易懂言語、肢體語言涵義、傾聽及分析等。依據講者之經驗，受訪者往往只會吐露其認為訪談者已知之訊息，爰於訪談前，須對訪談議題有充分知識，並充分瞭解構成舞弊或不當行為之重要證據、與訪談審訊有關之相關法律等，俾確保訪談遂行及確保受訪者權益；另對於訪談展示之證物，亦須妥為安排，原則上不展示實體證物，而係以影像投影或照片為之，以利訪談者藉機注意受訪者之表情變化及主導審訊節奏。在訪談過程中，應銘記 7 大原則：1.訪談目的係從目擊者、申訴人、嫌犯口中獲取正確且可靠資訊，以瞭解事情真相；2.秉持開放心態及合理懷疑，透過已知資訊或推論之可靠資訊，隨時檢測受訪者提供資訊之真偽；3.依據案情及調查環境，採取公平及公正之作為；4.不輕易採納受訪者所提出第 1 個答案，受訪者持續接受詢問，並未顯失公平；5.持續提出問題，縱使受訪者行使緘默權；6.稽核人員為找尋事實所詢問題不受限制；7.認真對待所有受訪者，包括目擊者、申訴人、嫌犯等。

(二)　資訊蒐集方法

科學內容分析(Scientific Content Analysis, SCAN)訪談係由以色列前測謊專家 Avinoam Sapir 所發展之一套科學內容分析方法，主要係透過分析受訪者陳述之架構及內容，判定其是否有欺騙之意圖，方法則是透過取得受訪者之無污染樣本，作為後續分析比對參考。訪談中須關注之關鍵字及片語，包括語句使用第一人稱、主動語態及過去式、想(would)、能夠(could)及或許(probably)等。受訪者敘事主詞使用「我們」而不用「我」，通常表示心態上是舒適及放鬆的，另於敘述案發經歷時使用過去式可信度較高，如使用現在式、未來式及被動式則可信度較低。

(三) 如何辨認謊言

訪談中常用辨認謊言方法包括：1.測謊器；2.非語言暗示：(1)眼神交流，性格內向者說謊時與訪談者眼神交流次數減少，外向者交流次數增加；另外說謊時眨眼頻率將出現異常變化。(2)臉部細微表情變化，諸如不自主短暫搖頭或出現負面表情。(3)神經語言行為(Neurolinguistic Behaviors)係研究語言及神經系統運作之關聯，諸如眼睛視線位置變化或眨眼頻率異常，可能表示說謊。(4)嘴部活動，諸如吞嚥次數增加、頻繁舔嘴唇、說話時有異音、喉結迅速來回移動等。(5)說謊時血液流速改變將刺激感官，導致受訪者出現揉眼、鼻及耳等動作，或臉色慘白；3.語言暗示：大多數人傾向不直接說謊，而係閃躲、省略關鍵資訊、選擇性遺忘及假裝無辜，爰回答問題時常有延遲、重複問題、結巴或使用較高語調等情。

二、瞬息萬變-亞太地區網路安全趨勢與威脅(Shifting Sands - Cybersecurity trends and Threats in Asia-Pacific)

本專題研討主講人艾利克・林(Eric Lam)先生係微軟公司亞太及日本地區網路安全部門主管，演講中闡述亞太地區最常見之 4 種網路威脅態樣，包括惡意軟體、加密貨幣挖礦軟體、勒索軟體及網路釣魚等，亞洲地區遭遇攻擊比率較全球平均各高出 37%、17%、40%及 22%，2017 年造成潛在經濟損失約 1.745 萬億美元，約占亞太地區國民生產毛額總額之 7%。至於如何加強網路安全，其建議企業組織應使用雲端儲存系統自動備份重要資料、存取控制、對員工進行網路安全教育訓練，並運用科技進行偵測及管控危害，個人則需具備網路安全意識、使用正版軟體、加強密碼管理、勤於備份資料及保持警戒。另外，於瞬息萬變之商業環境中，數化轉型係推動企業成長之動力，惟部分企業基於對網路威脅之擔憂，已考量放慢數位轉型過程，反不利整體競爭力，爰其提出下列建議：(一)企業組織應將網路安全視為數位轉型之必要條件，積極參與數位化過程，從正向思考，將數位化過程視為提升網路安全之機會，並隨著風險改變採用新型態之應變方法：(二)繼續投資加強安全措施，維持最佳實務之基本架構，可避免 90%之網路攻擊事件；(三)善用 AI 及自動化流程可以提高偵測能力，減少錯誤遺漏，並可快速處理大量數據，減少網管人力需求。

圖 3　Eric Lam

三、舞弊態樣(the shape of fraud to come)

本專題研討主講人麥元廷(YUEN TEEN MAK)係國立新加坡大學商學院助理教授，其認為舞弊態樣可分為賄賂、洗錢、交易、會計、網路等，至於公司發生舞弊可歸咎於 3 大失敗，包括道德失敗、董事會及高階主管失敗、三道防線失敗，其中道德失敗原因包括領導階層

圖 4　Yuen Teen Mak

未予重視、利益衝突被容忍、忽略吹哨者意見、不當行為反被稱許等；董事會及高階主管失敗，則係公司賦權不當，諸如董事會、創辦人、主席、CE 及大股東都屬相同派系，無法發揮相互制衡功能；或董事會成員過度兼任(overboarding)，致缺乏獨立性、競爭力及多樣性；或董事會文化薄弱，諸如認為交易因地制宜，可依當地習慣送禮或交付回扣等；三道防線失敗則係薪酬政策欠當、風險管理及法遵功能薄弱、內稽未發揮應有功能等。其更進一步指出，舞弊根源於公司文化，而公司文化則由董事會、企業主、出資者、大股東及高階主管所形塑，爰建立良好公司文化必須由上至下，先創建健全環境，再由下而上，發揮制衡效果，防止濫權舞弊，形成正向循環。其以新加坡吉寶公司(Keppel Corporation Ltd.)為例，集團成員岸外與海事公司(Keppel Offshore & Marine)於 2001 年至 2014 年行賄巴西官員逾 5,000 萬美元，以換取修船合同，2016 年遭罰款 4.22 億美元，裁罰金額為新加坡上市公司之歷史新高，即為公司文化不良衍生舞弊之典型案例。

肆、專題演講摘要

本次年會共計有 10 場專題演講，內容包括資訊科技之運用、與客戶之溝通、審訊及資料蒐集之技巧，以及新型態舞弊手法暨防範等。以下將針對各場次分別摘要介紹：

一、運用區塊鏈科技防治支付舞弊及數位犯罪(Using Blockchain Technology to Stop Payment Frauds and Other Digital Crimes)

本專題主講人安得魯・許(Andrew Koh)係新加坡哈比卜(Habib Bank Ltd.)銀行副總經理及風險部門主管，其認為隨著數位及行動支付科技興起，

新型態金融犯罪更層出不窮，而區塊鏈具有去中心化、分散式帳本及資訊加密連結等特性，可減低盜用身分情形，如遭盜用，亦可掌握時效即時追查金流，進而打擊犯罪。另因各種交易紀錄、文件及資訊均可加密儲存，經驗證上鏈後，幾乎不可竄改且可隨時查詢，可協助防止運用虛偽交易營造營收增加假象等舞弊行為，講者認為區塊鏈係未來風險管理之基礎科技，企業允宜與時俱進妥善運用，茲將重點臚述如次：

圖 5　Andrew Koh

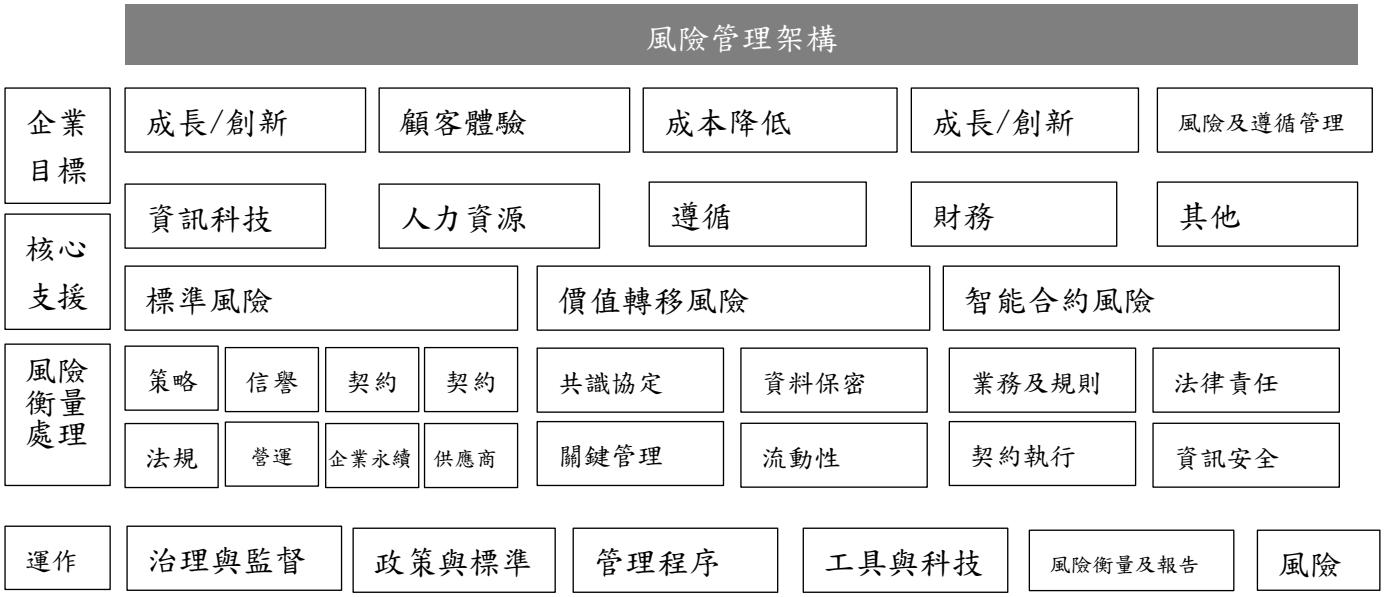
(一)區塊鏈：區塊鏈係運用加密運算，將各種資料塊相互串接，形同可永久保存且不可竄改之帳本(ledger)。最為人熟知之應用為比特幣，其後利用區塊鏈去中心化之特性，逐漸發展成智能合約(Smart Contract)，由人工撰寫程式，一旦合約條件滿足，則自動執行交易，省卻繁瑣交易及驗證文件；近年來隨著私有鏈及聯盟鏈之發展，應用領域更趨多元化，包括物流、生產履歷、身分確認、供應鏈、電子商務、物聯網等，諸如：金融機構平均每年在反洗錢（AML）與客戶身分驗證（KYC）項目支出費用達 6 千萬至 5 億美金之間，透過區塊鏈，鏈內成員可共享客戶資料，毋須一再驗證，有效降低法遵成本；消費者在線上購買衣服或貨品，透過智能合約，付款被託管，直到包裹標記已發貨或送達為止，買賣雙方均可降低風險，並藉此打擊詐欺或舞弊行為；產品生產供應鏈運用區塊鏈，驗證供應鏈流程每個環節之合法性，減少仿冒及造假情事等。

(二)防弊特質：包括分散性、即時性及不變性，區塊鏈本質上係分散式帳本，存在於所有網路節點(電腦)上，交易發生時，相關資訊均被載入所有節點帳本內，交易資訊在網路中共享且隨時對帳，爰其可提高區塊鏈內交易資訊之可見度及透明度，成員可隨時查閱資產之移轉及歷

史紀錄，便於識別舞弊交易，具有分散性及即時性；尚未上鏈之區塊，經成員透過共識流程同意區塊資料有效後，便加上時間戳，通過加密程序將其鏈結至前一個區塊，一旦經過鏈結，區塊鏈所記載之交易資訊幾乎無法竄改，爰具有不變性。

(三)風險評估：企業評估是否採用區塊鏈時，究係經過充分討論，審慎考量自身需求，抑或盲目追逐流行，將決定應用之成敗。依據勤業眾信聯合會計師事務所(Deloitte)發布區塊鏈風險管理(Blockchain Risk Management)一文指出，企業採行區塊鏈之風險評估事項包括標準風險、價值轉移風險及智能合約風險等 3 大類，其中標準風險係指類似於既有商業模式造成之風險；價值轉移風險係指未透過中間機構，直接點對點轉移資產、身分或資訊等有價事物，所產生之風險；智能合約風險則係指程式編碼情境無法準確映射實際合約，及部分條件須待外界觸發之風險，合計列有 16 項子風險項目，其風險管理架構如下圖。

圖 6　區塊鏈風險管理架構



二、亞太地區跨境調查(Cross-Jurisdictional Investigations in the Asia-Pacific Region)

本專題講者馬修·弗萊明（Matthew Fleming)係KordaMentha顧問公司之合夥人，該公司於亞太地區提供諮詢和投資服務，專注在犯罪，房地產，重組和投資等領域，講者負責複雜舞弊、境外賄賂、反洗錢等案件之調查，其曾於亞太地區多個國家執行查核工作，包括中國大陸、日本、南韓、菲律賓、印尼、越南、馬來西亞、泰國、新加坡及印度等，演講內容主要闡述亞太地區各地之差異性，並提醒稽核人員於執行調查時應行注意事項。

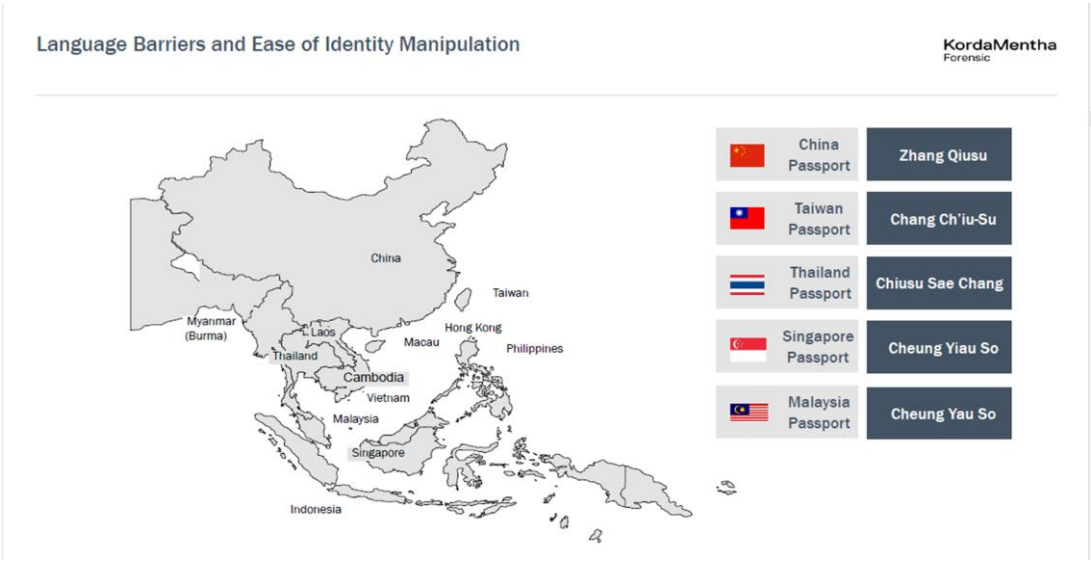
圖7 Matthew Fleming

依據ACFE出版2018年國家報告(Report to the Nations, 2018)列載，亞太地區之舞弊者，以職位進行分析，26%為老闆、41%為經理階級、30%為員工；男性占73%，女性占27%；舞弊案件被發現之原因，前三名分別為告密、內部稽核、主管審查。稽核人員於亞太地區執行調查時應注意下列事項：

（一）**安全性**：亞太地區之貧富差距相當懸殊，即使在同一國家內也是如此，例如中國沿海城市與內陸鄉村地區，因此各地之基礎建設、治安、醫療水準等也有一定差異，在執行調查時必須注意自身安全，也要因地制宜，擬訂適當之調查方式。

（二）**語言隔閡及文化差異**：亞太地區之語言非常多樣，且拼音方式亦未統一。同一姓名，在中國大陸、台灣、泰國、馬來西亞、新加坡翻譯均各不相同(圖 8)，跨境調查時經常造成調查者困擾。

圖 8　亞太地區語言隔閡案例



各國文化更是迥異，儒教、佛教、伊斯蘭教、印度教、基督教等形成不同文化圈，即使在同一國家中，也可能面臨新舊文化之衝突，例如遠離城市之鄉村和部落，可能家族或當地精神領袖對人之影響力大過法律制約。爰稽核人員允宜避免以同一認知或作法套用在所有亞太地區國家或一國內之不同地區。

（三）**地理及距離**：許多境外公司係以合資公司(Joint Venture, JV)方式進入亞太地區市場，惟可能因為不瞭解當地市場，或資訊不對稱，致簽訂不當契約，或無法確認及約束當地公司遵守契約，當地員工或管理者可能會循此漏洞作出舞弊行為。

除了上述差異之外，亞太地區熱情文化、商業活動大量依靠關係、送禮文化、政治上之干預及遊說、捐贈、收錢文化(在某些國家)、從屬關係影響治理等，均係調查者應多加注意之處。調查中過程中如有下列

事項，允應該提高警覺與懷疑：

（一）**與收付款有關**：要求以現金付款、請求付款給代理商以外之其他人、要求不合理之賠償、缺乏透明度之付款方式。

（二）**與「關係」有關**：代理人與外國官員存在直接或間接關係、商業夥伴與官員有聯繫、毫無關聯之捐贈、實習、獎學金或慈善禮品。

（三）**與合作夥伴有關**：業務合作夥伴要求支付金錢以「獲得業務」或「進行必要之安排」、對業務合作夥伴之補償過高、業務合作夥伴開具發票缺少詳細信息，或者說明與服務不符、審核期間業務合作夥伴不合作、業務合作夥伴拒絕證明合規經營、商業夥伴堅持匿名、商業夥伴缺乏執行服務之資源、業務夥伴係官方推薦等。

講者認為在執行調查規劃時，應該與公司內、外部人員合作，包括法務（內部與外部）、人力資源、會計及財務、資訊、內部稽核、採購等部門人員，以順利取得資料，調查時尤須注意應該避免打草驚蛇，舞弊者可能因為察覺調查開始執行而湮滅證據或將不法所得移轉，導致後續難以追回。

三、調查工作之多方交涉：如何達成客戶要求與期望，並維持專業誠信(Dealing with Multiple Parties During an Investigation: How to Navigate Client Input and Expectations While Maintaining Professional Integrity)

本專題主講人亞力山大．納斯爾(Alexander Nasr)係百峰公司(Blackpeak)香港地區之主管，負責處理複雜公司舞弊、貪腐及訴訟案件之調

圖 9 Alexander Nasr

查，講者提及舞弊稽核人員在調查內部舞弊、利益衝突或吹哨者舉報案件時，常需在公司政策、內部各單位之要求及期望中，相互交涉折衝，舉如各單位因考量成本、業務營運影響及風險等，間有提出以大相逕庭之方式進行調查、提前結束或擴大調查範圍等要求，爰調查人員須瞭解如何在壓力下保持專注，並維持專業誠信，儘可能與客戶保持溝通合作，以期圓滿達成任務。另長期且複雜之調查案件，常伴隨著客戶變動、調查優先順序及期望改變等風險，查核人員須在查核過程中(即參與度、工作範圍、更新、報告、溝通及費用申請)及與客戶關係上（瞭解變動隨時可能發生之基礎上，與所有相關單位保持合作關係），彈性應變處理，茲將重點臚述如次：

(一)高變更風險之查核類型：調查時間越長或涉及機密訊息越多，諸如檢查客戶或成員之電子郵件、電腦設備或偵訊成員等，則變更風險越高。以調查公司與競爭對手間之爭議為例，一旦雙方達成協議，調查方向將轉變為以法規遵循為主，此時客戶將限縮調查範圍，以降低成本費用；抑或調查高階主管或高貢獻度員工違反公司服務守則之案件，如無涉及犯罪、性騷擾情事，在公司內部易有不同看法，調查方向可能從涉及個人解雇，轉變為制度或內部控制檢討；又調查如涉及龐大商業利益，均有可能造成調查重點或結果產生重大改變。

(二)因應措施：調查人員應具備專業、處理經驗及掌握最佳實務，以妥善因應下列調查變更風險：

1. **參與客戶成員：**應充分瞭解欲參與調查之客戶人員及原因。客戶可分為過程導向及結果導向 2 類，過程導向客戶係對負面事件進行風險管理，諸如離職員工投訴或稽核發現異常情事，目標係透過獨立第三方瞭解真相，俾利進行內部處理及採取應對

措施。結果導向客戶則係欲獲取特定問題或事件之信息及證據，諸如侵犯智慧財產權、商業對手滲透情資等。倘客戶屬性轉變，將導致計畫變更。

2. **調查範圍：**對於複雜之調查工作，應慎用制式計畫或契約範本。鬆散、模糊或制式調查範圍易滋生誤解，尤其在計畫變更程序中，由委辦方新加入成員重新審視文句時，更易滋生爭議，爰調查計畫應敘明稽核工作內容及執行方式，諸如調查範圍是否明確定義司法管轄及用語、調查目標、所欲蒐集之各式信息及證據態樣及查閱範圍、計畫變更程序(提前結束或擴大調查範圍等)。

3. **調查收費架構：**客戶可能對其不瞭解之收費提出質疑，或不認同其已批可支用費用，爰明確之收費架構，有助減少爭議。

4. **報告：**客戶對調查報告提交方式可能有特殊要求，包括對重大調查發現是否先以口頭方式告知、書面報告先以草案形式提交及報告提交時程等，爰查核人員應先確認客戶需求，俾達成客戶期望。

四、瞭解舞弊者心態(Understanding the Fraudster’s Mindset)

本專題主講人安納瑪麗亞.庫爾托維奇(Annamaria Kurtovic)係誠信法務會計師事務所(Integrity Forensic Accounting and Fraud Investigators)之創辦人，其在國家及國際層級之舞弊與金融調查、資產追查和追回等方面擁有豐富經驗。講者認為舞弊如同其他犯罪行為，主要成因包括：有動機之罪犯、合適之目標及缺乏監管等，其中動機係促使一般員工轉變為舞弊者之關鍵，隨著資訊科技進

圖 10 Annamaria Kurtovic

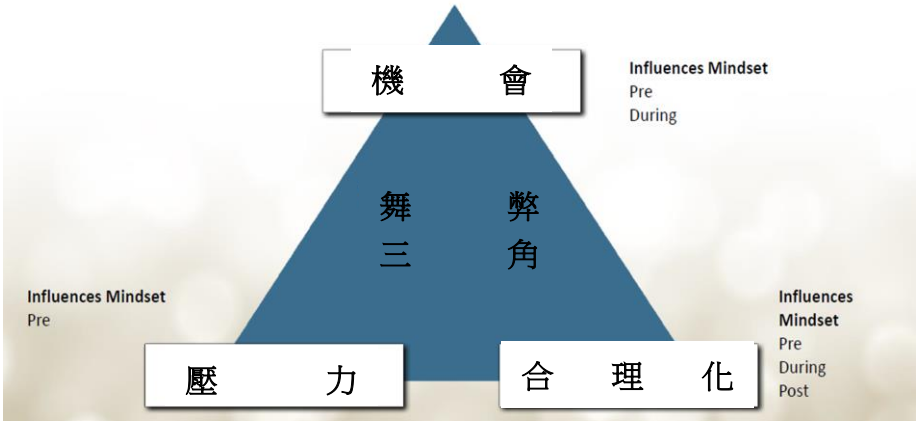
步，特別是社群媒體之發展，人們變得較以往更崇尚在人生早期成功，並追求更大房屋、最新科技產品、奢華假期及昂貴轎車等。對成功、金錢及財富之慾望，使人們產生舞弊動機。講者並運用舞弊三角來解釋舞弊者之心路歷程，其認為壓力通常出現在舞弊發生前；機會則存在舞弊發生前與發生中；合理化則是在整個舞弊過程都存在（圖 11），壓力、機會及合理化之成因可能包括：

（一）**壓力**：經濟因素、家庭因素、健康因素、癮症、貪婪、想達成他人之期望、不受認可、有（或沒有）獲得獎勵、保有頭銜、資源不足。

（二）**機會**：缺乏或無效之內部控制或防弊機制、不合宜監理制度、組織文化不倡導道德之重要性，及缺乏防弊訓練等。

（三）**合理化**：認為自己別無選擇、大家都這麼做、反正這些錢來源也不乾淨、這不會害到任何人、全都是別人的錯、不願負責、我是為了別人才這麼做。

圖 11　舞弊三角與舞弊者心路歷程



講者並舉例說明舞弊者之心路歷程，如個人感受到財務壓力後，會思考如何在短時間內讓情況變好，一開始可能只是想擺脫財務危機，並非想長期舞弊。爰其開始找尋機會，並找到了非常可行，而且可能是唯

一機會，接著會合理化自己想法以及後續行為，最後，即使財務狀況已經有所改善，因為其已將行為合理化，舞弊行為仍不斷重複實施。

理解舞弊者心態有助於執行調查，例如可以在詢問時設計貼近舞弊者之問題，讓他們說出更多，或是藉由辨認有無動機，篩選可能之舞弊者。並可藉由模擬舞弊者之心態，設想其從事舞弊之步驟及流程，再據以規劃蒐集證據的方法。理解舞弊者心態亦有助於發展舞弊防範策略架構，主要做法係從壓力最小化、去除機會以及去除合理化之心理狀態等方面著手。

五、領航而非追隨：採行國際反賄賂標準(Be a Leader Not a Follower: Adopting the International Benchmark for ABAC Compliance)

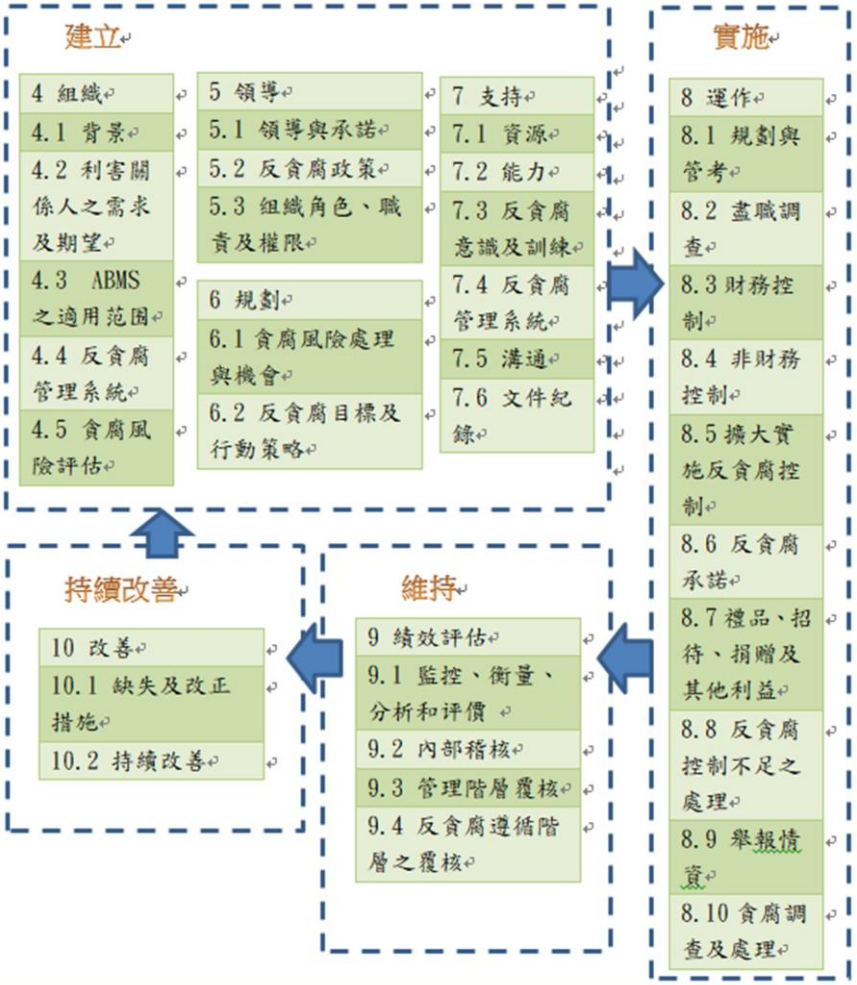
本專題主講人塞凱特．巴舍(Saket Bhartia)係安永會計師事務所(Ernst & Young)東南亞國家地區聯盟之副合夥人，其在舞弊風險評估、反賄賂審查等擁有豐富經驗。講者提及為換取不當優惠待遇，諸如加快申請程序或取得合約等，全球每年約有 1 萬億美元賄賂，嚴重影響市場公平競爭、抑制創新及加劇貧富差距。世界各國為打擊貪腐，已陸續訂頒相關法律，諸如美國於 1977 年制定反海外貪腐法(Foreign Corrupt Practices Act of 1977, FCPA)，明定每項賄賂行為將罰款 2 百萬美元等，英國於 2010 年訂定反賄賂法(the Bribery Act)，明定賄賂外國政府代表及企業未能防止貪腐均涉及刑事犯罪等。鑑於國際多有要求公司治理應納入更多打擊貪腐作為，爰公司如何加強內部防貪控制、促進商業道德文化及降低貪腐風險已成重要課題，講者爰介紹國際標準組

圖 12　Saket Bhartia

織 (International Organization for Standardization, ISO)於 2016 年 10 月發布 ISO 37001 反賄賂管理系統國際標準(Anti-Bribery Management Systems)，作為企業策進反貪腐作為之參考，茲將重點臚述如次：

(一)系統架構：ISO 37001 於 2016 年 10 月發布，旨在協助組織建立、實施、維護及改進反貪腐遵循計畫，該系統可融入既有內部控制程序中，並與既有管理系統結合(如 ISO 9001)，系統架構包括建立、實施、維持、持續改善等步驟，詳圖 13。

圖 13　ISO37001 標準架構



(二)採行情形：依據 ISO SURVEY 2018[1]，截至 2017 年底止，在 ISO 37001 認證有效期間者，計有 389 張證書及 1,541 個場域，包括微軟(Microsoft)、沃爾瑪(Walmart)、倍耐力(FIRELLI)、 博世家電(Bosch)等公司，如以採行國家進行分類，居前 3 名者，分別為義大利(140 張)、南韓(60 張)及墨西哥(26 張)。另各國政府亦開始重視及推廣採用 ISO37001，舉如新加坡政府參酌 ISO37001，於 2017 年 4 月 12 日發布反貪腐管理系統之新加坡標準（SS）ISO 37001，協助新加坡公司將其其反賄賂合規系統及流程增強至全球標準，進而提升產品及服務之信譽，增加全球競爭力。印尼政府將 ISO37001 納為其國家標準，另泰國政府宣稱公部門即將採用 ISO37001[2]。

(三)面臨挑戰：組織面臨賄賂風險高低，係取決於組織規模大小、所在地域、行業特性、活動屬性及複雜度等，ISO37001 主要係協助企業透過實施適當合宜之措施，用以預防、發現及處理風險，但無法確保賄賂絕不發生。另組織透過反貪腐管理系統，建立制度及程序，防範及處理貪腐，在公司發生貪腐面臨刑事調查時，雖可作為公司已善盡公司治理之攻防事證，惟實務上因各國國情不同，可能遭當地司法機關質疑其反貪腐管理系統是否健全，執行程序是否適當及落實等。

六、運用資料分析及商業智能辨識利益衝突（Identifying Conflicts of Interest Using Data Analytics and Intelligence）

[1] https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

[2]依據行政院 107 年 11 月 7 日「中央廉政委員會第 21 次委員會議」會議記錄，主席指示廉能是政府施政的根本，也是提升行政效能的重要關鍵，廉政反貪「預防勝於治療」，政府將研議導入 ISO 37001 企業反賄賂管理機制，作為台灣公私部門推廣反貪腐之參考依據，截至 108 年 11 月底止，已委外辦理可行性研究中

本專題兩位講者均來自英國之控制風險諮詢公司（Control Risks）。阿蘭娜・里格比(Allanna Rigby)擔任該公司亞太區負責人，黛安娜·恩戈（Diana Ngo）則係該公司合規、法證及調查部門副總監。利益衝突（Conflicts of Interest）係指某人為了個人利益（personal interest）偏袒自己或相關人士，導致專業服務或職業道德受損之情況，講者在演講中提及造成利益衝突之類型，及如何以數據為導向進行調查。

圖 15　Allanna Rigby

圖 14　Diana Ngo

常見利益衝突包括員工在採購或與他人簽約之過程中收取回扣、禮物或娛樂等、從事非法或不道德行為、將公司業務導向到自己、家人或密友所擁有或管理之第三方事業以獲取利潤、或面臨第三方之恐嚇或威脅，將業務從原承攬廠商轉移到第三方廠商、將公司資源用於個人利益等。講者認為傳統上收到吹哨者通報並進行通盤調查的方式，易使舞弊者有所警覺，並開始隱匿資料，爰須運用資料分析及商業智能(Business Intelligence, BI)，以數據倉儲、資料探勘等技術進行分析，先進行通盤檢視異常部分，俟獲得充分資訊後，再運用傳統方法（例如交易測試和電子郵件取證）蒐集證據，最後，才利用得到之證據詢問涉案者。其認為在運用商業智能時，應以兩個問題為核心，（1）涉案者是誰？（2）涉案者如何行動？我們可透過這些數據發現誰是可能之涉案者、他們如何相互影響、是否需要檢查更廣泛的人際網絡等，確認涉案者範圍後，可進一步分析

他們如何行動以及如何進行交易。以數據分析為主導之調查，可擴大查核範圍，使舞弊無所遁形，例如調查者可以檢查所有數據而不是只抽取一個小樣本,並利用程式及自動化減少人工檢查與縮小調查重點，將資源分配給高風險領域，另外還可以整合不同數據源以進行整體分析，以及將數據做為佐證資料。

講者以跨國公司進行舞弊調查為例，該公司總部懷疑某個地區的分公司出現舞弊行為，爰委託第三方進行調查，倘調查人員係以數據為核心執行調查工作，可能會採取下列步驟：(1)蒐集人力資源員工數據、會計數據、供應商列表、客戶列表以及任何其他相關數據源。(2)綜整及整合地區子公司之紀錄，包括個別案件之財務及應付帳款詳細資料，這些文件內應包括付款說明，供應商資料和案件內容等。(3)分析整合後的數據，運用關鍵字、重複之發票號碼、付款延遲及廠商與雇員關係等，識別是否有可疑之高額付款，亦可將子公司與母公司資料進行比對，找出是否有隱匿交易。(4)向客戶報告分析方法及結果，並運用數據視覺化凸顯調查發現。

七、新興資料分析及工具：風險與機會(Emerging Data Analytics and Tools: Risks and Opportunities)

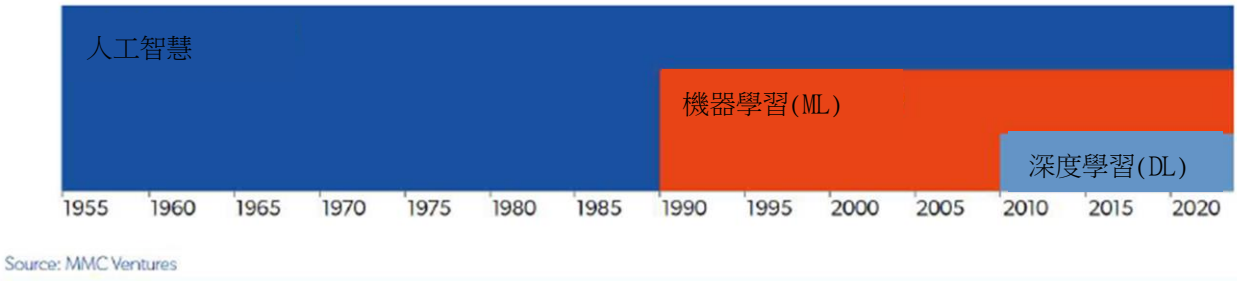
本專題主講人提姆・飛利普斯(Tim Phillipps) 係負責勤業眾信聯合會計師事務所(Deloitte)東南亞地區鑑識及分析業務，並擔任亞太地區金融犯罪戰略及應對中心之負責人，講者認為隨著邁入人工智能（Artificial Intelligence, AI）及機器學習(machine learning, ML)時代後，機會伴隨着風險，金融機構開始以人工智能（AI）工具來進行識別詐欺交易模式，標記

圖 16　Tim Phillipps

可疑活動，惟罪犯或駭客之技術方法亦日新月異，已逐漸減少受到高度關注之交易活動，另外創造其他舞弊交易模式，藉此規避系統或程式監督，爰人工智能猶如雙面刃，公司不可認為購買人工智能軟體即可有效阻止詐欺，因為每種軟體之防弊功能有所不同，仍須透過人為努力不斷持續檢討精進，始能發揮防弊功效，茲將講述內容重點臚述如次：

(一)人工智慧發展歷程：AI 自 1955 年開始發展，早期係藉由撰寫程式進行重複運算，減少人工作業，在 1990 年進入機器學習(Machine Learning)後，係透過輸入相關資料，在有限樣本中取得最佳化參數，用以預測未來趨勢(諸如：此筆交易有無涉及舞弊)，2010 年進入深度學習(Deep Learning)，係以人工神經網路為架構，對資料進行表徵學習之演算法，為機器學習分支之一，廣泛運用於圖像及文字解讀。

圖 17　深度學習之演進



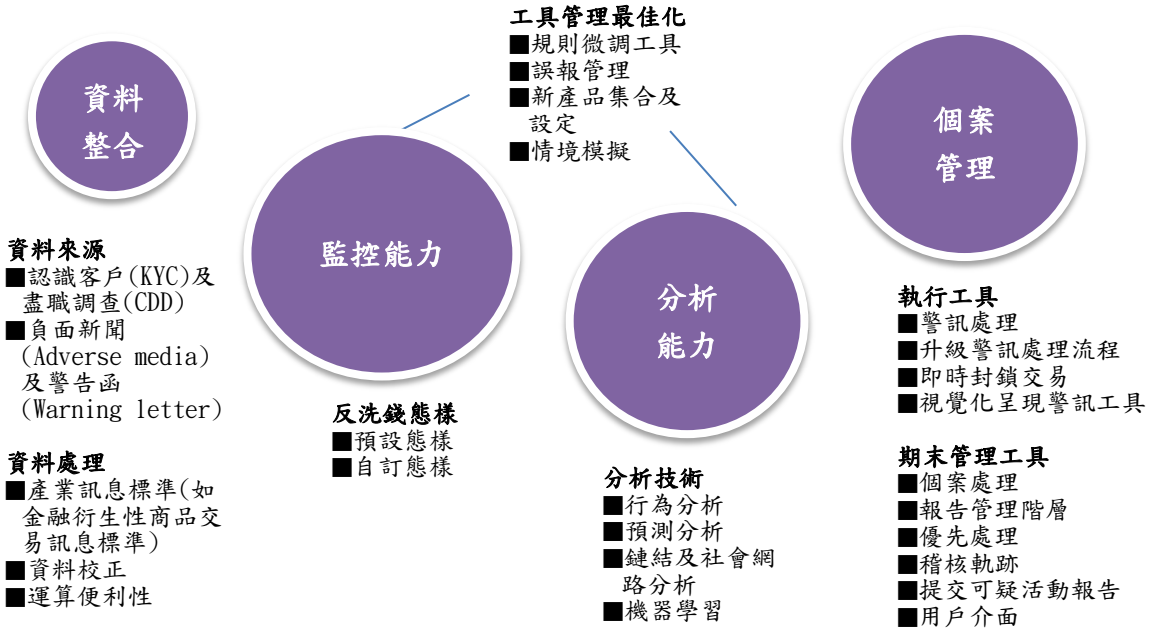
(二)人工智慧運用：依據 Gartner 發布 2019 年資訊長調查(CIO Survey)，經受訪者表示其公司運用 AI 之相關領域，居前 3 名者分別為聊天機器人(26%)、處理程序優化(26%)、交易資訊舞弊分析(21%)，預計超過 2/3 大型公司將在 2 年內開始運用 AI，成長規模達 3 倍。

(三)偵測金融犯罪遭遇困難：主要係資料數量、正確性、速度及多樣性，銀行及公司需要處理大量資料，當建立客戶資料檔案越多，

資料規模持續增長，同時如何解決資料間彼此不一致及維持資料正確性更加困難，數位銀行及行動支付之交易量持續增加，資料來源廣泛，包括結構性及非結構性資料，使得追蹤及偵測犯罪活動更加困難。

(四)金融犯罪偵測未來發展：銀行及金融機構需要處理大量資料，當建立客戶資料檔案越多，資料規模持續增長，亦衍生資料互不一致情事，數位銀行及行動支付之交易量持續增加，資料來源更為廣泛涵蓋非結構化、半結構化及結構化資料範疇，維持資料正確性更增困難，亦不利追蹤及偵測犯罪活動，為增加效率，企業可運用下圖所列科技偵測及防杜金融犯罪：

圖 18　金融犯罪偵測趨勢



(五)混合偵測舞弊方法：舞弊偵測方法可分為規則導向、機器學習(監督及非監督)及混合(Hybrid)等，其中規則導向係指預先設定規則(紅旗警訊或高風險標準)，標記異常活動；監督學習係指利用具有標示交易（正常/欺詐）的數據資料建立統計模型，非監督學習則係運用無標示資料由機械自行辨認及建立行為模型；混合方式

則係結合規則導向及機器學習，俾更全面檢視數據及發掘異常，諸如銀行透過蒐集瞭解客戶之歷史交易行為，包括購物行為及交易頻率，在何時及何處購物等，辨認非常態行為(以異常速度大筆下單付款等)。

(六)AI 面臨挑戰：AI 本質上為函數，在模擬現實世界時，可能因為人為偏見影響演算法及模型，導致輸出結果失真，犯罪者亦能運用 AI 模擬正常商業行為，將非法交易偽裝成合法交易，接管帳號、盜取身分及竊取智慧財產，另在監管方面，亦可能因資料透明度及稽核人力專業不足問題，衍生監管漏洞。

八、公開資訊調查及現場調查之方法與工具：整合途徑（Open-Source and Field Investigation Methods and Tools: A Combined Approach）

本專題主講人阿卜杜拉·阿洛馬里(Abdallah Alomari)係新加坡農業信貸銀行客戶身分驗證專家，同時擔任 ACFE 諮詢委員會成員及 ACFE 約旦分會財務主管。本次演講內容著重於公開資訊調查方法、地理資訊調查、現場調查可運用之資源，暨相關注意事項，講者認為公開資訊調查與現場調查可兩者並用，以獲得最大的成效，茲將重點臚述如次：

圖 19　Abdallah Alomari

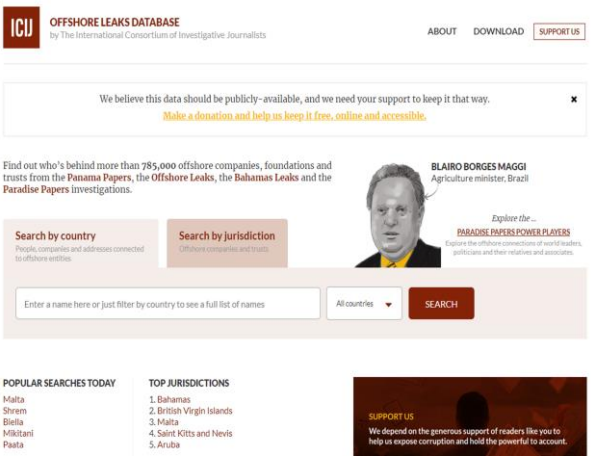
(一)公開資訊調查步驟，包括：1.確認範圍：調查權限、調查層次（負面新聞、一般資訊、財務資訊）、需調查之議題（單一議題或綜合議題）。2.執行調查：網路搜尋、僱用當地調查員蒐集較難從網路獲得資料。3.重新檢視與修正：調查意見須源自於所取得之證據，當所有必要之搜尋與分析程序皆已完成後，才能獲致結論。

(二)公開資訊類型，包括：1.負面新聞：腐敗或賄賂、制裁或出口控制、洗錢或財務犯罪、政府單位或高知名度政治人物、企業持續經營、違反環保法規、欠缺法遵架構、人口販運、童工、歧視、違反資安、不當處理個人資訊。2.註冊資訊：網路上會有公司登記資料，包括股權分配、經理人、公司統編、營運狀態、地址、開始營運日期等，但須注意各國要求公司需註冊之資訊不同，公開程度亦不同。另外，有些行業別註冊時必須取得營業許可證，例如，法律、醫藥、食品等，可以從其主管機關獲得該公司之公開資訊。3.媒體資訊：公司型態、經營所在國家、員工數、商業夥伴、競爭對手、大事紀、獲獎紀錄、顧客列表。4.股東及公司最終受益人：可從工商登記、公司之年報及財務報導、股票交易網站等獲得資訊。5.經理人及主要負責人：可從商業登記資料、工商目錄或社交平台找到資訊，包括別名、董事組成、學經歷等。6.財務資訊：主要由公司發布之財務報導獲得。7.其他資訊：諸如國際透明組織發布之腐敗指數、全球洗錢風險年度指數、無國界記者發布之新聞自由指數、租稅正義聯盟發布之金融保密指數及防治洗錢金融行動工作組織發布之高風險國家清單等。

除了前開資訊外，當地的報紙或網路新聞亦係資訊來源之一，某些社交平台，如 Facebook, RocketReach, ZoomInfo,LinkedIn, 及 Bayt 等，亦可獲得相關經理人或負責人之資訊；另某些特殊之資料庫，諸如 WikiLeaks 以及 ICIJ Offshore Leaks Database（圖 20）等，在尋找企業醜聞或與海外政商有關的資產時相當有用。

(三)地理資訊調查：由於資訊科技進步，調查人員可運用地理資訊系統找出公司位置，例如可利用 Google Maps 找到公司實際位置及建築物，以確認該公司實際存在。惟受限於某些國家地理資訊系

圖 20　ICIJ Offshore Leaks



統並不完善、公司在大樓內部、調查人員掌握公司地址資訊不完整等，可能影響此調查方式之有效性。

(四)調查人員僱用：當網路資訊不足時，就需考慮是否僱用當地調查員，特別在調查對象是個人而非企業體時，網路上可獲得之資訊相當有限，因此就有僱用當地調查員之必要。當地調查員可獲得之資訊，包括：商業註冊、訴訟檢索、聲譽調查、直接探訪公司、已知信息的詳細資料、個人的學經歷等。公開資訊與現場調查交互運用，可使調查獲得之證據更完整，並據以作出有力之結論。

九、創設具防弊知能之組織(Creating a Fraud-Intelligent Organisation)

本專題主講人薛蘭德・特內加(Shalinder Taneja)係是新加坡上市公司澳藍國際公司(Olam International Limited)內部稽核部門之副總裁，其提及每個組織發生舞弊之頻率及強度不同，舞弊風險雖無法完成消除，惟可透過健全組織環境，增加舞弊困難度，進而嚇阻舞弊發生。又組織對舞弊常有迷思，包括舞弊係由競爭對手策劃、舞弊不會發生在自己身旁、小額舞弊不嚴重、科技進步可阻止舞弊、好人不會欺騙等，長期漠視舞弊風

圖 21　Shalinder Taneja

險，導致組織道德文化薄弱、內部控制欠當或資訊科技系統弱化等，形同助長舞弊行為發生，並發生破窗效應(Broken windows theory)：任令環境中不良現象存在，就會誘使組織成員仿效，甚至變本加厲。破窗代表放任、散漫、不尊重法律，因此組織需打擊輕微罪行減少更嚴重罪案，破窗將緩慢侵蝕整個組織。爰創設具防弊知能之組織極其重要，茲將重點臚述如次：

(一)評估公司組織文化優劣指標：1.提問(questioning)：良好之機關文化，組織成員均勇於提問；2.勇於坦承知識不足；3.激勵正當行為；4.不會以資深為由藉以規避內部控制。

(二)管控舞弊風險架構：分為 4 大項目，包括：1.確立反舞弊之職責：賦予反貪腐職責予相關部門，專責成員包括內部稽核、法務、財務人員，並編列充足預算供其運作執行；2.執行舞弊風險評估：建立舞弊風險評估之目標及方法，辨認待進一步檢視之高風險舞弊事項，以及評估既存控制點及較佳反舞弊實務之差異等；3.稽核辨認舞弊：稽核工作包括評估有無舞弊風險，考量可能之舞弊情境及尋找舞弊跡象等；4.進行舞弊調查：協議調查啟始、執行及結束程序、重大舞弊升級調查程序、調查團隊遵守規範等。

(三)掌握反舞弊關鍵趨勢：隨著網路犯罪增加，網路舞弊偵測(online fraud detection, OFD)市場益趨擴大，部分網路支付公司直接透過收購相關反舞弊風險管理平台，強化線上交易安全性，諸如 PayPal 收購 Similit 等，俾提供值得顧客信賴之交易及溝通環境。另外隨著消費者透過手機、電腦、購物平台、實體店面等多元通路購物，部分通路資料遭竊後，在其它通路即可進行假交易，爰須實施全通路舞弊策略(Omnichannel Fraud Strategy)，將所有通路涵蓋至反舞弊政策內；另外有關舞弊前期活動偵測(Upstream

Detection Regime)，偵測高風險舞弊案件，在交易完成前，採取拒絕提供服務、產品，或舉報等積極作為，亦可有效減少犯罪。組織可運用舞弊防治及偵測工具包(Tool Kit)，如下圖：

圖 22　舞弊防治及偵測工具包

十、打擊網路詐欺：攻擊及因應措施（Combatting Cyberfraud: Attacks and Countermeasures）

本專題主講人帕拉格·迪奧達（Parag Deodhar）係威富公司（VF Corporation）亞太地區資訊安全總監，曾擔任安盛集團（AXA）亞洲區首席資安官。其在企業風險管理方面擁有超過 19 年經驗，專門研究舞弊風險管理、營運風險管理及資訊安全等議題。講者提及資訊科技日新月異，且組織相較於以往更加依賴科技，因此也更容易受到來自網際網絡的攻擊。鑑於這些攻擊經常透過新興技術進行，爰瞭解攻擊技術，有助檢測與調查網路詐欺以及制定有效對策。其中駭客會駭進家庭、公司及政府系統，盜取資料或金錢，造成巨額損失，爰有必要先認識駭客之種類，再瞭解其作案手法，並據以思考對策。駭客之種類包括：

圖 23　Parag Deodhar

(一)腳本小子：用來描述以「駭客」自居並沾沾自喜之初學者，他們

通常從某些網站上複製指令碼代碼，然後到處貼上，卻並不一定明白它們的方法與原理。與真正駭客不同的是，腳本小子通常只是對電腦系統有基礎了解與愛好，但並不注重程式語言、演算法和資料結構之研究。

(二)黑帽：組織有時會僱用白帽駭客去試探和入侵自身之電腦系統以確認這些系統之安全性，並提出建議以提高安全程度，白帽駭客之行為是合法的，因為他們取得了客戶許可，與之相對，黑帽駭客則是犯罪分子，他們侵入受害者之電腦系統只為了獲取自己之利益。

(三)犯罪集團：這些駭客使用黑帽技術，但組成了一個看似合法的事業體，以掩護其違法勾當。

(四)民族國家行為者：這些駭客通常獲得國家之支持，因此他們有相對充足之資源，他們也可能存在企業之中，藉由在該企業生產之軟體或硬體設備故意設下漏洞,使其國家在網路戰爭中取得優勢。另一個名詞，網路恐怖份子，則是指與自己立場相反之民族國家行為者。

(五)激進駭客：此類駭客主要是為了表達抗議而入侵他人或其他組織之電腦網路及系統，例如匿名者（Anonymous）。他們會癱瘓與自己理念不合之企業或政府之電腦系統，其動機是政治而非金錢。

(六)機會主義網絡罪犯:這類網路犯罪者通常是公司員工或合作夥伴，利用公司之內部資訊或內控弱點盜取利益。例如員工可能會偷取智慧財產或商業計畫。

駭客之技術高明與否，可用掌握多少零時差漏洞[3]（Zero-day vulnerabilities）來衡量，一旦駭客找到這些漏洞，就能對系統進行

[3]指還沒有修補程式的安全漏洞。

攻擊，常見的技術包括：

(一)假連結或假網站：通常是較無資安觀念者會被此方式詐欺，該連結會以贈品或誇張之優惠等，誘使人們點擊連結。

(二)釣魚：係指駭客運用假網站、電子郵件、手機訊息、惡意廣告等方式，獲取受害者之證件、個人資料、信用卡資料及個人識別資訊（personally identifiable information, PII）等；特定釣魚則是針對特定人士，精心設計之釣魚方式，會因應該特定人喜好變更網頁或訊息內容。

(三)手機病毒軟體：駭客仿造熱門遊戲或銀行之 App，這些 App 被下載後，會要求取得如相機、麥克風 GPS、手機內資料等權限，或是須輸入銀行帳號密碼等資料，造成個人資料洩漏。

(四)社交媒體攻擊：舉例如 LinkedIn[4]，駭客在平台上假裝寄送邀請參加討論社團之連結或寄發活動訊息之電子郵件，實則隱含惡意程式碼，人們在點擊後將使電腦系統產生漏洞。

(五)勒索軟體：這類惡意程式未經資料擁有人同意而將資料加密，使擁有人無法存取該資料，並要求收到贖金才把資料解密。此手法近年大為盛行，2019 年第一季即較 2018 年同期增加 195%。

(六)殭屍網路：是指一群彼此連接以執行特定任務之電腦。這些任務通常由駭客遠程發送命令，遭控制之電腦則被稱為「殭屍」（Zombies），因為這些電腦的主人並不知道自己電腦正在執行後台行程。殭屍電腦通常有兩件主要任務，第一是發動 DDoS 攻擊，第二個是發送垃圾詐騙郵件，發送詐騙郵件是駭客賺錢之途徑。

(七)挖礦劫持：指駭客劫持電腦，在受害者不知情之情況下挖掘加密貨幣。早期之惡意挖礦軟體須由受害者點擊惡意鏈接或電子郵件

[4]中文名為領英，是一款近似 Facebook 的社群網路。完成註冊後會自動產生和帶入電子名片。主要供商業人士使用。

附件，使系統在無意中被隱藏惡意程式感染。然而近年來，多數挖礦惡意程式都通過網站運行，意即連結至該網站就會開始挖礦。

(八)惡意廣告：未經使用者許可下派送廣告（如彈跳式視窗或網路連結）之軟體。通常透過木馬程式或是成為使用者下載安裝軟體之一部分來進入電腦。惡意廣告會根據使用者電腦上之間諜軟體追蹤及蒐集瀏覽習慣，並顯示高度針對性的廣告。

講者認為組織除了採取加裝防毒軟體或將機密資料分開儲存等措施，最重要還是加強資訊安全觀念，由上述駭客手法發現，多因人們點擊了釣魚連結或下載植入病毒之程式或檔案，才導致電腦系統遭到感染，爰提升資安意識將成為每個組織未來要務之一。

伍、研討心得及建議意見

一、參照 INTOSAI 莫斯科宣言，賡續強化審計人員資料分析技能、策略思考能力及軟實力，俾發揮審計前瞻功能及影響力，促進政府良善治理。

國際最高審計組織(INTOSAI)於 108 年 9 月 25 日至 27 日假莫斯科召開第 23 屆會員大會，就資訊科技促進公共行政發展及最高審計機關對國家推動優先治理事項及目標所扮演角色等主題提出討論，會後並發布莫斯科宣言(Moscow Declaration)，在有效因應科技進步帶來機會方面，認同審計機關在相關審計領域可更加善用資料分析技術(Data Analytics)，並聲明：數據分析係審計機關必要之創新，其可有效提升審計效率及落實改善追蹤，審計機關得綜整研析跨部會、領域、政府之數據，運用大數據技術方法，研提通案及整體性建議意見，協助政府解決相關施政問題；透過結合線上、實地及混合數據蒐集方法，定期更新數據，亦可針對重要議題及高風險領域進行實時(Real Time)監控；另在強化審計機關影響力方面，認同審計機關為持續強化創新，得鼓勵培育具備資料分析、人工智能及進階質性分析方法(qualitative methods)之審計人員，俾研提前瞻審核意見，以及擔任策略擬訂及知識分享者，並聲明：(一)將確保員工專業化列為關鍵策略目標之一，體認審計人員之專業技術及能力，係審計機關主要資產。(二)審計環境改變及利害關係人期望，將重塑審計人員所需具備之審計技能，包括：1.策略思考能力：可行性分析、以假設為導向之思考、確認因果分析、目標導向、前瞻、策略規劃、系統思考及優先順序等；2.資料分析技能：數據及資料庫之處理運用、資訊視覺化及複雜資訊之呈現；3.軟實力(Soft Skills)：有效溝通、情緒管理，促進專業信度、領導及凝聚共識之能力。(三)審計機關為強化資訊分

析能力，得設置特定分析部門處理特定問題，諸如風險管理及方案評估等。

經查本部為因應電子化政府發展，歷年來已持續導入及推動電腦輔助審計技術，依據本部 107 年度政府審計年報列載，當年度應用 POWER BI、GIS、ACL、Excel 等電腦軟體查核件數達 1,244 件，應用領域涵蓋收入面、支出面及經營管理面，又為因應大數據世代來臨，已成立審計部大數據分析審計應用推動小組，開發大數據分析平臺及審計軟體機器人等，均已獲致具體運用成效。惟在研提前瞻審核意見部分，據本部 107 年度績效報告列載，當年度針對各機關(基金)或跨機關(基金)政策、計畫、作業或職能之長遠影響、未來重大(新興)挑戰或關鍵趨勢之潛在風險事項及政府應變措施(能力)提出預警意見者，計 3 項，僅占 107 年度各級政府年度總算審核報告揭露審核意見總項數 2,243 項之 0.13%。鑑於 INTOSAI 莫斯科宣言已認同強化資料分析技能、策略思考能力及軟實力，有助研提前瞻審核意見及擴增審計影響力，為落實審計長赴立法院報告提出朝向落實監督、強化洞察及邁向前瞻三大審計主軸，建議參照 INTOSAI 莫斯科宣言，賡續強化審計人員相關專業能力，諸如開辦相關領域教育訓練、持續鼓勵及推動審計領域之大數據應用等，俾持續擴增前瞻預警審核意見項數，發揮審計前瞻功能及影響力，協助促進政府良善治理。

二、參酌洗錢防治顧客盡職調查作法，賡續加強蒐集及研析轄審機關非結構化資訊，俾落實風險導向之審計，提升選案查核成效。

國際洗錢防治金融行動小組（Financial Action Task Force on Money Laundering, FATF）為有效打擊洗錢、恐怖主義及大規模毀滅武器資金流動，爰訂定 40 項反洗錢建議事項，其中建議事項第 10 項，

明訂金融機構應採行顧客盡職調查(customer due diligence ,CDD)措施，瞭解客戶身分及評估交易風險，並記錄歸檔保存。一般實施程序包括瞭解客戶之實質受益人、是否為政治人物、有無負面新聞(Adverse Media)，或被列入制裁名單等。其中負面新聞係指在各種媒體來源中所發現客戶之不利信息，包括新聞報導、廣播及網路資訊等非結構化資訊。以我國臺灣集中保管結算所建構防治洗錢及打擊資恐查詢系統為例，系統建置負面新聞資料庫包括監管、競爭、金融、環境、生產、社會及勞動力等全球負面新聞名單。經查本部職司政府審計，107年度各級審計機關審核中央暨地方政府(含鄉鎮公所)機關、基金及事業機構計 8,601 個單位，總收支金額 19 兆餘元，審核規模龐鉅，為落實風險導向審計，已於政府審計共同規範第 45 條、審計機關普通公務審計作業規定第 35 條等規定，明訂查核(抽查)計畫內容應包括風險辨認及評估事項，並訂頒抽查轄審機關風險評估表，臚列內部控制欠佳、迭遭檢舉或媒體關注等 11 項評估事項，供各審計單位遵循運用。惟查其中「迭遭檢舉或媒體關注」1 項，尚未明列所應查詢政府開放資料庫、媒體報導平臺、立法院委員質詢、行政或司法判決資料庫等，易滋生資訊蒐集廣度及深度不一情事，不利妥為評估風險。建議參酌洗錢防治顧客盡職調查作法，賡續加強蒐集及研析轄審機關非結構化資訊，適時研議建立可供參考查詢資料庫或平臺清單，俾供審計人員查詢參考並將查詢結果作成紀錄存檔，落實風險導向之審計，提升選案查核成效。

三、因應監理科技發展，賡續強化本部 GBA 及審計機器人之自動化分析及示警功能，俾利提升查核成效，發揮審計監督及嚇阻功能。

監理科技(Regtech）主要係指以科技驅動監管，運用人工智慧（AI）、區塊鏈、機器人流程自動化（Robotic Process Automation）、大數據分析等新興科技，協助被監管者有效完成法遵作業，監管者亦得隨時監控活動，就異常或不符事項即時通知改善，俾免危害持續擴大。其中有關異常偵測及稽核部分，多涉及 AI 運用範疇，諸如勤業眾信聯合會計師事務所運用 Argus 讀取租賃、衍生品和销售契約等文檔，透過演算法研析契約關鍵條款、趨勢及離群值等，辨識高風險契約；資誠聯合會計師事務所(PricewaterhouseCoopers)運用 Halo 分析帳簿辨識潛藏可疑區域，諸如具可疑關鍵字、逾授權範圍或無授權之分錄帳。另外透過非指導式之機械學習，可分析各種資料間潛藏之模式或關聯，如有例外者則列為異常，作為選案查核參考[5]。經查本部為因應大數據發展潮流，已建置歲計會計資訊審核分析系統及審計軟體機器人，提供知識詢問、風險示警及流程自動化等服務，系統可產出異常報表或以電子郵件發送警訊分送相關人員，有助提升審核成效。惟查相關系統所設控制點或風險示警項目，多係預先設定規則由人工撰寫程式編碼，較少以機器(深度)學習為之，其中除屬明確違反法令性質者外(諸如決標予拒絕往來廠商、決標公告刊登逾期)，餘仍待進一步蒐集資料釐清(諸如次低標決標等)，較為耗時不便，且囿因審計人員專業領域及審核敏銳度不同，易影響審核成效。鑑於 ACFE 出版反貪腐科技標竿報告(Anti-Fraud Technology Benchmarking Report)[6]，調查組織打擊舞弊所使用資料分析科技，其中人工智慧或機械學習占比約 13%，未來 2 年將提升至 25%，漸成主流應用科技，建議因應監理科技發展，賡續強化本部 GBA 及審計機器人之自動化分

[5] Gabe Dickey,, Sandra Blanke, Machine Learning in Auditing: Current and Future Applications, the CPA Journal,。

[6] Anti-Fraud Technology Benchmarking Report .2019 Association of Certified Fraud Examiners, P7

析及示警功能，適時導入 AI 等相關新興分析科技，俾利加速查核及通知檢討改善，提升查核成效，發揮審計監督及嚇阻功能。

四、落實聯合國及臺灣 SDGs 反貪腐目標，持續選派審計人員參加 ACFE 國際研討會及鼓勵取得專業證照，以精進相關查核專業技能，協助政府形塑廉能政風。

廉正係普世價值，聯合國為加強打擊貪腐，已於 2003 年 10 月通過反貪腐公約，續於永續發展目標(Sustainable Development Goals ,SDGs)16.5 明訂 2030 年前應大幅減少各種形式貪腐之目標。行政院國家永續發展委員會臺灣永續發展目標 16.4 亦明訂整合肅貪能量、形塑「貪污零容忍」社會風氣，針對相關高風險業務進行清查。經查本部職司政府審計，102 至 106 年查核發現各機關人員有不法或不忠於職務上之行為且涉及刑事，依審計法第 17 條規定移送檢調偵辦並報告監察院者，合計 26 件，尚具成效。按舞弊或貪腐案件之查核，除客觀事實之認定外，主觀上亦須探究行為人無明知故意為之，其涉及心理學、專業慣例、各類知識與法令範疇，又因犯罪態樣及舞弊技術日新月異，爰審計人員仍需持續汲取新知與時俱進，始能遂行防貪任務。鑑於 ACFE 會員約有 5 萬餘人，係全球最具規模之民間反貪腐協會組織，負責辦理舞弊稽核師之考試、發證、教育訓練等，開辦訓練課程涵蓋調查與檢查、道德與遵循、預防與嚇阻、電腦與技術、調查及報告、會計審計、金融交易和舞弊、法律議題等，並不定期舉辦研討會或活動，本次參加 ACFE 亞洲區研討會，除會中討論議題外，亦可與其他國家與會人員交流調查舞弊經驗及技術方法，有助提升本職學能，為落實聯合國及臺灣 SDGs 反貪腐目標，建議持續選派審計人員參加 ACFE 國際研討會及鼓勵取得舞弊稽核師專業證照，以精進相關查核專業技能，協助政府形塑廉能政風。

五、因應工業 4.0 風潮，加強查核政府推動相關資通安全方案及資通安全管理法執行情形，適時研提相關前瞻及洞察意見，以協助維護我國整體資安環境，促進數位經濟發展。

資安即國安，政府為打造安全可信賴之數位國家，歷年來已積極推動資通安全基礎建設工作，諸如國家安全會議於 107 年 9 月提出「國家資通安全戰略報告」作為上位指導方針，臚列持續優化國家資安機制、強化國家資安體系運作效率及完備資安自主產業生態體系等 3 大未來努力方向；行政院核定「國家資通安全發展方案」(106 年至 109 年)，輔導政府機關試行導入資安治理成熟度評估模式，除定期辦理自評外，並建立政府機關第三方評審機制；資通安全管理法於 107 年 6 月 6 日制定公布，並自 108 年 1 月 1 日正式施行，建立資安責任等級分級制度，落實公務機關及特定非公務機關之資通安全管理等。惟據行政院 108 年 6 月公布「國家資通安全情勢報告」列載，該院 107 年度挑選 25 個重要機關辦理資通安全稽核作業，成績 75 分以上僅 8 個機關，60 至 75 分者 12 個機關，低於 60 分者 5 個機關，顯示機關資通安全管理及環境仍未臻完善。鑑於政府為因應工業 4.0 風潮，致力推動五加二產業、數位經濟、大數據應用分析及人工智慧等，多與資訊科技運用相關，資通安全維護儼然成為重要戰略項目，建議審計機關允宜加強查核前開報告、方案及資通安全管理法之執行情形，賡續運用專家諮詢及眾開講平台妥為規劃調查作業，適時研提相關前瞻及洞察意見，以協助維護我國整體資安環境，促進數位經濟發展。