出國報告(出國類別：其他)

2019 年金融檢查與稽核研修班

服務機關：臺灣銀行董事會稽核處
姓名職稱：黃素真　副處長
　　徐秋蓉　中級專員
派赴國家：新加坡
出國期間：108 年 9 月 1 日至 9 月 6 日
報告日期：108 年 10 月 28 日

摘　要

中華民國銀行公會與台灣金融研訓院本次特於新加坡舉辦第二十二屆「金融檢查與稽核研修班」，希望透過新加坡高度金融監理的經驗分享，提升台灣銀行業稽核品質管理、進而促進本國金融監理與稽核制度與國際接軌。

本活動從金融監理機關以及銀行經營管理決策角度，探討內部稽核如何從組織、管理、人才、流程與科技五大面向積極變革，以因應金融市場科技驅動、創新導向所帶來之新挑戰，並藉由透過機構考察形式，與新加坡金融管理局(Monetary Authority of Singapore, MAS)、跨國銀行(花旗銀行、渣打銀行、華僑銀行、星展銀行、大華銀行等)及國際知名會計師事務所(KPMG、PwC)等知名機構進行交流與學習，以締造創新與改變動能，帶領台灣內部稽核實務向國際標竿邁進。

目　次

壹、目的

為促進金融監理與稽核制度與國際接軌，並強化金融機構風險辨識、評估能力，使內部稽核資源更有效配置，中華民國銀行公會與台灣金融研訓院本次特於新加坡舉辦第二十二屆「金融檢查與稽核研修班」，希望透過以數據分析為基礎之風險評估與決策模式提升稽核品質管理，邀集在地資深金融專家共同探討以下重要議題：

★ 新加坡外資銀行法規監管科技之最新趨勢、應用與挑戰，金檢案例、科技創新與金融安全之平衡點。

★ 落實 Agile Management 提升內部稽核效率與品質。

★ 建構內部稽核人才未來發展藍圖，有效因應金融數位化對內稽所帶來之新挑戰。

★ 透過強化公司治理、內外關係人溝通與四道防線協作，提升內控環境總體品質與風險管理文化。

★ 新興數位科技崛起、金融服務流程與風險大為改觀，第三道防線如何為資安做好把關。

★ 應用數位科技，落實風險導向稽核，建構 Data Driven 之風險分析、監控模式及 RPA 導入等稽核之應用。

貳、行程

一、參訪行程

本次參訪期間為 108 年 9 月 1 日至 6 日，由中華民國銀行公會內部稽核委員會胡其相主任委員擔任副團長，率領中華民國銀行公會內部稽核委員會林偉賢副主任委員及中華民國銀行公會內部稽核委員會張麗珠諮詢委員，與台灣金融研訓院工作人員及銀行同業共 25 員，共計參訪六個機構，列表如下：

日期	參訪機構	討論議題	會面人員
Day 1 9/1(日) 下午		抵達新加坡	
Day 2 9/2(一) 上午	新加坡金融管理局	● 新加坡外資銀行法規最新監管趨勢 ● 近期外資銀行金檢案例分享 ● 主管機關對於銀行公司治理、風險管理、法令遵循與內部稽核之最新期待 ● 從監理角度談如何在科技創新與金融安全間尋求平衡點 ● 監管科技(Reg Tech)之最新趨勢、實際應用經驗分享與面對之挑戰	➢NEO Boon Sim, Director of Banking Department III (Division 2), MAS ➢CHONG Kok Leong, Deputy Director of Banking Department III (Division 2), MAS
Day 2 9/2(一) 下午	華僑銀行	法令遵循、管理、組織&文化、人才	➢Goh Chin Yee, Head, Group Audit ➢Patrick Chew, Group Risk Management
Day 3 9/3(二) 上午	星展銀行	Reimagining Internal Auditing through Agile and Data Analytics	主講者: Derrick Goh, Head of Group Audit

Day 3 9/3(二) 下午	渣打銀行	Audit Analytics	主講者：Colin Wan, Chief Operating Officer-Group Internal Audit
Day 4 9/4(三) 上午	大華銀行	Practical Internal Audit Approach to Cybersecurity	➢Adhi Narayan Ragupathi Executive Director, Head, Group Technology & Digitalisation Aduit
Day 4 9/4(三) 下午	花旗銀行	1.Internal Audit Methodology Overview 2.Internal Audit Innovation	➢Lo, Jiann, Chief Auditor ASEAN Cluster ➢Fu, Jasmine, Senior Vice President, QA IA
Day 5 9/5(四) 上午	KPMG	Technology enabling Internal Audit (Data Analytics)	主講者：Lem Chin Kok, Lead of Risk Consulting Business
Day 5 9/5(四) 下午	PwC	1. Leveraging technology to empower risk-based auditing 2. Risks and challenges in digital banking	➢Andrew Bronshtein, Director, ➢Kyra Mattar, Partner, Risk Assurance, PwC Singapore
Day 6 9/6(五) 上午	飯店	《小組心得分享》	
Day 6 9/6(五) 下午		返台	

二、參訪內容介紹

(一)參訪星展銀行

2019.09.03

- 參訪機構：星展銀行 (主講者: Derrick Goh/Head of Group Audit)
- 研討主題：Reimagining Internal Auditing through Agile and Data Analytics

1、內容概要

-工業 4.0 時代的內部稽核

-傳統稽核方法之轉變

-自動化及 AI 對於整體稽核程序之改變

-Cyber Security 之管理策略及架構

2、內容說明

(1)工業 4.0 時代的內部稽核

A.風險類型之演變

由於人工智慧(AI)、大數據、數位化、應用程式介面(API)、雲端儲存等新科技之運用，顯著提升處理交易的速度及資料量，金融機構已面臨使用新科技伴隨而來新的風險。此外金融機構內部系統與外部系統之互聯及整合日益增加，對金融機構產生更廣泛的風險。

B.審計委員會之期望

審計委員會及銀行管理階層期望內部稽核能對銀行所面對之風險提出具有前瞻性之看法，分析發現之內部控制弱點及其相關聯影響，並以提出解決方案為導向，提供銀行其專業建議。

(2)傳統稽核方法之轉變

針對傳統內部稽核的限制，如守舊心態、資訊落差、過時之方法論及工具，DBS 採用敏捷式稽核(Agile Audit)，以回應目前面臨較多變且複雜之環境。落實 Agile Audit，可以提升受查單位與內部稽核之協同合作，帶來即時及更新之資訊，廣泛且深入的運用資料分析及數據工具。因此，星展銀行推動內部稽核之三項改變：改變思考方式、改變工作方式及改變使用之工具，以確保內部稽核於目前及未來的金融環境可有效為銀行風險管理帶來貢獻。

A.改變思考方式

跳脫傳統上稽核人員被視為警察的印象，扭轉受查單位對內部稽核的逃避、敵視及拒絕態度，並改善利害關係人對內部稽核不情願的態度，鼓勵機構內部資訊的交換。

B.改變工作方式

星展銀行的 Agile Auditing 方法如下:個體及互動、回應改變、與客戶合作、

工作產品等，將可以化解不配合單位的限制、透過合作提升發現風險的能力、優先處理正確的風險提高稽核有效性、及時偵測及處理弱點。

C.改變使用工具

由以往使用紙質資料轉變為使用數位平台，整合宏觀的概況及細節資料。

(3)自動化及 AI 對於整體稽核程序之改變

延續長期以來與台灣金融同業之交流，星展銀行亦分享目前在稽核工作上使用自動化工具及 AI 的發展現況，除了對於受查單位風險分析自動化的開發進度外，另說明目前最新上線的工具:企業金融信用風險分析工具(PORTIA: Portfolio, Obligor, Transactional, Integrated Assessment)。PORTIA 係整合了銀行內部之 KYC 資訊、授信組合資訊、匯款活動、貿易融資及同業資訊等項目，可以從國家(地區)、集團客戶或單一授信戶之角度產出風險分析結果及警示資訊。PORTIA 使用原則導向的分析資料產出更有效的風險評估、提供主動的持續性監控與更敏銳的熱點辨識及異常測試、全面強化整合稽核程序品質。PORTIA 將可有效運用於風險導向稽核之年度稽核規劃、定期或不定期的監控或持續性稽核，以及稽核專案執行時之抽樣。

(4)DBS 表示其能如此改變，主要係獲得 CEO 的全力支持，首先由第三道防線做出令人驚豔的即時監控管理報表，使得業務部門(第一道防線)、風管部門(第二道防線)反過來分享其管理報表,因此 AI 及 Machine learning 的發展將促使即時偵測更提升為事先預測風險所在。

(5)Cyber Security 之管理策略及架構

為了因應現今內外部網路攻擊之威脅，星展銀行在 Cyber Security 之管理架構上，整合了第一道防線與第二道防線，以提升銀行於回應新興攻擊威脅之即時性，包含制定或修改防範網路攻擊相關政策及程序。星展銀行亦介紹了其防範網路攻擊之策略及程序，包含預測、延遲、預防、偵測及回應等實務作業。

(二)參訪渣打銀行

2019.09.03

- 參訪機構：渣打銀行新加坡分行

  (主講者：Colin Wan, Chief Operating Officer-Group Internal Audit)

- 研討主題：Audit Analytics

1、內容概要

由營運長 Colin Wan 引言說明渣打銀行導入數據分析模式(Analytics)之歷程、成功要素以及目前應用情形。

-數據分析法引入

-如何應對新制度導入之挑戰及幫助稽核員成功利用數據分析

-數據分析之應用情形

2、內容說明

(1)數據分析法引入

A.2015 年開始進行，最先以抽查樣本透過數據分析法進行者以 10%為目標，2019 年則計劃在未來兩年將數據分析法之查核比重提高至 70%。

B.培訓稽核員(Champion Program)，並允許稽核員共享資料庫。

(2)如何應對新制度導入之挑戰及幫助查核人員成功利用數據分析

A.人才

①除要會數據分析外，也要能了解風險，並具備稽核背景→找到對的人；

②解決辦法→由核心團隊(12 名)來幫助全球 550 名稽核員進行培訓(新加坡/中國/印度)，進而透過 Champion Program 培養 160 名學生，2018 年已有 58%的數據分析由該批學員完成。

B.數據

①挑戰在於數據蒐集，因為資料來源跨越 40 多個國家、1,000 個系統，故無法確保數據質量，另有很多國家的監管單位不願分享相關數據，如:韓國；

②解決辦法→自行設立數據庫，和各國監管單位購買數據(raw data)，實務上有 80%花在資料蒐集與建置。

C.改變心態

①稽核員及其他部門均有抗拒變化之心態；

②解決辦法→主動協助其他部門，分享數據方法之效益；提早讓業務單位熟悉新系統，並得以提早自我檢測可能缺失；腦力激盪，了解數據意義所在；納入 KPI 中。

(3)數據分析應用情形

A.現階段透過數據分析，渣打已應用在信用卡業務、分行審查、AML、MUREX 系統(檢核內部員工或交易員間是否有不當聯繫或行為)及判定各區域之風險等級

B.未來將應用在企金領域之信用風險分析(例:早期預警)及分行分析(透過分行風險評估預判全球各分行風險程度)。

(4)Q&A 摘要

A.如何做好 predict？

主要分為 on-site 及 off-site 兩類，其中 on-site 係透過檢視資料庫中訊息如財報及各類營運指標，或是 trade finance 之每月交易筆數或金額是否發生異常。off-site 則係透過外部產業或重大負面新聞逐筆檢視，先期確認其對客戶之影響並採行必要措施，目前臺灣同業普遍採用之 AML 案件管理系統即屬 off-site 應用。

B.對於稽核員之要求？

專業要求上，至少在資料分析(data)、稽核(audit)或風險(risk)三項專業背景中具備其中兩項。

C.資料品質對機器學習(Machine Learning)之影響？

機器學習對於前端資料彙集/整理及資料品質要求相當高，若資料筆數不足，則須透過搭配規則設定(rule based)做為輔助工具，例如財務數據及外部產業新聞。

D.數據分析稽核員之養成？

初期著重小規模團隊，組成精英及種子教官→大規模培訓，規劃學院授課→心態改變，透過 hackathon、導入 KPI 及協助稽核員完成數據分析審查。

(三)參訪花旗銀行

2019.09.04

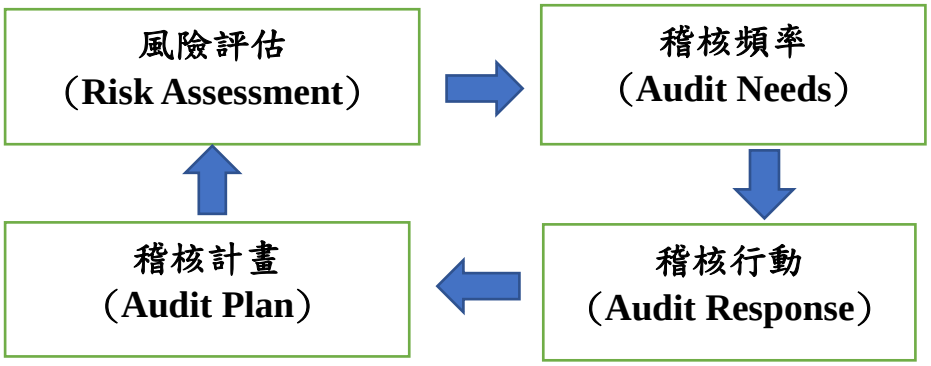
- 參訪機構：花旗銀行新加坡分行
  (主講者：Lo, Jiann, Chief Auditor ASEAN Cluster／Fu, Jasmine, Senior Vice President)
- 研討主題：
  1.Internal Audit Methodology Overview
  2.Internal Audit Innovation

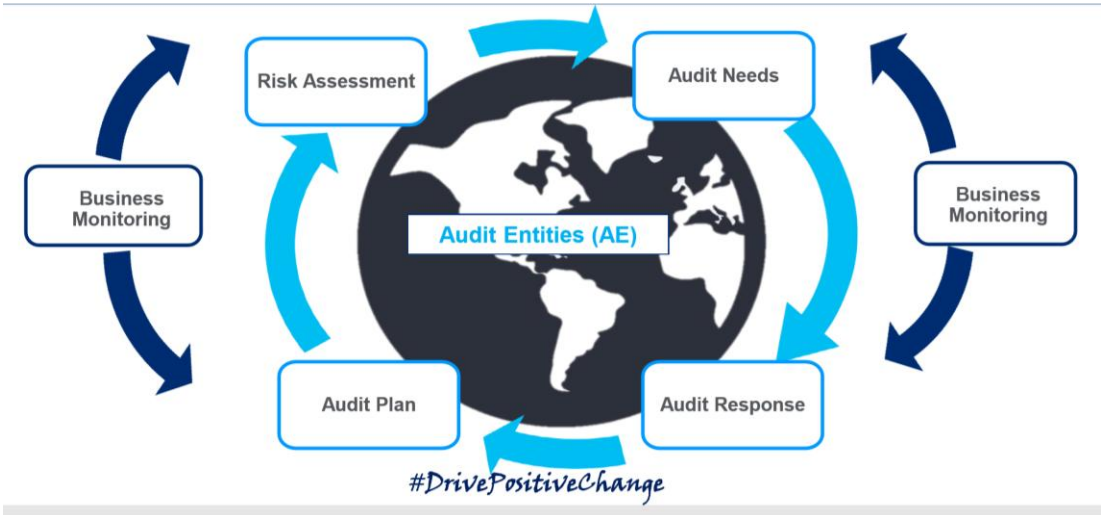
1、內容概要

本課程係由參訪銀行說明該行以風險為導向之稽核架構，並就實務運用面講述該行作業模式，包括風險評估、稽核程序及報告等議題，此外亦就該行在內部稽核創新之應用實例，現場實地操作系統並有詳細說明。

2、內容說明

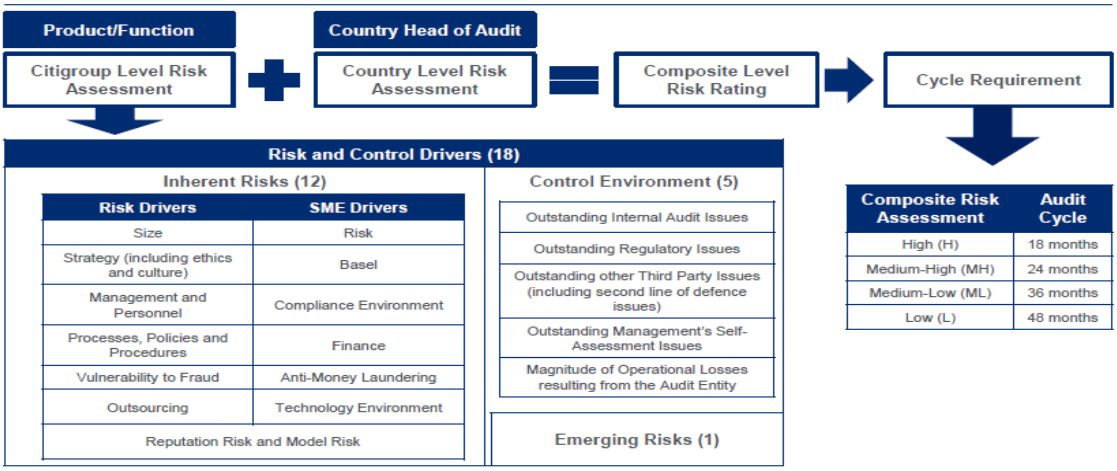
(1)風險導向稽核架構(Framework)





(2)風險評估程序

A.首先稽核團隊應就組織架構圖、對應之資料庫及管理功能來決定受查主體，大致可歸類為部門別(Business Unit)、功能別(Function)、產品別(Product)、程序別(Process)等。



Reputation, Model and Data Management risks are not standalone risk drivers. The implication of the existence of these risks is assessed during scoring of each of the 12 Risk and SME drivers, as applicable.

B.其後稽核團隊將就受查主體所訂 12 項固有風險，考量其風險程度後由低至高分別給予 0～4 分。

Risk Drivers	Size	Strategy (including Ethics and Culture)	Management and Personnel
	Processes, Policies and Procedures	Vulnerability to Fraud	Outsourcing
COE Drivers	Risk	Compliance Environment	AML
	Finance	Basel	Technology Environment

Each of the Risk and CoE Drivers is scored using a scale of 0 to 4.

Score	Description
0	Not Applicable
1	Minor
2	Moderate
3	Large
4	Substantial

C.再衡量 5 項控制因子所具有效性程度後，自低而高分別給予 1～4 分之抵減。

Impact of Outstanding Internal Audit Issues to the entity
Impact of Outstanding Regulatory Issues to the entity
Impact of Outstanding other Third Party Issues to the entity
Impact of Outstanding Management's Self-Assessment issues to the entity
Magnitude of Operational losses resulting from the entity

Each of Measurement of Control is scored using a scale of 1 to 4.

Score	Description
1	Not Applicable or Minor
2	Moderate
3	Large
4	Substantial

D.再評估是否具有新增風險(Emerging Risk)而以 0 或 1 分調整後，依總分級距

初評受查主體風險高、中高、中低、低等 4 級。

Citigroup Risk Score	Citigroup Level Risk Assessment
0.60 to 1.25	High
0.50 to 0.59	Medium-High
0.40 to 0.49	Medium-Low
0.25 to 0.39	Low

E.風險初評後，稽核長(Country Head of Audit)將考量所屬地區是否具國家風險後酌予調整，並確認最終風險等級。

F.最終風險等級分有高、中高、中低、低等四級，其對應之稽核頻率分別為 1.5 年、2 年、3 年、4 年。(此項與國內法規相較極具彈性，應可供主管機關參考)

Composite Risk Assessment	Audit Cycle
High	audited within 18 months
Medium-High	audited within 24 months
Medium-Low	audited within 36 months
Low	audited within 48 months

(3)稽核執行 (Lifecycle)

A.查核計畫(Planning)

①與受查單位及相關部門人員面對面溝通，並確認固有風險之管控措施有效的被執行，另風險胃納尚為可接受水準內。

②對於相關作業程序所建立之重要管控點，確認均足以提供書面文件，並進行有效性評估(DEA, Design Effectiveness Assessment)。

③備妥查核計畫備忘錄(APM, Audit planning Memorandum)及風險控管矩陣圖(RCM, Risk control Matrix)。

B.實地查核作業 (Fieldwork)

①對於重要管控作業進行有效性測試 (OET, Operational Effectiveness Testing)。

②查核如有發現缺失，應與相關業務主管討論及確認，並應確實找出所有缺失主要發生原因 (Root Cause)，此外亦應重視第二道防線管理部門之意見。

③對於查核缺失應與管理層確認可行及有效之改善方案，並就完成所需時間訂定預計完成日。

C.查核報告(Reporting)

①報告內容格式涵蓋 5C，包括：可能風險(Concern)、發生原因(Cause)、影響後果(Consequence)、事實情形(Context)及改善承諾(Commitment)。

②查核報告就受查主體之風險管控程序設計及執行，依其有效性程度給予評等，分別為足夠(Sufficient Assurance)、待改善(Room for Improvement)、有限(Limited Assurance)及不足(Insufficient Assurance)等四類。

D.該銀行對於上述三項查核程序所訂期間合計為 90 日曆天，其中查核計畫及實地查核作業各佔 40%，查核報告撰寫佔 20%。

(4)缺失改善追蹤及管控

A.內部稽核所提意見經管理階層確認並承諾改善後，依風險程度分為 Level 1～5，其中 Level 1、2 屬於嚴重程度者，應於 30 天期限內完成，Level 3 為 90 天內，其餘 Level 4、5 則由受查單位自行改善。

B.對於外部查核意見，營業單位應於 90 天之改善期間內完成，並由稽核單位進行確認。

(5)持續性稽核(Continuous Auditing)

A.內部稽核對於各項業務仍應持續進行監控(Business Monitoring)以及時了解風險和控制環境的變化，並評估潛在新風險及對業務可能之影響，進而能迅速反應或修正原有之稽核計劃。

B.執行業務監控活動將於每季記錄結果並編製摘要(Business Monitoring Quarterly Summary)後，更新受查主體之風險評估及檢討原有稽核計劃並研擬修訂之。

C.持續性稽核為持續多年之內部稽核策略規劃，針對選定之主要控制點，藉由循環性及經常性增加交易主體抽測樣本，以強化稽核品質之確信度。

(6)稽核監管報告(Governance Reporting)

A.內部稽核應向審計委員會及其他相關業務部門提供完整的季度評估報告，內

容涵括 23 項主要風險(PR, Principal Risk)及 9 項風險管理框架(RGF, Risk Governance Framework)。

B.23 項主要風險(PR)代表花旗集團共同面對之實際或潛在風險缺口，其中每項主要風險因子均被分配一個負責單位(owner)，該單位可能為第一線營業部門或獨立風險管理部門。內部稽核季度報告對於控制措施有效性意見，將會提供予集團所有的主要風險負責單位。

C.9 項風險管理框架(RGF)涵蓋了信用風險、利率風險、市場風險、法遵風險、流動性風險、作業風險、策略風險、信譽風險等八項重點風險項目以及一項道德文化風險，而主要風險報告為評估內容之來源，亦對主要控制環境評估結果。對於第一線營業部門或獨立風險管理部門未合規案例，報告亦將加強揭露以支持內部稽核所做之結論。另內部稽核還會根據季度評估結果以及整體風險管理框架，每年提供年度匯總報告。

(7) 流程機器人(Robotics)及機器學習(Machine Learning)之運用

A. 內部稽核程序之執行藉由資訊管理系統(AIMS, Audit Information Management System)提供支援，該系統具有完全整合、Web 網路運用、全球稽核平台適用等特性，提供做為風險評估、訂定年度計劃、稽核執行及主要缺失管控流程使用。

B.花旗集團內部稽核創新(Audit Innovation)

①建立大數據資料庫及風險管控點，藉由自動化方式測試全數母體資料，可避免抽樣誤差，提升查核效率及確信度。

②利用過去及現有資料之規則性，分析並建立系統預測功能，以協助稽核人員發現新風險。

③大幅節省稽核人員查核資料時間，因而可更關注於風險分析及與受查單位之溝通上。

④對於受查單位可即時發現缺失及其發生原因，並儘早建立強化管控機制。

(四)參訪 KPMG

2019.09.05

- 參訪機構：KPMG (主講者：Lem Chin Kok/亞太法證部門主管，Lead of Risk Consulting Business)

- 研討主題：Technology enabling Internal Audit (Data Analytics)

1、內容概要

(1)第一部份主要說明就其在主導風險顧問業務上之相關議題，第二部份則透過其調查報告說明為何 KPMG 特別強調電腦安全重要性。

(2)AI 快速發展的影響

A.AI 貢獻雖大，包括強大邏輯運算及人工替代功能→但該領域其實尚未被完全理解。

B.故對主管機關而言，AI 不可控性成為其關注點→如何管理 AI 運用之相關風險。

C.在決策上 AI 更具優越性→必須有效管理這些模型。

2、內容說明

(1)KPMG 發佈 2019 年全球銀行詐欺調查報告

A.統計有五項風險指標，電腦/資料外洩係美洲、歐洲/中東/非洲及亞太區所共同面臨最大的挑戰，第二至第五項指標與科技相關(digital and technology related)，如快速支付(FPS)、虛擬貨幣、開放銀行、支付服務指令、社交工程、數位管道演變等：

①電腦/資料外洩:數位罪犯藉由資料外洩取得被害者的個人資料，並於詐騙中使用被害者個人資料獲取信任或接收他們的帳戶。數位轉型同時改變詐欺型態，銀行須快速更新詐欺風險預防體系、提升資訊科技、尋找下一代預防/偵測方案

②數位平台及快速支付：調查中有 78%的受訪者表示表示有 25%的商品及服務是透過數位平台推出。由於數位銀行的放寬及無現金交易方式等行為模式改變，全球出現關閉分行的趨勢。

-減少銀行及顧客的面對面溝通，因組織罪犯及詐騙犯運用該方式進行跨境詐騙。

-提供豐富的客戶數位行為資料，有利於發現潛在支付詐欺。因 pull payment 對增加的詐欺必須要有警覺。特別是考慮到更快的付款速度，預計回收率會更低。

-銀行透過即時欺詐預防和偵測工具，並對高風險的交易施加交易限

額及授權機制。

B.數據分析法與詐欺監控

①監控系統-一種反饋機制，確保系統運作及交易處理依規進行，如此可降低詐欺風險(預防及嚇阻)、強化管理有效性、確保法令遵循、展現妥善的治理及自動回報；但也有其挑戰，如確認監控項目、結合數據分析及決定欲採用之技術和軟體(無一體適用的情形)。

②機器學習之導入

KPMG 自九年前開始導入機器學習概念，取代傳統 Rule based Analysis，重新訓練稽核員以因應。

差異比較：

Rule based Analysis	AI & 機器學習
須透過專業知識發掘特定因子	從數據中學習，並主動發現其中異常數據，而無須事先輸入或標定特定因子
結論係基於事先考量的因素	節省人力檢視和更快的分析
有效性端賴分析師的專業知識	適用於金融犯罪偵測
適用於重覆性、異常時段或具備相同特徵的交易(相同帳號及相同地址)檢視	監督式(Supervised) 機器學習 VS 非監督式(Unsupervised)機器學習

③Supervised 機器學習

從一組“correct answer”資料中進行學習，以找出類似問題的答案，如同一名學生藉由考古題來學習；例如:模擬交易監控警示的 level one review，機器學習可以藉由學習過往人為錯誤判斷的警示案例來決定新警示案件錯誤的機率。(例如:辨識信用卡交易詐欺)

④Un-supervised 機器學習可以更接近所謂的真正 AI，因為電腦可學習識別複雜的流程和模式，其過程中無須人工提供指導。此種學習另一功能係執行分類，例如:客戶分類(Group different customers)，其未事先決定客戶類別，而是依客戶的行為及個人資料自動進行分類，向客戶推薦產品。

C.KPMG 提及過去與客戶討論數據分析系統導入時經常碰到的謬誤

①客戶認為其只需要一個基本現成的模型(錯誤觀念)，然而數據分析模型是一個持續學習及改善的流程，系統建置完成後仍要不斷透過人工監控，

以確保系統啟用後常保有效。

②客戶認為其只要雇用資料分析師就可解決所有數據分析問題(錯誤觀念)，但人力有其限制；且數據分析模型的成功導入有賴管理團隊是否可以有效確認問題和方向(correct dimensions)，並持續改善模型。

D.結論

①新加坡銀行業者在 AI/Machine Learning 之應用上除業務端外，已普遍使用在信用風險分析、法遵及內部控制等方面。而對主管機關來說因關注 AI 的複雜度及不可控性，故其相對強調 AI 管理之風險(業者必須要有對應之框架及政策)。

②不同於傳統 Rule based Analysis，AI/Machine Learning 可在人力節省、正確性、更多面向之風險監控上幫助銀行執行內部控制，但必須輔以持續修正模型以確保有效性。同時銀行須給予足夠誘因應對新科技之導入。

(2)網路安全

A.根據 KPMG 的「Singapore CEO Outlook 2018」報告，92%的 CEO 認為其數位轉型計劃將在接下來三年逐步展現成果，有 42%的公司則認為網路安全是未來公司成長的最大威脅，另有 33%的 CEO 不確定網路威脅的型態。

B.KPMG 對於 2019 年網路安全趨勢之預測包含：

①金融機構仍為網路罪犯之主要攻擊對象；

②相關法令仍缺乏共識(因涉及不同國家和當地規範)；

③假新聞層出不窮；

④網路罪犯會著重攻擊雲端及物聯網；

⑤勒索軟體及加密貨幣挖礦；

⑥隱私與透明度，但許多機構將收到第一次罰款；

⑦網路罪犯及企業端同時採用 AI 和機器學習；

⑧供應網絡風險增加；

⑨社交工程更富創意；

⑩敏捷概念的運用。

C.對企業資安產生威脅的路徑主要有：惡意/勒索軟體、網路釣魚、中間人攻擊(man in the middle)、鍵盤及螢幕側錄、魚叉式網路釣魚及內部威脅等六

種型態，目標則由竊取身分或服務轉向破壞商譽、竊取知識產權、財務資訊或策略等；為此，其因應策略由過去的預防(prevention)轉為偵測(detection)和回應。

D.內部稽核在網路安全所扮演之角色

防線	角色及責任
第一道 業務及 IT 功能	-業務執行應以 risk-informed 為基礎； -確認可接受的風險程度； -採行適當之風險抵減作為。
第二道 IT 風險管理功能	-建立風險治理，包括基準、政策及標準； -採行風險抵減工具、程序及監控; -監督風險
第三道 內部稽核 (有鑑於最近發生的重大網絡攻擊、資料損失及法規要求，內部稽核必須了解網絡風險並準備處理審計委員會和董事會提出的問題和疑慮。)	-獨立判斷各流程之有效性； -向董事會報告風險管理之有效性； -在網路安全相關風險方面做到符合主管機關規範及資訊揭露要求。

(五)參訪 PwC

2019.09.05

- 參訪機構：PwC (主講者：Andrew Bronshtein, Director, Risk Assurance, PwC Singapore; Kyra Mattar, Partner, Risk Assurance, PwC Singapore)
- 研討主題：
  1. Leveraging technology to empower risk-based auditing
  2. Risks and challenges in digital banking

1、內容概要

數位革命，引發大量的網路風險。

2、內容說明

(1)安全威脅面

A.網路安全一般的威脅：

近年來主要面臨的網路威脅有哪些：網路斷線導致營運中斷、網路服務業者停止

提供服務，例如：

①由信任的第三方的 app 中感染了勒索病毒致影響組織營運：

2017 年 5 月，一個名為“**WanaCryptor**”的惡意軟體突襲 **NHS**(英國國民健保署)。勒索軟體導致英格蘭和蘇格蘭的醫院營運異常，影響救護車派遣與例行操演，而患者資料被鎖定除非受感染的電腦交付贖金得以解鎖。

②DDoS(Distributed Denial of Service)阻斷服務攻擊，是一種網路攻擊手法，即攻擊者造成網站伺服器充斥大量要求回覆的訊息，消耗網路頻寬或系統資源，導致網路或系統不勝負荷，以至於癱瘓而無法提供正常服務，其目的在於妨礙正常使用者使用服務。

B.網路安全金融服務的威脅：

連線中斷製造市場巨幅動盪及商譽損失：

例如：2012 年 RBS 遭受 DDOS 駭進銀行服務系統，英國金融監理機關，針對銀行資訊安全問題處以重罰五千六百萬英鎊的罰款。

RBS、NayWest 以及 Ulstet 的客戶於 2012 年 6 月，因為銀行執行的軟體更新發生技術上問題，在使用服務(包含線上服務)時，遇到存款結餘及付款執行的正確性問題。針對此項資訊上的問題，英國審慎管理局(PRA)亦罕見地再以違反「金融機構應以適當風險管理系統以及合理之注意義務，有效管控其服務」規定之理由，另對該銀行處以一千四百萬英鎊的罰款。這是首次 2 個主管機關對於銀行未能有效辨識及管理其已暴露之資訊風險共同處罰之案例。

C.竊取個人可識別資訊騙取他人財產：

①美國第三大消費者信用評級機構 Equifax 在 2017 年被駭客入侵，導致超過 1.4 億消費者的個資外洩，其實美國政府曾在事發前警告 Equifax 內部系統有安全漏洞，但 Equifax 卻未有效修補。

②英國航空(British Airways)2018 年發生個資外洩事件，因違反歐盟個資法 GDPR，遭英國主管機關重罰 1.83 億英鎊(約 64 億元台幣)。英航因網站和行動 app 遭駭，導致透過 ba.com 網站連上公司系統的用戶都被導向假網站，並遭攻擊者取得用戶資訊，估計將近 50 萬名用戶受害。主管機關英國資訊專員辦公室(Information Commissioner's Office，ICO)調查後認為，這起事件出於英航的安全管理不佳，致使多種資訊包括信用卡、旅行訂位代號及個人姓名、

住家地址等個人資料外洩。

③2018 年萬豪國際旗下連鎖飯店喜達屋的訂房資料庫遭入侵，導致全球近 3.4 億名住客資料外洩，英國資訊專員辦公室(ICO)以違反 GDPR 為由，計畫判罰該集團將近台幣 40 億元的罰金。

D.駭客侵入電腦支付服務系統，竊取資產造成損失：Malware 惡意軟體攻擊 SWIFT 系統竊取資金，SWIFT 系統遭駭銀行清單：

* 2013 年索納利銀行

* 2015 年厄瓜多銀行、菲律賓銀行、越南先鋒銀行

* 2016 年孟加拉中央銀行、烏克蘭多家銀行

* 2018 年台灣遠東商業銀行

(2)客戶的情感面

A.調查發現，83%的受訪者在使用網路上的金融 app 時，很重視其個人隱私。

B.67%的受訪者則認為，在網路上分享個人資料時，網路安全是他們主要考量之一。

C.顧客不願意使用數位方式執行交易，其中一個主因是，電腦系統是否會故障及可信賴性考量。

D.當金融服務的系統供應商能確保客戶資料安全，銀行當然毫無疑問的投入大量資金，發展金融數位科技。

E.若提供金融服務者對網路安全及法令遵循不重視，將失去顧客的信任。

(3)數位銀行的主要挑戰

A.需遵循外部監理機構要求:

面對日新月異的創新及科技進步，金融及網路的版圖與其風險也快速的進化。數位銀行必須確保能跟上並遵循新加坡金融管理局(MAS)的法令及規範。

B.建立長久的數位信任:

客戶所關心的個資隱私，安全及系統的可信賴性，數位銀行將建構自己的數位信賴優勢以符合顧客期待。

C.建立顧客信心:

數位銀行是市場的新參與者，也將面臨建立新品牌及客戶及主要管理階層信賴的難題。

(4) 2018 年新加坡發生有史以來最大規模的網路攻擊案件，負責網路維安的技術人員欠缺安全意識，未及時採取防範因應措施，結果造成跨國網路攻擊得逞。

事件情形：

A.2018 年 6 月 11 日~26 日，IT 管理者注意到在 SingHealth 的系統資料庫檢測到異常活動。新加坡保健服務集團(SingHealth)2018 年 7 月遭網路攻擊，總理李顯龍(Lee Hsien Loong)病歷遭駭，駭客主要針對李顯龍個資與門診就醫紀錄，以及其他患者資料。網路攻擊雖有跡可循，但未採取恰當因應行動，維安人員缺乏危機意識，未能及時應對。

B.這次的網路攻擊者技術高超、駭客手法老練、潛伏 3 個月，網路釣魚採橫向移動模式，以竊取更多的帳戶，其中包含管理者的領域。新加坡網路防禦並非牢不可破，仍難以避免高端網路威脅入侵。

C.根據新加坡先前調查，駭客網攻是經過精密策劃，侵入新保集團的電腦系統，攻擊新保集團數據資料庫中存放的個資，而入侵的駭客不斷試圖尋找有關李顯龍的紀錄，因此認定李顯龍是這次駭客網路攻擊的主要目標。

D.新保集團數據資料庫遭網路攻擊，駭客入侵系統，從 2018 年 6 月 27 日到 7 月 4 日竊取約 150 萬名病患個資。這些資料包括患者姓名、身分證號碼、地址、出生年月日。16 萬人的開藥紀錄也被竊取；而至於遭竊取的患者資料是從 2015 年 5 月 1 日到去年 7 月初赴新保集團旗下診所問診的病患。新加坡政府成立獨立調查委員會調查。

E.根據調查報告指出，網路管理員在 2018 年 6 月就注意到有 1 次未經授權登錄新保集團的紀錄，不過駭客在這之後持續非法登錄新保集團的伺服器，時間長達 11 個月之久，駭客利用安全性較差的 Citrix 伺服器進行攻擊，事實上，管理員應可在上頭啟用雙重身份驗證，但相關人員並沒有這樣做。更糟的是，負責管理病患資料的新加坡健康資訊系統中心 IHIS(Integrated Health Information Systems)曾被警告存在安全漏洞，包含密碼不完整、跟不健全的網路隔離系統。儘管之後採取了補救措施，但調查報告指出，補救之後仍存有安全漏洞，使駭客有機可乘。

F.根據駭客攻擊的時間顯示，IHIS 還有故意延遲有關網路安全漏洞報告的情況。

參、心得與建議

● 學習心得內容

[現況分析與心得]

在現今過多銀行、過度競爭的金融環境下，國內銀行多以業務為導向，未投入太多資源於內部稽核及內部控制，以致內稽內控的思維、技術及作業系統均相對落後於國外金融機構。近年來主管機關雖積極推動風險導向內部稽核制度，希冀藉由稽核資源的有效配置，聚焦於重要風險並加強查核深度，以提升內部稽核執行效益，惟受限於人力與物力，恐非短時間可達到理想目標。

隨著時代科技的進步，在 IT、大數據、數位資訊、雲端設備的大量使用下，交易速度、交易量迅速成長，加上系統間的交叉連結與運用，均加劇銀行曝險。為因應時代改變，內部稽核應跳脫傳統稽核模式，改變以往警察抓弊的心態，拋棄資訊落後及過時的稽核方法與工具，取而代之的是改變思維、改變使用的工具、改變工作方法，除強化本身發現風險的能力外，並藉由風險的分析、著重重要風險，以先進的查核工具與方法，作有效率的查核；並進一步的與第一、二道防線合作，建立資源共享平台，以達成預測風險、有效控管風險及避免風險發生等目標。

另為達成有效的稽核目標，金融業應強化資安風險的稽核效率，並以下述四個面向強化資安風險查核：

一、稽核人員應具備資安技能與知識：熟悉法規規定，洞悉各種新攻擊技術，具備偵測資安風險的能力，面對資安風險威脅時，能作有效的控管，並藉由外部稽核的測試，以確保控管的有效性。

二、風險評估：電腦資訊網路設備及付款裝置設備等面臨資安威脅、當地及海外對資安之要求、資安破壞其衝擊分析及持續營業計畫、危機處理計畫等。

三、建立良好資安組織架構：涵蓋系統、資產等資安風險辨識能力，以有效的防衛風險；偵測風險事件、因應策略及恢復作業計畫等。

四、資料分析：運用資訊系統留存軌跡進行資料分析，掌控銀行所面臨的風險與威脅；瞭解各控管點所面臨風險，作有效的監控並訂定持續性查核與風險評估的控制環境，俾利持續性監理。

[國際經驗借鏡]

透過本次參訪交流，茲就以下觀念認為可作為台灣金融同業之借鏡：

一、本國金融機構之建構數位化轉型

在與渣打銀行座談中提到其過往在導入數據分析法時的歷程，提到分享數據分析能成功有 3 大要素，而這 3 大要素分別為人才、數據及改變。

(一)在人才方面特別提到大量的資料須靠優秀的人才相互合作才能組成成功的團隊，以建立可靠的數據資料庫及分析方法，且能彼此有良好的互動來持續討論並檢視數據是有效。

(二)在數據方面則強調建立數據資料庫及利用數據分析工具進行分析，重點包括確認哪些數據是有效的，並了解可從哪些跨部門的平台取得數據、訂定數據存取及保護數據的管理政策。

(三)最重要者在改變人員心態，必須從管理階層的轉變來帶動稽核人員對工作型態改變的認知，並由資深稽核人員帶領，以群體協作及腦力激盪的方式尋找問題，並加以討論問題的所在風險，亦可以利用 Scorecard 及 KPI 來轉變以風險為本的查核結果。

二、稽核觀念的轉變

為因應金融環境因新興科技崛起所產生的變化及挑戰，星展銀行從內部稽核觀念上的轉變、工作型態的轉換及自動化和數據分析工具的經驗，提供了傳統內部稽核轉型為敏捷性稽核的方法。

(一)首先為稽核人員心態要徹底改變，即稽核的角色要從維安思惟轉變成與第一及第二道防線成為相互合作夥伴關係的協作思維，摒除過往只擔任偵錯且對立的角色。

(二)第二為改變工作方式，從與第一及第二道防線相互討論當中，可以集思廣益發現控制流程有哪些地方需要加強或有尚未被發現的風險，以提升發現風險的能力，並以評估風險優先順序來提升稽核的效益。

(三)第三為改變使用的工具，從只關注過去所發生之交易或事件去執行合規性之稽核(過時的方法和工具)，轉變為利用數位工具進行數據分析，並從自動化系統分析評估出首要風險、次要風險等風險排序，並依風險評估結果做稽核計畫，透過資訊科技的分析技術將可有效提升稽核效益。

(四)因此，內部稽核面對這資訊爆炸的大數據時代，若不懂得如何從各式數據中

取得有用的資訊，並運用適當的分析方法檢視數據，「稽核」這個角色，將很難為銀行創造出更高的價值，所以內部稽核應要有隨時面臨轉型的準備。

三、重視網路安全，特別是面對不斷演化的攻擊型態，應更加著重相關風險的偵測，而非被動預防。

(一)KPMG 對 2019 年全球銀行業欺詐調查結果分析，全球銀行在減少欺詐風險方面面臨的最大挑戰，主要在網路和資料洩露、快速支付及不斷發展的數位通道(Evolving digital channels)，KPMG 分享在防堵網路詐欺解決的方法為運用 AI(artificial intelligence)監控欺詐流程：積極主動尋找並分析欺詐和不當行為的案例(Client's Need)→進行全面性深入分析(Deep Dive)→識別有用的數據納入分析(IDENTIFY)→每天將數據進行分析檢視並將產出異常報告(Monitor)→定期/週期性檢視數據及分析以確保資料可用性(Refine)。

(二)在 KPMG 分享的過程中體認到 AI 正在改變這個產業的遊戲規則，我們應該要改變職能，培養具創造力、能溝通、非定型化能力並要有對 AI 及數位技術的活用能力，以維持競爭力，並提升職能。

四、預測性稽核

對內部稽核的未來趨勢方面，國際性銀行將從目前利用數據分析法進行持續性的稽核，進而提升為預測性的稽核。此發展方向對台灣金融機構才剛開始導入風險導向的查核制度(RBA)來說，已與國際化金融機構對稽核方法思考方向已有不小的差距，因此如何加速與國際接軌，亦是本國銀行及主管機關應關注的議題。

五、內部稽核單位面對數位轉型風潮下，日新月異的科技，應思考內稽人員是否有能力掌握下列事項？

(一)委外業務的安全規格是否規範清楚？招標過程很難對廠商資安投入進行衡量？資安是否落實？

(二)既有的資安防護設備，是否能有效阻擋威脅？

(三)防火牆被入侵後，能否阻擋機敏資料外洩？

(四)當惡意程式或連結被開啟後，是否有足夠偵測及反制能力？

(五)當惡意程式在內部網路滲透或橫向感染其它主機時，是否引起警覺？

(六)當機敏資料外洩時，是否被阻擋？

六、PwC 對 2018 年全球資訊安全調查報告指出，全球有 44%企業沒有完整資安策略、

48%企業缺乏員工資安意識訓練計畫、54%企業缺乏事故緊急應變計畫。網路攻擊情況嚴重，台灣企業界資安危機意識待提升，金融業更應加強資安危機意識。

- **建議**

一、稽核人員專業知識及教育訓練，應增加新科技及其所衍生之風險相關內容，並包含對於各國重要金融監理法規。此類課程師資及內容之準備，較不易由各銀行自行執行，因此建議台灣金融研訓院、銀行公會或主管機關可就金融機構內部控制及內部稽核持續性訓練之需求，提供業者相關之協助。

二、加強機器學習銀行業務功能：透過機器學習，將銀行產品規格化與一致化，如貸款審核、信用卡審核、存款開戶等。同時對內部稽核之風險導向查核及場外監控，經由機器學習及分析，能隨時因環境變化或組織異動而調整風險評估模式。

三、主管機關對各銀行間應有差異管理：以風險導向原則功能而言，對內控功能較佳之銀行，其監理情形應有差異，如對某一業務(或產品)或專案之清查，不應該全台灣之銀行業一體適用，應有分級管理。

四、主管機關與銀行業者間之信任：新加坡金融管理局(MAS)與當地銀行業者能充分信任與合作，互創雙贏。

肆、活動照片

20190902 上午新加坡金管局(MAS)

20190902 下午華僑銀行(OCBC)

20190903 上午星展銀行(DBS)

20190903 下午渣打銀行(Standard Chartered Bank)

20190904 上午大華銀行(UOB)

20190904 下午花旗銀行(CITI BANK)

20190905 上午 KPMG

20190905 下午 PwC