出國報告（出國類別：第五類-其他）

參加 2017 年金融檢查與稽核研修班

服務機關：臺灣銀行股份有限公司 董事會稽核處
姓名職稱：何 佳 妍　稽核
派赴國家：香港
出國期間：106 年 10 月 15 日至 106 年 10 月 20 日
報告日期：106 年 12 月 22 日

摘　　要

本次參加中華民國銀行公會（主辦單位）及金融研訓院（執行單位）在香港舉辦之第二十屆「金融檢查與稽核研修班」，研修期間為 106 年 10 月 15 日至 10 月 20 日，本活動透過機構考察形式，與香港金融管理局及具代表性之跨國銀行集團高階稽核主管進行交流。

本次活動研討議題主要為主管機關於推動之「風險導向內部稽核制度」與「銀行內部控制三道防線」以全面強化銀行風險治理效能，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、流程、專業 Know How 與人才四大面向積極變革，以因應金融市場國際化與數位化所帶來之新挑戰。

目　　次

頁次

壹、目　的

為促進金融監理與稽核制度與國際接軌，「金融檢查與稽核研修班」自 1998 年開始每年輪流於國內外金融重鎮舉辦，迄今已歷二十屆。本活動每年邀請臺灣及海外主管機關與業界優秀專家與會分享金融監理與檢查制度發展趨勢、以及強化內部稽核功能之具體方針，成為連結臺灣與海外金融監理稽核專業領域之指標性知識交流平台。

本次活動於 106 年 10 月 15 日至 10 月 20 日於香港舉行，透過機構考察形式，與香港當地金融監理機關及具代表性之跨國銀行集團高階稽核主管進行交流，締造創新與改變動能，期藉由雙邊經驗分享與反饋，加速臺灣金融監理與內部稽核實務向國際標竿邁進。

本次活動研討主題聚焦主管機關於推動之「風險導向內部稽核制度」與「銀行內部控制三道防線」以全面強化銀行風險治理效能，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、流程、專業 Know How 與人才四大面向積極變革，以因應金融市場國際化與數位化所帶來之新挑戰。

貳、行　程

一、參訪行程

日期	行程
10 月 15 日	下午抵達香港
10 月 16 日	香港金融管理局（HKMA）、中國銀行香港
10 月 17 日	東亞銀行、渣打銀行
10 月 18 日	星展銀行、PwC（HK）
10 月 19 日	香港上海匯豐銀行
10 月 20 日	小組心得分享、下午返臺

二、參訪內容簡介

(一) 銀行業面對的最新挑戰及從監理觀點談內稽應對之道

1.科技風險

香港金融管理局(以下簡稱 HKMA)為服務社會、為客戶帶來更好的體驗，鼓勵銀行使用金融科技，以風險為本和科技中立為監管原則，在方便與安全之間取得

平衡，落實「以客為本」及「普及金融」的理念。

HKMA 提出七項措施推動智慧銀行發展：(1)推出「快速支付系統」，創造一個高效的零售支付系統滿足 P2P(person-to-person)和 P2B(person-to-business)的連接，且在企業、銀行第三方支付之間完全連接所有付款參與者；(2)金融科技監管沙盒升級版 2.0，將現有的 Fintech 監理沙盒升級至沙盒 2.0，除現行銀行業界可提出創新金融科技外，將建立一個 Fintech 監督聊天室，在項目開發的早期階段與利益相關方進行溝通，科技公司為可直接進入沙盒，通過尋求來自聊天室的反饋來測試他們的創新，並提出改善，以縮短科技創新計畫從概念到成熟的時間；(3)引入虛擬銀行，鑒於香港地區地產昂貴，虛擬銀行可降低業者成本；虛擬銀行可在不同的服務模式下運作，有助於促進金融包容，亦會為香港 Fintech 的應用提供更多動力，並為行動/數位銀行提供新的客戶體驗；(4)推出「銀行易」，與銀行溝通，研究有哪些可能窒礙科技應用的監管要求或程序，並作出適當的修訂或簡化，如簡化低風險戶口的開戶程序；(5)促進開放應用程式介面(開放 API)，在銀行的背景下，Open API 是指一組公開的編碼，使得認可的第三方服務提供商，在適當的情況下，允許客戶與 IT 系統進行連接，並進行數據交換；開放 API 可用於許多用途，銀行客戶可以通過第三方應用程序進行整合，以分析其現金流和銀行帳戶中的投資(6)加強跨境金融科技合作；(7)提升科研及人才培訓。

HKMA 關注的科技風險有(1)網絡安全風險；(2)銀行過度依賴服務供應商風險，例如提供雲端運算科技公司之監理，係由委託之銀行業監管，監管是否到位；(3)科技事故造成的聲譽和財務損失；(4)網路轉帳交易盛行之流動性風險，網絡取得資金容易，倘銀行發生擠兌將形成壓力；(5)客戶保障-訊息批露、私隱保障和產品適合度；(6)科技發展對銀行營運模式的衝擊。

HKMA 監管計畫係平衡金融科技發展與風險管理：(1)推出網絡防衛計畫（Cyber security Fortification Initiative），制定一套銀行應對網絡風險能力的評估框架和模型，所有銀行都須在 2018 年底前完成「網路防衛評估框架」評鑑；制定一套培訓及認證計畫，為網絡安全從業員提供專業認可的機制；建立一個銀行間互通訊息的網路風險資訊共享平台；(2)加強網上股票交易的保安；(3)要求銀行留意和不斷檢討數碼化策略及科技發展對營運模式的衝擊。

HKMA 對於內部稽核職能評估，相當重視內部稽核的獨立性，且視內稽為執法之延伸，對於銀行內稽的監管期望，期能具備科技風險評估能力、審核網路安全的管控措施、檢視科技事故的成因及預防措施的成效。

2.洗錢及恐怖分子資金籌集風險

對於銀行業的挑戰在於國際間監管要求日益收緊，巨額罰款影響銀行財務表現、聲譽和經營模式；大型銀行基於眾多原因收緊風險胃納，導致企業開戶困難；地緣性政治風險等。HKMA 對於銀行的主要關注點為管理層應做好監督；風險評估程序和落實「風險為本」方法；處理高風險客戶作為和數據質素；法遵和內稽人員對監管要求的理解；合規資訊系統的資源投放。

HKMA 監管工作重點為透過持續監管過程審查銀行管控制度和措施的成效（包括合規及內稽職能）、審視銀行是否有效地應用「風險為本」方法；透過專案審查以評估銀行篩查系統的成效。而對於銀行內稽的監管期望，則希望稽查銀行有關風險評估是否足夠，是否有效落實「風險為本」的方法（特別是辨識及管理高風險客戶）；審查風險管理的成效，如數據質素、合規資訊系統的有效性等。

3.信貸風險

香港銀行業整體貸款增長加快，2016 年 12 月~2017 年 6 月新增整體貸款 8,208 億港元；其中大陸相關貸款增加 4,260 億港元(占 52%)為主要增長動力，尤其是大陸民企借款增幅顯著，台資銀行香港機構之大陸相關貸款亦屬同樣明顯增長情形。

對於信貸風險，HKMA 監管關注銀行審核大陸民企貸款需要改善的地方，例如對借款人母公司背景、集團架構及借貸狀況了解不足、就內保外貸背後質押存款的資金來源進行盡職審查存在困難、對借款人高槓桿及經營現金外流風險分析不足或現金流分析粗疏等，而 HKMA 監管的重點在於繼續檢視大陸大型企業的信貸風險、監察及評估它們可能帶來的系統性風險；與大陸監管機構保持溝通，跟進如何處理民企在港借款情況；進行專案實地查核，檢視銀行對大額信貸的審核標準。

對於銀行內稽的監管期望，則希望確保管理層充分考慮政治和經濟因素對銀行信貸質素的潛在影響；獨立評估前台及中台的審核流程，確保銀行維持審慎的信貸審核準則及風險管理。

4.財富管理業務相關風險

HKMA 監管要求為「公平對待客戶」：(1)三大基本要求，即產品盡職審查、合適性評估及風險披露；(2)加強保障客戶（包括錄音和審閱期要求）、就複雜和高風險產品採取更謹慎的銷售手法。對銀行的監管關注點在於銷售手法及落實監管要求，例如產品盡職審查是否顧及香港法規及產品的風險、是否充分了解和考慮客

戶的情況，以提供適當的投資建議、是否在跨境業務方面，訂立足夠的規範及管控等，HKMA 監管工作將會繼續就銀行銷售複雜和高風險產品提供規範及進行審查；監察銀行落實企業文化改革的情況，而對於銀行內稽的監管期望，則希望審查銀行落實監管要求與規範的情況，包括就銷售複雜和高風險產品的相關要求、銀行企業文化改革規定與執行情形。

另 HKMA 認為對於財富管理業務，根本性杜絕不道德、不公平對待客戶行為之方式，便是形塑銀行良好企業與風險文化，高層應建立良好員工行為守則與推動風險文化，由上而下清楚傳遞，除了高層的認知與要求，並應對中層員工定期評估其對於風險文化的認知，還要有前線員工的意見反應機制（Tone from the top vs. Echo from the bottom），並與獎懲形成連結，以改革企業文化。

(二) 網絡安全（參訪 PwC HK）

隨著科技快速發展，人們各種行為都更依賴網路，也帶來更多的網路攻擊與資安問題，對金融業來說更重要的是如何透過創新科技的應用來增加風險與法令監管，也就是監管科技(regtech)。

透過機器學習、人工智慧、認知技術等科技來管理資安、交易安全、法遵等問題，如幫助進行 KYC 盡職調查、偵測金融詐欺等，也都是監理可以思考科技應用的方向。

網路釣魚 mail 頻傳、駭客攻擊風險，網路安全管理更形重要，影響金融機構在風險管理方面的布局。為此，金融機構勢必須投入更多的時間及資源，以更積極的態度來因應風險。

HKMA 網路安全規範(“CFI”)：(1)Cyber Resilience Assessment Framework (“C-RAF”) 制定「網路防衛評估框架」，建立一套以風險為本的架構，由銀行自我評估風險概況並將防禦等級標準化，以及所須加強的程度；(2)Professional Development Programme (“PDP”)制定培訓及認證機制，以增加網路安全專業人才；(3)Cyber Intelligence Sharing Platform (“CISP”)建置分享平台，與各銀行分享網路威脅情資，以提升各銀行間協作與系統性網絡防禦能力。

制定「網路防衛評估框架」，由銀行執行自有風險評估及成熟度評估，並依低中高等級分類，對於中至高的風險，要求必須參與網路攻擊的模擬測試（iCAST），HKMA 將蒐集與分析各銀行的評估結果以制定統一的風險框架。評估固有風險包括流通管道、產品與技術服務、企業規模與組織特徵、網路威脅追蹤紀錄及技術；

成熟度評估（1）治理（制度面）-整體網路安全耐受度、策略與政策、網路風險管理、稽核機制、人員配置與訓練（2）辨識內部環境-識別 IT 資產、網路風險識別與評估（3）內部環境之保護-基礎設施保護控制、存取控制、資料安全、程式編譯安全度、補漏洞管理、補償性措施管理（亡羊補牢）（4）內部環境的偵測-漏洞偵測、異常行為偵測、網路事件偵測、威脅監控與分析（5）內部環境的應變與恢復-應變計畫、事件管理、事件風險等級的升高與陳報（6）對外部環境的瞭解、意識-威脅的情資、威脅情報的分享（7）第三方風險-外部聯繫管道的入侵、管理及掌控第三方、持續監控第三方風險。

(三) 三道防線與風險導向內部稽核

要有效的提升國內銀行業內部控制品質與提升風險聚焦查核能力 ，銀行業必需具備明確的內部控制三道防線機制及差異化評比標準，並藉由建立內部控制之三道防線，重新檢視如何強化風險管理與內部控制減少弊端發生。第一道防線要為其日常業務中所產生的風險負責，確保所有操作過程中的主要風險都能被識別出來，並且能夠適當的被內部控制所減緩或監控；第二道防線如風險管理、財務管理、法令遵循等，負責制定規章制度及作業規範供第一道防線遵循，於必要時對其提供建議或指導；第三道防線為內部稽核單位，負責就第一與第二道防線的功能向高階管理層與董事會提供獨立的確認，除負責稽核檢查與整改驗證工作外，尚負責獨立測試上述檢查與整改驗證的工作品質，因而獨立測試團隊有第 3.5 道防線之稱。

國際內部稽核協會（IIA）立場聲明書之「內部控制三道防線實務守則」，所謂「內部控制制度」三道防線之概念：

1. 第一道防線：銀行各單位就其功能及業務範圍，承擔各自日常事務所產生之風險謂第一道防線，其應該負責辨識及管理風險，針對該風險特性設計並執行有效的內部控制程序以涵蓋所有相關之營運活動。
2. 第二道防線：第二道防線係獨立於第一道防線且非為第三道防線的其他功能及單位，依其特性協助及監督第一道防線辨識及管理風險。第二道防線包含風險管理、法令遵循及其他專職單位，其就各主要風險類別負責銀行整體風險管理政策之訂定、監督整體風險承擔能力及承受風險現況、並向董（理）事會或高階管理階層報告風險控管情形。
3. 第三道防線：第三道防線係內部稽核單位，應以獨立超然之精神，執行稽核業務，協助董（理）事會及高階管理階層查核與評估風險管理及內部控制制度是

否有效運作，包含評估第一道及第二道防線進行風險監控之有效性，並適時提供改進建議，以合理確保內部控制制度得以持續有效實施及作為檢討修正內部控制制度之依據。

銀行內部各單位依三道防線分工，各道防線間應充分溝通、互相分享資源，確實執行其職責，並與第四道防線(主管機關)連結、充分溝通，強化公司治理及內部控制機制，提升內控內稽品質。

如何導入風險導向的內部稽核：

1.了解企業環境、經營策略、業務發展及風險程序，從流程的角度辨識、評估風險。

2.諮詢審計委員會、高階管理人等對內部稽核的需求及期望。

3.與第二道防線合作、溝通交流。

4.確認風險評估範圍-決定受查主體：依據所經營業務範圍、組織、業務特性、產品，以及主管機關法令規範擬定。

5.訂定風險種類-依各受查主體發展策略目標、業務規模及海外分行地主國之特殊規定等決定其風險類型，如：流動風險、利率風險、信貸風險、操作風險、市場風險、信譽風險、合規風險、策略風險…等。

6.建置風險評估模型-必須包含法令遵循、內外部資料，並能自動計算、評核產出風險等級。擬訂固有風險因子、控制風險，構成剩餘風險，並持續評估確認各受查主體的控制措施是否發揮功效，就其有效性依重大性判斷風險等級。（註：參訪之銀行業，其風險評核產出之風險等級區分 3 個或 4 個或 5 個等級，據以排定其稽核計畫）

7.擬定年度查核計畫-聚焦風險的查核計畫，包括受查主體、查核頻率、範圍及查核方式，審閱計畫與評估結果之妥適性彙總訂定。年度稽核計畫及風險評估結果應經審計委員會核議並經董事會通過。

又，僵化的稽核計畫將無法即時反應風險，內部稽核應依據風險的變化動態評估風險，以滾動的方式更新稽核計畫，使稽核計畫更能與銀行的目標契合。

8.持續監控及蒐集內外部資訊，將下列訊息納入訂定或修訂年度稽核計畫的重要參考，俾風險評估結果能即時反應受查主體之風險，及金融監理環境之改變：

(1)國內、外主管機關監理重點、重要法令異動及金融環境變化；

(2)銀行經營策略目標與重要政策變化；

(3)業務營運管理資訊及重要監控指標；

(4)主要利益關係人意見；

(5)風險改變；

(6)重大風險事件發生情形。

9.執行查核計畫、產出報表。

10.內部稽核品質評核。

(四) 內部稽核組織、管理與人才發展

內部稽核組織與管理：內部稽核部門設置前、中、後台，各司其職，確保有效的內部風險管理及控制機制，彰顯稽核核心價值。

1.前台：依據擬定之查核計畫及特定專案查核需要，以風險為本原則執行實地查核，包括規章制度檢視、面談溝通、系統測試、實地觀察、實地盤點、調閱文件抽樣查核等。

2.中台：執行非現場持續監控、開發電腦輔助工具(如數據分析)及監控報表、以風險為本的原則擬訂稽核重點及查核項目。

3.建立內部稽核品質評核機制(後台)：由資深稽核人員擔任，以獨立超然的精神評估內部稽核職能及質量管理成效，包括是否掌握風險方向，評估風險方法論是否有效、稽核計畫是否有效執行等，並提供改善、精進意見。

稽核人員應集合資訊、風險、法律人才，以系統化、規範化促進穩定經營，提升銀行價值：

1.配置具有一定學歷、技能、專業知識與能力及溝通技巧之內部稽核人員，並與第二道防線人員輪調交流或跨部門崗位實習，建置人才庫。

2.培訓計畫：優化人員素質，持續性的教育訓練，及給予適當的發展機會，注重專業資格的取得，提升稽核與業務專業知能及養成多構面管理能力。

3.內部稽核的新價值與新方向：(1) 具備 productive(有效的)、proactive(積極主動的)、predictive(可以預測的)、preventive(預防性的資料分析)的稽核工具及能力，積極運用科技投入大量資源；(2) Transparent(透明的)、nimble(靈活的)、seamless(無縫的)、hassle-free(無障礙的)稽核制度與三道防線的協調合作，及第四道防線的溝通交流；(3) From hindsight to insight to foresight 從事後的見識去洞察遠見，具完整性、及時性、預警偵測與防範等功能。

(五) 行為與文化風險評估

文化所體現的是一種價值觀，用以潛移默化地誘導管理階層和員工的思維和行為，良好的企業文化和價值能引導員工擇善而行，動機並非為避免受罰，而是

打從心底明白自己要做、應該做的事。

穩健、良善、值得信賴的經營之道在於穩健獲利，亦即要秉持負責任及公平待客的原則，才能永續經營。型塑銀行良好的文化不只是 Tone from the top(從上而下)，還要 Echo from the bottom(從下而上)，將企業的價值觀、穩健良善經營之道明確訂定員工行為守則。

如何進行員工行為與企業文化的風險評估：

1. 瞭解高階管理人的經營策略及經營管理之道
2. 審查規章制度-如公司治理、恰當的獎勵制度
3. 審查公平待客原則-如：契約是否不利於客戶、是否披露產品風險、是否充分了解客戶
4. 對於複雜度高及高風險產品進行審查
5. 交易的監控-如：客戶是否於短期內進出同一資產規模或類似之商品
6. 觀察員工的行為、作業流程及基層的聲音
7. 審查客訴案件

叁、心得與建議

一、心得

全球銀行業面對的挑戰差異不大，香港金融管理局所關注的科技風險、洗錢防制及打擊資恐風險、信貸風險及財富管理風險等，亦是我國所關注的重點，HKMA 對於網絡安全制定一套風險評估框架和模型，所有銀行都應於限期內完成「網路防衛評估框架」的評鑑，以及建置網路威脅情資分享平台，實值得我們參考取經，此外，並應密切注意國際相關網路金融之監理措施可能發展之新方向，提升網絡防禦能力。

內部控制與風險管理的有效性攸關企業是否得以永續經營，在網路數位及金融科技的快速發展、產品及服務多樣化且複雜、主管機關監理強度增加及全球經濟瞬息萬變的環境下，金融業面臨複雜的風險形態，明確的內部控制三道防線機制及風險聚焦查核的內部稽核制度，有助於提升銀行業整體的風險觀念，強化內部控制品質。

稽核人員需要轉型，傳統上對於稽核人員的印象是保守的、嚴肅的、沒有笑容的，稽核工作似乎只是找出錯誤，然隨著金融環境快速的變遷，稽核工作所呈現的

是團隊精神，將每個人所作業的、發現的拼接起來，從大方向檢視組織、整體流程，從動態環境中確認風險，提醒管理層應對新發生的問題及改變方案；而稽核人員需具備良好的溝通能力、分析思考能力、提供諮詢能力，積極主動提出建議，提升稽核團隊的技能，以因應未來的變化。

二、建議

因應金融市場國際化與數位化所帶來的新挑戰，內部稽核應利用持續性稽核工具來發現銀行的潛在風險，及科技創新帶來的新興風險，並提出風險預警，以使銀行及早因應改善，是以稽核人員除不斷的學習，充實專業知識外，提升電腦相關技能的知、能更是刻不容緩，建議稽核人員應持續參加網絡安全、運用電腦進行稽核等相關課程及實務演練，以提升稽核效能。