出國報告(出國類別：其他)

2017 年金融檢查與稽核研修班

2017 Bank Examiners and Auditors Program

服務機關：臺灣土地銀行
姓名職稱：邱天生　總稽核
派赴國家：香港
出國期間：106 年 10 月 15～20 日
報告日期：106 年 12 月 3 日

目　錄

一、 活動宗旨

為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,主管機關特別於今年推動「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,值此內部稽核轉型關鍵時刻,本次「金融檢查與稽核研修班」特於國際金融中心-香港舉行,邀集在地資深金融專家共同探討以下重要議題:

- ✧ 香港外資銀行法規最新趨勢
- ✧ 從內外部利害關係人觀點談內部稽核之角色與價值定位
- ✧ 有哪些銀行內外部新興風險值得關注?如何辨識與掌控?
- ✧ 風險導向內部稽核制度導入策略
- ✧ 銀行內部控制三道防線之權責角色與合作機制
- ✧ 因應銀行國際化布局、金融環境數位化,如何從組織與管理模式啟動內部稽核新變革

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、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,活動中將透過機構考察形式,提供給參與者向香港金融產官學界學習借鏡之寶貴機會,以交流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。

二、 活動特色

(一) 本次活動於香港舉行，內容結合研討會與金融機構實地考察活動，提升活動豐富性。

(二) 受邀演講及參訪之機構涵蓋香港當地金融主管機關及全球各大金融集團，締造標竿學習之絕佳契機。

(三) 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，主管機關特別於今年推動「風險導向內部稽核制度銀行內部控制三道防線」以全面強化銀行風險治理效能。

三、 活動行程

日期	時間	機構參訪/交流研討
10/15 Sunday	下午	抵達香港
10/16 Monday	10:00-12:00	**交流研討：HKMA & McKinsey & Company**
	14:00-17:00	**機構參訪：中國銀行(香港)**
10/17 Tuesday	10:00-12:00	**機構參訪：東亞銀行**
	14:00-17:00	**交流研討：渣打銀行**
10/18 Wednesday	09:30-12:00	**機構參訪：星展銀行**
	14:00-17:00	**機構參訪：PwC(HK)**
10/19 Thursday	09:30-12:00	**機構參訪：HSBC Bank**
	14:00-17:00	
10/20 Friday	09:30-12:00	小組分享會
	下午	返台

四、 研討內容摘要

香港金管局(HKMA)

- **參訪摘要**

一、 香港金管局(HKMA)阮國恒副總裁在本次參訪中

（一） 主要談到「香港金融科技的最新發展」以及「香港銀行業面對的最新挑戰及從監理觀點談內稽應對之道」,其中香港銀行業面對的最新挑戰如下：

1.科技風險；

2.洗錢及恐怖分子資金籌集風險；

3.信貸風險；

4.財富管理業務相關風險。

（二） 同時說明 HKMA 對上述風險議題的關注重點與監管工作,以及對內部稽核職能的要求與期望，並特別強調內部稽核獨立性。

（三） 另也談到 HKMA 與金融業界有定期性的溝通機制,以傳達監管理念與要求及傾聽業者心聲。

- **參訪內容**

一、 香港金融科技的最新發展

香港金融管理局(以下稱 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，並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，藉拋出「安全與便利如

何取得平衡」之社會觀點議題，由公共討論形成輿論共識，據以為平衡點而決定監管強度，而為推動香港邁向智慧銀行新紀元，HKMA 提出七項措施帶領及協助銀行業提升至更高層次，把握銀行與科技結合帶來的龐大機遇。

二、 銀行業面對的最新挑戰及從監理觀點談內稽應對之道

HKMA 阮國恒副總裁談到香港銀行業面對的最新挑戰有科技風險、洗錢及恐怖分子資金籌集風險、信貸風險、財富管理業務風險等議題，同時說明 HKMA 對上述風險議題的關注重點與監管工作，以及對銀行內部稽核職能的要求與期望，茲敘述如下：

(一)科技風險：

HKMA 鼓勵銀行使用金融科技及推動香港邁向智慧銀行新紀元，監管原則以風險為本和科技間中立，監管目標在於民眾方便性與銀行保障客戶之間取得平衡。

對於科技風險監管，HKMA 關注於網路安全風險、銀行過度依賴或集中同一服務供應商風險(含銀行對委外之監管是否到位)、科技事故造成的聲譽和財務損失、網路轉帳交易盛行之流動性風險、客戶保障(訊息披露、私隱保障和產品合適性)、科技發展對銀行營運模式的衝擊等。

而 HKMA 監管計劃係平衡金融科技發展與風險管理，推出網路防衛計劃、加強網上股票交易的保安、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等，其中網路防衛計劃 (Cyber

security Fortification Initiative)係為提高香港銀行業抵禦網路攻擊的能力，共有三大主要元素並納入監管規定，分別是「網路防衛評估框架」、「專業培訓計劃」及「網路風險資訊共享平台」，所有銀行都須在 2018 年底前完成「網路防衛評估框架」評鑑；對於人才培訓制定一套培訓及認證計劃，為網路安全從業員提供專業認可的機制；與銀行界合作，建立一個銀行間互通訊息的「網路風險資訊共享平台」且 HKMA 也積極與新加坡談跨國互通機制，以期擴大訊息分享來源。

針對科技發展對銀行營運模式的衝擊，HKMA 拋出議題讓銀行思考，請銀行自行思索因應金融科技的發展，未來五年後銀行到底會變成什麼樣子，部分銀行認為五年後應轉型為科技公司的方式來經營，而 HKMA 對於銀行內稽的監管期望，則希望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。

(二)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(特別是識別及管理高風險客戶)；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。

(三)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。

(四)財富管理業務相關風險：

HKMA 監管要求有 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。

(五)其他

1. HKMA 與金融業界有定期性溝通機制，藉以傳達其監管理念與要求及傾聽業者心聲；了解業者對於面對之經營環境挑戰與風險問題，如每年與各銀行的董事會分別交流 2 小時；每年與各銀行的獨立董事單獨座談半小時；每半年與銀行高階管理層

級 round table meeting；定期與銀行間就監管要求蒐集訊息，藉此回饋及時檢討修訂監管政策要求等。

2. 內控的第一、二、三道防線是合作關係、各道防線的目標相同，都是為了強化公司治理及內部控制，愈前面的防線做得愈好，後面的防線愈能發揮功能。

3. HKMA 對於內部稽核職能評估，相當重視關於內部稽核的獨立性，且視內稽為執法之延伸；HKMA 規定內稽的資源及報酬應直接由董事會或指定委員會審批以顯示對內部稽核獨立性的重視。

4. 另 HKMA 阮國恒副總裁提醒即使台資銀行由總行負責內稽，亦應充分了解香港當地監管要求，投放妥適的稽核資源， 此為其對台資銀行內稽的期望，亦為銀行業海外拓點時應謹記之最高原則。

中國銀行(香港)

➢ **參訪摘要**

一、參訪中銀(HK)

二、三道防線機制

三、風險導向內部稽核

四、質量管理

五、變革與挑戰

六、高階管理層的期望

➢ 參訪內容

1. 內部稽核

2. 非常古老而年輕的話題

3. 監管的要求從未有底線

4. 質量管理

(1) 香港金管局(HKMA)要求

A. 對內部審計職能的獨立審查

B. 內部審計職能的監管評估

C. 評估內容

D. 評估範圍

(2) 國際內部稽核協會(IIA)要求

A. 總體要求:須建立並維護質量保證與改進程序

B. 程序:必須包括內部評估和外部評估

C. 報告:必須向高管層和董事會報告結果

E. 披露:須披露未遵循事項及其影響

5. 變革與挑戰

(1) 發揮先進的內審職能

(2) 應對銀行業未來發展趨勢

(3) 銀行監管環境日益嚴峻

(4) 高端人才相對稀缺

(5) 反洗錢監管要求提高

(6) 金融網絡安保不容樂觀

6. 高階管理層的期望

(1) 問題導向、以風險為基礎

(2) 五見：見人、見事、見機構、見原因、見責任

(3) 查改一體化：檢查與改善同時進行

(4) 隊伍建設：稽核檢查小組優秀的人才、資訊科技人才的晉用與團隊的組合

東亞銀行

➢ 參訪摘要

本次參訪課程首先介紹第 4 次工業革命對內部稽核的衝擊，並藉由案例說明科技創新對內部稽核的影響，並強調內部稽核應利用持續性稽核工具來發覺銀行潛在的風險，並提出風險預警，以使銀行能及早改善避免損失，另分享稽核人員只有不斷的學習，充實自已的專業知識，尤其電腦相關技能，才能在未來的競爭中「適者生存」。

➢ 參訪內容

一、 第 4 次工業革命的衝擊

第 4 次工業革命變革規模極大、範圍極廣，所以各項科技創新發展的速度比以往任何時候都快，對各個產業的影響更加激烈，如：2006 年時世界前 5 大企業依市值分析只有 Microsoft 一家科技公司列名，但到 2016 年時世界市值前 5 大企業均為科技公司，依序分別為 Apple、Alphabet、Microsoft、Amazon 及 Facebook 等 5 大企業。

二、 科技的發展對稽核業務而言是危機也是轉機

(一)持續性稽核及風險提示

持續性監控(Continuous Monitoring，CM)由第一道及第二道防線人員執行，在確保政策與程序之有效運行，並評估控制的妥適性及有效性， 並由稽核人員獨立評估各項控制活動的適當性。

(二)發展行為分析工具來監控交易員之行為

在持續性監控的活動中，對交易員的行為監控應該是各家銀行關注的重點，發展行為分析工具並設計各種行為分析模式，自動收集相關資料及分析交易員之行為是否有異常之狀況，若有異常之狀況即發出警告，由相關人員採取後續監控措施，以預防交易員之違規行為。

(三)Free WiFi 的攻擊方式

東亞銀行在每月內部人員之培訓工作中，均會包含各項資訊安全之議題，於本次參訪中特提出有關智能手機最新的攻擊方式，以供參考。

三、 顛覆內部稽核之傳統思維

(一)內部稽核應持續與第一道及第二道防線溝通，以提升受查單位的風險及控制意識，減少風險的發生。

(二)內部稽核應分享稽核工具及方法給第一道及第二道防線，使其了解稽核單位的檢查重點，以達到預防勝於治療的目標。

(三)減少稽核報告的產出

1. 稽核報告應聚焦於管理階層關注的事項，著重表達未來可能發生的風險，另稽核報告所提出之稽核建議應先考量是否能促使組織有正面改變，這樣的稽核報告對組織而言才是有價值的稽核報告。

2. 傳統的稽核報告是以稽核人員的角度，說明檢查情形及發現，受查者不易了解，有時甚至會誤解稽核人員的檢查建議，未來的稽核報告則應站在第一道及第二道防線人員的角度，說明受查者需要知道的資訊，使其能確實改善稽核建議。

四、 如何訂定稽核計劃

(一)內部稽核隨著主管機關的要求、法令的變更、重大事件的影響、 業務流程的變化等，會不斷的改變稽核目標與重點，僵化的稽核計劃將無法即時反應風險，因此內部稽核應根據風險的變化，動態評估風險，以滾動的方式更新稽核計劃，使稽核計劃更能與銀行的目標契合。

(二)隨時將新出現的風險因子納入稽核範圍。

(三)在排定稽核計劃時，對於稽核人員工作之分配，不應以現有人力來局限稽核檢查工作，而應考量稽核檢查之需求，調派相關專案人力，必要時在符合獨立性的前提下，得要請其他單位之專業人員配合查核，如此不僅可以建立未來稽核人才庫，亦

可藉由其他單位人員參與使其了解稽核單位查核之重點及查核之方法，提昇其風險意識。

(四)由於風險導向稽核有賴組織整體風險管理之建立，在面對組織各種不同性質的業務時，可配合使用不同稽核及諮詢方法，來達成稽核目標。

五、 如何建立正確的風險導向內部稽核

(一)對各項業務應有深刻的認識，並了解風險所在。

(二)加強對一般稽核人員對資訊技術之訓練，使其可以利用稽核工具，藉由大數據分析及尋找問題，並協助第一道及第二道防線對其業務風險點完善控制措施。

(三)內部稽核人員必須重新審視在組織內之定位，檢討是否已具備足夠之專業知識，以協助銀行找出可能發生的風險，以達成預警的目標，而不是著重於檢查已發生的缺失。

渣打銀行

- **參訪摘要**

一、 Risk Based Internal Audit System 風險導向的內部稽核制度

二、 Transformation of Internal Audit 內部稽核轉型

三、 Audit Strategy on Overseas Operation 海外業務稽核策略

- **參訪內容**

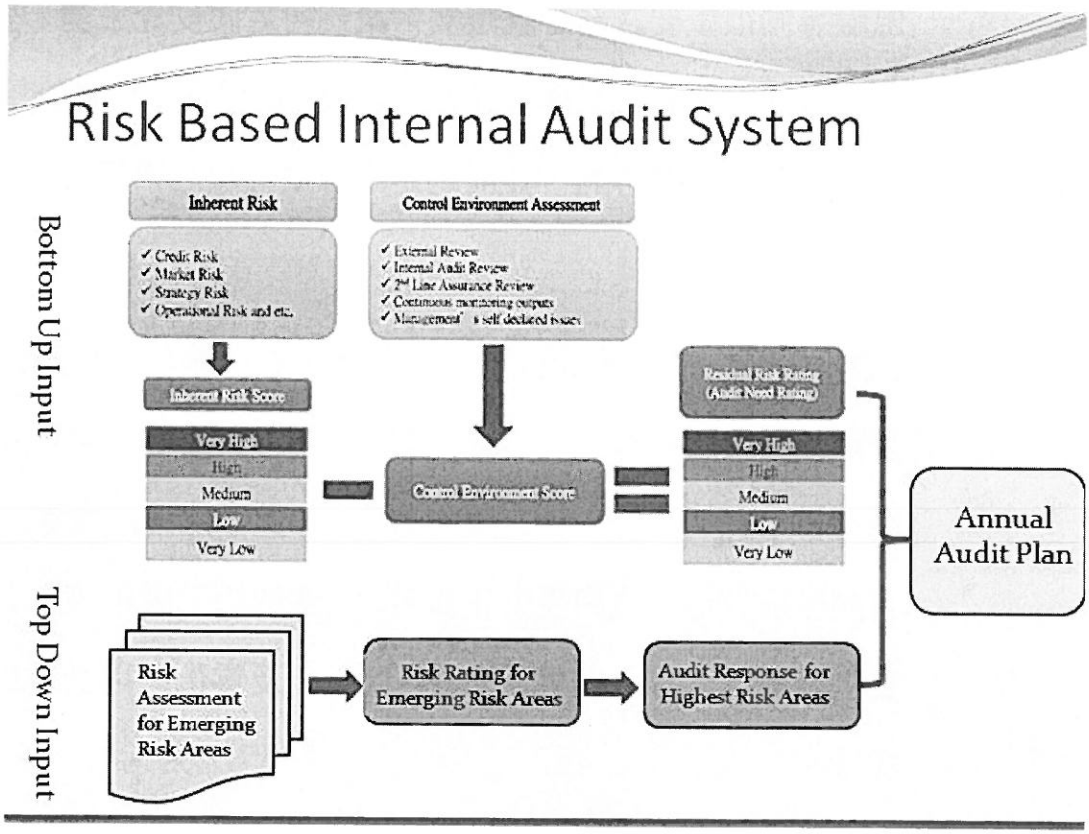
一、「Risk Based Audit Sharing」

(一)Risk Based Internal Audit System(風險導向的內部稽核制度)：

1. 渣打銀行訂定 26 個風險種類固有風險(Inherent Risk)評估減去控制環境(Control Environment)評估，差額即是剩餘風險 (Residual Risk)，渣打銀行剩餘風險評估依分數由高到低排序，再依所設定標準差之常態分配做區隔，劃分出 5 個級距 (Very High、High、Medium、Low、Very Low)，每年重新調整各個級距之分數標準。

   據此做年度計畫之週期安排，這是由內部稽核角度根據受查主體風險分析之結果，即由下往上(Button Up Input)之方式，另外亦考量由上往下(Top Down Input)之因素，即是依據主管機關、董事會或審計委員會之期望以及最近金融環境發生之新興風險評估所產生之風險評級，綜合考量 Button Up Input 及 Top Down Input 之風險因素後，再據以決定年度稽核計畫。

   (如下圖所示)這部分與我國銀行公會所發佈之風險導向稽核考量之風險架構類似。



資料來源：渣打銀行簡報資料

2. 有關受查主體、風險管理框架、定量和定性風險因子、整合式稽核

(1) Defined Auditable Entities 定義受查主體

(2) Risk Management Framework (RMF)風險管理框架

- Risk Types 風險類型
- Risk Control Owners 風險控制所有者

(3) Quantitative and Qualitative Risk Factors 量化及質化風險因子

(4) Integrated Audits 整合式稽核

風險導向很重要之部分就是要考量如何定義受查主體，才能涵蓋銀行整體之業務及運作之功能，這個部分於實施風險導向之初即要審酌，並需制定出風險管理之架構及分類。

風險評估之定義分級及看法，不單僅考慮稽核部門之看法還需包括風險管理部門、法律遵循部門及業務單位之意見，所有單位必須遵守一致之風險架構，如此才能達成共識。有關風險評估也會與受查主體分享，讓他們了解稽核對受查主體風險之評估結果，並依各種量化及質化之指標計算風險。

稽核方式係採整合式查核，每次查核不僅查核一個單位或一個功能別，或是僅查核一個系統，實務上作法可能係採業務稽核與電腦稽核整合，或前、中、後台跨單位，或跨業務線整合之查核方式。

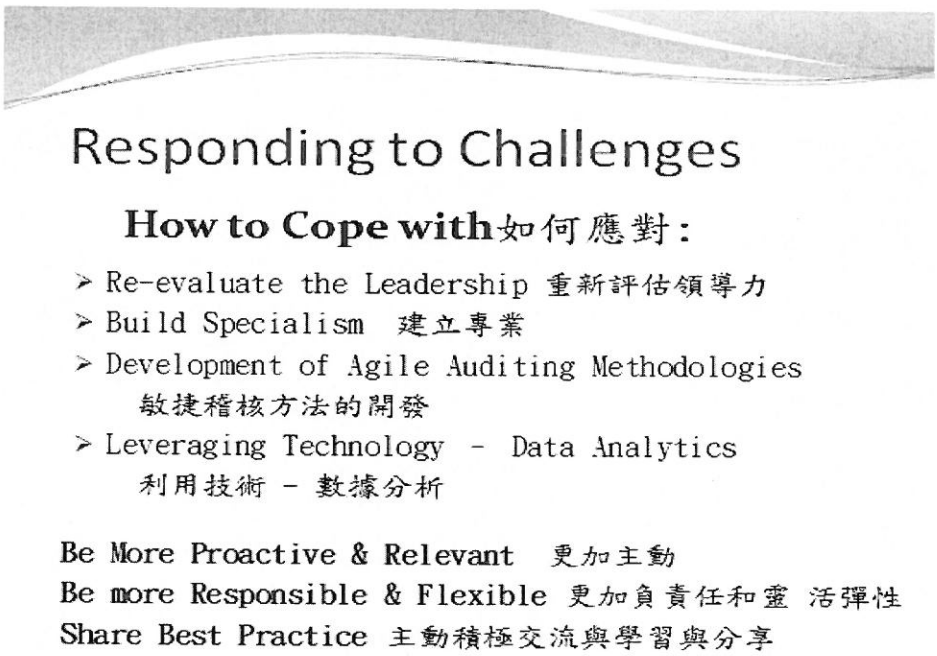
(二)「Transformation of Internal Audit 內部稽核轉型」

1. 稽核人員需要轉型，傳統上對稽核人員之印象是保守、嚴肅沒有笑容，然面對現今金融環境之快速變遷，稽核人員更需改變與轉型，高管階層對內稽人員有所期待，要求稽核獨立並具效率，不要讓高管階層

surprise，期待能以更具效率之方式提出稽核之看法。

2. 需提升稽核人員之專業形象，增進查核效能並採敏捷行動，以具說服力及堅定之立場將稽查意見與受查單位充分溝通，讓組織打破對稽核人員刻版印象，稽核人員也應加強數據分析之能力，以強化稽核人員之工作技能。

(三)稽核的 15 個行為，要能與受查單位充分溝通，過程要透明，經由充分交流使溝通能更有效，最好能面對面接觸溝通，經由與人感情之交流而不是僅以 email 溝通而已，要能與受查單位互動，對每個受查主體要有一致之原則及立場，勿因稽核人員與受查對象有私交就有不同標準，渣打銀行提供之 15 個行為準則



星展銀行

➢ 參訪摘要

一、 星展銀行(DBS)內部控制架構係依據三道防線的基礎概念(Three Lines of Defense)所建立的：

- ➢ 第一道防線：策略、執行及風險管理；負責辨識及管理營業活動及交易相關的風險。
- ➢ 第二道防線：政策制制定及監控；負責整體風險監理的架構及報告產出。
- ➢ 第三道防線：提供獨立角色的保證；檢視各項程序及控制是否適當及有效。

二、 執行有效能及效率的稽核工作，強化內部稽核機制：

推動稽核 4Ps 以增加稽核價值—即具效率(Productive)、具主動性(Proactive)、具偵測力(Predictive)、具預防能力(Prevention)。

三、 為強化內部控制及內部稽核功能，採行管理階層內控意識評估機制(Management’s Control Awareness, MCA)：

(一)分為(Good, Satisfactory, Fair, Poor)四個評等等級

(二)評估項目：如

- ➢ Risk Culture Measurement
- ➢ Tone at Senior Leads
- ➢ Risk & Resource Management

要求經理部門應評估其所轄單位內部控制狀況，以反應其風險控管程度，各單位彙整後，即可初步瞭解 DBS 風險管理文化的健全狀況，該機制協助管理階層發展工具以評估單位內風險管理文化，並據以培育 DBS 管理文化；協助內部稽核、高階管理層能快速了解各項業務的風險；管理階層可採行相關控制行動以降低風險，內部稽核可綜合內部控制評等結果及管理階層內部控意識評估結果，作為評估受查單位的風險。

四、 編列稽核計畫：

(一) Audit Universe：Size of Audit Entities, Risk Profile, Scope of Audit Entities 受查單位規模、業務風險等

(二) Risk Assessment：Based on Basel 九項風險評估因子為評估架構

(三) Key Audit : Top 10 Area of Focus 考量全球性、區域性等業務重點，訂定前十大查核重點

(四) Audit Project

(五) Sampling à Computer Assisted Audit Ratings

五、 持續性稽核：

透過 ERICA(Early Risk Identification and Continuous Assessments), Computer Assisted Auditing Technique,

(一)即早發覺問題，回饋給一、二線單位

(二)Narrow Down Our Audit Scope

(三)Adjust Our Review Frequency

六、 內部稽核新價值

(一)The Future of Audit is to Audit the Future.

(二)Auditing Without Auditing

(三)Transparent, Nimble, Seamless, Hassle-Free

(四)From Hindsight to Insight to Foresight

七、 實施風險導向稽核制度思考方向(Auditing Journey)

八、從第三道防線觀點談數位金融風險管理

銀行業近年來逐漸發展網路數位及金融科技，產品及服務多樣化且複雜，銀行的經營風險大為提高，資安議題應獲得董事會與高階管理人員之有效監督，並儘早與國際接軌，積極導入風險導向內部稽核制度，發揮三道防線功效，有效提升內稽內控品質、保障客戶權益。

(一)數位金融風險：

1. 網絡安全風險；

2. 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物損失；

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；

4. 客戶保障—訊息批露、隱私保障和產品適合度。

(二)第三道防線應具備之專業知能及查核技巧：

1. 提升專業知能及定期培訓；

2. 瞭解網路金融業務風險之來源、類型及評估風險；

3. 善用資訊科技工具及資料分析方法以增加查核的廣度深度。

(三)查核第一、二道防線是否落實：

網路銀行內部控制包括管理面及技術面是否到位，如：網銀風險管理及措施(包括客戶終端軟體)、內部網路控管、應用程式檢核、緊急應變措施、對委外廠商的監控、電腦是否連結智慧型行動裝置、電子郵件點閱、密碼管理等。

四、 行為與文化風險評估

(一)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。

(二)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。

(三)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. 規章制度之訂定—如公司治理、恰當的獎勵制度；
3. 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—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. 客訴案件。

PwC HK

一、如何攻擊銀行網路的滲透測試

(一)Cyber security: The new reality

(二)Regulators have been moving with the cyber trend

(三)Insights from Hong Kong Monetary Authority("HKMA")

Cybersecurity Fortification Initiative ("CFI")

(四)Intelligence-led cyber attack simulation testing ("iCAST") end-to-end attack simulation

二、HKMA網路安全規範("Cybersecurity Fortification Initiative‧CFI")

(一)網路防衛評估架構

(二)專業培訓計畫

(三)網路風險資訊共享平台

三、網路安全防衛評估

四、資安模擬演練與執行

HSBC Bank

- **參訪摘要**

一、 HSBC-HSBC Internal Audit Structure

(一)集團內部稽核章程；

(二)集團內部稽核單位的組織架構；

(三)三道防線組成模式；

(四)風險導向的內部稽核；

(五)內部稽核功能之轉型。

二、 HSBC-Managing Conduct and Culture Risks (管理行為及文化之風險)

(一)文化的定義；

(二)Risk 5 Pillars(風險 5 支柱)；

(三)15 Types of Conduct Outcomes(15 種行為態樣)；

(四)Measure the Risk Culture (衡量風險文化)。

三、 HSBC- Quality Assurance and Improvement Program (QAIP 品質保證與改善計畫)

(一)QAIP 的定義

(二)有效的「品質保證與改善計畫」之五個關鍵特徵

(三)QAIP Challenges(QAIP 品質保證與改善計畫的挑戰)

➢ **參訪內容**

一、 集團內部稽核章程(Global Internal Audit Charter)：

(一)目的(Purpose)

(二)權威性(Authority)

(三)獨立性(Independence)與客觀性(Objectivity)

(四)可歸責性與工作範圍(Accountabilities and Scope of Work)

二、風險導向的內部稽核

(一)稽核計畫的制定：

1. 決定稽核實體(Audit Entity)：可以依照集團準則來單獨做風險評估的一個區塊，可以是組織內的一個單位、一項業務、一個產品或是一個國家。

2. 確定稽核範圍(Audit Universe)：確認所有的實體組織、第一道與第二道防線、利潤與成本中心、與關鍵應用資訊系統都被包含在內。

3. 做好稽核風險管理(Audit Risk Management)：

(1) 固有風險(Inherent Risk)

(2) 控制環境(Control Environment)：除了控制的有效性之外，尚須將管理階層自行發現的問題與發生損失的機會納入考慮。

(3) 新生風險與行為考量(Emerging Risk and Conduct Consideration)：對於重大新生風險或是特殊行為(如：舞弊)可列為特別考慮因素。

4. 稽核需要評估(Audit Needs Assessment)：評估等級分為High、Moderately High、Moderate與Low等四個等級，據以排定稽核計畫。

五、 感想與心得

(一)銀行應形塑良好企業與風險文化，檢討銀行內是否已建立良好員工行為守則與推動風險文化，落實企業文化的改革應由高層自上而下清楚傳遞其要求，除了高層的認知與要求，並應建立對於中層員工定期性評估其對於企業與風險文化的認知。

(二)推動內部稽核第三道防線與第二道防線夥伴、合作關係。

(三)未來銀行需加強稽核人員對新金融商品之教育訓練，並透過參訪互相交流以達了解世界金融趨勢及吸收新知之效。

(四)風險導向內部稽核制度應著重於銀行本身對於風險的認知及管理，不僅是內部稽核單位需瞭解之問題而已，更是銀行所有單位需共同面臨之議題。

(五)銀行所有業務風險之管理需以風險為本之管理為基石，應強化三道防線間功能之有效發揮及緊密相互間之合作關係，才能有效進行風險導向之內部稽核制度，以達聚焦於重要風險議題之查核深度及提高內部稽核之查核效能。

六、活動照片


2017年
金融檢查與稽核研修班