

出國報告（出國類別：其他）

2017 年金融檢查與稽核研修班

服務機關： 中國輸出入銀行
姓名職稱： 曹盛啟（三等專員）
 陳冠宏（高級辦事員）
派赴國家： 香港
出國期間： 2017.10.15 - 2017.10.20
報告日期： 2017.12.22

摘要

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」在海內外主管機關支持下，自 1998 年首度舉辦迄今已歷十九屆，每年輪流於台灣及海外地區國際金融重鎮舉行，邀集海內外優秀專家共同研討金融政策與內稽實務關鍵議題，成為連結台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。

本年度活動之特色：

- 一、 本年度活動於香港舉行，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及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」與「銀行內部控制三道防線」以全面強化銀行風險治理效能。

目次

一、	目的	3
二、	參訪香港金管局(HKMA)	4
三、	參訪中國銀行(香港)	8
四、	參訪東亞銀行	12
五、	參訪渣打銀行	18
六、	參訪星展銀行	21
七、	參訪 PwC(HK)	27
八、	參訪滙豐銀行	31
九、	心得與建議	41
十、	建議事項	44
十一、	活動照片	47

一、目的

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，今年度「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：

- (一) 香港外資銀行法規最新趨勢。
- (二) 從內外部利害關係人觀點談內部稽核之角色與價值定位。
- (三) 有哪些銀行內外部新興風險值得關注？如何辨識與掌控？
- (四) 風險導向內部稽核制度導入策略。
- (五) 銀行內部控制三道防線之權責角色與合作機制。
- (六) 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。

本次活動行程分別參訪香港金管局(HKMA)、中國銀行(香港)、東亞銀行、渣打銀行、星展銀行、PwC(HK)及滙豐銀行等金融監理機關以及銀行，相關參訪行程如下：

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：香港金管局(HKMA)
	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：滙豐銀行
	14:00-17:00	
10/20 Friday	09:30-12:00	小組分享會
	下午	返台

二、參訪香港金管局(HKMA)

➤ 參訪摘要

香港金管局(HKMA)阮國恒副總裁在本次參訪中，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：

- (一) 科技風險；
- (二) 洗錢及恐怖分子資金籌集風險；
- (三) 信貸風險；
- (四) 財富管理業務相關風險。

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。

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：

1. 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。

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。

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。

5. 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) 內控的第二、三、四(董事會)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。

三、參訪中國銀行(香港)

➤ 參訪摘要

- (一) 參訪中國銀行(香港)概述
- (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

(一) 概述：

中國銀行(香港)(下稱「中銀」)今年適逢成立百年，有 200 家分行、1,000 多台 ATM，為香港三家發鈔銀行之一，亦為香港人民幣業務的清算銀行。中銀 2016 年底總資產 2.3 兆港幣、稅前淨利 295 億港幣。總員工 13,000 人、平均年齡 38.25 歲，40% 碩、博士學位；稽核人員約 130 餘人、占 1%。內部稽核是一非常古老而年輕的話題，監管的要求從未有底線。中銀業務朝集團化、跨界經營、跨區域經營。因應 FinTech 衝擊，稽核人員集合 IT、風險、法律等人才以系統化、規範化，促進穩定經營，提升銀行價值。

(二) 三道防線機制：

中銀具有一套成熟的三道防線機制，全行各級機構、各業務管理部門和每個員工在承擔業務發展任務的同時也承擔內部控制的責任，是內部控制的第一道防線，通過自我評估、自我檢查、自我整改、自我培訓，實現自我控制。法律合規部門與業務條線部門負責統籌內部控制制度建設，指導、檢查、監督和評估第一道防線的工作，是內部控制第二道防線。稽核部門負責通過系統化和規範化的方式，檢查評價全行經營活動、風險管理、內部控制和公司治理的適當性和有效性，是內部控制的第三道防線。

(三) 風險導向的內部稽核：

1. 董事會及管理階層的任務：

- (1) 由董事會負責評估及釐定中銀達成策略目標時所願意接納的風險性質及程度，確保中銀設立及維持合適及有效的風險管理及內部監控系統，並監督管理層對風險管理及內部監控系統的設計、實施及監察，根據董事會的授權範圍，管理層負責日常運作及各類風險管理工作，

而管理層需向董事會確認所提供的有關系統是否有效。

- (2) 風險管理及內部監控系統旨在管理而非消除未能達成業務目標的風險，並只能對不會有重大的失實陳述或損失作出合理而非絕對的保證；並管理運作系統故障的風險，以及協助達致中銀的目標。除保障中銀資產安全外，亦確保保存妥善的會計記錄及遵守有關法例及規定。

2. 每年進行風險檢討及評估：

中銀每年對風險管理及內部監控系統的有效性進行檢討，涵蓋所有重要的監控方面，包括財務監控、運作監控及合規監控以及風險管理。有關檢討工作是以監管機構及專業團體的指引、定義為基礎，根據監控環境、風險評估、控制活動、訊息與溝通及內部監督的五項內部監控元素進行評估，涵蓋所有重要的監控及措施，包括財務、運作及合規和風險管理功能；檢討範圍亦包括會計、財務匯報、內部審計職能的資源、員工資歷和經驗及培訓的足夠性。有關檢討由中銀內部審計部門統籌，透過管理層及業務部門的自我評估，並經管理層確認有關系統的有效性，內部審計部門對檢討過程及結果進行獨立檢查及後評價工作。

3. 建立且落實執行各項監控程序及措施：

- (1) 建立相應的組織架構和各級人員的職、權、責，制定了書面的政策和程序，對各單位建立了相互牽制的職能分工，合理地保障各項資產安全，並能在合法合規及風險控制下經營及運作；
- (2) 管理層制定並持續監察中銀的發展策略、業務計劃及財務預算的執行情況，並已設置了會計管理制度，提供衡量財務及營運表現的依據；
- (3) 中銀制定相應的風險管理政策及人力資源管理政策，對信譽、策略、法律、合規、信貸、市場、業務操作、流動性、利率等風險均設既定單位和人員承擔職責及處理程序，並建立了處理及發佈內幕消息的程序和內部監控措施；並另制定了及時識別、評估及管理各主要風險的機制，建立相應的內部監控措施，及解決內部監控缺失的程序；
- (4) 中銀的資訊科技管制架構，設有多元化的資訊系統及管理報告，包括各類業務的監察資料、財務資訊、營運表現等，為管理層及業務單位、監管機構等提供衡量及監控的訊息；各單位、層級亦已建立了適當的溝通管道和匯報機制，以確保訊息的交流暢通；
- (5) 中銀內部審計部門採用風險為本的評估方法，根據董事會轄下審計委員會批准的內部審計計畫，對財務範疇、各業務領域、各風險類別、

職能運作及活動進行獨立檢查，直接向審計委員會提交報告。內部審計部門對須關注的事項及須改善的方面有系統地及時跟進，並將跟進情況向管理層及審計委員會報告；及

- (6) 審計委員會審閱外部會計師在年度審計中致管理層的報告以及監管機構提出的風險管理及內部監控建議，並由內部審計部門持續跟進以確保有計畫地實施有關建議，並定期向管理層及審計委員會報告建議的落實情況。

4. 滾動式調整年度審計策略：

中銀制定審計策略結合銀行策略及業務策略綜合制定，定期檢討以往年度工作計畫的落實情況，並結合來年年度工作計畫，以滾動方式適當地調節三年計畫。

5. 建置適當地風險評估模型：

- (1) 依項目風險評級，設定銀行的固有風險，而所謂固有風險主要係根據各風險的影響及發生的可能性進行評級，以中銀為例，其設定八大風險分別為：市場、利率、信貸、流動、策略、操作、信譽及合規。
- (2) 設定完成固有風險後，應檢視就各該固有風險是否有相對應的控制措施，以確認各該固有風險是否適當地被控制且各該控制措施是否有效地被執行，並據此設定控制風險的風險值高低。
- (3) 完成檢視固有風險及控制風險後，產生各風險項目的剩餘風險，並依據各項目風險值高低，訂定一至三年不等的審計週期。

(四) 質量管理：

1. 遵循香港金管局(HKMA)要求：

對內部審計職能進行獨立審查，並就內部審計職能進行監管評估，評估範圍應確認使否具有充足資源、獨立性及權力等，評估內容應包括政策與程序的適足性及妥適性，並據以提出改善建議。

2. 遵循國際內審協會(IIA)要求：

建立並維護質量保證與改進程序，包括內部評估及外部評估、向高階管理層級及董事會報告的結果，並應揭露未遵循事項及其影響。

3. 中銀內部審計功能有效性評估的 5P 模型：

- (1) Profile：權責、獨立性及客觀性。
- (2) People：人員資歷、專業能力、規模及持續培訓。
- (3) Plan：年度計畫制定、執行及完成情形。
- (4) Performance：管理及質量控制。
- (5) Product：報告及改善建議。

(五) 變革與挑戰：

為因應國際金融環境之快速變化及監理機構日趨嚴格之要求，內部稽核職能需先進化，並加速調整變革的步伐，以迎向未來的挑戰。內部稽核所需面對之挑戰如下：

1. 高端人才相對缺乏。
2. 反洗錢監管要求提高。
3. 新科技及大數據時代下的內部稽核革新。

(六) 高階管理層的期望：

1. 中銀高階管理層首先著重在問題發生之問題導向，大致分類為系統性問題、苗頭性問題、趨勢性問題及重要性問題等不同面向的問題思考解決之道。
2. 其次，就問題本身則提倡所謂的「五見」，即見人、見事、見原因、見機構及見責任。其寓意在於探究並釐清問題發生之根本原因，是否有人為疏失？事件之起因為何？何以會發生此類問題案件？發生問題時各相關單位如何應對？就問題個案是否有相對應疏失人員應負責任之處。
3. 再者，其強調「查改一體化」，亦即檢查發現問題的同時，就要進行問題改正，以避免類似問題再度發生，強調治標並治本的查核觀念。
4. 最後，中銀強調，有足夠相對應的資源投放，才會有健全及有效率的內部控制及稽核制度，因此如何建置一支完善的查核團隊，是該集團高階管理層非常重視的項目。

高階管理層的期望



資料來源：中國銀行(香港)簡報資料

四、參訪東亞銀行

➤ 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，充實自己的專業知識，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

2016 年世界經濟論壇(WEF)創辦人兼執行主席 Klaus Schwab 向人們宣告「第 4 次工業革命」的到來，第 4 次工業革命將數位、物理及生物技術融合在一起迸發出強大的力量影響著所有的知識領域、經濟及工業。物理技術方面的科技有無人駕駛汽車、3D 打印、機器人等；數位技術方面則有人工智慧、物聯網、共享經濟等；生物技術方面則有 DNA 定序、合成生物學等，正因為人工智慧及機器人等科技快速發展，稽核人員應加強資訊相關專業技能，才能趕上未來稽核需要。

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。



資料來源：東亞銀行簡報資料

此外「第4次工業革命」所帶來的人工智慧、機器人及生物科技的發展，將對未來工作機會造成衝擊，依世界經濟論壇(WEF)預測在未來的5年內，將會有500萬個工作機會因此消失。另對稽核人員及會計人員之影響，依經濟學人之研究報告預測，於20年內約90%以上之稽核人員及會計人員將被機器人取代，因此對所有稽核從業人員均應時時警惕，並加強自身的專業技能，以因應未來的衝擊。



資料來源：東亞銀行簡報資料

(二) 科技的發展對稽核業務而言是危機也是轉機

1. 持續性稽核及風險提示

現在所有的資料已數位化，儲存於內部網路的各個伺服器中，因此當我們發現問題時可以藉由持續性稽核工具大量抽查，對問題進行深入了解，以決定是冰山一角或是個案；另現在對稽核之要求不僅是發現缺失提出檢查意見，而是要在問題發生前即能防範於未然，透過持續性稽核工具及相關報表持續監控各項風險點，若發現問題透過風險提示要求各相關單位改善。

風險提示是東亞銀行執行持續性稽核的一項措施，它並不屬於稽核作業，但仍要求相關單位在規定期限前對稽核單位發現之問題，確認並執行改善，相關單位並不需要將改善情形回覆稽核單位，惟稽核仍單位將透過持續性稽核工具監控改善情形，如果有需要將採取適當的稽核措施。

持續性稽核(Continuous Auditing, CA)由第三道防線稽核人員執行，於日常中持續性監控稽核相關的作業活動，包括自動鑑識例外及異常事件、分析趨勢及測試控制措施之有效性等。

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。

2. 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。

3. 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：

(1) 以往的網絡攻擊，主要針對以 Windows 平台為主的個人電腦，不過隨著智能手機成為每個人的隨身電腦開始，網絡攻擊的目標已經漸漸轉移到手機上面；其中針對 Free WiFi 的攻擊方式，即為中間人攻擊(Man-in-the-Middle Attack, 縮寫：MITM)，毋須在手機上安裝任何惡意軟件，而且不著痕跡，令人防不勝防。

中間人攻擊(MITM)是指攻擊者與通訊的兩端分別建立獨立的聯繫，並交換其所收到的資料，使通訊的兩端認為他們正在通過一個私密的連線與對方直接對話，但事實上整個對談都被攻擊者完全控制。

(2) 中間人攻擊(MITM)難以防禦之處在於：

- 駭客在進行竊聽時，一般網路活動仍能正常運作不會斷線，故鮮少有人會主動發現。
- 使用者電腦上不會被安裝木馬或惡意軟體，也難以被防毒軟體發現。
- 駭客在欺騙網路協定時，雖然可能會留下一些蛛絲馬跡，但基於效能與磁碟空間考量，網路裝置一般而言都不會保留太多紀錄檔，造成事後追蹤極為困難。

(3) 受制中間人攻擊(MITM)的影響

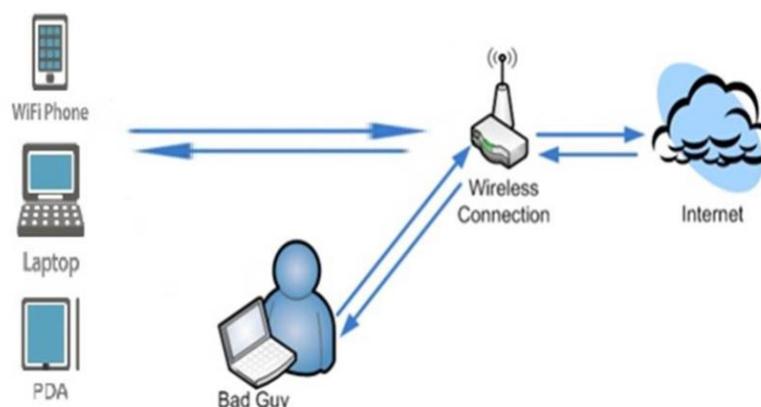
駭客會竊取受害者以手機透過 Free WiFi 連接網站時登錄之帳號及密碼，使任何有密碼保護的各種網路服務將喪失保護(如網路銀

行、社群網站、Webmail 等)，將造成金錢損失、遺失個人資料及信用卡資料等。

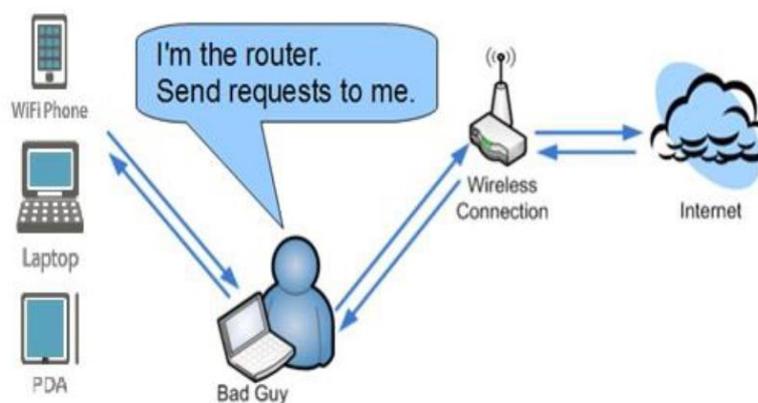
(4) 如何預防中間人攻擊(MITM)

- 只有需要使用 WiFi 時才打閉 WiFi，使用完畢即關閉。
- 如要使用 Free WiFi 不要輸入密碼及信用卡等資料。
- 盡量避免連結 Free WiFi。
- 移除已於內儲存之「無線網路名稱(SSID)」。
- 應隨時注意手機作業系統及應用軟體是否有應安裝最新的修補程式。
- 若手機出現不正常遲延、當機或出現警告訊息請馬上中斷網路。

Scenario setup



Man-in-the-Middle (“MITM”) Attack



資料來源：東亞銀行簡報資料

(三) 顛覆內部稽核之傳統思維

1. 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。
2. 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。
3. 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

1. 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。
2. 隨時將新出現的風險因子納入稽核範圍。
3. 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。
4. 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

1. 對各項業務應有深刻的認識，並了解風險所在。

2. 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。
3. 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。

五、參訪渣打銀行

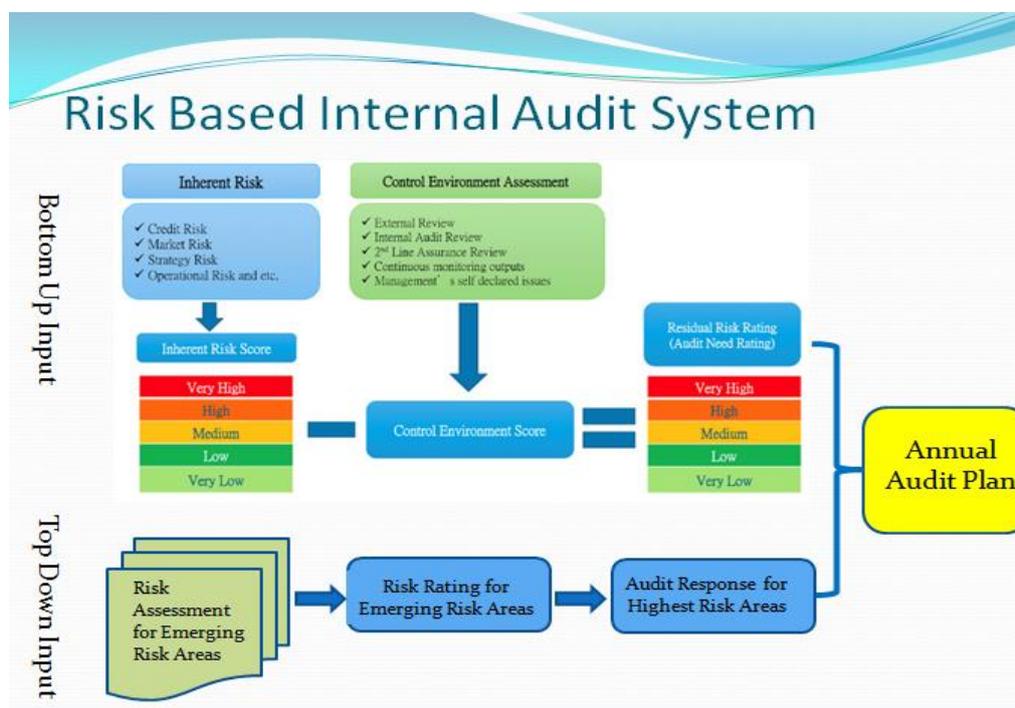
➤ 參訪摘要

- (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 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。



資料來源：渣打銀行簡報資料

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。

2. Defined Auditable Entities 定義受查主體

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。

3. 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

4. Quantitative and Qualitative Risk Factors 量化及質化風險因子

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。

5. Integrated Audits 整合式稽核

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」：

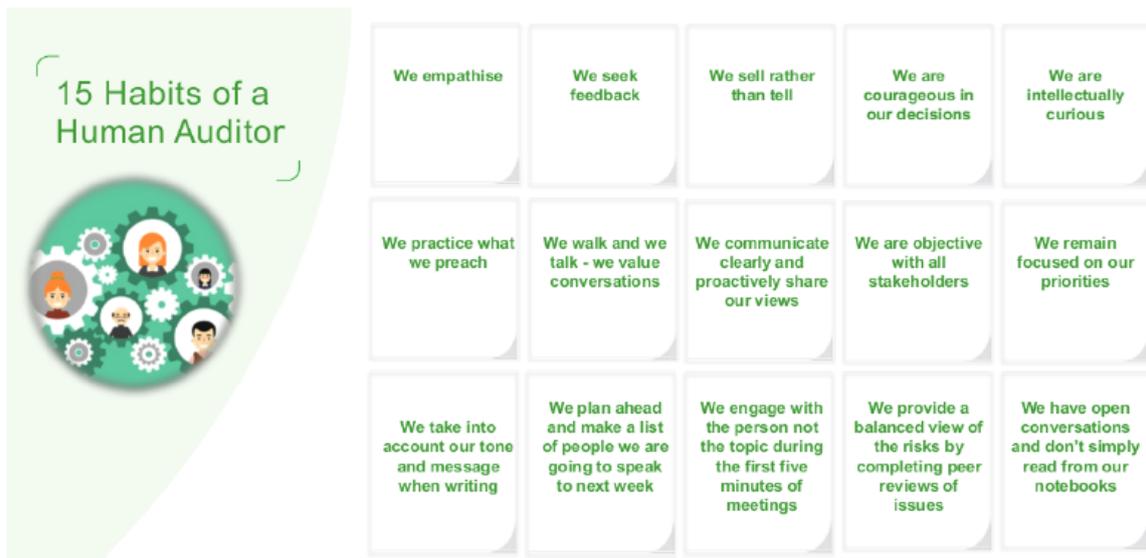
1. 稽核人員需要轉型，傳統上對稽核人員之印象是保守、嚴肅，沒有笑容，然面對現今金融環境之快速變遷，稽核人員更需改變與轉型，高管階層對內稽人員有所期待，要求稽核獨立並具效率，不要讓高管階層 surprise，期待能以更具效率之方式提出稽核之看法。
2. 需提升稽核人員之專業形象，增進查核效能並採敏捷行動，以具說服力及堅定之立場將稽查意見與受查單位充分溝通，讓組織打破對稽核人員刻板印象，稽核人員也應加強數據分析之能力，以強化稽核人員之工作技能。

(三) 稽核人員如何面對未來之挑戰

1. 提升稽核人員之專業能力，不僅要加強金融專業知識，還需增進電腦知識及增加對其他業務專業知識之涉獵，所以稽核部門要有不同領域的同仁，形成好的團隊互相學習與合作，使團隊更加多元。
2. 稽核人員要利用各種數據分析，快速敏捷的將稽核結果與受查主體溝通。
3. 主動積極參與交流及學習分享。

(四) 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 (如下圖所示)可作為稽核人員行為之參考及借鏡。

15 Habits of a Human Auditor



資料來源：渣打銀行簡報

(五) 「Audit Strategy on Overseas Operation 海外業務稽核策略」

海外業務稽核策略不僅需了解當地語言，亦需了解當地之一般文化，並給予跨國支持與協助，同時需在權力下放與集中化之間取得平衡，並要增加數據分析的使用，強化對海外業務進行持續監控。

六、參訪星展銀行

➤ 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)：

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：

1. Audit Universe：受查單位規模、業務風險等
2. Risk Assessment：Based on Basel 九項風險評估因子為評估架構
3. Key Audit：考量全球性、區域性等業務重點，訂定前十大查核重點
4. Audit Project
5. Sampling →Computer Assisted→Audit Ratings

(五)持續性稽核：

透過 ERICA(Early Risk Identification and Continuous Assessments), Computer Assisted Auditing Technique, (1)即早發覺問題，回饋給一、二線單位、(2)Narrow Down Our Audit Scope、(3)Adjust Our Review Frequency。

(六)內部稽核新價值

(七)實施風險導向稽核制度思考方向(Auditing Journey)

➤ 參訪內容

(一)三道防線與風險導向內部稽核實務導入

1. 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。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。

2. 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。

3. 風險導向內部稽核實務導入

(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) 訂定內部稽核規章。
- (4) 與第二道防線溝通交流。
- (5) 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。
- (6) 訂定風險類型-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：流動性風險、利率風險、信用風險、作業風險、市場風險、信譽風險、策略風險、法令遵循風險、科技風險…等。
- (7) 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。
- 固有風險：係指在未採取任何措施改變風險發生的可能性及影響的情況下，達成目標的風險。
 - 控制風險：如採取的適當控制措施被有效的執行，其控制風險水平評為低，反之則為高。
 - 剩餘風險：係指固定風險採取控制措施後剩下來無法達成目標的風險。

固有風險		發生可能性		
		高	中	低
影響程度	高	高	高	中
	中	高	中	低
	低	中	低	低

剩餘風險		控制風險		
		高	中	低
固有風險	高	高	高	中
	中	高	中	低

	低	中	低	低
--	---	---	---	---

(8) 持續監控及蒐集內外部資訊，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。

甲、國內、外主管機關監理重點、其他個別指定事項與重要法令異動及金融環境變化；

乙、銀行經營策略目標與重要政策變化；

丙、業務營運管理資訊及重要監控指標；

丁、主要利益關係人意見；

戊、重大風險事件發生情形。

(9) 擬定年度查核計畫-以風險為本的原則依據風險評估結果擬定，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。

(10) 實地查核。

(11) 產出內部稽核報告。

(12) 辦理內部稽核執行品質之評核。

(二)內部稽核組織、管理與人才發展模式如何與時俱進

1. 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。

2. 人才發展

- (1) 配置具有一定學歷、經驗、專業知識及之內部稽核人員，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，提升稽核與業務專業知能及養成多構面管理能力。
- (3) 稽核轉型：
 - 具備電腦與資訊安全的專業能力，從懂電腦的稽核人員到懂稽核的電腦人員。
 - 具備多構面管理能力(如溝通、協調、分析、前瞻性…等)，能從動態環境中確認風險。

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。

(三)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。

1. 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；
- (4) 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、隱私保障和產品適合度。
- 2. 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。
- 3. 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

- 1. 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。
- 2. 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。
- 3. 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) 規章制度之訂定一如公司治理、恰當的獎勵制度；
 - (3) 公平待客原則一如：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。

七、參訪 PwC HK

➤ 參訪摘要

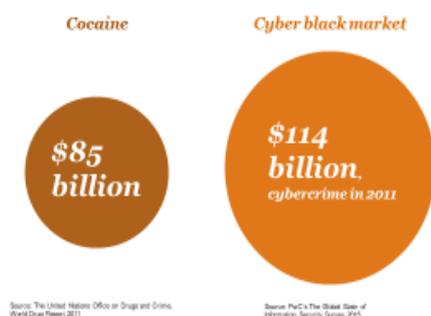
- (一) 網路安全之概述
- (二) 監理機構推動的網路趨勢
- (三) 香港金融監理局(HKMA)推動之網路防衛計劃
- (四) Intelligence-led cyber attack simulation testing (“iCAST”) 點對點攻擊模擬

➤ 參訪內容

(一) 網路安全之概述：

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，對金融業而言更重要的是如何透過創新科技的應用來加速發展，但也會對銀行增加新的風險，及對金融監理機構增加監管的困難。

Cyber black market is bigger than the “cocaine” market



People aren't robbing banks anymore...

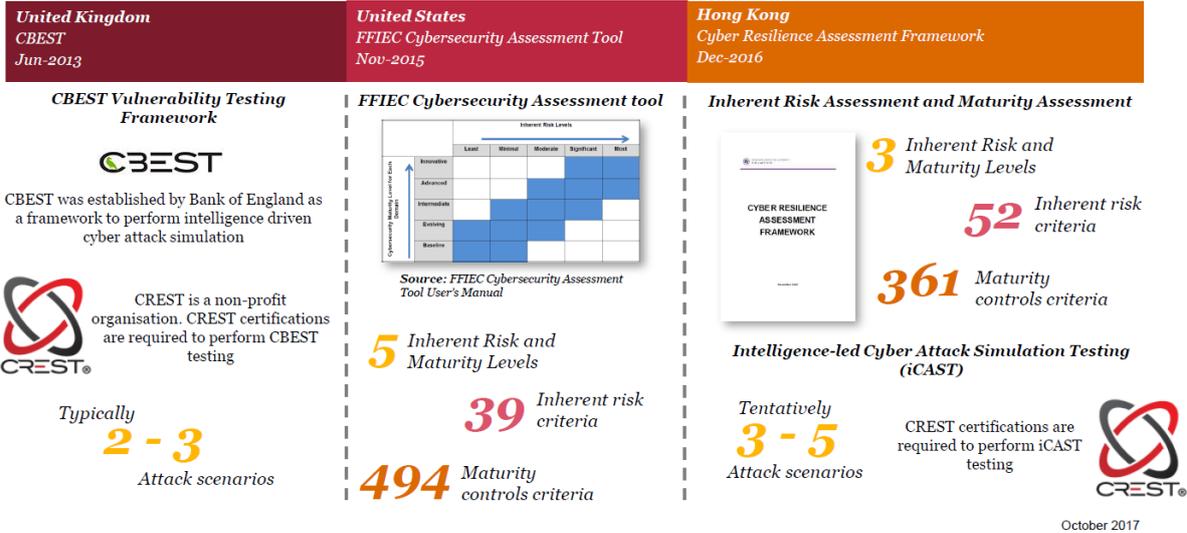


資料來源：PwC HK 簡報

(二) 監理機構推動的網路趨勢

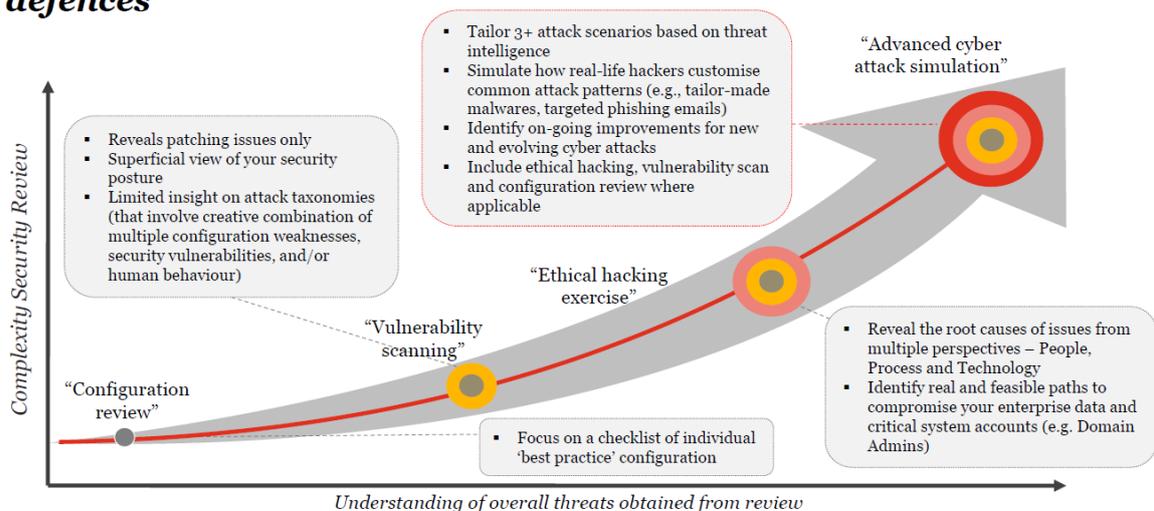
網路釣魚 mail 頻傳、駭客攻擊風險，網路安全管理更形重要，影響金融機構在風險管理方面的布局。為此，金融機構勢必須投入更多的時間及資源，以更積極的態度來因應風險。因此香港金融監理局(HKMA)推動網路防衛計劃(Cyber security Fortification Initiative)係為提高香港銀行業抵禦網路攻擊的能力。

Cybersecurity initiatives from financial regulators



資料來源：PwC HK 簡報

Moving from assessing IT Controls to validating Cybersecurity defences



資料來源：PwC HK 簡報

(三) 香港金融監理局(HKMA)推動之網路防衛計劃

香港金融監理局(HKMA)推動之網路防衛計劃(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」，以期擴大訊息分享來源。

1. 香港金融監理局(HKMA)網路安全規範(Cyber security Fortification Initiative)：

香港金融監理局(HKMA)於 2016 年 12 月 21 日發出的通函

The HKMA has taken on board many of the industry's comments received during the consultation in finalising the C-RAF. In terms of the implementation timeline, the industry has raised a practical issue concerning the availability of qualified assessors to undertake the assessment. Taking this concern into account and having regard to overseas experience, the HKMA will adopt a phased approach to implementation as follows:

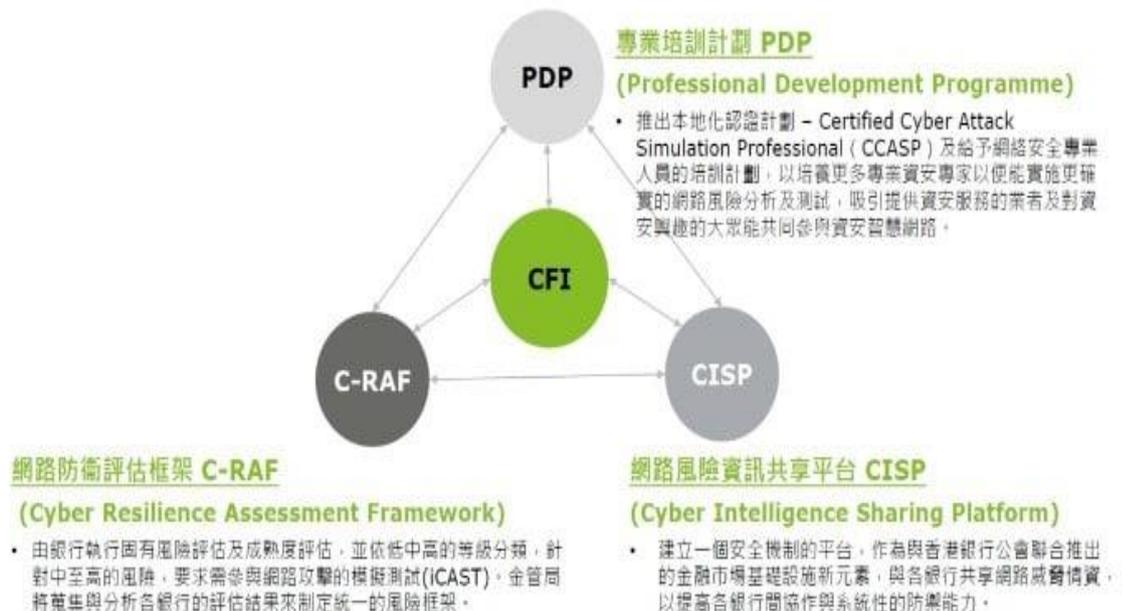
(i) The first phase will cover around 30 AIs including all major retail banks, selected global banks and a few smaller AIs. The HKMA will inform these AIs individually;

(ii) The expected timeline for completing the C-RAF assessment under the first phase is:

- Inherent Risk Assessment and Maturity Assessment End-September 2017
- iCAST (if applicable) End-June 2018

(iii) Depending on industry feedback and the experience gathered from the first phase, the second phase will cover all the remaining AIs. They will be expected to complete the Inherent Risk Assessment and the Maturity Assessment by the end of 2018. The HKMA will take into account the assessment results of the second phase in determining a timeframe for the remaining AIs to complete the iCAST. Although AIs covered in the second phase are given a longer timeframe for implementation, they should familiarise themselves with the C-RAF and take steps to strengthen their cyber resilience at an early stage where necessary.

資料來源：PwC HK 簡報



資料來源：PwC HK 簡報

2. 網路安全防衛評估：

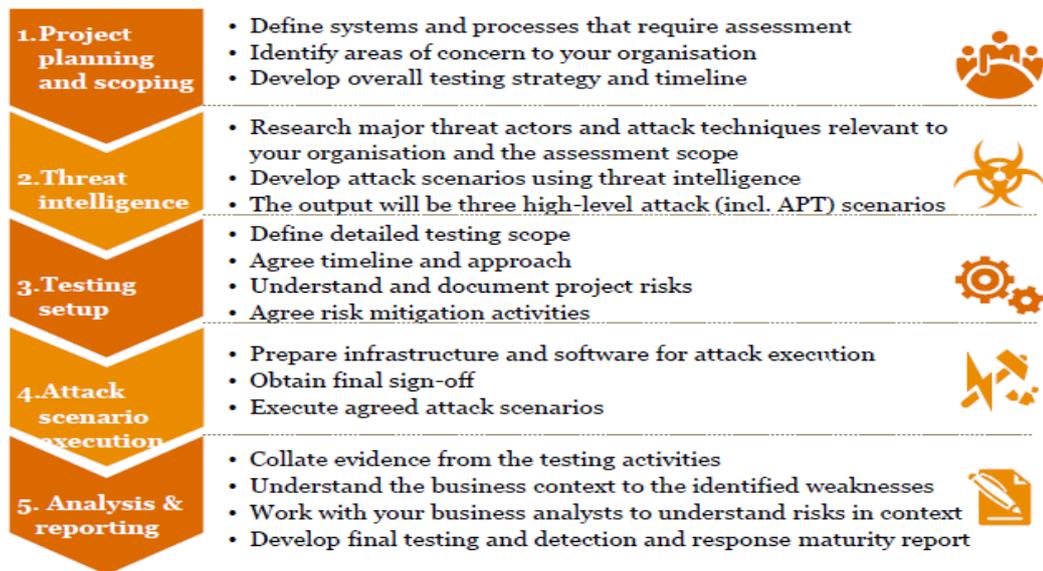
網路防衛評估框架建議因應作法



資料來源：PwC HK 簡報

(四) Intelligence-led cyber attack simulation testing (“iCAST”) 點對點攻擊模擬

情報主導的網路攻擊測試 Intelligence-led cyber attack simulation testing (iCAST)是點對點網路攻擊類比測試框架，利用情報主導的網路攻擊情景，評估各銀行對網路攻擊的識別及回應能力。



資料來源：PwC HK 簡報

八、參訪滙豐銀行

➤ 參訪摘要

(一)HSBC-HSBC Internal Audit Structure

1. 集團內部稽核章程
2. 集團內部稽核單位的組織架構
3. 三道防線組成模式
4. 風險導向的內部稽核
5. 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)

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

➤ 參訪內容

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

1. 目的(Purpose)

- (1) 集團內部稽核單位的主要角色是以幫助董事會及高階管理層來共同保護滙豐集團的資產、聲譽，及確保集團的永續經營為其目標。
- (2) 集團內部稽核單位就管理層所規劃並運作的集團風險管理體系、控制與治理流程，關於其規劃與作業方面的有效性，提供獨立且客觀的確信。

2. 權威性(Authority)

- (1) 集團內部稽核單位得到集團審計與風險委員會及集團董事會的充分授權，可以在工作上不受限制且不限時間地接觸所有的集團文件紀錄、人員、財產及作業。
- (2) 集團總稽核的資格、任命與解職係由集團審計委員會來批准。
- (3) 集團總稽核在功能上係向集團審計委員會主席報告，而在行政上則需向集團行政總裁(Group Chief Executive)報告。

3. 獨立性(Independence)與客觀性(Objectivity)

- (1) 獨立性是集團內部稽核單位在工作上的最根本的要求。同時，集團內部稽核單位應該具有不偏不倚的公正態度並且要避免有任何的利益衝突情

形。

- (2) 集團內部稽核單位在決定稽核對象、範圍、程序、查核頻率、查核時程或報告內容上都應該保持獨立不受任何因素所干擾，以維持一個必須的獨立且客觀的心理態度。

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

- (1) 集團總稽核的職責如下：

- 甲、 每年向審計委員會提出風險為本的稽核計畫與工作方案；
- 乙、 執行被批准的稽核計畫，包含監管或是當地審計與風險委員會所要求進行的法規上或是特別的工作；
- 丙、 招募、適性發展與留用有適當技能、知識、經驗與專業資格的員工。此外，對於特定的專業領域，集團內部稽核單位可以採取共享資源及客座稽核員的方式來支援稽核工作；
- 丁、 就在稽核活動中發現的關鍵議題定期向審計與風險委員會報告；
- 戊、 監督與控管集團內部稽核單位的日常運作。

- (2) 稽核工作的結果與對整體風險管理與控管架構的評估應該被適當地報告給集團及當地的審計與風險委員會。

- (3) 集團內部稽核單位應該與當地外部稽核保持良好的工作關係，外部稽核人員應該知悉集團內部稽核單位的活動與結果，而且可以接觸到內部稽核報告與相關的佐證文件。

- (4) 對於防舞弊措施的有效性，集團內部稽核單位應該提供獨立的確信。當有重大舞弊案發生時，集團內部稽核單位應該要去檢視案件的本質和最近稽核檢查覆蓋範圍的正確性以確保舞弊案件可以/應該被發現，並且確保可能發生舞弊可能的控制弱點都能被偵測出來。

(二) 集團內部稽核單位的組織架構：

區分為以下五個區域：

1. 歐洲地區(Europe)
2. 美國地區(U.S.)
3. 亞太地區(Asia Pacific)：其下轄有大中華區(Greater China)，此區包含有中國大陸、香港、澳門及臺灣。
4. 拉丁美洲及加拿大地區(Latin America & Canada)

5. 中東與北非地區(Middle East & North Africa)

(三) 三道防線組成模式

1. 第一道防線：每位員工要為其日常業務中所產生的風險負責，第一道防線要確保所有操作過程中的主要風險都能被識別出來，並且能夠適當地被內部控制所減緩或監控。第一道防線既是風險的擁有與管理者，也是控制活動的設計者，需要發展出適當的控制活動來降低風險或是監控風險的發生。
2. 第二道防線：如：風險管理(Risk Management)、財務管理(Finance)、法規遵循(Compliance)等單位，負責制定規章制度(policy)或是作業規範(guideline)供第一道防線去遵循，並且在第一道人員有疑問時，可提供一些建議或指導。此外，第二道防線還要監督第一道防線的日常活動是否符合規章制度或是作業規範的要求。
3. 第三道防線：由集團內部稽核單位擔任，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。其下除了有稽核檢查團隊(testing team)與整改驗證團隊(validation team)分別負責稽核檢查與整改驗證工作之外，尚設置有稽核品質確認團隊(quality assurance team)，負責獨立測試前二個團隊的工作品質，因此這個團隊也有第 3.5 道防線之稱。

(四) 風險導向的內部稽核

1. 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)：
 - 甲、固有風險(Inherent Risk)
 - 乙、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。
 - 丙、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。

2. 稽核種類(Types of Audit)

(1) Processes and Controls Audit：

在同一個稽核實體內，針對特定的流程或控制所做的查核。

(2) Thematic Audit：

主題式查核，針對同一主題在不同稽核實體內辦理的查核。

(3) Risk Governance Framework (RGF) Audit：

治理架構風險查核。

(4) Regulatory Audit：

針對法規或是主管機關要求而辦理的查核。

(5) Investigation and Special Audit：

調查式或特別查核，如：舞弊或客訴案的查核。

(6) Project Audit：

專案查核，如：針對新系統或新流程所辦理的查核。

(7) Branch Audit：

針對一般分行所辦理的查核。

3. 持續監控(Continuous Monitoring)：

目的在確保集團內部稽核單位對稽核範圍(Audit Universe)的認知是與現況相符的、確認集團內部稽核單位的風險評估是最新的、找出重大的風險變化、及時提供新生風險的預警。

(五) 內部稽核功能之轉型

1. 現今高階主管對內部稽核的期許(Expectation of Top-Level for IA)

(1) 成本效益：希望內稽人員能夠發現多餘的控制，以節約成本支出。

(2) 找出潛在更為有效率的作業模式。

(3) 改善控制方式。

(4) 對現狀提出質疑來降低風險。

2. 內部稽核如何回應高階主管對內部稽核的期許：

(1) 人員(People)方面：人員須具備技能、專業知識與能力、溝通技巧，並

給予適當的訓練及發展機會，注重專業資格的取得，招募與留用關鍵有天賦的員工等。

- (2) 流程(Process)方面：過程要注重分析性、採取動態風險評估模式、持續性監控並適時調整稽核計畫、採用品質確認與協助改善的稽核程序。
- (3) 系統(System)方面：採用標準稽核管理系統，將關鍵績效指標(key Performance Indicator)的表現與缺失改善追蹤納入管理。

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

1. 文化(Culture)的定義：

- (1) 所謂文化，就是指「在這裡做事情的方式」，也是我們工作的態度 (Culture - It's the way we do things around here.)。引導企業中的人們如何進行工作和自我行事的非正式，不成文的指導。
- (2) 文化可簡單定義為「共同做事方式」，根據 G30 對金融機構文化定義，是指組織的價值觀(Values)與行為(Conduct)，此二者可以塑造組織文化，由於價值觀(Values)與行為(Conduct)可觀察及衡量，且被規範於各種準則與標準中，因而提供了檢視、改善與稽核組織文化的平台。
- (3) 優良的文化是建立在雙向溝通，以合作方式決策，團隊合作把工作完成。了解組織文化可藉由檢視一個組織對主管機關態度、與客戶關係、對組織而言甚麼是重要的、如何對待員工、對負面事件反應、對競爭者與同業之態度。

2. 文化的形成主要由行為開始，產生價值(Value)，再演變成文化，因此對於銀行現有之文化及行為應進行衡量，以評估現有之文化及行為是否會產生風險：

- (1) 在發生風險的缺失或事件中，應瞭解衍生問題的根本原因，對於缺失肇因於公司文化下的行為風險，惟有從根本治起，才能真正改善。
- (2) 導致稽核缺失發生之銀行文化及行為，是否嚴重到足以影響之業務運作。
- (3) 應對稽核缺失建立管理行動，並區分管理行動之等級(滿意/須改善/不滿意)
- (4) 銀行應該調整對風險文化整體思維方式，以避免風險發生。
- (5) 對於因銀行文化及行為之產生之缺失，應依公司治理之精神，提高問責制。

(6) 建立績效管理和激勵制度使同仁樂於遵循正確之文化及行為。

(7) 透過員工發展和推廣，建立正確之文化及行為。

(8) 建立有效的三道防線。

3. 查核與評估面向

查核組織文化時，下列事項可納入考量，內部稽核人員應確認查核項目適合其組織，且能聚焦於該組織所處之特有環境、機會與競爭。

(1) 對員工滿意與意見關心程度

甲、員工對錯誤行為與揭發內容一致性之看法；

乙、員工對同儕環境與組織文化之認知；

丙、員工對高階管理層經營理念之認同；

丁、員工對遵法及道德標準之看法；

戊、員工及顧客問卷調查結果；

己、客訴案件。

(2) 訓練

甲、現行對新進及現任員工全面性訓練計畫，以及依員工在組織內角色，安排合適之訓練；

乙、訓練頻率與出席情形；

丙、評估訓練有效性之機制。

(3) 遵法

甲、對吹哨者職位及權益的保護；

乙、組織面臨法令問題的頻率；

丙、由內外部稽核發現風險及控管問題的數量，與自我發現、自願揭露及主動提出的數目做比較；

丁、及時與有效的改善措施。

(4) 人力資源、激勵與強化措施

甲、組織遭媒體負面報導頻率。

乙、違反規定遭懲罰的適當性與一致性。

丙、對無心之過(Honest Mistakes)處理方式的妥適性。

丁、離職率。

戊、是否有辦理離職員工訪談，訪談之問題是否可以評估離職者已發現公司內部有非道德事件正在發生。

(5) 非正式控制(Soft Controls)之證據

- 甲、能力：適應力強及願意學習。
- 乙、信任及開放。
- 丙、強有力的領導：以身作則方式領導。
- 丁、高預期：努力改善，提高標準。
- 戊、價值分享：在正確時間做正確的事。
- 己、高道德標準。

4. 如何稽核「文化」

- (1) 善用可用資源：並非所有組織文化面項皆須辦理查核，需要注意查核困難度及查核限制等因素，善用現有資源辦理查核。
- (2) 檢視員工參與感(Employee Engagement)調查報告，或組織滿意度與預期績效表現等相關調查結果，可探究該等結果與查核發現的差異。
- (3) 董事會、審計委員會與管理階層的支持
- (4) 要決定最適合組織的查核組合工具或方式；另外亦要決定查核範圍。
- (5) 加強稽核人員「文化」查核訓練。
- (6) 要確認稽核人員沒有因主觀資料而導致錯誤的結論，因此在查核任一階段都需要與管理階層溝通。

5. 匯豐銀行對行為及文化風險稽核，已設有相關查核問卷(Audit everywhere)，不論執行什麼樣的稽核主題，都會先請受檢單位填寫問卷，再由稽核評估。目前該問卷有9個評核事項，每年檢視妥適性。

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

1. QAIP 的定義

依據國際內部稽核協會(IIA)發佈之準則，內部稽核主管須訂定及維持一套涵蓋內部稽核單位所有層面之品質保證與改善計畫，用以促使評估內部稽核單位對於內部稽核定義及遵循國際內部稽核執業準則情形以及評估內部稽核人員是否遵守職業道德規範，該項計畫亦評估內部稽核單位之效率及效果，並辨識改善之機會。

2. Five Key Characteristics -the Foundation of an Effective QAIP

Five Key Characteristics the Foundation of an Effective QAIP

1. Policy

1. The internal audit activity charter establishes the requirement for the QAIP.
2. The internal audit policy and procedure manual requires the QAIP.
3. The CAE is responsible for establishing and maintaining a QAIP.
4. The CAE communicates the results of the QAIP to senior management and the board.



2. Methodology and Process

1. The QAIP methodology is based on The IIA Standards and related Implementation Guidance.
2. The QAIP requirements are documented in the internal audit policy and procedure manual.



3. People

1. Internal audit staff are aware of their responsibilities related to the QAIP and have received appropriate training.
2. Personnel who are assigned responsibility for the implementation of the QAIP are independent and objective.
3. Periodic internal quality assessments are performed by internal audit staff with strong experience in internal auditing and a deep understanding of the Standards.
4. External assessments are conducted by qualified personnel who are independent from the organization.



資料來源：渣打銀行簡報

Quality Assurance & Improvement Program

4. Systems and Information

1. A standardized audit management system is used to document workpapers and can be heavily relied upon during the quality assessment process.
2. Relevant key performance indicators that are monitored and used during the internal quality assessment process are supported by company systems.



5. Communication and Reporting

1. The results of periodic internal assessments are summarized and discussed with audit management and action plans for improvements are developed and implemented.
2. The results of periodic internal assessments are reported to and reviewed with senior management and the audit committee.
3. Client feedback is solicited from each client and documented within the workpapers to assist in continuous improvement of the internal audit processes.
4. External assessment providers deliver qualitative and quantitative benchmarks that are reported to both management and the audit committee to facilitate continuous improvements.



資料來源：渣打銀行簡報

3. 有效的「品質保證與改善計畫」五個關鍵特徵

政策	<ul style="list-style-type: none"> ● 內部稽核活動章程(載明「品質保證與改善計畫」的要求)。 ● 建立符合「品質保證與改善計畫」之內部稽核政策和程序手冊。 ● 內部稽核主管負責建立及維護「品質保證與改善計畫」。 ● 內部稽核主管負責將「品質保證與改善計畫」執行結果傳達給高階管理層及董事會。
方法與過程	<ul style="list-style-type: none"> ● 「品質保證與改善計畫」所採行的方法，是依據國際內部稽核協會(IIA)所發佈之標準和相關實施指引。 ● 將「品質保證與改善計畫」所要求之規範，記錄於內部稽核政策和程序手冊。
人	<ul style="list-style-type: none"> ● 內部稽核人員瞭解其與「品質保證與改善計畫」相關之職責，並接受適當的訓練。 ● 負責執行「品質保證與改善計畫」的人員，應具備獨立性和客觀性。 ● 執行「品質保證與改善計畫」，應由具備豐富稽核經驗及對IIA標準有深刻理解之內部稽核人員擔任。 ● 外部評核由獨立於組織外之合格人員或團隊進行。
系統和訊息	<ul style="list-style-type: none"> ● 建立一個標準稽核管理系統，記錄工作軌跡及文件，且可充分被信賴與運用於質量評估程序。 ● 於系統建立相關關鍵績效指標，於內部評核時以進行監控。
溝通和報告	<ul style="list-style-type: none"> ● 稽核管理層應定期摘要及檢討內部評核之結果及改善計劃。 ● 定期內部評核結果向高階管理層和審計委員會報告。 ● 客戶反饋，從每一個客戶及工作底稿文件中徵求，以協助持續改進內部稽核流程。 ● 外部評核單位提供質與量的評估基準，報告管理層和審計委員會，以促進持續性的改善。

4. 品質保證與改善計畫(QAIP)的挑戰

QAIP 團隊人員通常都是由內部稽核單位之資深人員任，主要係因 QAIP 工作在評估內部稽核人員是否遵守職業道德規範，因此 QAIP 團隊人員除具

備金融相關知識外，並需具備相當之內部稽核查核經驗，而這些人員通常在內部稽核單位中都具有重要之工作責任；另主管機關、董事會或審計委員會對 QAIP 團隊日益加重要求之查核責任，且因 QAIP 人員少須負責區域性內部稽核單位之查核，必須經常出差至世界各地辦理稽核業務檢查，工作壓力大，造成 QAIP 人員之高流動性；其次稽核資源之分配偏重內部稽核單位，致排擠 QAIP 團隊等情形，均是銀行高層管理人員須重視，QAIP 團隊與內部稽核單位須溝通協調之挑戰。

八、感想與心得

(一) 組織與管理

1. 銀行實施風險導向內部稽核制度，係透過風險評估之方法，審慎評估稽核範疇內各個受查主體之風險，並依據評估結果決定稽核資源之最有效的配置，聚焦於重要風險並加強查核深度，因此風險導向內部稽核制度著重於銀行本身對於風險的認知及管理。銀行所有單位辦理業務時，應以風險為本之管理為基石，強化三道防線間之功能，相互緊密合作，才能有效進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。

如何推動內部控制三道防線之合作關係：

- (1) 持續於銀行內部推動內控三道防線觀念，協助型塑良好內控文化。
 - (2) 稽核工作與銀行策略目標連結，各項稽核活動攸關銀行策略及策略性風險，多方蒐集及關注與銀行經營風險相關的資訊，俾能即時提出建議，降低銀行經營風險。
 - (3) 透過系統預警監控機制，及時執行風險評估與監督，產生監控表報，回饋一、二道防線單位，並適時地修正稽核重點。
2. 隨著新種金融商品及電子銀行業務之日新月異，銀行傳統業務已不敷大眾需求，內部稽核人員均應與時俱進，拋開舊思維，接受新觀念，透過參訪互相交流不斷吸收金融同業之長處，以達了解世界金融趨勢及吸收新知之效。未來銀行除加強稽核人員對新金融商品之教育訓練外，仍需增進電腦知識之學習及強化其他相關業務專業技能之涉獵，由於銀行業務涉與多樣專業有關，故稽核部門需有不同領域之同仁，以形成良好團隊，藉由彼此間之互相學習與合作，使團隊人才更多元、查核更具效率。

如何提昇稽核生產力及建立稽核工作價值觀：

- (1) 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。
- (2) 盤點稽核人員業務專長，設計每一稽核人員的訓練地圖，實施適切性培訓課程，以建立彼此互補之稽核團隊。
- (3) 參與銀行各項業務會議，與一、二道防線單位互動，延伸稽核的領域，使稽核工作有正向的循環。

- (4) 導入品質保證與改善計畫(QAIP)，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。
- (5) 鑒於金融環境日新月異，稽核人員應研究「員工行為」及「組織文化」查核方式，將監控主題與範圍擴大至更多「員工行為」查核，期能即早發現問題，避免舞弊或重大缺失事件發生。

(二) 查核計畫

1. 此次參訪之香港同業在決定年度稽核計畫時，除參考由下往上(Button Up Input)之因素，即依據受查主體風險分析之結果外，亦同時考量由上往下(Top Down Input)之因素，即依據主管機關、董事會或審計委員會之期望、最近金融環境發生之新興風險評估因子、銀行經營風險、第二道防線(風險及法遵單位)關注重點、評估受查單位各項業務內控措施(如：第二道防線監控情形、內外部查核意見、重大風險事件等)等。亦會對各業務管理單位進行訪談，再依據實際業務執行情形與訪談結果，每年調整各風險因子與風險級距之分數，作為未來編製年度稽核計畫之參考。
2. 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，因此內部稽核應不斷評估風險，以滾動的方式更新稽核計劃，使稽核計劃能契合銀行的目標。

如何訂定更具彈性之稽核計畫：

- (1) 定期對銀行各項核主體(業務/服務/單位等)進行持續性風險評估，以檢討稽核計畫是否適時調整
- (2) 依實地查核結果及場外監控回饋，如銀行各項核主體遇有重大風險變動時，應機動調整查核計畫，優先查核高風險項目，以落實風險為本的稽核制度。
- (3) 在排定稽核計劃時，對於稽核工作人員之分配，不應依現有人力局限稽核檢查工作，而應考量稽核檢查之需求，調派相關專案人力配合查核。

(三) 實地查核

風險導向的稽核制度已成為世界銀行業的趨勢，稽核人員在查核業務時，應以風險為導向之稽核方式，先決定查核之風險因子與控制流程，並加強對高風險因子控制作業流程進行查核。查核作業除相關業務項目外，

應同時關注受查單位個體與整體內控風險文化認知情形是否良好，關切科技及洗錢防制等風險。

如何加強實地查核及場外監控：

- (1) 運用資源並致力開發其他可用工具，將資料分析實際運用於實地查核及場外監控。
- (2) 運用先進的稽核系統，選取有代表性、有較高風險的查核樣本，避免以往盲目的隨機抽樣方式。
- (3) 參考國際銀行的經驗，善用數據分析，發現缺失後可提供分析方法或報表供管理單位進行日常管理。
- (4) 建立持續監控與風險評估機制，並能將各訊息整合。
- (5) 評估已開發成熟的場外監控工具與模式是否能移交給第二防線，納入其日常監控範圍，以收更即時監控之效，協助第二道防線建立更齊備之功能。

九、建議事項

(一) 參採香港金管局(HKMA)金融科技之監理政策：

1. 香港金管局(HKMA)採行原則性監管理念，以風險為本和科技中立之監管原則：
 - (1) 訂定原則性監管大方向，不對細節作規範，可培養銀行檢視自身條件採以風險為本的運作思維模式。
 - (2) 在民眾方便性與安全之間取得平衡，由公共討論形成輿論共識，據以為平衡點而決定監管強度，既對金融科技鼓勵發展也順應民情監管風險安全。
2. 在金融科技監管框架下，原則性監管理念具有彈性且迅速的特點，符合金融科技工具新穎、創新的特性；但另一方面，在負責任創新(Responsible Innovation)的角度，某些重要的基本價值如消費者權益保護、資訊安全及金融犯罪防治等仍有受嚴格監管之必要。
3. 建議可參採香港金管局(HKMA)對於金融科技以原則性監管態度，並站在負責任創新的監管原則下，鼓勵金融科技創新發展。

(二) 積極推動監理沙盒制度：

香港金管局(HKMA)相當積極推動監理沙盒制度，我國現已有行政院所提出本國版監理沙盒之「金融科技創新實驗條例草案」，得一併檢視國內行政程序面是否有彈性運用空間，並應加速法案審議通過流程，以幫助銀行業者在科技迅速進步的現實環境中不致落後腳步。

(三) 建立監管機關與銀行業者之定期性溝通機制：

以香港金管局(HKMA)為例，該局為傳達監管理念及傾聽銀行業者心聲，了解銀行業者對於面對之經營環境挑戰與風險問題，定期與銀行業者辦理交流：

1. 每年與各銀行的董事會分別交流 2 小時；
2. 每年與各銀行的獨立董事單獨座談半小時，以了解獨董功能是否能夠充分發揮；
3. 每半年與銀行高階管理層級 round table meeting；
4. 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。

5. 出席旁聽大型銀行董事會。

(四) 推動銀行業管理階層內控意識評估機制(Management's Control Awareness, MCA)：

1. 加強管理階層內部控制功能，避免過度仰賴內部稽核的查核。
2. 強化銀行業內控文化，內部稽核可將管理階層內控意識評估結果，作為受查單位風險評估項目之一，加強風險性稽核業務之查核。

(五) 強化金融科技發展風險管理：

參考香港金管局(HKMA) 刻正推動之網路防衛計劃(Cyber security Fortification Initiative)，以「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」為三大支柱，對於我國人才進行培訓；建立一個銀行間互通訊息的「網路風險資訊共享平台」，並積極與他國洽談跨境互通機制，以期擴大訊息分享來源。

(六) 加強推動風險導向的稽核方式：

1. 風險導向的稽核制度已成為世界銀行業的趨勢，且國際主要銀行已採行多年，國銀若是想要打亞洲盃甚至是世界盃，建議主管機關應將風險導向的稽核制度從許可制修改為報備制，開放給各銀行去發展適合自己經營策略與規模的風險導向稽核制度，早日跟上世界潮流。
2. 風險導向查核已是世界金融趨勢，在歐美先進國家已行之有年，且風險導向內部稽核制度著重於銀行本身對於風險的認知及管理，監理機關之較佳立場應是站在輔導業者盡速採行風險導向之查核，故建議監理機關放寬申請條件之審查程序，然其可對實施風險導向業者有關風險辨識、評估等風險管理程序之適切性加強查核。

(七) 重視內部稽核獨立性：

落實內部稽核之獨立性，內稽的資源及報酬應直接由董事會審核，並給予足夠支持與資源以發揮內部稽核功能。

(八) 建立良好內控文化：

1. 定期評估管理階層與員工風險認知杜絕員工不道德、不公平對待客戶之行為，以及養成員工關注與反應風險情形，方法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企業與風險文化的認知，並要有前線員工的意見反饋機制，且與獎懲形成適當連結，Tone from the top vs. Echo from the bottom，藉以形成根本地改革企業文化。

2. 董事會為內部控制制度負有最終之責任，稽核單位為協助董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，期待董事會能對稽核單位提供協助，增加稽核人力或引進具專業能力之稽核人力(如：專業資訊人員)。

(九) 積極落實內部稽核三道防線功能：

1. 內部稽核第三道防線主動扮演銀行內部控制三道防線的推手，與一、二道防線建立夥伴、合作關係：
2. 在現今金融業務變化如此快速之情形下，良好的內部控制制度文化環境為最基本及重要之一環；內部控制三道防線已為國際趨勢，國內主管機關已將三道防線訂於內控內稽辦法，銀行公會也訂有實務守則以供銀行業者遵循；內部稽核主動推動內部控制三道防線之理念，加強第一道及第二道防線內控觀念之建立，熟悉自身於三道防線架構中的角色及功能，並且落實於日常業務運作中；各防線充分合作，互相分享及交流資訊，以期稽核工作與銀行內控弱點連結。

(十) 接受內部稽核工作的挑戰：

1. 關注主管機關的監理重點。
2. 內部稽核策略應結合銀行策略與業務策略。
3. 除查核業務項目外，應同時關注受查單位個體與整體內控文化。
4. 關注科技風險、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。
5. 面對金融科技發展與風險日益升溫，內部稽核人員必須提高本身電腦資訊科技能力，以達到具備對於科技風險評估能力、審核網路安全管控措施能力、檢視科技事故成因及預防措施成效能力等工作需求挑戰。
6. 內部稽核應投入大量資源運用科技，得以發展新的稽核方法與技巧，擷取內部稽核優點及整合組織內其他控管單位的報表範本和流程，並協助其能與其他控管單位合作，往特定風險觀點前進。
7. 透過同業間互相交流分享，可充實自身銀行查核廣度與深度。

十、活動照片



20171016 上午－香港金管局(HKMA)



20171016 下午－中國銀行(香港)



20171017 上午—東亞銀行



20171017 下午—渣打銀行



20171018 上午—星展銀行



20171018 下午—PwC HK



20171019 全天－滙豐銀行