行政院所屬各機關因公出國人員出國報告書

（出國類別：其他）

美國紐約聯邦準備銀行舉辦之

「作業風險管理與內部稽核」訓練課程

服務機關：中央銀行

姓名職稱：蕭洙欣 辦事員

派赴國家：美國

出國期間：106 年 5 月 13 日至 5 月 20 日

報告日期：106 年 8 月 10 日

摘要

隨著資訊科技快速變遷及金融創新蓬勃發展，內部控制制度、風險管理方式及內部稽核人員均持續面臨各項變革及挑戰。內部控制、風險管理及內部稽核制度皆是促使企業健全經營之機制，2016年相繼發生的第一商業銀行ATM鉅額盜領案及兆豐國際商業銀行遭美裁罰案，究其原因，皆與內部控制及風險管理息息相關。為因應數位化時代之浪潮，內部控制之相關設計與有效執行及風險管理政策之具體落實，皆是企業需重視之議題。

本次研習課程著重於內部控制制度與風險管控機制，藉由風險管理三道防線模式說明企業內各單位之職責，並探討資訊及網路安全對企業風險管理及內部稽核之影響，最後說明內部稽核功能之轉變及其因應資訊科技快速發展之挑戰。

目錄

壹、前言

資訊科技快速變遷及金融創新蓬勃發展，企業經營模式及其所面臨之風險與過去截然不同，內部控制制度、風險管理方式及內部稽核人員均持續面臨各項變革及挑戰。在充滿不確定性的經營環境下，各式風險環伺，企業須塑造並提升整體風險文化、加強風險意識及積極落實風險管理政策，始可達成永續經營目標。在數位科技時代下，內部稽核人員則須改變傳統思維，積極汲取資訊科技新知並進一步運用於稽核工作，才可提升稽核之價值。

一、 研習目的

本次「作業風險管理與內部稽核」研習課程係由美國紐約聯邦準備銀行(Federal Reserve Bank of New York, FRBNY)舉辦，課程內容聚焦於內部控制制度與風險管控機制，藉由風險管理三道防線模式說明企業內各單位之職責，並探討資訊及網路安全對企業風險管理及內部稽核之影響，最後說明內部稽核功能之轉變及其因應資訊科技快速發展之挑戰。透過多元之課程內容，學習該行風險管理及內部稽核等相關經驗，並瞭解資訊科技及金融科技發展趨勢對資安與內部稽核之影響，藉由借鏡他國實務經驗，俾強化現有風險控管機制，以因應瞬息萬變之金融創新變革與挑戰。

二、 研習經過

本次研習課程由FRBNY選派之各部門專家擔任講座。研習期間自106年5月15日至5月18日止，為期4天，計有來自各國央行、國際清算銀行(Bank for International Settlement, BIS)及國際貨幣基金(International Monetary Fund, IMF)等相關機構共71位學員參加。本研習課程進行方式係由講座簡報相關課程內容及學員提問進行雙向意見交流，並結合理論與實務，以增進學員對作業風險管理與內部稽核之瞭解。

三、 報告內容

本報告共分六個部分，除前言外，第貳章以企業風險管理為主軸，介紹FRBNY所面臨之主要風險及其企業風險管理組織架構；第參章說明風險管理三道防線模式；第肆章說明第二道防線，涵蓋作業風險管理、營運不中斷計畫、法規遵循及資訊安全；第伍章為第三道防線-內部稽核相關內容；第陸章為心得與建議。

貳、企業風險管理

現今企業處於瞬息萬變之經營環境，其所面臨之風險及不確定性亦日趨複雜，為有效因應相關風險，須建立一套適當的企業風險管理架構，以協助其達成營運目標。

本章依序說明企業風險管理之定義、目標、組成要素及實施步驟，並簡述 FRBNY 面臨之主要風險及其企業風險管理組織架構。

一、企業風險管理簡介

COSO[1](Committee of Sponsoring Organizations of the Treadway Commission) 於 1992 年發布「內部控制－整合架構 (Internal Control-Integrated Framework)(簡稱原始架構)」，該架構用以建立及評估內部控制之有效性，獲得全球廣泛認同及運用。惟自原始架構發布後，各界紛紛建議內部控制架構應與風險管理結合，COSO爰於 2004 年 9 月提出「企業風險管理－整合架構 (Enterprise Risk Management-Integrated Framework)(簡稱ERM架構)」，以原始架構為

[1] COSO於1985年由美國註冊會計師協會(American Institute of Certified Public Accountants, AICPA)、內部稽核協會(Institute of Internal Auditors, IIA)、美國會計協會(American Accounting Association, AAA)、管理會計師協會(Institute of Management Accountants, IMA)及國際財務主管協會(Financial Executives International, FEI)五個專業團體贊助成立，其所發布之反詐欺、內部控制、公司治理及財務報告等準則常被政府及民間組織奉為行為圭臬。

基礎，將內部控制三大目標(營運、報導及遵循)及五大要素(控制環境、風險評估、控制作業、資訊與溝通及監督作業)分別擴充為四大目標(策略性、營運、報導及遵循)及八大要素(內部環境、目標設定、事件辨識、風險評估、風險回應、控制作業、資訊與溝通及監督)，以提供企業發展更完善之風險管理。

企業風險管理(Enterprise Risk Management, ERM)亦稱整合性風險管理(Integrated Risk Management, IRM)，COSO將企業風險管理定義為企業管理過程中的一部分，包含企業認知潛在風險、衡量風險及用以制定策略決定管理風險之方式，使風險不超過風險胃納(Risk Appetite)，確保企業目標之達成。

為達成企業之目標，管理階層須訂定企業使命(Mission)或願景(Vision)，並基於使命或願景設定策略性目標(Strategic Objectives)，進而選擇並執行策略。企業風險管理架構將企業之目標分為下列四類：

(一)策略性(Strategic)：層級高於其他三類目標，用以支持並達成企業之使命。

(二)營運(Operations)：資源運用之效果及效率。

(三)報導(Reporting)：報導之可靠性。

(四)遵循(Compliance)：相關法令之遵守。

企業風險管理包括八項相互關聯之組成要素，說明如下：

(一)內部環境(Internal Environment)：內部環境塑造組織文化，進而影響內部人員對風險的看法，包括風險管理態度、風險偏好及營運所處之環境。

(二)目標設定(Objective Setting)：管理階層應建立制定目標之程序，且選定之目標須支持其使命，並符合其風險偏好。

(三)事件辨識(Event Identification)：辨認可能影響企業目標達成之內

部及外部事件係屬風險或機會。

(四)風險評估(Risk Assessment)：藉由分析風險發生之可能性及影響，決定應如何管理風險。

(五)風險回應(Risk Response)：考量企業之風險承受度及成本效益，選用適當的風險回應方式(包括規避、抑減、分擔及承受)。

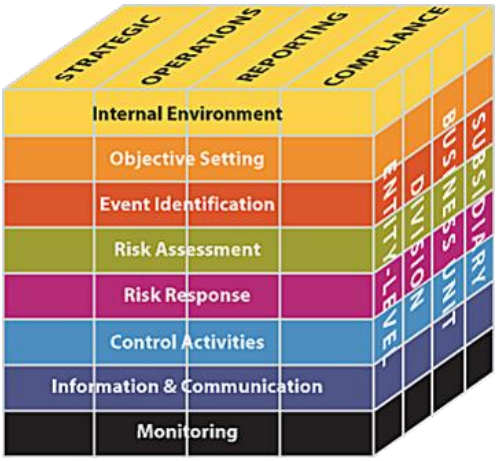
(六)控制作業(Control Activities)：建立內部控制政策及程序，以確保風險回應能有效執行。

(七)資訊與溝通(Information and Communication)：管理階層適時蒐集、溝通相關資訊，使內部人員能履行其責任，有效之溝通範圍包括由上而下、由下而上及相互間之橫向溝通。

(八)監督(Monitoring)：為確保企業風險管理整體之有效性，可藉由持續監督、個別評估或二者並用之方式進行監督。

在企業風險管理架構下，目標與組成要素存有直接關係，目標是企業致力欲達成的結果，而組成要素是達成目標不可或缺之必要因素，COSO以立方體架構(詳圖1)說明目標與組成要素之關係。

圖 1　COSO 企業風險管理架構



資料來源：COSO(2004), Enterprise Risk Management-Integrated Framework

二、企業風險管理之實施步驟

實施企業風險管理時，應訂定風險管理計畫，並依據下列七個步驟執行：

(一)成立風險管理小組：風險管理小組包括董事會、高階管理階層、風險所有者(Risk Owner)及內部稽核。若企業欠缺風險管理專門知識與經驗，可聘請專業風險管理顧問提供相關教育訓練及建議。

(二)辨識風險與機會：風險管理小組成員應檢視營運計畫之每項業務活動，找出可能對各項業務產生重大影響之內部及外部事件和趨勢，對未來有利之事項或趨勢應善加把握；對未來不利之事項或趨勢則應妥為因應。

(三)確認風險胃納及風險容忍度：風險胃納係指企業為達成其使命或願景所能接受之風險；風險容忍度則指企業為達成某一目標時，可接受的績效變動程度。企業可利用風險地圖(Risk Map)列示風險發生之可能性及影響而設定其風險胃納，若風險超出風險胃納，管理階層應採取適當之行動，將風險控制在可接受範圍內。

(四)辨識風險和機會之關聯性：評估風險時，須注意不同風險間的潛在關聯性。有些風險之間呈現正相關，亦即當某一項風險增加，另一項風險亦隨之增加，可能產生相乘或放大之效果；反之，有些風險之間則呈現負相關，亦即兩項風險發生之可能性呈反向變動。企業利用衍生性商品進行避險時，即利用衍生性商品與相關金融商品間之反向關係，抵銷原有之風險。

(五)訂定風險和機會優先順序：利用風險評估圖(Risk Assessment Chart)辨識高風險活動，優先處理高風險活動；非高風險活動則依風險等級分配適當資源進行控制。

(六)決定所應採取之行動：辨認各項風險及排定優先順序後，管理階層須採取適當之行動，以便有效管理企業風險。

(七)建立企業風險管理系統：長期而言，為發揮企業風險管理之效益，須建立一套整合性的風險管理系統，方可持續監控及有效因應風險。

三、FRBNY面臨之風險及其企業風險管理組織架構

FRBNY肩負貨幣政策之制定與執行、金融機構之監理、對各國央行和國際金融機構提供金融服務及維持金融體系之穩定等職責，其風險胃納較其他金融機構保守，係以達成營運目標及符合公眾利益為優先考量。其主要面臨之風險說明如下：

(一)財務風險(Financial Risk)：包含信用風險(Credit Risk)及市場風險(Market Risk)，前者係因交易對手無法履行其財務義務所致之風險；後者則為市場價格變動，導致資產負債表內及表外部位產生損失之風險。

(二)財務報表報導風險(Financial Statement Reporting Risk)：因財務報導相關內控不佳，致財務報表不實表達之風險。

(三)作業風險(Operational Risk)：因企業內部之作業程序、資訊系統、人員疏失或外部事件造成企業損失之風險。

(四)法規遵循風險(Compliance Risk)：因違反法律、監理法規及業務準則等而遭致主管機關處分，導致財務或聲譽損失之風險。

(五)策略風險(Strategic Risk)：因策略規劃不當或無效，致無法達成目標之風險。

(六)聲譽風險(Reputational Risk)：因銀行行動失當使外界對銀行產生負面印象之風險。

(七)法律風險(Legal Risk)：因契約不具法律效力或未正確記載，致銀行價值減損之風險。

FRBNY採用企業風險管理控管風險，其企業風險管理組織架構

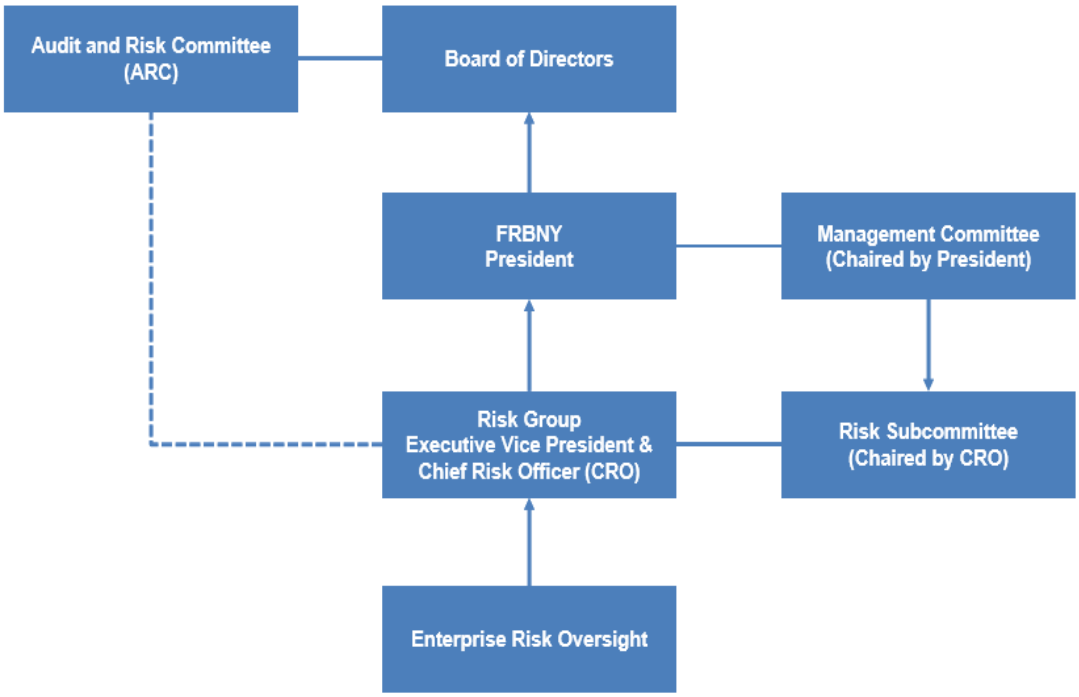
(詳圖2)，說明如下：

(一)董事會(Board of Directors)：設置稽核及風險委員會(Audit and Risk Committee, ARC)，負責核准風險策略。

(二)管理委員會(Management Committee)：設置風險小組委員會(Risk Subcommittee)，由銀行各部門高階主管組成，定期討論其業務相關風險事務、內控問題及處理方法。

(三)風險部門：執行風險管理流程評估，以銀行整體角度分析風險，並向ARC報告。

圖 2　FRBNY 企業風險管理組織架構



資料來源：FRBNY 課程資料

參、風險管理三道防線模式

2001年至2002年間，美國安隆(Enron)及世界通訊(WorldCom)等財務醜聞案相繼爆發，為提振投資人對資本市場之信心，美國國會爰

於2002年10月通過沙賓法案(Sarbanes-Oxley Act)，以增進企業財務資訊透明。在沙賓法案及金融海嘯等事件後，為達公司治理及法規遵循等相關要求，金融業開始採用風險管理三道防線架構，以強化並確保內部控制之執行。

本章介紹風險管理三道防線模式，並舉例說明如何結合COSO內部控制整合架構與風險管理三道防線模式。

一、 風險管理三道防線模式概述

風險管理三道防線模式(The Three Lines of Defense Models)明確釐清三道防線之權責範圍，使銀行內各單位瞭解其在整體風險架構所扮演之角色。關於三道防線模式(詳圖3)，分述如下：

(一)第一道防線：由承擔風險之各業務單位負責，在既定之營運目標下，負責辨識、評估及控管日常業務所產生的風險，針對該風險設計並執行有效的內部控制程序。

(二)第二道防線：包括風險管理、法令遵循、人力資源及資訊等專職單位，負責銀行整體風險管理政策之訂定，並監督整體風險承擔能力及風險承受現況，向董事會或高階管理階層報告風險控管情形。

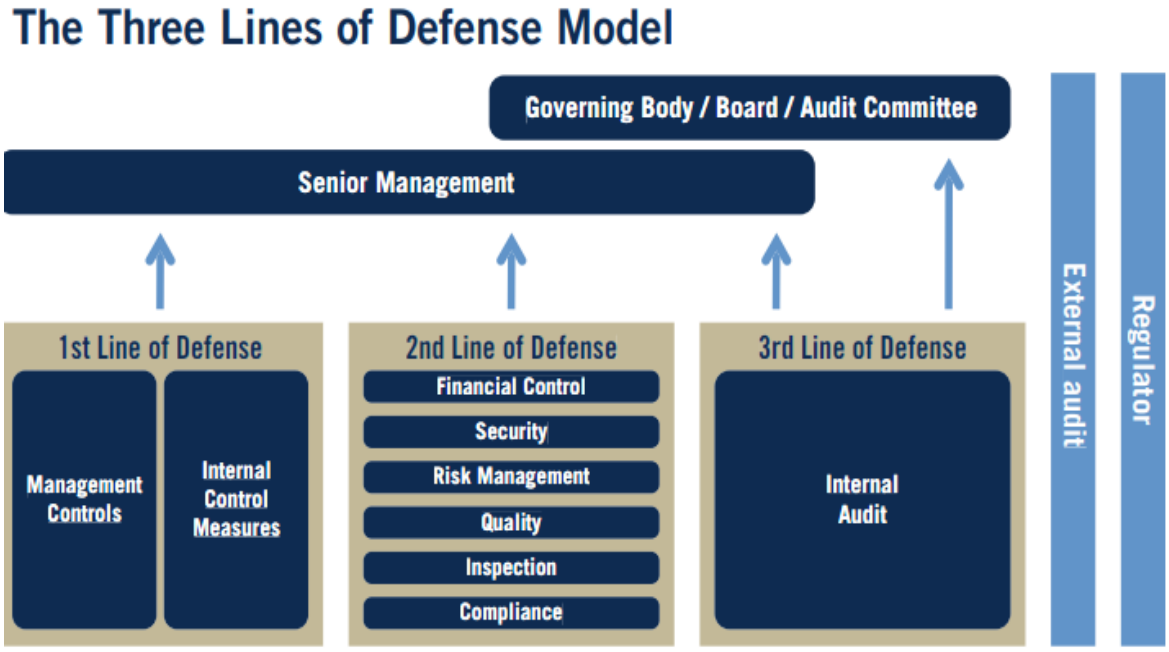
(三)第三道防線：內部稽核以超然獨立之立場執行稽核業務，協助董事會和高階管理階層查核與評估內部控制制度及風險管理之運作，包含第一道及第二道防線風險監控之有效性，以合理確信內部控制制度得以持續有效實施。

董事會及高階管理階層雖未列入三道防線模式之任一道防線，惟其負責訂定銀行之目標及策略，應持續確保銀行符合三道防線原則，並對該模式運作之有效性負最終之責任。另可加上第四道防線–外部審計人員及第五道防線–主管機關，外界對外部審計人員及主管機關這兩道外部防線寄予厚望，惟內部控制及風險管理是企業之責任，而

非外部審計人員及主管機關之責任。

當三道防線可清楚辨識並明確定義每道防線之角色和責任，且每道防線之間可達到資訊共享及作業協調，其風險管理效果最佳。強化內部控制及風險管理是企業永續經營的重要關鍵，董事會及高階管理階層應認真檢視企業營運現況，落實內控及風險管理以除弊興利，為公司創造價值。

圖 3　風險管理三道防線模式



資料來源：FRBNY課程資料

二、 運用COSO架構於三道防線模式

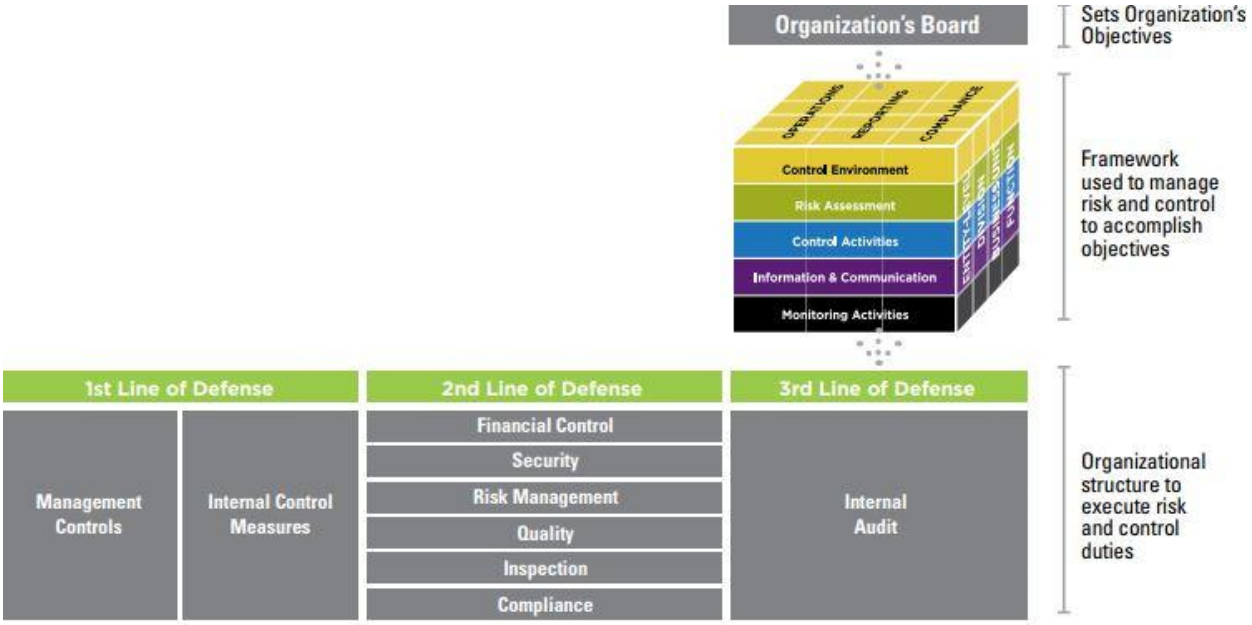
2015年7月COSO發布與內部稽核協會(IIA)合作之「運用COSO架構於三道防線(Leveraging COSO Across the Three Lines of Defense)」研究報告，COSO架構定義內部控制三大目標(營運、報導及遵循)、五大要素(控制環境、風險評估、控制作業、資訊與溝通及監督作業)和17項原則(詳表1)，17項原則係由五大要素衍生而出，運用每一項原則即可達成有效的內部控制。三道防線模式連結COSO內部控制整合架構，可協助每道防線之人員瞭解相關風險和控制範圍及其應負之責任。前述COSO及IIA研究報告勾勒之關係詳圖4。

表 1　COSO 架構之五大要素及 17 項原則

控制環境	1. 展現誠信與道德價值之承諾 2. 行使監督責任 3. 建立結構、權限與責任 4. 展現適任人才之承諾 5. 強化課責性
風險評估	6. 具體指明適合目標 7. 辨識及分析風險 8. 評估舞弊風險 9. 辨識及分析重大改變
控制作業	10.建立控制作業 11.建立資訊科技之一般控制 12.透過政策與程序建置
資訊與溝通	13.使用攸關資訊 14.內部溝通 15.外部溝通
監督作業	16.進行持續監督或個別評估 17.評估及溝通缺失

資料來源：王怡心(2015)，「運用 COSO 建立內部控制三道防線」

圖 4　目標、架構和三道防線模式之關係



資料來源：FRBNY 課程資料

以下謹就COSO架構之第17項原則「評估及溝通缺失」，列示如何將該原則之責任分派至三道防線(詳表2)：

表2　運用COSO第17項原則建立風險管理三道防線

原則17：評估及溝通缺失		
第一道防線	第二道防線	第三道防線
1. 溝通內部控制缺失 2. 追蹤缺失是否改善	負責監督及報導內部控制缺失	向董事會及高階主管提供關於內部控制有效性的確認服務

資料來源：本報告整理

肆、第二道防線

第二道防線是指專責之風險管理單位，負責規劃相關風險管理制度及監控風險。風險管理單位、法律遵循單位及資訊安全單位等皆扮演第二道防線之角色，負責協助並監督第一道防線相關控制活動。

本次訓練課程著重於第二道防線及第三道防線相關職責，故本章以第二道防線為出發點，說明作業風險管理、營運不中斷計畫、法規遵循及資訊安全等議題。

一、 作業風險管理

國際清算銀行(BIS)所屬之巴賽爾銀行監理委員會(Basel Committee on Banking Supervision, BCBS)為維護資本市場之穩定，於1988年提出巴賽爾資本協定 (Basel Capital Accord)，2004年於原資本協定基礎下發展出新巴賽爾資本協定(Basel II)，Basel II正式將作業風險增列為最低資本要求之計算項目，其定義為因內部作業程序、人員及系統之不當或失誤，或因外部事件造成損失之風險，故作業風險發生之原因可分為四類：

(一) 人員：因內部人員有意或無意之行為所致，例如缺乏經驗或專業

知識、疏失及舞弊等。

(二) 系統：因資訊設備或基礎設施發生問題所致，例如系統中斷、程式或資料錯誤等。

(三) 作業流程：因交易、清算及營運流程錯誤所致，例如模型設定或參數錯誤、安全控管不周等。

(四) 外部事件：因「第三者行為」導致損失發生，例如恐怖攻擊、天然災害、政治動盪及經濟環境改變等。

Basel II 要求作業風險管理應融入日常風險管理程序，其可視為企業風險管理之一環。作業風險遍及企業內部，為有效控管作業風險，需要企業全體人員參與，故作業風險管理是企業全體人員之責任，旨在藉由建立完善及有效執行作業風險管理機制，以降低作業風險，進而達成營運之目標。以下說明作業風險管理流程：

(一) 風險辨識及評估：應建立有效之作業風險管理機制，以辨識及評估現有及潛在之作業風險。當內在及外在環境改變時，應立即採行風險辨識及評估程序，確保既有作業風險管理機制之妥適性。

(二) 風險衡量：以定性或定量標準，衡量各風險類型及曝險程度，並以衡量結果作為控管作業風險之依據。

(三) 風險監控：應定期監控並及時偵測作業風險，以有效降低作業風險，且應定期評估風險監控之有效性。

(四) 風險溝通：分為對內呈報及對外揭露，前者係指建立逐級呈報機制，使相關人員明確瞭解須呈報之風險種類及層級；後者則指建立對外揭露政策，使市場參與者能獲悉並評估其作業風險管理情況。

近年金融科技創新蓬勃發展，銀行面臨之經營環境日趨複雜，作業風險管理之重要性亦日益提升。FRBNY歸納成功之作業風險管理

包括下列要素：

(一)董事會及高階管理階層之支持。

(二)建立風險資料庫，訓練員工對風險種類及其影響之瞭解，並熟悉風險專業術語，且分享相關資訊。

(三)跨部門討論與合作有助於風險辨識及管理。

(四)積極管理風險並持續檢視風險承受能力。

二、 營運不中斷計畫

營運不中斷計畫(Business Continuity Program)是作業風險管理之一環，旨在當發生重大事故或災害之急難狀況下，仍能確保組織持續營運，降低災害所致之作業、財務、法律及聲譽等方面之重大負面影響。FRBNY扮演穩定全球金融體系之重要角色，為不中斷其貨幣政策、維持金融穩定及提供金融服務等任務之執行，參考國際清算銀行之高度營運持續原則(High-level Business Continuity Principles)及國際災難復原協會(Disaster Recovery Institute International, DRII)之專業實務，建立營運不中斷計畫。

造成營運中斷之風險類型諸多，其影響程度也不同，FRBNY將造成營運中斷之風險類型分為人為災害與自然災害，說明如下：

(一)人為災害：以資訊科技之威脅為首，如駭客與匿名網路攻擊、恐怖攻擊(911事件)、示威抗議活動(佔領華爾街運動)及內部威脅(內部人員破壞)等。

(二)天然災害：與天候相關(例如颶風)、流行性感冒(H1N1)或病毒等。

上述風險造成之威脅可能持續數天、數月或更長久之期間，影響範圍可能是局部或全面性，可能可預期或無法預期，故建立營運不中斷計畫時應考量下列情況：無法進入大樓辦公、無法通訊(網路或電信中斷)、無法聯繫員工及前三者同時發生之情形。針對這些情形，

FRBNY在保持營運彈性原則下，採取異地備援、夥伴銀行機制(定期與其他聯邦準備銀行分享業務訊息)、居住地辦公機制(若員工無法在辦公場所辦理業務，可在居住地辦公，確保業務順利執行)。

依據FRBNY制定之營運不中斷計畫，其內容包括下列項目：

(一)描述業務性質。

(二)辨識重要營運流程及應用系統。

(三)目標復原時間。

(四)確認內部及外部聯絡資訊。

(五)各部門或應用系統間之相依程度。

(六)基礎設施及辦公空間需求。

(七)備援地點。

營運不中斷計畫隨著時間、環境變動而改變，應每年進行評估，以確定計畫是否有效。關於員工方面，則以安全為首要目標，定期進行測試與模擬演練，確保每位員工瞭解本身職責所在。

FRBNY提出以下最佳實務運作方式，分述如下：

(一)確保重要員工瞭解其在事件發生時之角色與職責。

(二)盡可能在事件發生前，就相關人員完成適當配置，優先安排適當員工於重要職務上。

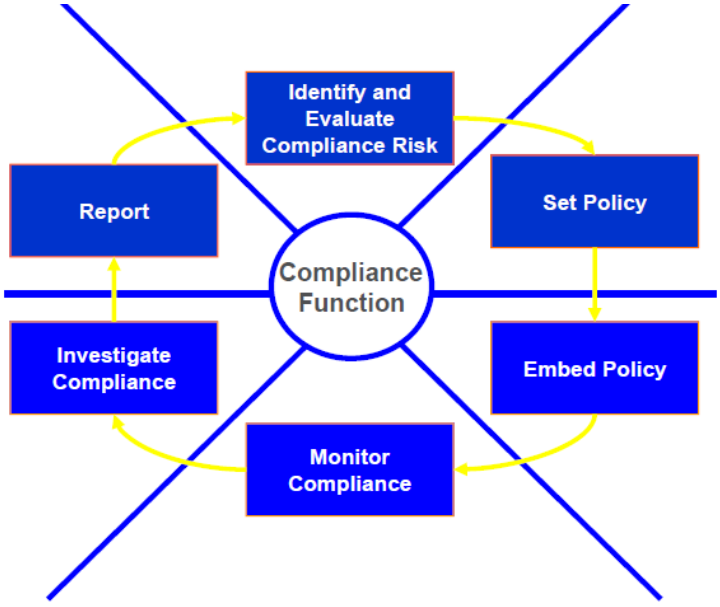
(三)若應變管理小組無法即時提供協助，亦能確保異地備援機制能持續正常運作。

(四)定期更新內部員工及客戶聯絡資訊，並與外部團體(如貿易夥伴或聯邦政府等)維繫良好關係，對內、對外聯繫均能保持暢通。

三、 法規遵循

銀行之營運過程係以法令規章、要點及辦法等為營運基礎，其作業程序應遵守法規規範。法規遵循(Compliance)係指遵守法律、監理法規、業務準則、相關自律規範及銀行內部作業準則等，FRBNY於2005年建置法規遵循部門，該部門負責發展法規遵循計畫，協助辨識與評估並處理法規遵循風險之相關議題。FRBNY係以全面且有系統的遵循架構，落實其法規遵循職能，謹就其法規遵循架構(詳圖5)說明如下：

圖5　FRBNY之法規遵循架構



資料來源：FRBNY 課程資料

(一)辨識與評估法規遵循風險：辨識及瞭解環境改變導致之法規遵循、法律及聲譽風險，評估法規遵循情形，優先運用資源因應此類風險。

(二)政策規劃：規劃政策因應已辨識之法規遵循及聲譽風險，必要時適時更新政策；整合整體組織法規遵循事項以建置政策；建立政策、程序及其他法規遵循方案等之溝通管道。

(三)政策實施：將政策轉化為法規遵循具體行動，使營運活動符合法

規遵循目標(例如改變營運流程、發展新的內部控制活動及教育訓練等)，並建立這些政策之溝通管道。

(四)法規遵循監控：包括每日主動及定期監控法規遵循計畫，每日藉由系統及流程監控法規遵循情形；定期監控則包含評估整體法規遵循計畫及其有效性。

(五)法規遵循調查：透過法規遵循監控，分析法規遵循議題及缺失，採取改正措施，並藉由發現之缺失改善整體法規遵循計畫。

(六)報告：向主要利害關係人報告事項應包括各項計畫法規遵循要求、計畫之有效性、法規遵循重大缺失、改正措施執行情況及應考量之新興法規遵循風險。

落實法規遵循可避免企業因違反某些法令規範而發生重大損失，2016年兆豐國際商業銀行紐約分行因未遵循銀行保密法(Bank Secrecy Act, BSA)及洗錢防制法(Anti-Money Laundering, AML)等規定，遭美國紐約州金融服務署(New York Department of Financial Services, DFS)重罰1.8億美元，該事件除突顯該行存在法令遵循風險外，因裁罰金額頗鉅引發負面觀感，亦造成該行聲譽風險。兆豐案喚起金融機構提升風險意識，法規遵循應確實落實並內化於企業文化中。

四、 資訊安全

資訊科技不斷推陳出新，企業大量使用資訊系統處理相關交易及財務等資料，資訊安全(Information Security)為當前極為重要之議題，資安風險是作業風險之一環，應將其納入企業風險管理之範疇，以確保企業能永續經營。資訊安全之主要目標為保護資訊之機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，避免資訊被非法存取、不當修改或毀損，且經授權之使用者可適時存取所需資訊。

資訊化環境為企業帶來便利性，在享受資訊便利性之際，須體認資訊科技可能引發之風險，例如應考量網路安全(Cyber Security)、營運不中斷及復原方案、第三方風險(Third Party Risks)、內部威脅(Insider Threat)、資源及技能短缺等，加強資訊安全工作，俾便有效掌握風險並採取相關因應措施。

資訊科技快速變遷亦帶來新興資安威脅，企業須採取政策生命週期管理(Policy Lifecycle Management)確保企業資訊安全。政策生命週期是一項從政策形成、執行與維護等不斷持續改善的循環，經由政策之落實執行以達成資訊安全目標。政策生命週期管理包括以下內容：

(一)政策形成(Policy Creation)。

(二)檢視、核准及溝通(Review, Approval and Communication)。

(三)政策建置及認知(Policy Implementation and Awareness)。

(四)監控、例外情況及強制實施(Monitoring, Exception, Enforcement)。

(五)政策維護及廢除(Policy Maintenance/Retirement)。

網際網路的普及使企業經營模式改變，愈來愈多新型態的進階持續性威脅(Advanced Persistent Threat, APT)出現，APT是有計畫性、有目標的攻擊行為，而APT入侵最有效且最簡易之方式即為透過社交工程電子郵件騙取收件者信任而開啟郵件。面對網路攻擊環伺之環境，企業必須建立因應網路攻擊之復原措施，網路攻擊復原(Cyber Resilience)係指受到網路攻擊後，可確保重要業務不中斷而持續運作。

面對金融科技創新趨勢，唯有及早採取資安防禦行動，建立並落實資訊安全管理計畫，才能有效防堵惡意攻擊，降低資安風險，維持企業正常營運。

伍、第三道防線-內部稽核

本章依序說明內部稽核之職責、FRBNY之內部稽核流程、內部

稽核與企業風險管理之關係，以及資訊科技稽核趨勢與內部稽核之挑戰。

一、 內部稽核之職責

內部稽核係內部控制之一環，旨在查核及評估內部控制制度、風險管理及治理架構是否有效運作，並適時提供獨立且客觀的改進建議及諮詢服務，用以改善企業營運並提升企業價值。為強化內部稽核之獨立性，應明確訂定內部稽核隸屬於董事會，並賦予充分權限以確保內部稽核制度能持續有效實施。

FRBNY之內部稽核人員角色及任務係規範於該行之內部稽核規程，其主要業務內容包括：協助管理階層履行其任務、檢查各項資源運用是否有效率、確認財務報導之可靠性及相關法令之遵循等。

二、 FRBNY之內部稽核流程

FRBNY之內部稽核流程依序為規劃(Planning)、實地查核與分析(Fieldwork and Analysis)及出具報告(Reporting Results)，茲將各流程說明如下：

(一)規劃：FRBNY係採風險導向稽核(Risk-based Audit)，事前規劃有助於內部稽核人員將稽核範圍聚焦於高風險區域。規劃階段包括執行背景分析及風險評估、分配案件予稽核小組、總結規劃階段執行之工作、寄發正式聲明予受查者、與受查者開會討論當次稽核工作相關事宜。

(二)實地查核與分析：實地查核之目的係為瞭解受查者內部控制執行情形，其方法包括穿透性測試(Walkthrough Testing)及細節測試(Detailed Testing)。穿透性測試是藉由詢問適當人員、觀察企業營運狀況、檢查相關文件及重新執行該控制活動等方式，以獲取內部控制之設計是否適切之證據；細節測試則是透過詢問、觀察內

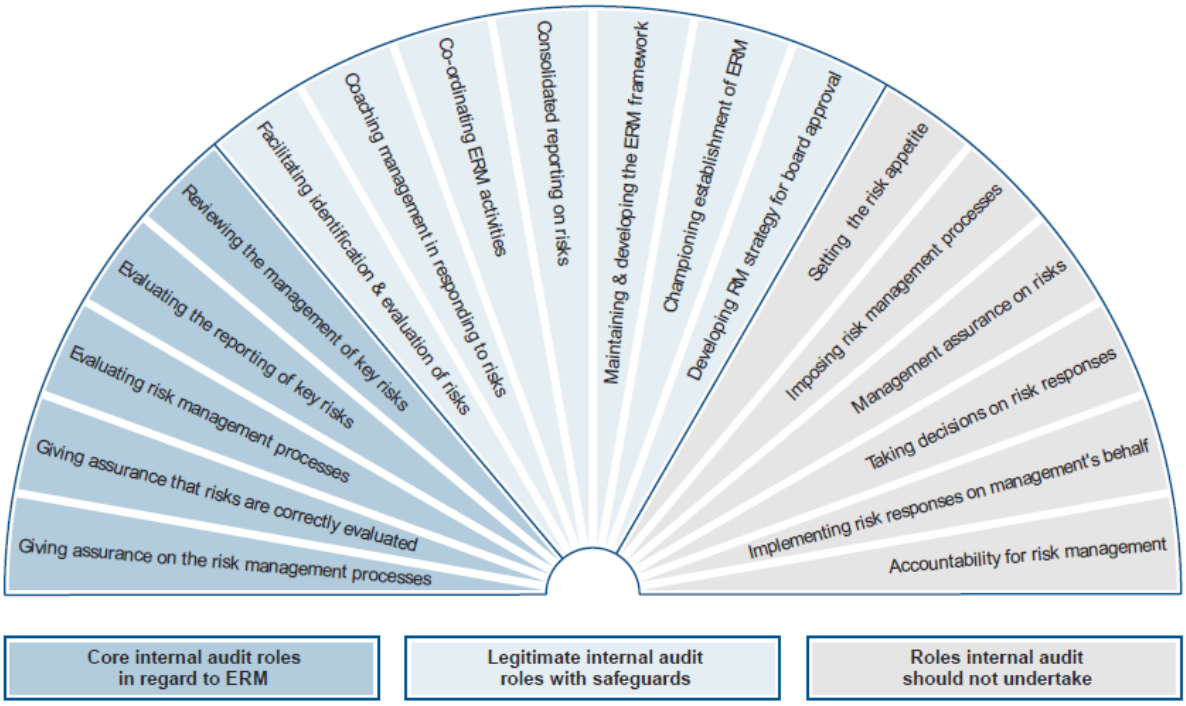
控流程、檢查相關文件、重新執行相關控制活動、抽樣及資料分析(Data Analytics)等方式，以評估內部控制之運作是否有效。

(三)出具報告：將稽核結果書面化出具報告，並與受查者管理階層討論，報告主要內容包括受查者基本資料、稽核目的與範圍、稽核結論、稽核建議及受查者之回應等。

三、 內部稽核與企業風險管理之關係

內部稽核與企業風險管理息息相關，內部稽核評估企業風險管理活動之有效性，向董事會提供諮詢服務，以協助確保內部控制制度有效運作及關鍵經營風險已妥善控管。內部稽核與企業風險管理之關係詳圖6。

圖 6　內部稽核與企業風險管理之關係圖



資料來源：FRBNY 課程資料

內部稽核在企業風險管理所扮演的核心角色臚列如下：

(一)確認風險管理流程。

(二)確認風險評估之正確性。

(三)評估風險管理過程。

(四)評估主要風險及控制的相關報告。

(五)檢視主要風險的管理，包括控制的有效性及對風險的回應措施。

內部稽核在企業風險管理不應承擔之角色如下：

(一)設定風險胃納。

(二)設計風險管理流程。

(三)確認風險管理。

(四)制定風險回應決策。

(五)代管理階層執行風險回應措施。

(六)承擔風險管理之責。

四、 資訊科技稽核趨勢與內部稽核之挑戰

資訊科技及各項破壞式創新對企業之影響無遠弗屆，加劇企業面臨之資安風險，資訊科技稽核(IT Auditing)順勢而生，其關注網路安全、營運不中斷、第三方風險及內部威脅等新興風險。傳統稽核扮演事後偵查錯誤、發現舞弊之角色，在現今充滿不確定性之環境下，則可透過敏捷稽核(Agile Auditing)或動態稽核(Dynamic Auditing)辨識正在發展之干擾事件，俾使企業可依據不斷演變之風險擬定稽核計畫，彈性的稽核規劃可配合企業節奏而改變其行動，進而提升稽核之效率與效果。

本次訓練課程亦簡介雲端運算(Cloud Computing)、大數據(Big Data)、物聯網(Internet of Things, IoT)、區塊鏈(Blockchain)及人工智慧(Artificial Intelligence)等新興科技對未來生活之影響。本文以物聯網為例，說明其對資安及內控之影響。

根據歐盟無線射頻識別相關活動與標準化(Coordination and Support Action for Global RFID-related Activities and Standardization, CASAGRAS)提出的實務定義，物聯網係一項全球化的網路基礎建設，透過通訊資料擷取與溝通機制，連結實體或虛擬物件，並可進一步透過特定機制與網際網路設施，將所有物件連結在一起，提供控制、偵測、識別及資訊交換服務。物聯網將現實世界數位化，統整物與物之數位資訊，其應用範圍十分廣泛，包括健康醫療、運輸物流、智慧型環境(家庭、辦公、工廠)等領域，應用市場十分廣闊。物聯網發展迅速，惟資安議題亦引發關注。2016年10月21日美國東部發生大規模網路癱瘓災情，主因負責提供網路服務之Dynamic Network Service(Dyn)公司受到分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊，造成許多網站無法連線；此事件發生後，美國國土安全部(Department of Homeland Security, DHS)發布「保護物聯網策略準則」，呼籲物聯網開發者及製造商等業者在設計、生產及使用物聯網裝置應負保護物聯網安全之責任。由以上案例可知，物聯網雖帶來便捷，亦衍生資安風險問題，企業須評估可能面臨之風險，制定相關管控機制以為因應，內部稽核亦須瞭解物聯網發展趨勢，以協助企業評估風險管理之有效性。

內部稽核人員從傳統「缺失發現者」之角色轉變為「企業價值提升者」及「受企業信任之諮詢顧問」，須具備良好的溝通能力，包括主動傾聽、尊重多元觀點等；此外，欲提升內部稽核人員在企業之定位與貢獻度，則須具備與時俱進之專業能力，掌握產業、科技與法律之最新脈動，以創新思維因應各式挑戰，協助企業創造更大的價值。

陸、心得與建議

本次訓練課程探討企業風險管理、作業風險管理、風險管理三道

防線、資訊安全及內部稽核等多項議題，透過豐富的課程內容得以學習企業風險管理、作業風險管理架構及內部稽核機制，並瞭解資訊科技及金融科技發展趨勢對資安與內部稽核之影響。謹研提以下建議事項供參：

一、 本局經理國庫業務，除辦理國庫存款及保管品相關收付業務外，並負責代庫機構之管理，屬風險管理三道防線模式之第一道防線。藉由本課程可建立並提升同仁對國庫業務相關作業流程之風險意識，並增進內部控制及稽核等專業知能，建議持續派員參與相關訓練課程。

二、 本局辦理各項國庫收付業務，營運中斷將影響國庫資金調度，本行已建置營運不中斷機制及緊急狀況處理準則等，應持續檢視風險現況並適時修正調整，以確保危機發生時營運不受影響。另應強化同仁風險意識及緊急應變能力，辦理教育訓練模擬各式災變情境，培養同仁危機管理能力，平時即訓練有素之員工，在面臨緊急狀況時才能隨機應變，即時採取適當之因應措施。

三、 內部稽核人員之角色已由傳統偵測舞弊者轉變為提升企業價值者，其與受查者之關係亦從對立轉變為互相信賴。面對日趨複雜之科技創新及企業環境，內部稽核人員將面臨艱鉅之挑戰，除須積極充實新知掌握資訊科技發展現況及企業動態外，並應深入瞭解其對內部控制之衝擊，協助企業控管相關風險並創造更大之價值。

四、 近年資訊科技與金融科技多元發展，內部稽核人員除會計、金融專業外，亦應具備科技、法律等素養，故應積極培養具備IT專業之跨領域稽核人員，以充分發揮內部稽核之職能與價值。

參考資料

1.COSO(2004), “Enterprise Risk Management-Integrated Framework,” September.

2.COSO(2013), “Internal Control- Integrated Framework,” May.

3.IIA and COSO(2015),“Leveraging COSO Across the Three Lines of Defense,” July.

4.IIA(2013),“The Three Lines of Defense in Effective Risk Management and Control,” January.

5.IIA(2009),“The Role of Internal Auditing in Enterprise-wide Risk Management,” January.

6.本次訓練課程主辦單位提供與會學員講義資料(2017)。

7.林正弘(2016)，「參加美國紐約聯邦準備銀行訓練課程『作業風險管理與內部稽核』出國報告」，中央銀行，8 月。

8.陳證吉(2015)，「參加美國紐約聯邦準備銀行訓練課程『作業風險管理與內部稽核』出國報告」，中央銀行，7 月。

9.陳雅慧(2015)，「參加 SEACEN『銀行全面風險管理』訓練課程報告」，中央銀行，8 月。

10.王怡心(2015)，「運用 COSO 建立內部控制三道防線」，內部稽核季刊，第 90 期，8 月。

11.王怡心、楊文安(2013)，「COSO 內部控制：整合架構」，中華民國內部稽核協會，10 月。

12.沈大白、黃追(2007)，「金融機構作業風險管理」，財團法人中華民國證券暨期貨市場發展基金會，12 月。

13.翁世吉(2015)，「物聯網架構下的支付產業發展趨勢」，財金資訊季刊，第 84 期，10 月。

14.Price Waterhouse and Coopers(2009)，「銀行風險管理實務範本-作業風險管理分論及彙編」，中華民國銀行商業同業公會全國聯合會。

15.美國紐約聯邦準備銀行網站，https://www.newyorkfed.org/。
16.金融監督管理委員會網站，https://www.fsc.gov.tw/ch/index.jsp。