出國報告（出國類別：其他）

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

服務機關：中央銀行
姓名職稱：林正弘/四等專員
派赴國家：美國
出國期間：105 年 5 月 14 日至 5 月 21 日
報告日期：105 年 8 月 12 日

目錄

壹、前言

當前環境劇烈的變動，如科技進步、高齡化社會、氣候變遷、恐怖攻擊等，但任何的變動總有一體兩面，一面是機會，另一面是威脅，變動既然無可避免，只有面對變化、觀察變化，學習如何避開變化帶來的傷害，並從改變中發現有利的機會。很多變化雖然不是發生在我國，但既然已經發生，我們仍需居安思危，所以職於 105 年 5 月 14 日起至 105 年 5 月 21 日奉派參加美國紐約聯邦準備銀行(以下簡稱 FRBNY)之專業訓練課程－作業風險管理與內部稽核(The Operational Risk Management and Internal Audit)，期能增進作業風險的管理知識，及借鑑紐約聯邦準備銀行內部稽核做法。

本次課程共有 69 人參加，來自各國央行及 IMF 等機構，其中 24 人為內部稽核部門、17 人為風險管理部門、11 人為檢查監管部門，17 人為其他部門。課程內容由 FRBNY 選派各部門專家講授，具備高度專業理論及多年實務經驗，又經由課堂上回答同學的問題，將理論結合實務進行討論與解答，為作業風險管理與內部稽核之優良課程。

本次課程先介紹企業風險管理的基本理論，再以風險管理的三道防線為架構，將作業風險管理以第一、二道防線說明，內部稽核則屬於第三道防線。作業風險管理著重在介紹第二道防線風險管理各項理論及風險報告、法規遵循、持續營運計畫、資訊安全等課程，然後介紹內部稽核的相關課程，最後以實際的例子介紹第一道防線的作為。

貳、企業風險管理

一、風險定義：事件發生的可能性對目標達成有影響，且在影響的嚴重性和發生可能性被衡量。(IIA)

二、作業風險定義：凡起因於內部作業、人員及系統的不當或失誤，或因外部事件造成損失的風險，均稱為作業風險，包括法律風險，但不包括策略風險及聲譽風險。(Basel Ⅱ)

三、COSO 委員會(Committee Of Sponsoring Organizations of the Treadway Commission 以下簡稱 COSO)企業風險管理定義：企業風險管理係一項遍及企業各層面之過程，該過程受企業董事會、管理階層或其他人士之影響，用以制定策略、辨認可能影響企業之潛在事項、管理企業之風險，使其不超過企業之風險胃納(Risk Appetite)，以合理保證其目標之達成。

每個企業均因其為利害關係人提供價值而存在，在提供服務的過程中所有企業均面臨不確定性，而管理階層之挑戰在於為利害關係人創造價值而努力時，須視其風險胃納及環境狀況決定其欲接受之不確定性有多高。不確定性代表風險或代表機會，企業之價值可能因此而遭侵蝕或因此而提高；企業風險管理讓管理階層能有效處理不確定性及其相關的風險與機會，使企業創造價值之能力提高。

四、COSO 企業風險管理組成要素：控制環境、目標設定、事項辨認、風險評估、風險因應、控制活動、資訊與溝通、監督。企業風險管理不是環環緊扣的順序過程，一個組成要素不只是影響下一個組成要素，它是一個多方向，且反覆進行的過程，任一個組成要素都能夠、也的確會影響其他組成要素。其中與風險較直接相關者為目標設定、事項辨認、風險評估及風險因應，介紹其定義如下：

目標設定：必須先有目標，管理階層才能辨認影響目標達成的潛在事項。企業風險管理保證管理階層訂有制訂目標之過程，以及所選中之目標能支持企業之使命，追隨該使命，並與企業之風險偏好一致。

事項辨認：企業須辨認會影響目標能否達成之內部事項及外部事項，這些事項可區分風險與機會二類，管理階層應把機會導回設定策略或目標之流程中。

風險評估：企業分析風險、考量其發生之可能性及影響，並藉以決定風險應如何加以管理。風險之評估應基於固有風險及剩餘風險。

風險因應：管理階層選擇風險因應(規避、承受、抑減及分擔)之方式，並進行一連串行動使風險能與企業之風險容忍度(risk tolerance)及風險胃納(risk appetite)相配合。

五、COSO 的內部控制架構

COSO 於 1992 年發布「內部控制整合架構」(Internal Control – Integrated Framework；COSO-IC)，簡稱 COSO 報告，提出了內部控制的定義與評鑑內部控制效益的架構，並很快獲得美國政府採用。

2013 年 5 月 14 日 COSO 發布更新其 1992 年的架構，稱為"Internal Control – Integrated Framework：2013"，新增 17 項原則於五項要素中。主要係考量自 1992 年至 2013 年間國際經濟環境重大的變更、企業營運模式改變、法令之國際化與複雜化、企業對於不斷進步科技之依賴度，及企業預防及偵測舞弊之期望等原因而新增 17 項原則(principle)，並將 17 項原則明確編纂至五大要素中。

表一、2013 年版 COSO 整合式內部控制架構之 17 項原則

控制環境	風險評估	控制活動	資訊與溝通	監督
1.組織之誠信承諾與道德價值觀。 2.執行監督責任。 3.架構、主管權責之設定。 4.承諾之強化。 5.強化課責性。	6.界定合適之目標。 7.風險評估與辨識。 8.舞弊風險評估。 9.重大變動之辨識與分析。	10.選擇及發展控制活動。 11.選擇及發展資訊科技一般控制。 12.研擬政策與程序。	13.使用相關品質資訊。 14.內部溝通。 15.外部溝通。	16.持續辦理與(或)個別評估。 17.就不佳之處進行評估與溝通。

資料來源：FRBNY 課程資料。

參、風險管理的三道防線理論

管理階層的責任：定義目標並決定高階的策略，強調誠信與道德的價值觀，建立且同時監督三道防線的架構，並將架構指定適當負責人員，建立一個良好的組織環境。

第一道防線：營運單位擁有並管理風險，執行作業且對風險負責，包括辨認和評估風險或利用第二道防線提供的工具管理風險，設計及執行控制措施，找出不適當的程序和控制缺失，並與高階管理者溝通。

FRBNY 由市場事業群、金融機構監理事業群及金融服務事業群等各業務單位負責，執行銀行的貨幣政策及維持金融的穩定，同時辨識及管理各營運活動之固有風險，各事業群主管定期將評估結果向資深管理者或風險管理委員會報告。

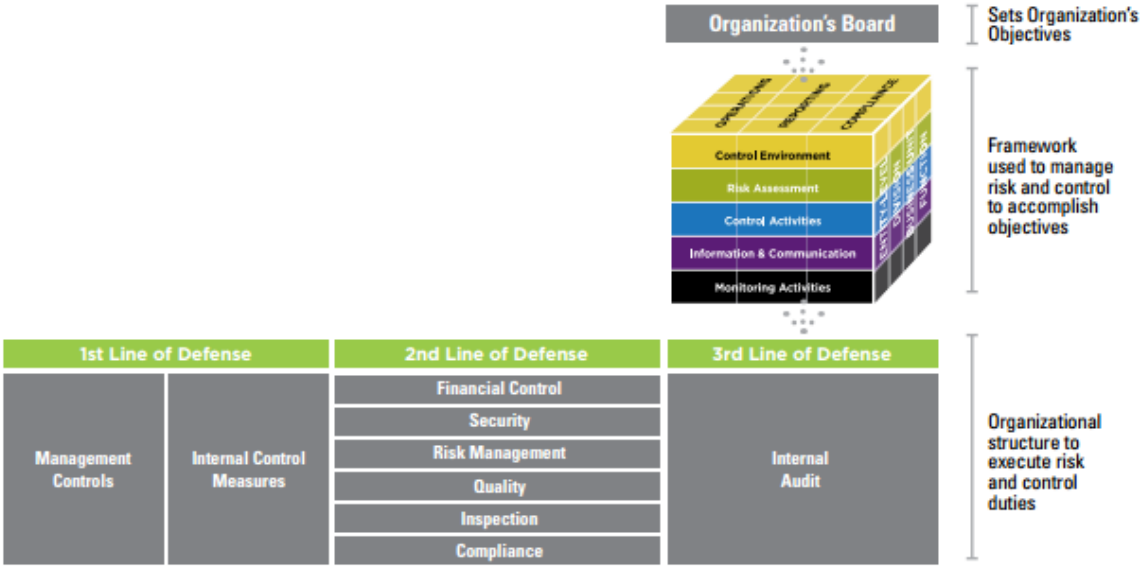
第二道防線：風險控管單位以其專業的知識，執行政策和收集資訊，進行流程優化，設計風險管理工具，產生企業整合觀點的風險和控制，並持續監控，幫管理者確認第一道防線的控制與風險管理程序被適當的設計，並如預期的運行，但仍接受高階管理者控制和指揮。

FRBNY 由風控長領導之風險管理事業群負責,監督及協助第 1 道防線執行風險控管，並建置風險管理架構，與法規遵循、資訊安全等部門為風險管理的夥伴，制訂及推行相關風險政策，並將評估結果向資深管理階層及董事會報告。風控長並定期向總裁報告。

第三道防線：內部稽核單位維持其獨立性，執行稽核工作並向董事會和高階管理者提供風險和控制有效性的確信。由稽核長領導之內部稽核部門負責，對風險管理及內部控制提供其獨立之評估意見與結果，包含對第 1 道及第 2 道防線之評估意見。稽核長將評估及稽核結果直接向董事會報告。

COSO 與內部稽核協會(IIA)於 2015 年，將風險管理的三道防線，與內部控制的管理架構整合如圖一，有效管理風險需要運用 COSO 目標、要素和原則，來執行內部控制，而三道防線說明了 COSO 的內部控制架構應由組織中何種部門負責，及應如何合作。

圖一、風險管理三道防線與內部控制架構圖



資料來源：FRBNY 摘自 COSO。

肆、紐約聯邦準備銀行風險管理

工作目標：風險管理主要在因應內部和外部的不確定情況，增進銀行達成目標的能力，並將風險降低至可接受水準。有效的風險管理，有助決策制定和計畫，在多種可能的未來場景中，計算風險承擔，提供資深管理者曝險程度是否在可接受水準的相關資訊，主動承擔對的風險，並將風險決策的責任指派至適當階層以增進組織的彈性。

可容忍風險：代表銀行可接受未來結果的範圍，由風險管理委員會及董事會制定，記載於可容忍風險報表，並每年更新。

風險管理的活動遍及整個銀行包括：風險辨識、風險分析、風險降低、風險報告和監視活動。風險辨識係基於要達成的目標，辨認其為機會或威脅，並對風險發生的可能性，威脅性的大小進行評估，若超過可容忍風險，必須採行降低風險的控制或活動，持續監控以確信風險管理是否達到效果。

風險管理由風險長 CRO(Chief Risk Officer)負責，建立風險管理架構，以風險管理

的三道防線定義風險管理的角色與責任，並向風險管理委員會及董事會報告。工作範圍包括作業風險、財務風險、財務報告風險、策略風險、名譽風險、法律風險、法規遵循風險，說明其定義如下：

作業風險：直接或間接的損失，由不適當或失敗的內部程序、人、系統、或外部事件的衝擊影響內部程序、人、系統。

財務風險：由無能償還的借錢者造成的直接財物損失，資產價格和利率與市場價格走勢相反的操作造成的損失。

財報風險：不適當的財報內控架構造成重大財務報表誤述。

策略風險：因業務或資源的錯誤計畫無法完成目標，或對外部環境改變沒有反應。

名譽風險：社會大眾對銀行的負面觀感影響任務的完成。

法律風險：無法執行的合約、訴訟或不利的判決影響完成目標的能力。

遵循風險：來自不遵守法律、規定和內部政策或道德標準的法律處分、財務或名譽的損失。

伍、第二道防線

一、FRBNY 作業風險報告

(一)風險報告的種類：作業風險報告包括風險事件報告、風險與控制自我評估報告(每年)、稽核與風險管理委員會報告(每季)，分別說明如下：

1.風險事件報告

(1)當事件發生時，不論職位高低，都有報告的責任，第一個報告的應被獎勵而不被懲罰。

(2)內容包括對事件的描述，事件的影響及嚴重性分析，發生的原因，及可能的解決方式(含長期及短期)。

(3)加強辨識業務和控制的弱點並在事件發生後建立對策。

2.風險和控制自我評估報告內容

各業務單位每年報告一次,內容詳盡但不易於對銀行的整體剩餘風險有了解。內容如下：

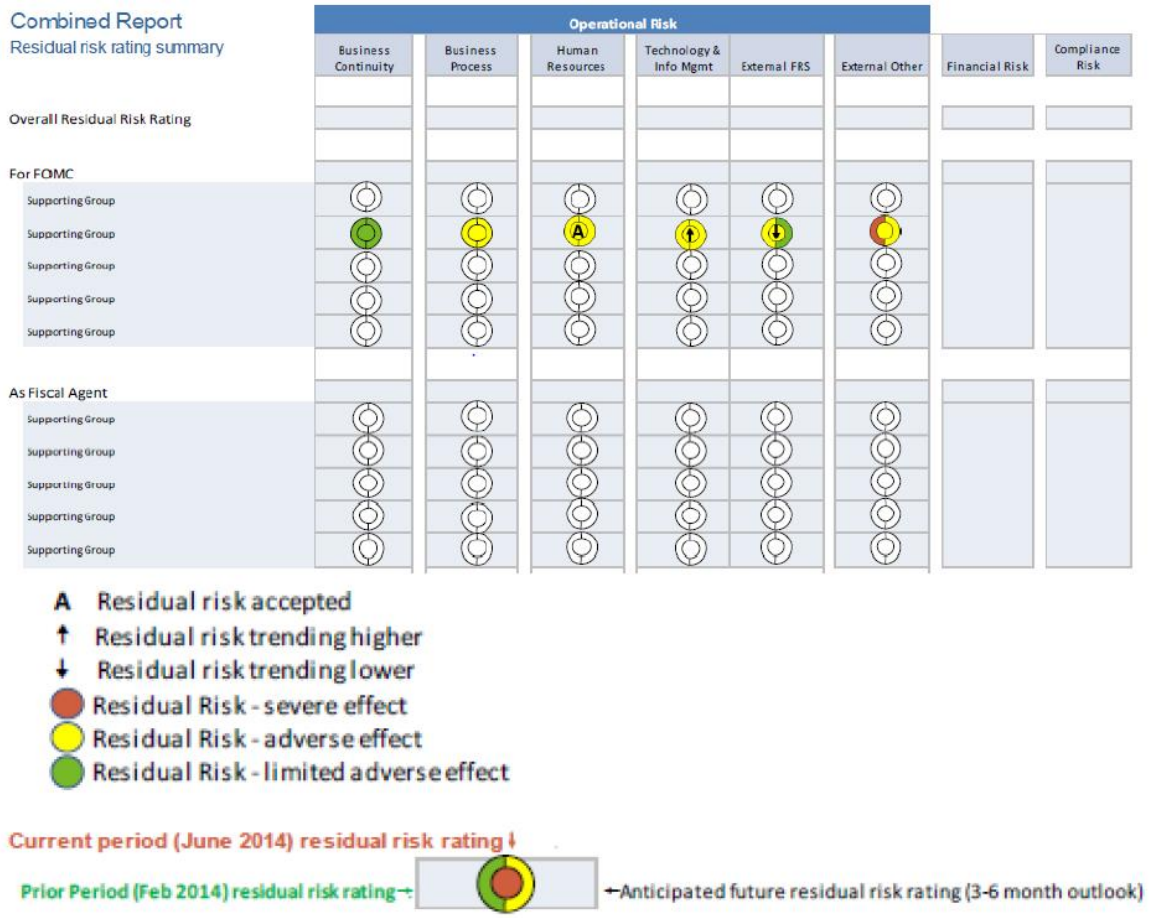
表二、風險與控制自我評估報告項目

項目名稱	項目概述
風險標題	對所評估之風險做簡要的總結
風險描述	闡述所評估之風險
可能性	在一定的時間範圍內，以低、中、高去評估風險事件發生的可能性；一般時間定為一年。
影響	衡量意外事件、問題或變動，發生時或可能發生所引發的效果，以低、中、高去評估。
固有風險分級	此風險之於企業,乃管理階層沒有採取行動去改變該風險發生的可能性或衝擊，按其可能性或衝擊評估風險，以低、中、高去分級。
影響的減輕(Mitigation)	說明為了降低經辨識之風險發生的可能性及/或影響所採取的行動，說明中對於經由特定的控制可以減輕風險，以及無法減輕風險兩方面，均應表達出來。
殘餘風險分級	固有風險中在經由控制或採取其他減輕行動後剩餘的部分,按低、中、高去評估。
風險接受度或未來減輕風險的步驟	如果殘餘風險評估無中或高級時,需將未來進一步降低殘餘風險等級之步驟的計畫,或企業可接受殘餘風險的等級列為報告表。
新興風險	可能對銀行產生影響之新起的發展中或變動中的風險。

3.稽核與風險管理委員會報告(每季)

以核心責任分類表達全行的剩餘風險，較為全面並使用風險標記，須對過去、現在和未來的風險進行評估，分析影響的嚴重程度、風險趨勢向上、向下及是否可接受等，較能促進跨功能組織、風險及管理委員會、稽核等之討論(如圖二)。

圖二、稽核與風險管理委員會報告



資料來源：FRBNY 課程資料

(二)風險報告的發展

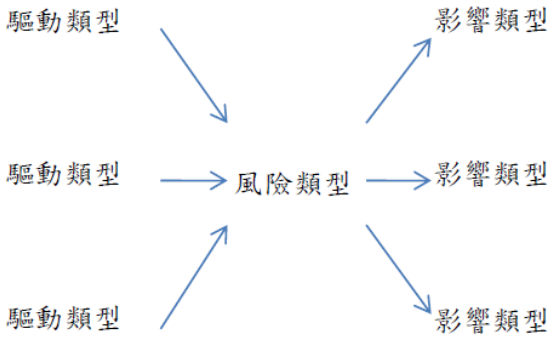
1.發展嚴格定義的分類辭庫

由於上述三種不同報告之間不容易產生連結，FRBNY 發展五個分類辭庫，包括：程序類型(Process Type)、驅動類型(Driver Type)、風險類型(Risk

Type)、影響類型(Impact Type)、控制類型(Control Type)，使所有業務單位的風險報告的用語可以一致。

FRBNY 利用蝴蝶結理論(Bow-Tie)，以風險事件為中心，一個風險類型成因可能是多個不同的驅動類型，並產生多種影響類型，對各種影響類型做詳盡的定義，可以同時用在風險事件報告的嚴重程度和風險與控制自我評估報告的影響，使不同報告間有一致性。

圖三 分類詞彙庫表



程序類型 Process Type	驅動類型 Driver Type	風險類型 Risk Type	影響類型 Impact Type	控制類型 Control Type

資料來源：FRBNY 上課資料整理

2.將統一定義的分類辭庫應用到風險與控制自我評估報告(年)

(1)為每項業務增加風險與控制自我評估的方法學

①辨認合適的程序類型

②為每個程序類型辨認風險類型

③為每個風險類型指定可能性和影響類型，算出一個風險等級

④驅動類型和影響類型被選擇來解釋風險等級

⑤全部的控制類型有四個屬性來計算出控制等級

⑥因為漸增的控制等級使固有風險分級下降

(2)所有中、高、非常高的剩餘風險需要判斷接受風險或降低風險。如果接受風險要有正當理由，如果降低風險要有行動計畫、負責人、目標完成日、預估計畫完成後的剩餘風險並與策略目標連結。

二、法規遵循

法規遵循部門於 2005 年 7 月成立，FRBNY 雖早已具有道德的企業文化和健全的業務處理，但缺乏一個綜合的架構可以評估這些做法，並將它文件化，做為一個監理機構，決定建立法規遵循部門。

FRBNY 有較成熟的風險管理架構及較廣泛的職責，如公開市場操作、各國央行國際帳戶服務、代表美國政府進行交易、國際美元運送、金融監理與穩定等，且是聯邦準備銀行中唯一具有法規遵循職能的分行。

法規遵循部門的任務是辨認、評估、監理和更正銀行的相關風險，必須對銀行的每項業務有所瞭解，並建立全行風險盤點(Comprehensive Risk Inventory)與記錄每項控制，與各部門緊密合作，提高全體職員對此風險的認知。每一個事業群均被賦予責任，於各業務領域建置和落實各項法規遵循計畫，並提供確信與諮詢服務，因此團隊必須具備各種不同專業的員工，包括法律、分析、技術和監管等，以便在發生影響分行聲譽或法律事件時有立即反應的能力。部門設有法規遵循、道德辦公室、確信和諮詢四個子部門，並向總法律顧問、風險長、風險及管理委員會報告。

目前部門執行的重要計畫包括舞弊、洗錢、道德與行為、保管品、交易和敏感性資料管理等。

FRBNY 反舞弊的方式如下：

(一)舞弊相關資訊覆核：使管理階層有效確認關於舞弊的所有知識差異或員工、離職員工等提供的舞弊傳聞。

(二)建立檢舉熱線。

(三)對檢舉者的政策：如何保護或獎勵檢舉者。

(四)舞弊風險評估：針對用機密資料獲取私人利益、採購實務舞弊、操縱財務結果以達到獎勵條件、具特殊權力的人犯下舞弊進行評估。

表三　法規遵循的實施架構

程序	內容
辨識與評估法規遵循風險	辨識、瞭解及監控法規遵循風險環境之變動，辨識適用的法律及規範、法律與聲譽風險，初步評估法律遵循情形並加以強化，優先運用資源因應此類風險。
政策規劃	規劃政策因應已辨識之法律及規範要求、法規遵循及聲譽風險，必要時隨時更新政策。整合正式的程序及其他初步評估情形，以執行政策。建置政策溝通、程序與其他初步評估之管道或平台。
政策實施	將政策轉換為初始評估法規遵循，促進各相關人員及營運活動合乎法規遵循目標(例如改變營運程序、強化流程、規劃新的內部控制程序與教育訓練等)。建置這些初步評估結果之溝通管道。
法規遵循監控	包含主動、定期與逐日監控法規遵循計畫。逐日監控應由系統及程序支援；定期監控應包含評估整體法規遵循計畫與計畫之有效性。
法規遵循調查	透過監控程序，分析法規遵循議題及缺失，採取修正行動，並藉由發現之缺失及調查程序，改善整體法規遵循計畫。

產製報告	向主要利害關係人之報告應包含各項計畫要求之法規遵循標準、計畫有效性、重大的未符合規定情形、修正行動之執行情形，以及新納入考量之法規遵循風險。

資料來源：FRBNY 上課資料整理

三、持續營運計畫

持續營運計畫是參考國際清算銀行所定的金融機構高階營運持續原則(High-level Business Continuity Principles for the financial sector)與國際災難復原組織專業實作要點(Disaster Recovery Institute International professional practices)，制定出整個聯準會的持續營運架構準則，提供一套基本的標準給所有分行，定義持續營運業務的範圍，並給予持續營運計畫極高的權限，以獲取所需的資源。

持續營運計畫的訂定目的，是為了使銀行的核心業務包括執行貨幣政策、維持金融穩定、提供各種財務服務，能在發生人為或非人為重大災變時持續地進行，有效的持續營運計畫，可以減輕營運中斷的影響，加速復原並降低整體的作業風險。

持續營運計畫主要由持續營運辦公室負責，監督所有業務單位對其計畫的持續發展，領導銀行對可能的威脅和可能的事件產生回應，並對計畫進行評測。

威脅的來源包括人為的及自然的，人為的包括資訊的威脅、恐怖分子的攻擊、抗議、內部破壞等，自然的包括暴雪、颶風、地震等，由於無法預測威脅的影響區域大小、發生的時間及持續的時間，因此保持彈性是重要的。

FRBNY 考慮的情況包括：建築物無法使用、溝通管道中斷、員工短缺及以上的綜合情況。

採取的措施包括：

(一)備用辦公地點：熱/冷的臨時辦公地點、與鄰近的大樓簽約承租辦公室、分散式的辦公、在家辦公等。

(二)備用溝通管道：擴音器廣播、EMAIL、語音留言、黑莓機、衛星電話、行動網路站台(air card)、由行外連線到行內取得資訊的連線、免費電話、備用電源及充電器。

(三)人員安全的考量：以員工的安全為第一要務，發給每位員工緊急應變手冊，準備雪鏟、食物等生活用品，以備緊急時使用，並發給管理階層可以立刻隨身帶走的災難包。

持續營運計畫的內容：

(一)業務的說明。

(二)關鍵性的程序及其實際上的應用。

(三)系統可容忍的中斷時間、上次備份資料的時間點。

(四)內部和外部的關鍵資訊。

(五)各項業務和系統的交互關係。

(六)基礎設施的空間需求。

(七)其他辦公地點的要求。

(八)尋找並和供應商討論需求。

持續營運計畫必須每年度進行認證，以確信其品質不會隨時間失效，因此持續的演練是重要的，平時及定期在電腦上進行各項狀況的模擬演練、實地進行大樓的疏散程序、緊急通知、消防演練、業務恢復、變換地點上班等，並每年五月訂一週時間為颶風週、定九月為預備月。

在各項演練中員工可以加強自己在計畫中扮演角色的了解,及各個角色的權限，熟悉各項業務的流程和優先順序，記錄演練的各項數據，如恢復系統需要的復原時間，聯繫同仁的速度，參與的員工比率等，發現演練的結果和計畫的差異，辨認和分享最好的做法，更好的改進計畫並調整目標，使員工對該項計畫的應變效果產生信心。

四、資訊的風險管理

駭客的攻擊行動逐漸演進，從原本的單兵作戰到團隊作戰，再演進成使用國家或組織的豐沛資源為後盾的進階持續性攻擊，針對鎖定的目標攻擊，極難防範，因此必須建立一個企業觀點的網路安全風險管理計畫來增進銀行的網路安全。

FRBNY 注意的資訊風險包括：

(一)網路風險及網路的持續營運(復原時間)：美國國家的安全威脅，嚴重程度可與恐怖主義相提並論，2016 年以綁架電腦付贖金的軟體為最大挑戰，醫院和醫療系統受到沉重的打擊。

(二)第三方風險：提供專業化的服務和節省成本，但安全度較低。

(三)內部威脅：惡意的員工、不知情的使用者錯誤的使用，社交工程已成為駭客網路攻擊的第一選項。

(四)資訊技能、人力的短缺：由於資訊的快速發展，系統採用的軟體、技術是否需要更新，過新或過舊的系統均有可能發生維護人員、技能的短缺。

(五)資訊安全。

(六)資訊資產管理。

(七)行動運算(Mobile Computing)。

(八)新科技：雲端、物聯網、機器人和大數據等。

(九)應用系統開發。

(十)法令遵循。

計畫的策略包括預防、偵測和回應。計畫內容為辨認、監視、檢測背景情況和報告固有的網路安全風險。計畫應考量成本效益，目的不在完全避免被入侵，而是快速反應，聚焦在保護系統中的重要項目，由高階管理階層評估實質效益，維持精簡、一致化、敏捷即時的安全系統。

預防措施：辨認風險後將風險列清單，進行評估風險和減低弱點，主動降低攻擊面、為攻擊者製造困難逼迫其放棄攻擊，並將對網路安全的警覺和訓練建立在所有的計畫中。

偵測：使用自製的或購買商業軟體等廣泛的自動偵測工具，自動化且持續的偵測系統，從政府、工商夥伴或外部蒐集各種威脅的資訊，送到智慧的情報庫進行判斷，且將同樣的事件資訊在不同的時間點重新運算。依照環境的歷史資料決定何為正常的事件發生頻率及門檻值，以注意異常為基礎偵測新的、陰險的攻擊方式，並警示差異以便迅速反應。

五、社交工程防範

社交工程是利用人性的弱點，應用形式簡單的溝通和欺騙技倆，以獲取使用者帳號、密碼、身分證號碼或其他機敏資料，來突破資訊安全防護，遂行其非法的存取控制、破壞行為。目前的駭客已將金融業列為目標，企圖利用社交工程的方式進入系統，取得內部的權限，攻擊系統進行盜領，並清除作案的軌跡。

社交工程的做法通常包括：

(一)釣魚：寄發電子郵件利用連結網址，以假的網站頁面騙取重要資料，如帳號、卡號、密碼等。

(二)利用隨身碟、電子郵件、檔案植入病毒，使人遭到入侵而不自知，並可以暗中蒐集機敏性資料、鍵盤側錄等。

(三)利用電話假扮委外廠商或上級機關的資訊人員，騙取帳號及密碼。

(四)黑函：利用極敏感的個人資訊，脅迫對方採取行動，要求贖金或取得所需要的資源。

使員工對資訊安全保持警覺是唯一的辦法，提醒員工：

(一)保管好自己的帳號及密碼，不告訴任何人。

(二)社交工程的攻擊者會從社群網站蒐集資訊，對公開內容要謹慎。

(三)注意保管日常使用的機敏資料。

(四)注意網站、郵件或文件等看起來不相關的微小差異。

(五)若誤觸可疑的網站、郵件或檔案立即通報請求協助。

FRBNY 建立的內控作為：

(一)對員工進行警覺力的訓練及測試。測試計畫包括設計一個電子郵件，決定受測試的使用者範圍，執行測試並立即通知未通過者，收集並統計資料，分析什麼情況下容易上當，並調整系統及測試計畫。

(二)對收到的電子郵件須有保護措施，不允許信件預覽、執行安全掃描等。

(三)對安裝軟體和使用個人儲存裝置進行控管，僅允許使用正版軟體、經過資訊部門許可的軟體和公務用的儲存裝置等。

六、沙賓法案的遵循

沙賓法案的內容自 2002 年公布，FRBNY 雖非其適用範圍，但已主動遵循其規定，介紹如下：

管理階層每年須向董事會提出財務報表與附註的內部控制有效性聲明，管理階層的聲明必須經過適當的評估程序，每一個業務區有獨立的沙賓遵循小組負責測試，記錄所有的業務流程、關鍵風險及控制，並使用量化的計算方法進行測試，計算出會計報表誤述的值，及評估品質化的因素，且經過外部稽核單位 KPMG 查核 FRBNY 的內部控制。

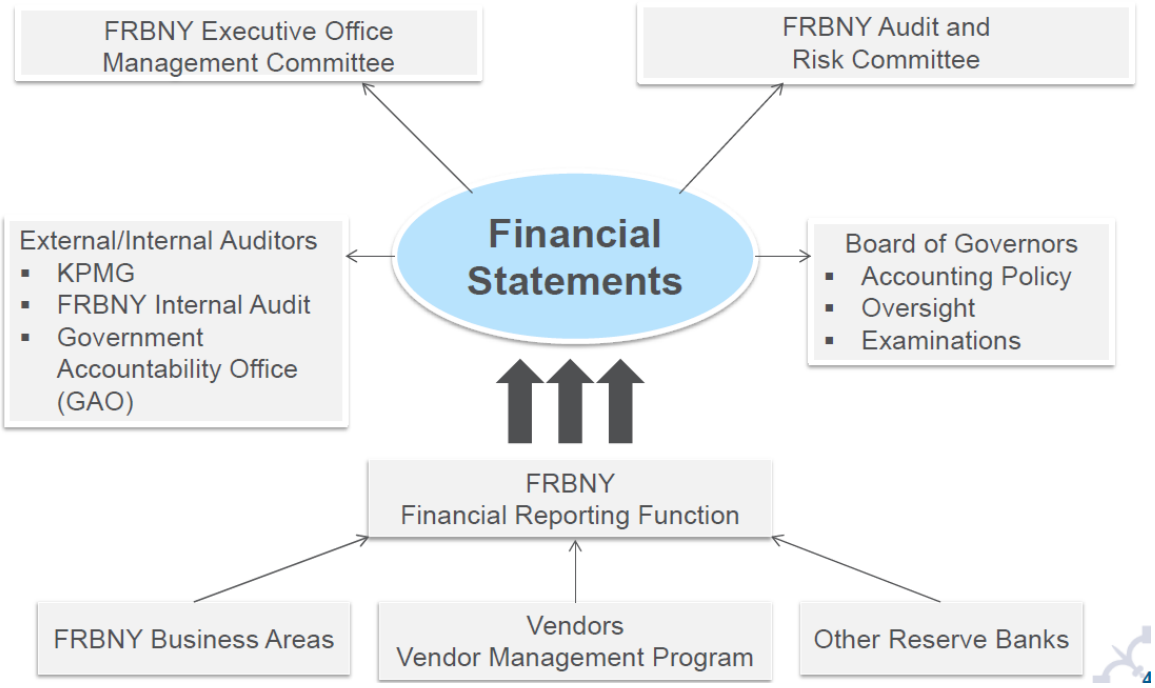
在採用 COSO 內部控制架構及其 17 項原則之後，需加強注意的事項：

(一)外包商(OSP)：要求外包商取得 SSAE No.16(即 SOC1 報告)稽核意見，以確認其內部控制有效性。

(二)對其他聯邦準備銀行提供的中央化服務，如有重大影響財務報表元素須提供信賴信(Reliance Letter)。例如：里奇蒙分行(Richmond)提供資訊科技的信賴信。

(三)舞弊，請參閱法規遵循章節中做法。

圖四、沙賓法案管理架構



資料來源：FRBNY 上課資料

陸、第三道防線－內部稽核

一、內部稽核執行程序

(一)計畫階段

FRBNY 使用風險基礎審計，計畫程序的綜合風險評估有助於聚焦在高風險區域，降低稽核的時間和成本。計畫的方式如下：

1.執行背景分析和風險評估：首先藉由各種稽核聯絡(Audit Liaison)蒐集財務或資訊科技等各種重大改變或事件的資訊，考慮上次稽核到目前發生過的

風險事件、取得高階政策或程序文件，再與業務部門管理階層、稽核小組、外部的審計員、董事長、稽核長等開會討論，內容包括 FED 總體的風險，對業務單位的稽核風險評估，及管理風險的自我評估。

2.摘要計畫期間應被執行的工作：首先洽詢業務單位最適合查核的時間，列出業務單位的活動，開會討論執行範圍，做成摘要。

3.發布正式稽核聲明給業務單位：將有關高階稽核範圍、計畫的時間軸、稽核小組的資訊和客戶溝通，規劃分工表及預算以完成稽核計畫，附稽核範圍摘要向稽核長(GA)報告獲得同意後方可進行稽核。

4.和業務單位進行啟始的會議，提出要求的文件清單。

(二)實地查核 Fieldwork

進行方式包括穿行測試(Walkthrough)、細節測試、提出稽核意見。只有重要影響管理者目標和相關風險的控制活動，才需要進行穿行測試和評估。細節測試是利用詢問、觀察、檢查、重新執行、系統詢問(IT 應用控制)、抽樣及資料分析進行。

(三)提出稽核意見、報告、追蹤

執行測試發現的結果分為有效、一般、和無效，如果發現內部控制有缺失，將與業務單位的主管討論，依其嚴重性分為四個等級，進行不同的後續處理與追蹤：

1.高度重要：立即採取行動，列為高階管理者須處理的問題，當該問題已得到糾正，稽核將進行後續工作驗證。

2.重要：迅速處理並使管理階層注意問題，稽核將每月追蹤，直到問題得到糾正。

3.較不重要：值得管理階層關注，稽核人員將於業務單位提供的預計修正日期後，再追蹤這一問題。

4.不重要：在稽核的過程中，或在收尾會議上討論，且不追蹤。

追蹤的程度應足以斷定問題已得到糾正和新程序已實施，高度重要和重要問題的追蹤應包括具體問題的糾正且進行額外的實質性測試，所有的追蹤應作成詳盡的紀錄並被適當階層覆核。

(四)稽核小組的考評

稽核計畫評量被視為領導能力的表現，考評方式如下：

1.在計畫階段組長就將考核表發給每一個組員，給予充裕的時間。

2.稽核人員自我評量：要求提供可量化數字或特定例子而不是主觀的評量分數。

3.組長在組員的自我評量加註評論。

4.評量表和管理專案的關係領導人(Relationship Leader,RL)討論。

5.完成的評量表給關係領導人 RL 和稽核長 GA 確認。

考核表內容項目：

1.預算和實際的結果。

2.稽核員有什麼優良事蹟。

3.小組哪裡可以改進。

4.跟客戶的互動是好、一般或較差(Good/Fair/Poor)。

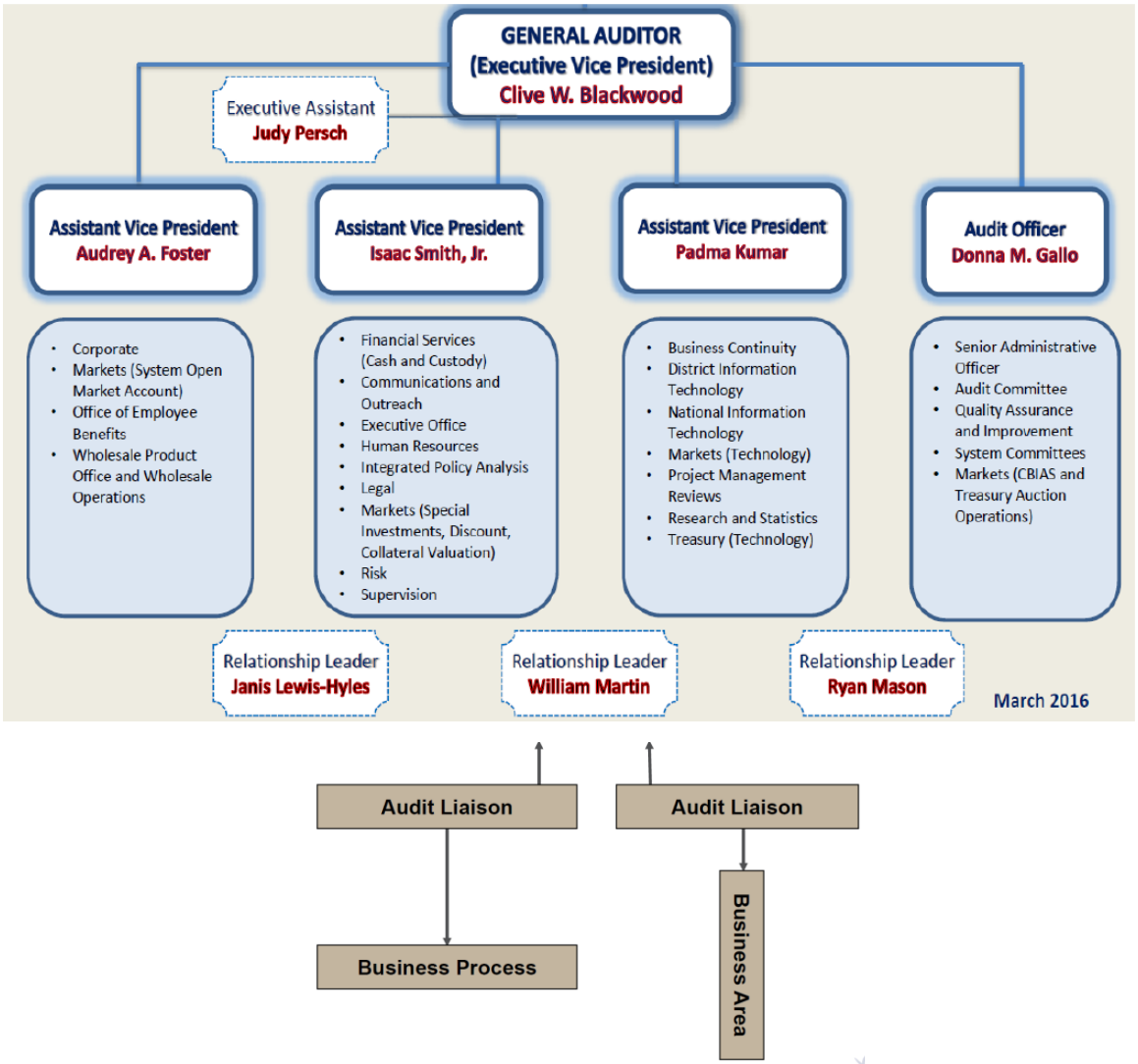
5.是否建立良好關係。

(五)關係領導人(Relationship Leader,RL)與稽核組織架構

FRBRN 相當重視內部稽核與受查單位的關係，因此設立關係管理人，目的在借重其於指定業務運作和風險全面的了解，持續與業務溝通建立有效

的關係，新的業務變化、科技、稽核意見(Audit Issue)的溝通和所有的稽核聯絡(Audit Liaison)均由其管理。

圖四 稽核組織與關係領導人責任



資料來源：FRBNY 課程資料整理。

二、內部稽核的風險評估方式

風險評估要基於固有風險、剩餘風險，並思考新興的風險，以系統性的程序，進行專業的判斷。FRBNY 風險評估的方法第一步是將所有受稽核單位的活動列出，考量風險的高低及計算風險分數，介紹如下：

(一)風險因子：包括作業面的業務處理、科技和資訊管理、人力資源、財務、策略；信譽風險之前單獨列示，目前已併入其他風險。

(二)權重：風險因子的權重是經過討論事先決定的，為了因應日漸增加的資訊科技風險，將信譽風險的 10 分加入資訊科技風險。

(三)指定風險等級 1-4(4：高；3：中高；2：中；1：低)。

(四)風險分數=風險因子權重 X 風險等級。

(五)計算總分。

表四 分數計算表

風險因子	舊權重	新權重	等級	舊分數	新分數
作業風險					
1. 業務流程	20	20	4	80	80
2. 科技和資訊管理	20	30	4	80	120
3. 人力資源	20	20	2	40	40
財務和重大事項	20	20	3	60	60
策略	10	10	3	30	30
信譽	10	0	3	30	0
合計	100	100		320	330

資料來源：FRBNY 課程資料整理。

計算完成後，根據風險分數排名，並決定稽核頻率及調度稽核範圍。

表五 風險等級與稽核頻率表

風險等級	舊風險分數	舊稽核頻率	新風險分數	新稽核頻率
高	326-400	每年，但有重要因素可以延至 2 年	350-400	最久二年稽核一次
中高			276-349	最久三年稽核一次
中	251-325	每 3 年	200-275	最久四年稽核一次
低	100-250	稽核長裁量	100-199	稽核長裁量

資料來源：FRBNY 課程資料整理。

柒、第一道防線－以躉售支付部門(Wholesale Product Office)為例

躉售支付部門負責管理、作業、支援和發展新的大額支付服務、提升服務、定

價模型、確認傳送大額支付服務的科技是安全、有彈性和符合業務的需求。

目前的服務有

一、跨行資金移轉服務(Fedwire Funds Service)

二、登錄債券移轉服務(Fedwire Securities Service)

三、全國清算服務(National Settlement Service)

躉售支付部門使用風險管理部門設計的政策和工具衡量和管理風險，執行風險的自我評估，記錄風險事件和決定風險原因，在日常業務的決策中同時管理風險的可容忍度，使風險降低至銀行的可接受程度。

表六　風險類型的活動、角色和責任

風險類型的活動	角色和責任
辨認，分析，回應，報告和監視	確認躉售支付部門的程序、人和系統的相關風險，及外部事件都被辨認和了解。
定義可接受風險程度	建立躉售支付部門的風險可接受程度和管理大額支付服務的風險，以及銀行的風險可接受程度。
確認適當的風險控制	設計、執行和測試適當的預防性控制，並輔以偵測控制和更正控制。
風險事件原因分析	了解風險事件和標記直接和間接的成因，包括外包的業務活動。
以風險為基礎的決策制定	將風險因素納入戰略制定，確定優先事項，並定期決策。
風險管理架構	確認客觀地評估，分析，回應，報告和風險升高。
和第二道、第三道防線溝通和合作	企業風險監視、作業風險監視、沙賓法案的遵循、遵循功能、內部稽核緊密的合作。
記錄流程以降低風險	確保操作流程均已適當記錄。
監測，報告和升級風險	促進及時監測，報告和風險升高流程使得銀行的高級管理層意識到顯著事件和重大變化對運營風險的影響狀況。
管理和減輕風險	實施行動計畫和維持內部控制以適當減低風險
參與聯邦儲備體系風險群	促進和共享各地的風險管理和最佳實踐

資料來源：FRBNY 上課資料

捌、心得及建議

一、外部環境的快速變化造成作業風險的升高

(一)資訊與科技

繼電腦之後手機興起，連上網路的裝置越來越多，使用網路的時間也越來越多，享受便利的同時，也暴露在越來越高的資訊安全風險中。如孟加拉央行的盜領事件，駭客經由攻擊行動轉走鉅額的存款，環球銀行金融電信協會 SWIFT 警告金融業已經成為駭客的重要攻擊目標，銀行中的每個人、使用的每個機器都必須小心相關的資訊風險，避免自己成為駭客的跳板，造成重大的損失。

本行資安制度及相關內部電腦稽核工作已遵循國內外相關標準相當完備，且已對本行員工介紹社交工程的攻擊方式及進行測試演練，將測試結果統計分析，作為改進的參考，並通知未注意的操作者以提高其警覺性；對於新興的資訊科技、資訊風險亦開辦課程對員工講授，但資訊科技日新月異，隨時可能有新的攻擊方式出現，因此仍須繼續提高警覺注意相關風險。

(二)極端氣候或災難

氣候越來越極端，脫離以前的規律，例如：夏天氣溫不斷創歷史新高、颱風強度創紀錄、降雨越來越集中強度也越來越大，同時乾旱的地方也越來越乾，氣候變化對作業環境帶來更大的風險，水災、風災、旱災、熱傷害、停水、停電等。

FRBNY 對於各種災害情況進行實際演練，不斷與各單位溝通檢討，了解作業環境的各種變化，以改進持續營運計畫。目前本行已考量各種災害建立處理應變措施，並定期演練，應繼續保持，未來亦將視演練情形繼續改進。

二、內部稽核的角色逐漸改變

FRBNY 稽核人員以往擔任發現錯誤的角色，經常造成與受查部門關係緊張，如今轉為以注重工作關係為優先，與受稽核單位建立互相信賴的關係，及擔任諮

詢的角色，期能提升稽核在組織中的價值與能見度。

但由於環境的快速變化及資訊科技的發展，稽核人員面臨相當大的挑戰，不只是目前受稽核單位的業務面需要瞭解，還包括未來可能的發展，新興的風險、科技等，才能應付當前的環境。

FRBNY 的課程內容豐富且實務做法相當具有參考價值，建議考量組織的需要，持續參加相關課程，提升內部稽核人員的能力，以面對各種新興變化產生的風險。

參考資料

1. Review of the Principles for the Sound Management of Operational Risk, BIS, Oct 2014.
2. Leveraging COSO Across the Three Lines OF Defense, COSO, 2015
3. FRBNY 課程資料
4. 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。
5. 游金鳳(2014) 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。
6. COSO 企業風險管理執行摘要，2004。