行政院及所屬各機關出國報告

（出國類別：其他）

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

服務機關：中央銀行

姓名職稱：陳證吉/四等專員

出國地區：美國紐約

出國期間：104 年 5 月 16 日至 23 日

報告日期：民國 104 年 7 月 27 日

「作業風險管理與內部稽核」訓練課程出國報告

目 錄

「作業風險管理與內部稽核」訓練課程出國報告

壹、前言

職奉准於 104 年 5 月 16 日至 23 日參加美國紐約聯邦準備銀行(以下簡稱 FRBNY)舉辦之「作業風險管理與內部稽核」訓練課程，為期 3 天半，計有 50 個國家及國際貨幣基金(IMF)、國際清算銀行(BIS)等派員，共約 81 人參加，除由該行所選派之各部門專家講授課程外，並安排 IMF 講師介紹 IMF 提供會員國融資時之保障評估(Safeguard Assessment)措施，透過講師講授課程暨與其他國家學員間之意見交流，課程兼具理論與實務。借鏡 FRBNY 之經驗與制度，可作為各國央行強化作業風險管理及內部稽核之參考。

本次課程全體參訓學員於報名時需先至該行網站填寫基本資料、工作內容與所屬央行風險控管機制之問卷調查，依問卷統計彙整結果，參訓學員多來自各國央行之內部稽核、風險管理及企業持續營運部門，多數國家央行設有正式之風險管理委員會(67%)，訂定作業風險管理計畫(85%)及持續營運計畫(87%)，並對海外大額之投資部位設立正式之審議委員會及訂定投資專案計畫(65%)。

本報告共分為七個部分，除前言外，依序為內部控制與作業風險管理，探討內部控制架構及風險控管機制；其次為資訊及網路安全，探討資訊安全控管、持續營運及備援機制等；第三部分為企業風險管理，探討企業風險涵蓋範圍及防線機制；第四部分為法規遵循，探討法規遵循職能及相關業務範圍，包含道德辦公室之設置；第五部分為內部稽核，探討稽核人員的角色及功能，以及內部稽核職能與現行運作機制；最後為結語與建議，另將 IMF 之保障評估措施收存於附錄。

貳、內部控制與作業風險管理

一、COSO 整合式內部控制架構

FRBNY 採美國「反舞弊性財務報告委員會所屬發起組織委員會」(Committee of Sponsoring Organizations of the Treadway Commission，以下稱 COSO)2013 年新版之整合式內部控制架構，包含控制環境、風險評估、控制活動、資訊與溝通及監督等 5 大要素共 17 項準則。新版 COSO 保留原版本內部控制定義和五大要素之基本精神，內部控制受先天的限制，對財務報告可靠性、營運之效果及效率與法規遵循等，僅能提供合理(而非絕對)之確信。

新版 COSO 特別強調管理階層之職能，組織之管理階層對內部控制制度良窳應負全責，其在設計、評估及判斷內部控制之有效性時可由資深業務與稽核等專業人員協助。良好的內部控制架構有助於對治理監督之期望，因應法律、規章、條例及準則的要求及複雜化、市場及營運的全球化、日趨複雜之業務變動，並滿足適任性、課責性、預防及偵測舞弊之期望等，2013 年新版 COSO 整合式架構內容如**表 1**。

表 1　2013 年 COSO 整合式內部控制架構之 17 項準則

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.承諾之能力 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。

二、以作業流程圖控管作業風險

(一)作業風險定義

新巴塞爾協定(Basel II)將作業風險定義為「因內部作業、人員及系統之不當或失敗，或因外部因素導致損失之風險」。作業風險發生的主因可歸納為人員、系統、作業流程及外部事件四大類，分述如下：

1.人員：由組織內部人員之故意或是無心行為所導致，例如分權不適當、人力不足、缺乏經驗或能力、舞弊或疏忽等；

2.系統：由於資訊及各類基礎設施失效所導致，例如系統或通訊中斷、控管不佳、程式或資料錯誤等；

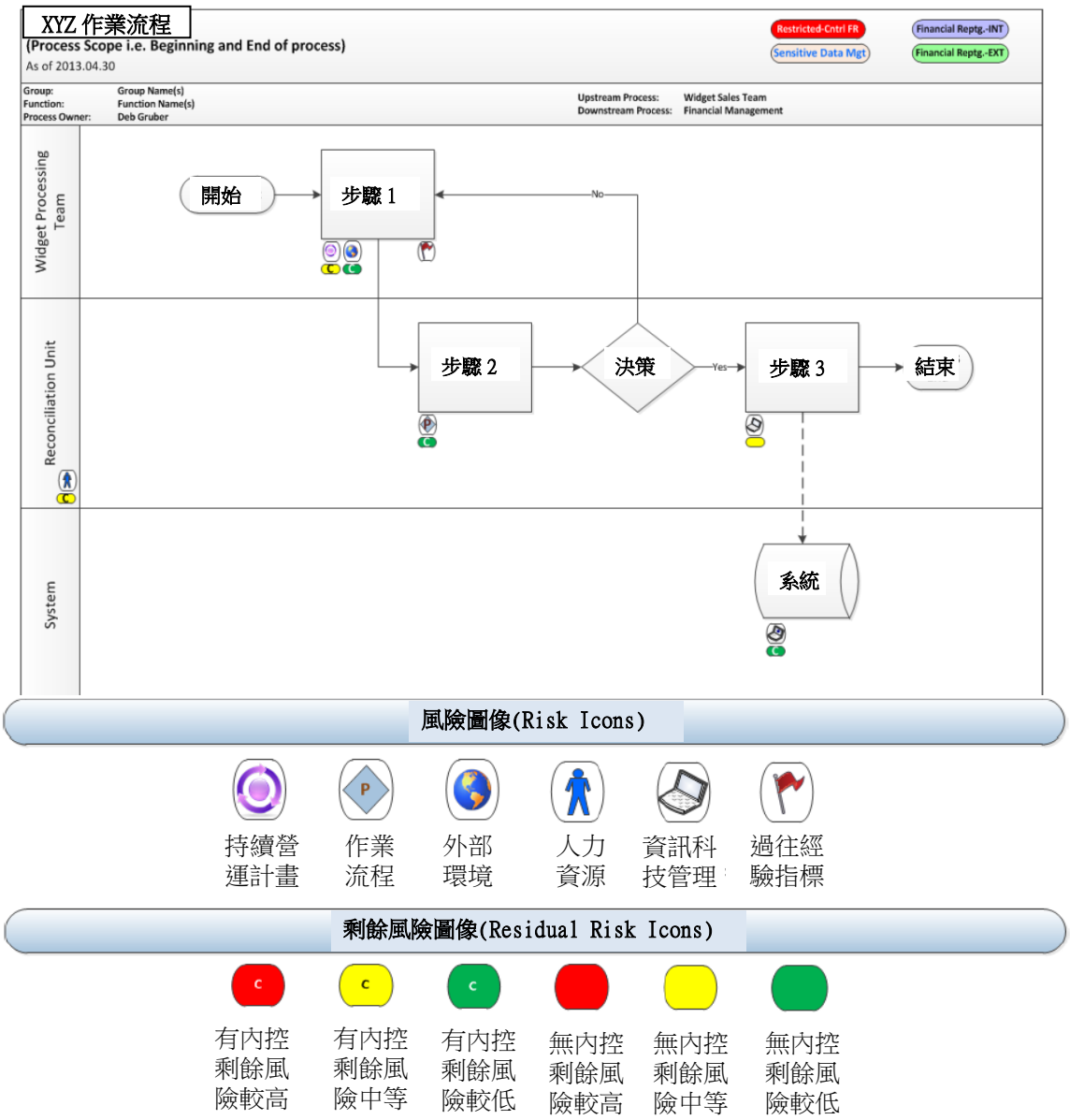
3.作業流程：由於交易、清算及營運流程之失誤所導致，例如模型或參數設定錯誤、執行錯誤、錯帳、產品過於複雜、逾越授權等；

4.外部因素：由於外部詐欺、實質資產毀損，以及各類法令改變影響業務持續營運之外部第三者行為所導致，例如政治因素、賦稅、法令與經濟環境變動、天災或恐怖攻擊等。

(二)以作業流程圖控管作業風險

FRBNY 近年持續研發內部控制相關工具及程序，以辨識與評估實際及潛在之風險，改善其風險架構及監控措施。該行採用近似作業流程圖之營運風險與控制圖(Business Risk and Control Mapping，BRCM)，用以控管作業風險。相較於一般流程圖之各階段評估結果僅以 2 分法列示「是」或「否」，營運風險與控制圖輔以風險圖標(Icon)及殘餘風險圖標，明確表達各階段風險之屬性(如屬於持續營運、作業程序、外部環境、人力資源等相關風險)、內控措施是否存在(有或無)及殘餘風險之高低(高度、中度及低度)等，以更貼近實務運作情形，使用者可更明確瞭解作業流程之評估結果，採取因應措施。

圖 1　FRBNY 營運風險與控制圖



資料來源：FRBNY 課程資料

(三)新巴塞爾協定之作業風險評估相關規範

美國自導入新巴塞爾資本協定（Basel II）後，有關資本適足率之計算，區分為大型及其他(非大型)銀行，各適用不同之計算標準；2007 年之「最終規定(Final Rule)」中，採以風險為基礎之資本規範—進階資本適足架構（Risk-Based Capital Standards: Advanced Capital Adequacy Framework），明定總資產大於 2,500 億美元之核心大型銀

行應採行各類風險之進階衡量方法，另有部分非大型銀行亦選擇採用(Opt-in Banks)。為強化銀行之資本品質與銀行體系之穩健性，聯準會(Fed)與聯邦存款保險公司(FDIC)於 2012 年公布市場風險資本規範之最終規定（Basel 2.5），將 Basel III 相關重要規範納入該規定。

最終規定要求銀行業以系統化評估作業風險，方式如下：

1.內部作業損失事件資料法

聯準會要求 19 家主要大型金融機構，定期傳送全部之損失資料，且至少需採用 5 年之觀察期(樣本點)，並依 Basel II 所規範之事件型態評估，每季並彙報其評估結果。

2.外部作業損失事件資料法

銀行向外部供應商購買套裝軟體或事件資料庫，協助建置資本模型、進行模擬情境分析並產製報告，惟可能有適用上之困難。因此，聯準會允許銀行採用內部及外部損失事件資料法混合運用方式。

3.情境分析法

設想各種可能情境，該法仰賴資深管理人員之專業判斷，與前 2 項之歷史資料損失事件資料法相較，較具前瞻性，並可採模型或定性分析(Qualitative analysis)[1]。

4.自我評估法

為近期最新發展之方式，本法需定期對營運環境及內部控制進行回溯測試(Back-test)，常見的有控制測試法、風險控制與自我評估法[2]等。

[1] 定性分析(Qualitative analysis)：與量化分析(Quantitative analysis)相對，係依經驗綜合判斷風險大小排序，例如將風險依影響專案目標達成的嚴重性分成大、中、小三類風險。

[2] 風險控制與自我評估法(RCSA)為風險自評之工具，其主要目標在辨識機構內部主要業務流程之潛在風險及現存控制機制是否有效。檢視流程以辨識營運過程中可能發生之作業風險點，依造成原因將作業風險事件進行歸類，並對事件發生之影響程度與發生機率進行分析。

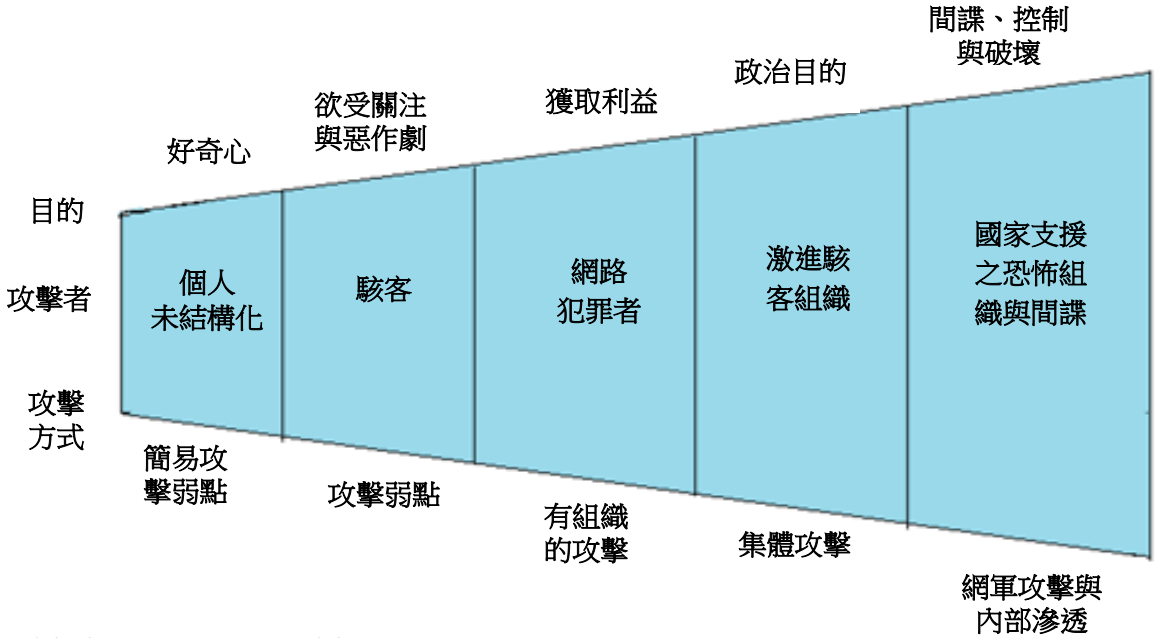
參、資訊及網路安全

一、採整合式策略規劃以控管資訊安全風險

(一)網路攻擊模式持續進化

資訊環境係屬組織營運作業中，最重要環節之一，近年網路駭客攻擊手法持續進化，資訊安全議題受到高度重視。網路攻擊已由過去單兵作戰之非結構化模式，蛻變為組織化、系統化，利用組織或國家豐沛資源為後盾之進階持續性威脅(Advanced Persistent Threat) **(詳圖 2)**。

圖 2 網路攻擊模式之演化



資料來源：FRBNY 課程資料

近期源於組織內部之新興威脅，則更令人防不勝防，可分為下列 2 模式：

1.內部威脅(Insider Threat)

組織內部因員工無心及偶發因素，如開啟不明電子郵件或登錄惡意網站遭植入程式；抑或駭客收買組織內部員工或直接派員滲透組織等方式，直接由組織內部癱瘓系統。

2.第三方威脅(Third Party Threat)

由於組織與其系統或採購合約廠商間之資料介接或網路連結，往往未設置防火牆機制，若廠商系統遭駭客入侵或滲透，將直接或間接影響組織之資訊安全。

(二)FRBNY 因應之道

FRBNY 認為目前不論如何提升資訊安全控管，欲完全避免遭駭客攻擊與入侵，幾乎是不可能。為降低資訊安全風險，FRBNY 自 2009 年開始進行一系列長期計畫，由基礎作業、政策及設施，以主動積極態度，聚焦於資訊科技生命週期，適時修正政策及規範；目前正持續發展整合式策略規劃，籌組「資訊安全策略架構」部門，專責控制環境、資訊安全評估及服務管理；並因應資訊專業人員供不應求而持續進行人才培訓；以及規劃未來將上開資訊安全部門與企業營運活動更緊密之整合。

二、持續營運計畫

(一)設立持續營運計畫辦公室，定期演練備援機制

持續營運計畫為 FRBNY 年度風險評估重要項目之一，目的係消弭及降低人為及非人為(天然)之災害導致下列 3 大核心任務營運中斷之影響及風險：

1.貨幣政策之執行

2.對存款機構、市場與支付系統之監督，與其最後放款者(Lender of the last resort)之角色，以支援金融穩定。

3.提供金融服務予金融機構、政府與外國央行等。

FRBNY 於其企業事業群(Corporate Group)下設立持續營運計畫辦公室，規劃當建築物毀損、通訊或交通中斷、員工無法出勤，抑或前述情境同時發生之複合式情境等應變機制。主要解決方案除於備援場所異地營運外，另有借用鄰近其他銀行及飯店、員工在家工作等方案。特別強調「員工安全至上」，制定安全演練及疏散程序，並修訂全體職員緊急因應手冊，最關鍵要素為模擬各種可能情形及「持續定期的演練」，使全體職員，尤其是業務核心人員，熟悉在緊急事故發生時，其所扮演的角色及職責。FRBNY 持續營運計畫包含：

1.業務概況

2.業務影響因素分析

3.關鍵程序辨識與應用工具

4.復原時程與目標

5.基礎設施及場地需求

6.連絡資訊

7.異常處理與備援地點

由於在發生特殊情形採異地營運時，人員可能分散於各不同地點，因此良好及有效的通訊為最關鍵要素，FRBNY 規劃採多元之通訊替代工具，包含大樓廣播、與銀行獨立之緊急電話、電子郵件、語音信箱、App 通訊軟體、黑莓機(Blackberry)及衛星電話等。另於營運及各備援場建置緊急發電機及不斷電系統，若供電中斷時仍可維持基本運作，以及確保食物及飲水之供應無虞。

(二)事件回應小組(Incident Response Team)

為有效執行持續營運計畫，FRBNY 設置事件回應小組，由各部門資深且經良好訓練之人員組成，目的係為快速及正確處理與資訊安全有關之緊急突發事件，協助處理並回復正常運作。該小組係任務編組，平時組員係隸屬各部門且均有例行業務職掌。但當有突發狀況需處理時，手邊工作可立即擱置(Drop)或交由職務代理人處理而赴小組報到。在處理突發事件時，該小組成員具有某種程度之決策權，以採取即時行動。事件回應小組主要職能及因應程序，列舉如下：

1.辨識組織程序，以處理資訊安全事件。

2.尋找所需資源。

3.協助調查、保全證據。

4.事件結束後，探討發生原因與降低風險措施，以避免再次發生。

5.小組人員編制可隨時調整且具彈性。

圖 3 事件回應小組處理程序

資料來源：FRBNY 課程資料

(三)案例研討—Sandy 超級颶風

近年 FRBNY 所面臨之最大災害，為 2012 年 10 月 Sandy 颶風所引起營運所在地點曼哈頓下城之大水災。在颶風影響期間，約有 850 萬戶停電至少 1 星期，通訊及地鐵中斷，以及橋樑與隧道封閉數星期、機場停止營運 4 日、暖氣中斷 10 日，且有能源短缺的情形，為典型複合式災害。

FRBNY 將該颶風視為檢視與強化其持續營運計畫之契機，在颶風影響之 2 天前，該行即啟動持續營運計畫，各事業群相關人員及立即反應小組均密切以電話連繫，並將全體員工分為 2 組，分別配置於原辦公大樓及鄰近備援場所。在水患期間 FRBNY 為下城地區少數仍有電力之建築物，使其仍得以維持營運不中斷，且全體員工未有任何傷亡。FRBNY 事後檢討，這歸功於平日紮實之演練，事前規劃及事發時因應得宜，使其得以快速因應，惟其體認辦公處所之下城先天環境具脆弱性，此仍為未來所面臨最大的挑戰。

肆、企業風險管理

一、企業風險管理

(一)COSO 企業風險管理之構成要素

COSO 對企業風險管理的定義為：「企業風險管理是一個過程，受企業董事會、管理階層和其他員工的影響，包括內部控制與企業整體策略之應用，旨在為實現經營的效率和效果、財務報導可靠性，以及法規遵循等提供合理確信。」COSO 委員會自 1992 年發布「內部控制—整合架構」以來，理論界和實務界紛紛建議內部控制架構應與風險管理相結合。該委員會爰於 2004 年 9 月提出「企業風險管理—整合架構」，結合沙氏法案(Sarbanes-Oxley Act)在財務報告方面的要求，在內部控制五大要素的基礎上，COSO 企業風險管理之構成要素擴增至八項：除原內部控制五大要素外，另新增目標設定、事件辨識及風險因應等三項。

(二)企業風險管理目標

組織存在之目的係為其利害關係人創造利潤，且面臨各項不確定性。管理階層之挑戰，在於當為利害關係人創造利潤極大化時，需決定企業可接受之不確定性有多高。不確定性包含風險和機會，使企業之價值因此減損或提高。管理階層於評估策略方案、設定目標，與訂定管理相關風險之機制時，應考量企業之風險偏好[3]，使企業在報酬與風險偏好範圍內，取得最適之平衡，有效率及有效果的分配企業資源，為企業創造最大的價值。

二、FRBNY 企業風險管理實務

(一)風險管理型態

自 2014 年起，FRBNY 之風控長(Chief Risk Officer, CRO)開始採行企業風險管理之程序，評估潛在機會，以強化風險管理。該年 12 月，風控長並於風險管理事業群新增「企業風險管理職能」。目前企業風險管理職能包含作業風險、法令遵循、策略風

[3] 風險偏好(Risk Appetite)或譯為風險胃納，為組織所願意承受或可以承受之最大損失。

險及財務風險等。

1.作業風險

作業風險之定義本報告前已描述，FRBNY 於其風險管理事業群中設置「集中化」之作業風險職能，即考量企業整體之營運，以控管風險。

2.法令遵循風險

法令遵循風險係指因違反法律或相關準則而遭主管或監理機關處分，導致重大財務或聲譽損失之風險。FRBNY 於其法制事業群下設置法令遵循職能，以控管風險。有關法規遵循風險於下一章中有更詳盡之描述。

3.策略風險

策略風險來自於總體經濟、政治及法律等不確定因素，對企業實現其策略目標和計畫的影響，即任何的不確定性，一旦發生即會影響策略目標的達成。FRBNY 於其風險管理事業群下設置企業風險管理職能，以控管風險。

4.財務風險

財務風險包含信用風險及市場風險。信用風險指交易對手不願意或無法履行約定義務對企業實現其既定目標的影響；市場風險係指因國內外經濟因素變動，造成資產或負債價值產生波動的風險。FRBNY 於其風險管理事業群下設置信用風險管理及風險分析職能，以控管風險。

(二)風險管理與辨識程序

企業風險管理必需先有目標，管理階層始可辨識影響目標達成之潛在因素。FRBNY 採策略規劃程序，由風控長及風險委員會共同決定目標。在風險評估上，以量化及質化之風險分析技術，經由自我評估方式，分析風險發生之可能性及影響。採即時化及有效的風險回應模式，各業務主管部門為風險回應之主要負責單位，風控長及風險委員會則負責風險業已被揭露及監控。在風險監控上，各業務主管單位負責向風險管理事業群報告，風險管理事業群彙整風險揭露相關資訊，並向隸屬董事會之稽核與風險委員會報告。風險辨識程序可分為下列 2 方式：

1.由下而上

由各業務主管單位定期蒐集、彙整及分析各項風險事件，並進行自我評估。風險管理事業群彙整各單位所陳報之作業風險、法令遵循風險及財務風險等評估結果，向隸屬董事會之稽核與風險委員會報告。

2.由上而下

基於各部門主管之經驗及專業判斷，辨識影響 FRBNY 達成其政策目標之關鍵企業風險項目。由於各部門主管之資訊多源自於單位平時所蒐集與彙整之報告，本方式高度受由下而上程序之良窳所影響。

(三)採業務單位、風險管理及內部稽核部門等 3 道防線

目前 FRBNY 採各業務單位、風險管理及內部稽核部門等 3 道防線架構，以控管風險：

1.第 1 道防線

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，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總裁報告。

2.第 2 道防線

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，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。

3.第 3 道防線

由總稽核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。總稽核將評估及稽核結果直接向董事會報告。

FRBNY 規劃未來持續強化企業風險管理職能，研議支援跨風險型態之整合式風險分析模式，整合各部門之風險管理程序，期創造企業整體最大的價值。

伍、法規遵循

一、法規遵循長督導各項法規遵循評估事務

(一)設置緣由與目的

過去 FRBNY 雖具企業道德之文化，營運亦相當健全，但缺乏正式之綜合性法規遵循(Compliance)評估機制。此外，與聯邦準備體系其他銀行相較，其具有較廣泛的職責，如公開市場操作、各國央行國際帳戶服務、監理與金融穩定及境外美元之分配等，並提供多元之金融服務，於 2005 年在其法制事業群中，建置法規遵循職能，目前為聯邦準備體系中唯一具有法規遵循職能之分行。

法規遵循部門負責發展法規遵循計畫及控管已實施之道德計畫。建置法規遵循職能之主要目的，係作為協助辨識及解決法規遵循風險之相關議題，增進全體職員對該風險之認知，與當發生影響分行聲譽及法律風險時，具有立即反映之能力。並提供確信與諮詢服務，以協助辨識可能之風險與弱點，並提出建議。FRBNY 之法規遵循職能，係以整合式及系統性之程序，高度依賴組織中各單位之分工合作，每一個事業群均被賦予責任，於各業務領域協助建置並落實法規遵循職能，FRBNY 之法規遵循程序與實施內容詳**表 2**。

(二)設置法規遵循長

FRBNY 於其法制事業群中設置法規遵循長(Chief Compliance Officer)一職，督導全行有關舞弊、洗錢防制、道德及行為、資訊管理、保管品及交易等法規遵循評估事務。制定檢舉政策，設置匿名檢舉熱線，鼓勵職員檢舉可能之不法情事，若發現屬實，視情節輕重採取懲戒、降級或解雇等處份。並透過定期與不定期與現職暨離職員工之溝通，期有效掌握任何舞弊之資訊。

表 2 法規遵循程序與實施內容

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課程資料

二、道德辦公室之設置

(一)道德辦公室規範員工行為準則

FRBNY 法制事業群下設置道德辦公室(Ethics Office)，功能近似我國之政風單位，主要負責規範員工個人利益及對銀行責任之員工行為準則規範，員工須「將銀行利益列為第一優先」，且禁止獲取不當之財務利益，不論是直接或間接之財務利益。另在收受饋贈之規範上，除符合下列條件者外，FRBNY 原則上禁止員工收受與業務相關來源(Covered Source)之饋贈：

1.成本小頻率低

小於等於 20 美元，且不常發生。

2.廣泛參與的活動

雖享有降低、減免入場費與餐點招待，但員工參與該活動有助於對銀行之職責。

3.與銀行業務無關

饋贈係源自外部活動，且該活動與員工對銀行之職責無關。

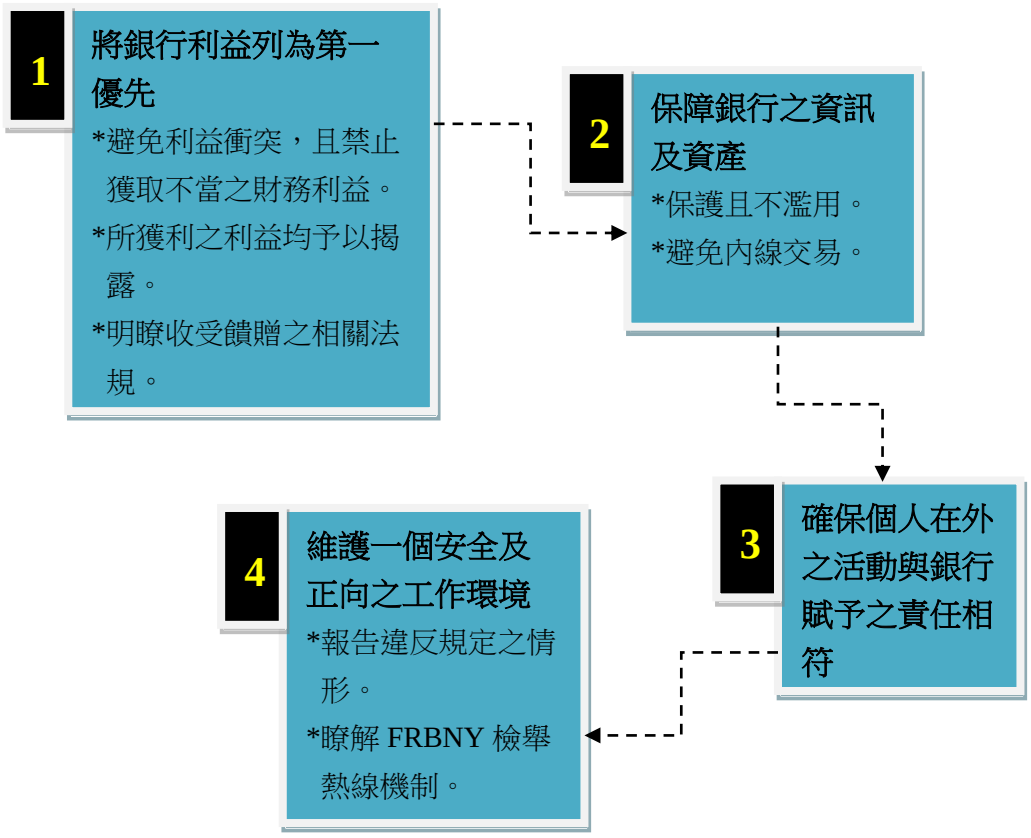
4.普羅大眾均可獲得

折扣減免或優惠活動對普羅大眾機會均等，不限特定對象。

5.易腐敗之生鮮商品

收受此類饋贈需獲道德辦公室同意，且與部門全體人員分享。

圖 4　FRBNY 員工行為準則



資料來源：FRBNY 課程資料

(二)案例研討

茲列舉本次課程介紹之案例並說明如下：

1. 某甲任職聯邦準備體系資訊部門並於近期新婚，其配偶於富達(Fidelity)資產管理公司之投資帳戶持有花旗銀行之股票，該股票來源為其配偶於數年前任職於花旗銀行時所獲取之員工紅利。當某甲於獲悉此情事時，當如何處理？

→即使聯邦準備體系科技部門與花旗銀行之直接關連性不高，但該員工仍需立即將其配偶持股情形陳報道德辦公室。

2.某乙任職聯邦準備體系，受邀參加某銀行所主辦之大型會議，參加人員源於各銀行、組織及民眾共 500 人，在會議結束後，並安排抽獎活動。一星期後，該會議主辦銀行通知抽獎結果某乙獲得一台 iPad Air，某乙是否可收受該獎品？

→雖然此會議係參加對象廣泛，惟某乙係因任職於聯邦準備體系而受邀，故不可私下收取該獎品。

陸、內部稽核

一、內部稽核之角色與責任

(一)內部稽核之職責

內部稽核人員之主要職責為「獨立」評估組織內部控制、風險管理與治理程序之有效性，瞭解與分析關鍵風險因子，針對發現之控制弱點及可能風險，提出建議改進意見。在評估內部控制上，其基於充份之測試活動，仔細檢視各項業務之內部控制程序，稽核範圍並擴及法律相關議題。FRBNY 列舉下列影響內部稽核有效性之關鍵因素：

1.審計委員會監督之有效性

→審計委員會由獨立董事組成，負責審議年度稽核計畫與檢視年度稽核報告。

2.稽核事業群之獨立性及能力

→內部稽核部門直接隸屬董事會，經由定期專業訓練，提升稽核人員專業能力。

3.資深經理人之參與情形

→邀請資深經理人參與稽核會議，討論風險評估相關議題。

4.綜合性審計計畫

→採用多元資訊與工具協助稽核程序，包含總分類帳、組織結構圖與部門清冊、作業流程圖與稽核軟體等。

5.風險評估程序之有效性

→風險評估包含財務風險(信用、市場、利率與流動性)、作業風險、資訊科技風險、聲譽風險及法律風險等。

6.適當的稽核頻率

→每年制訂年度稽核計畫，對跨年度之計畫，至少每 18 個月稽核一次。

7.辨識及測試內部控制

→依各單位屬性不同，採客製化之稽核程序。

8.產製綜合性報告

→包含稽核之範圍、目標、評論、建議與管理階層之回應等。

9.列管議題之後續追蹤

→針對重大或例外事項，於對程序及系統進行事後追蹤，必要時並就改進措施之有效性進行測試。

10.稽核事項之即時說明與回覆

→強化與受查業務單位之溝通。

為提升獨立性，FRBNY 之內部稽核部門直接隸屬董事會，其不負營運管理責任，內部控制環境之管理亦非內部稽核人員之職責。實務上，對內部控制有效性評估，常引起糾紛之來源，內部稽核人員依其專業判斷，針對內部控制弱點，提出強化及改進建議，惟業務單位常有不同之見解。業務單位常主張現行內部控制程序已足夠，內部稽核人員除非可明確找到逾越內控之證據，否則常不易說服業務單位修改其內控流程。另如果發生某不良事件(Adverse event)，內部稽核人員應檢視業務單位之事後分析報告，檢視事件造成之原因，並決定是否需建議增加額外的內控措施。

(二)內部稽核人員之能力與能見度

內部稽核單位應致力提升其於組織之能見度，主要為改善利害關係人對內部稽核人員之偏見，彰顯內部稽核之職能與價值，有助於提升全體利害關係人對組織之信賴度，使組織內部溝通管道更順暢。另可建置網站或其他宣傳方式，以提升稽核部門之能見度，聯準會曾對全球主要 18 個國家央行之內部稽核單位進行問卷調查，多數國家央行網站對其內部稽核職能有專屬介紹，包含稽核人員角色、獨立性、稽核目標、績效衡量指標與稽核報告等。內部稽核不僅具有風險控管之防弊功能，對組織之業務流程提出之改進建議，可使業務流程及資源配置更有效率，具興利之功能。

因此，組織亦應給予內部稽核單位適宜的資源，經由定期專業訓練，提升稽核人員專業能力。在評估稽核人員專業能力上，FRBNY 參採美國內部稽核協會(IIA)制定之內部稽核人員能力模型(IA-CM Model)，包含初始草創階段、建置基礎架構、全面整合、影響管理決策與最佳化等 5 個能力層級，以及內部稽核之角色與責任、人事管理、專業實務、績效管理與課責性、組織關係與文化及治理架構等 6 項基本要素(詳**表 3**)。每一層級包含數個關鍵流程項目，以評估是否已提升至下一個層級。FRBNY 目前已達第 3 能力層級，部分要素已達第 4 能力層級。但特別注意的是，理論上層級愈高對

內部稽核執行具正面之影響，惟需考量成本效益分析，若組織規模較小或內部稽核人員能力或人力相對不足時，不需亟於提昇至較高之層級。

表 3 內部稽核能力模型矩陣

	內部稽核之角色與責任	人事管理	專業實務	績效管理與課責性	組織關係與文化	治理架構
第5級 最佳化階段	*內部稽核被視為改變之關鍵角色	*參與專業組織之領導決策 *辦理人事預測	*持續改善專業實務架構 *策略性之內部稽核規劃	*公開報導之內部稽核有效性	*有效與持續之關係	*內部稽核活動具獨立性、具有權利與授權
第4級 管理階段	*治理、風險管理與控制之整體確信	*內部稽核有助於管理發展 *內部稽核活動支援專業組織 *人事規劃	*稽核策略影響組織之風險管理	*績效衡量之質化與量化整合	*總稽核建議影響高階管理階層	*內部稽核活動之獨立監督 *總稽核對高階管理階層報告
第3級 整合階段	*諮詢服務 *績效與貨幣價值稽核	*建置團隊與能力 *專業合格職員 *人力整合	*品質管理架構 *風險基礎審計計畫	*績效衡量 *成本資訊 *內部稽核管理報告	*與其他覆核團隊協調 *整合管理團隊	*內部稽核活動之管理監督 *融資機制
第2級 基礎架構階段	*法令遵循稽核	*個人專業能力發展 *辨識與招募具專業技能人員	*專業實務與流程架構 *以管理階層與利害關係人為基礎制定稽核計畫	*內部稽核營運預算 *內部稽核業務計畫	*內部稽核活動之管理	*對組織資訊、資產與人員可全面接觸。 *產製已建置之治理架構報告
第1級 初始階段	臨時、未結構化；個別人員稽核，文件及交易正確性、法規遵循與報告產製決定於稽核人員之個人技能；除專業協會提供者外，未訂定專業實務架構；資金需求係由管理階層核准；缺乏基礎架構；稽核人員可能隸屬於大型組織轄下之單位；專業能力未建置，因此沒有任何關鍵流程項目。					

資料來源：FRBNY課程資料。

二、風險評估

(一)風險評估方法與程序

依 COSO 定義，風險係指對組織達成其目標之任何威脅事項，可經由良好的內部控制程序加以消除或減輕。風險評估係指對可能影響組織之不利事件，以系統性之程序，進行專業之整體性評估。聯邦準備體系於內部稽核所進行之風險評估，係選定適當的稽核範圍，運用風險基礎之程序，評估與衡量組織整體營運之相關風險，具有客觀、彈性、易於瞭解及實施與通用之特性，聚焦於固有風險、人力資源風險、重大變動及複雜性之新型態風險(Emerging Risks)。

風險評估程序為界定稽核範圍與稽核活動、選用適宜之風險評估模型、年度風險評估與分級，稽核人員依分級結果與專業判斷制定年度稽核計畫。在風險評估模型上，主要採用風險評分矩陣(Scoring Matrix)，評分程序如下：

1.預先訂定各風險因子之權重

2.訂定各風險因子風險等級(第 1 至 4 級，等級與風險成正比)

3.將上述風險權數與等級相乘得到各風險因子之分數

4.將各風險因子評分加總得到整體風險之分數

(二)內部稽核頻率與實務

依風險因子評分之結果，設定稽核頻率，對評分較高者(風險較高)，原則上每年至少稽核 1 次，並得視情形而延長為 2 年；至評分較低者(風險較低)，稽核頻率則由總稽核決定(詳**表 4**)。

表 4 風險評分區間與稽核頻率

風險等級	分數區間	稽核頻率
高	326-400	每年至少1次
中	251-325	每3年至少1次
低	100-250	由總稽核決定

註：高風險等級之項目之稽核頻率可視風險影響因子而延長為2年。
資料來源：FRBNY課程資料。

FRBNY 評分時將風險因子分為作業風險、財務與重大事項風險(含信用風險市場風險等)、策略風險與聲譽風險等四大類，各項目配置權重並完成評分(詳**表 5)**，依風險評核結果並與前次相比較後，稽核人員採取後續因應行動，評估維持、增加或減少稽核頻率，並提出建議改進之時程，分為立即或 1 年至 3 年不等，協助各業務單位消除風險。

表 5　風險評估評分矩陣

風險因子	權重	風險等級 (高=4，中高=3，中=2，低=1)	分數 (=權重*風險等級)	前期分數
作業風險				
1.業務流程	20	3	60	80
2.科技與資訊管理	20	3	60	80
3.人力資源	20	3	60	60
財務與重大事項風險	20	2	40	60
策略風險	10	2	20	20
聲譽風險	10	1	10	20
總計	100		250	320

註：權重欄依課程提供資料；風險等級欄及前期分數欄則由作者編製。
資料來源：FRBNY課程資料。

三、資訊科技稽核

為因應近年資訊科技之發展所衍生與資訊安全相關之風險，美國聯邦政府體系對資訊相關之網路安全、第三方風險管理、資料保密及營運復原計畫等之內部稽核架構訂定一系列規範與指引。內部稽核協會並制定資訊科技稽核計畫**(詳表 6)**，包含瞭解組織之營運、辨識、資訊科技架構、進行風險評估，以瞭解組織運作與資訊科技服務如何協助組織達成其目標，依風險評估結果擬定稽核計畫。

FRBNY 參考上開內部稽核協會制定之架構，根據其資訊科技流程、資訊科技服務架構及其業務屬性，擬定其資訊科技稽核計畫，目的係為辨識及瞭解組織策略與目標、關鍵業務流程、資訊科技支援模式、應用工具與基礎設施等，並擴大非資訊相關人員之參與。資訊科技稽核人員執行之工作包含：

1.資訊科技流程及架構之稽核

2.參與業務流程之整合式稽核

3.專案審查

4.新事項之協商

5.持續聯繫

表 6 資訊科技內部稽核計畫

*辨識組織營運策略與目標 *瞭解組織高風險營運項目 *瞭解組織架構及各部門業務運作 *瞭解資訊科技服務支援營運之模式	*分析組織營運環境 *辨識主要支援企業營運之資訊科技應用工具與架構 *瞭解支援技術之角色 *辨識主要計畫 *決定稽核主題	*發展辨識風險之程序 *評估風險暨採用資訊科技風險因子將稽核主題排序 *評估風險且採用營運風險因子將稽核主題排序	*選擇稽核主題並歸納各稽核工作 *決定稽核周期與頻率 *依管理要求或討論結果適量增加稽核量 *驗證稽核計畫

資料來源：FRBNY 課程資料

四、聯邦準備體系年度稽核計畫

(一)總稽核會議與分工

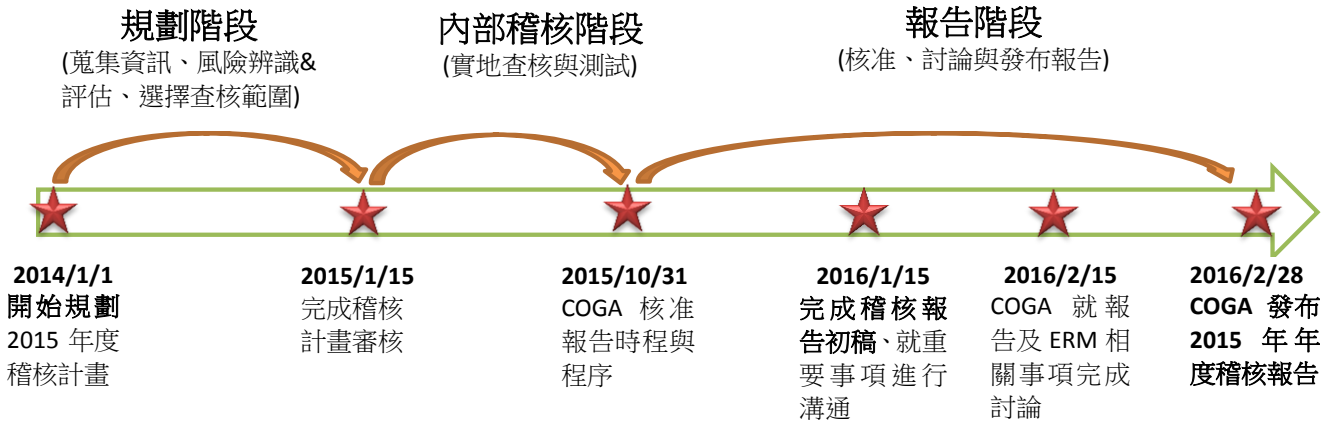
聯邦準備體系共有 12 家分行，各地區聯邦準備銀行之總稽核輪流籌劃每年度之總稽核會議(Conference of General Auditors；COGA)。該會議主要任務為制定體系之年度稽核計畫，提供聯邦準備體系獨立、客觀、創新與前瞻性之內部稽核服務，以改善體系之風險管理、內部控制及治理程序，協助目標之達成。各地區聯邦準備銀行之總稽核均有各自負責協調之稽核業務，舉例而言，FRBNY 總稽核負責協調公開市場操作、信用風險管理及員工福利業務之稽核與評估；至國庫相關業務之稽核與風險評估，則由聖路易分行之總稽核負責。里奇蒙(Richmond)及達拉斯等分行為資訊科技、網

路與復原方案等之風險控管專責人員(Risk Champions)，專責聯邦準備體系之資訊安全相關之稽核與風險評估。

(二)年度內部稽核周期

聯邦準備體系每年之年度內部稽核周期，可分為規劃、稽核與報告 3 階段，整體時程為期 26 個月。規劃階段於前一年度 1 月 1 日即開始進行，包含資訊及資訊蒐集、關鍵風險辨識與評估，選擇年度查核範圍及重點等，時程為期一整年；稽核階段則於當年年初開始，除體系之內部稽核外，各分行亦辦理其內部稽核；報告階段則於 10 月開始至隔年 2 月底止，該期間由總稽核會議審核報告時程、討論報告初稿，並就重要事項行溝通，約為期 1 至 2 個月，核准後於隔年 2 月底公布報告。

圖 5 聯邦準備體系年度稽核計畫時程



資料來源：FRBNY 課程資料與作者整理

柒、研習心得與建議事項

一、賡續推動及落實持續營運與備援演練機制

鑑於近年全球暖化使氣候變遷劇烈，環境日趨脆弱，導致重大天然災害頻繁發生；另網路攻擊模式持續進化，駭客蛻變為結構化與組織化，挾豐沛資源為後盾進行持續性攻擊，甚且以收買內部人員或透過第三方合作廠商，採內部滲透之方式進行攻擊，令人防不勝防。由於本行業務屬性較為特殊，若上述各項環境及人為因素導致本行無法正常營運，在總體方面，對我國貨幣政策操作、市場交易清算、外匯市場交易與管理、國庫業務之運作，攸關甚鉅。在個體方面，將使本行面臨聲譽風險，爰短期宜持續強化與定期演練現行異地備援機制；中長期似可參酌 FRBNY 之作法，成立專責單位，模擬各種可能之情境預作準備。

二、持續派員參加相關課程，俾提升風險意識與專業知識

參考 FRBNY 之風險管理架構，本局為業務單位係屬第 1 道防線。本局與財政部簽訂代庫合約經理國庫業務，並臨櫃辦理國庫、機關專戶存款及保管品收付業務，同仁對相關作業流程宜抱持高度風險意識及審慎態度，從源頭即落實風險管理。本次課程內容豐富，FRBNY 之實務機制可供借鏡學習，未來可鼓勵同仁持續參加相關課程，俾提升風險意識與內部控制及稽核等專業知識。

參考資料

1.本次訓練課程資料—FRBNY。

2.游金鳳(2014)，「參加紐約聯邦準備銀行『作業風險管理與內部稽核』訓練課程出國報告」，中央銀行，8月。

3. Andrew Tweedie(2010), “Safeguards Assessments—Review of Experience”, IMF Report, July.

4.The Institute of Internal Auditors(2010), “Internal Audit Capacity Model(IA-CM)”, IIA Research Foundation.

5. The Institute of Internal Auditors(2010), ”CIA Review Part I Internal Audit Role in Governance, Risk, & Control”, 14th edition.

6. The Institute of Internal Auditors(2010), ”CIA Review Part II Conducting the Internal Audit Engagement”, 14th edition.

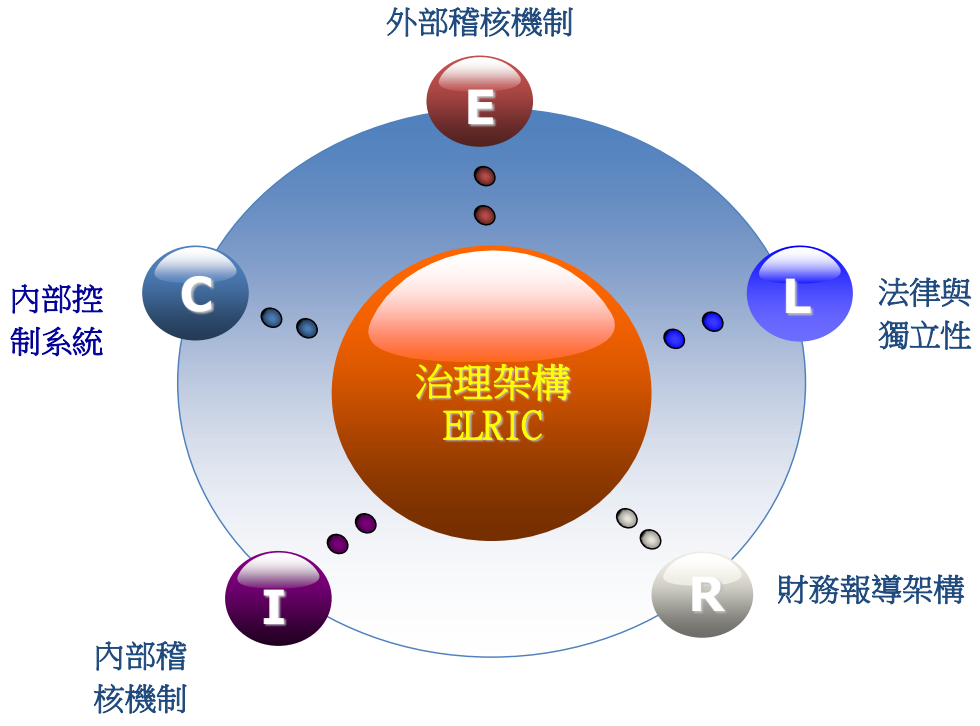
7. The Institute of Internal Auditors(2010), ”CIA Review Part III Business Analysis & information technology”, 14th edition.

8. Sawyer’s(2008), “Internal Auditing”, 5th edition.

附錄-IMF 保障評估措施

自 2000 年，當 IMF 提供參加會員國之央行融資時，採行保障評估措施(Safeguards Assessments)。保障評估措施規範借款國之央行，需建立內部控制、帳務處理、報告和稽核等制度，以管理資源並確保誠信經營。該政策的主要目的是減輕或消除 IMF 資源遭濫用(Misuse)，以及提交之貨幣計畫資料錯誤報導(Misreporting)之潛在風險。為實現此目標，於公司治理架構之相關五大關鍵領域(ELRIC)作好評估，包含外部稽核(**E**xternal Audit)、法律與獨立性(**L**egal and Autonomy)、財務報告(Financial **R**eporting)、內部稽核(**I**nternal Audit)與內部控制系統(Internal **C**ontrol)，並參考該國財務之透明度、課責性、監理機制與央行之獨立性等。

附錄圖 IMF 保障與評估措施之治理架構評估



資料來源：FRBNY課程資料

若融資案件於上述各關鍵領域之評估結果屬允當，且評估報告中相關強化措施之建議獲該國央行同意且經適當執行，則即可辦理該筆融資協定。自訂定保障評估措施之2000

年起至2015年4月，IMF已依該措施辦理272件融資案件之評估，並對94個國家之央行貸款，融資的高峰期為2009年至2010年，主要受金融海嘯之影響，當時部分國家央行面臨流動性不足之情形。另依IMF之評估，目前多數國家央行對信用、市場風險與持續營運計畫均主動控管並建立良好機制，而作業風險管理則尚在發展與建置中；目前僅極少數之央行已實施企業風險管理(ERM)之機制，以整合式架構管理組織整體面臨之風險。