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)

作業風險管理與內部稽核

服務機關：中央銀行
姓名職稱：游金鳳/副科長
派赴國家：美國
出國期間：103 年 5 月 10 日至 5 月 17 日
報告日期：103 年 8 月 11 日

目錄

前言 1

第一章 基本概述 2

第一節 內部控制的起源 2

壹 美國 COSO 委員會簡介 2

貳 我國推動內部控制的緣起 4

第二節 內部控制、內部稽核及有關名詞的定義 5

壹 內部控制 5

貳 內部稽核 6

參 內部控制與內部稽核的關係 7

肆 風險(risk) 8

伍 風險評估(risk Assessment) 8

陸 各項風險 9

第二章 作業風險管理 12

第一節 作業風險與作業風險管理之定義 12

第二節 FRBNY 風險暴露與管理的發展 14

第三節 FRBNY 的治理架構 15

第四節 風險報告的發展與要項 17

壹 風險報告的發展 17

貳 風險報告的要項 18

第三章 營運持續計畫（Business Continuity Planning） 22

第一節 FRBNY 的營運持續計畫 23

壹 營運持續環境中風險及危害的認知 23

貳 制定營運持續計畫的依據 24

參 營運持續計畫的內涵 25

第二節 FRBNY 的危機管理 26

第四章 優化業務流程 29

第一節 FRBNY 優化業務流程的應用 30

第二節 FMEA 風險評估工具(FMEA Risk Assessment Tool) 32

壹 何謂失效模式與效應分析 32

貳 FMEA 分析法之步驟 33

第五章　風險評估方法.....38
第一節　FED 風險評估方法.....38
第二節　風險模型的應用.....39
壹　風險模型.....39
貳　風險評估計分矩陣範例(部分節錄資料).....40
參　年度稽核計畫.....44
第六章　內部稽核能力模型.....46
第一節　內部稽核能力模型的緣起.....46
第二節　內部稽核能力模型矩陣.....47
第七章　稽核執行方法論.....51
第一節　FED 稽核規劃方法.....51
壹　稽核規劃方法的重點說明.....51
貳　以計畫為中心之查核方法的優點.....54
第二節　整合式稽核.....55
第八章　資訊科技安全管理與稽核.....57
第一節　資訊安全風險管理.....57
壹　IT 的共同及新興風險.....58
貳　資訊安全管理計畫.....58
第二節　IT 稽核的趨勢.....60
壹　IT 稽核的新趨勢.....60
貳　IT 稽核依循的標準.....61
結論與建議.....65
參考文獻　.....68

前言

職於 103 年 5 月 10 日起至 103 年 5 月 17 日奉派參加美國紐約聯邦準備銀行之專業訓練課程 - 作業風險管理與內部稽核(The Operational Risk Management and Internal Audit)，該專業課程的講員包括紐約聯邦準備銀行的資深官員，著名大學或重要商業及投資銀行的傑出教職員，以及金融機構的專家。

在全球化與電子化的金融業界，需有涵蓋整體組織的風險管理，以衡量並監控整體組織的風險，並陳報其暴險情況。然「風險」並非指要去避免某事件的發生，而是指在一個組織營運中伴隨而生之不可避免的產物，既是不可避免，就需要有強健的風險管理制度來控管風險，而要建立一個強健的風險管理制度，則有賴於內部稽核與內部審查委員會的適度運作。本次訓練課程的重點即在於 -「作業風險管理與內部稽核」。

本次參訓學員來自世界各國央行，大多來自稽核及風險管理部門，其中 43%來自歐洲，32%來自非洲及中東，17%來自亞洲，8%來自美洲。

在第一章中首就風險、內部控制與內部稽核等名詞做定義與概述，先有清楚基本概念後，再逐章深入談論作業風險管理，持續營運計畫，優化業務流程，風險評估方法，內部稽核能力模型，稽核執行方法論，資訊科技安全管理與稽核，最後提出結論與建議。由於時間短促，匆忙成書，闡述粗淺心得，難免有疏漏之處，至盼先進長官不吝指教。

第一章　基本概述

本章簡述內部控制的起源，及內部控制、內部稽核並相關名詞的定義，以為後續各章節論述時的基本概念。

第一節 內部控制的起源

壹　　美國 COSO 委員會簡介

內部控制議題首先被提出，起源於 1920 年代的美國，當時美國面臨經濟大恐慌，企業為免於破產，開始重視內部的監督與牽制，之後歷經多年沿革；到了 1980 年代企業假帳風波不斷，1985 年，遂有美國會計學會 AAA (American Accounting Association)、美國會計師公會 AICPA (American Institute of Certified Public Accountants) 、內部稽核協會 IIA (Institute of Internal Auditors)、管理會計學會 IMA (Institute of Management Accountants)、財務主管協會 FEI (Financial Executive Institute)等五個專業組織，共同組成「不實財務報導全國調查委員會」(National Commission on Fraudulent Financial Reporting，通常簡稱 Treadway Commission)，主要目的在探討如何解決企業日益嚴重的不實財務報導問題。1987 年該委員會在其報告中提出了許多建議，包括呼籲所有的贊助組織共同努力來整合各種不同的內部控管的概念與定義，於是成立了內部控制專門研究委員會，稱為 Committee of Sponsoring

Organizations of the Treadway Commission，簡稱 COSO。

COSO 成立之後即著手研究內部控制的問題，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之效益的架構。將內部控制分成控制環境、風險評估、控制活動、資訊與溝通、監督等五項組成要素，此乃內部控制最早的架構；並於 1994 年進行增修。

COSO 報告很快得到美國審計總署(Government Accountability Office；GAO)的認可，美國會計師公會(AICPA)也依其內容於 1995 年發布了審計準則公報第 78 號，美國聯邦政府即在美國審計總署的要求下，採行 COSO 所訂的內部控制準則。

是以，COSO 的內部控制整合架構成為現代內部控制最具有權威性的架構，在美國及全球倍受推廣及應用。

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。此外，COSO 以該 17 項原則為企業設計內部控制五大要素中最基本應具備的標準。有別於 1992 年概念式的架構，2013 年架構於該 17 項原則項下提出更為明確的「聚焦點」(points of focus)，協助管理階層於評估該 17 項原則是否適用於內部控制制度設計時之參考。

COSO 對於適用 1992 年架構建置內部控制制度架構之企業，建議從 2013 年 5 月 14 日到 2014 年 12 月 15 日為轉換期間，2014 年 12 月 16 日以後 2013 年架構將正式取代 1992 年架構。

貳　　我國推動內部控制的緣起

審計部97、98年度中央政府總決算審核報告指出，部分機關因內部控制機制未臻健全，間有施政效能不彰、投入鉅資興建設施閒置浪費及未依法制執行預算等，致有重大弊案陸續發生。當時各機關財務涉有違失案件，96至98年間平均每年約300件，顯示建構健全內部控制機制，以防杜違失，實已刻不容緩。

之後，審計部99年度中央政府總決算審核報告，提出參酌先進國家作法，完備政府內部控制機制之意見。行政院即於民國99年12月30日籌組成立跨部會之「內部控制推動及督導小組」，簡稱「行政院內部控制小組」，負責整體規劃及推動內部控制事宜。行政院內控小組於100年7月完成審議「內部控制制度設計原則」，完整規範內部控制觀念架構及設計步驟等，供各機關研訂內部控制制

度。

幕僚作業則由行政院主計總處辦理，行政院主計總處乃採用美國COSO之「內部控制-整合架構」，設計我國政府行政機關適用之內部控制之觀念架構，將政府內部控制視為一種管理過程，幫助機關達成「確保施政效能、遵循法令規定、保障資產安全、提供可靠資訊」四項目標，包含了控制環境、風險評估、控制作業、資訊與溝通及監督等五項組成要素。

第二節 內部控制、內部稽核及有關名詞的定義

作業風險及控制評估常是一個公司實施作業風險管理的第一個步驟。內部控制包含在風險管理之內，係風險管理不可或缺的一部分。而風險管理自內部控制延伸，其涵蓋的範圍比內部控制廣泛，且著重風險觀念。

做風險評估之前須先瞭解各風險的定義，再對各風險因素進行評估與監控，免除或減低危害或損失，才能增進作業風險管理的效益。至於風險管理與控制過程的效益如何，則需由一個獨立的職務，亦即稽核專業人員進行各項的評鑑。

本節先就內部控制、內部稽核、風險、風險評估、風險因素等名詞的定義做解釋，以便後續各章節在論述風險評估與稽核的方法時，有清楚的延續觀念。

壹　內部控制

一、COSO報告定義：內部控制是一個過程，由企業董事會、管理階層和其他同等級人員所執行，藉以合理確保下列目標的達成：

-營運的效果及效率

-財務報導的可靠性

-現行法規的遵循

二、我國審計準則公報第5號之定義，「內部控制是指受查者之組織規劃及其所採用之各種協調方法與措施，目的乃為保護資產安全、提高會計資訊之可靠性及完整性、增加經營效率，並促使遵行管理政策達成預期目標」。

貳　內部稽核

一、美國內部稽核協會(Institute of Internal Auditors;以下簡稱IIA)的定義：「內部稽核是組織內部一種獨立的功能，檢查及評估組織的活動，對組織提供服務」。意即，「內部稽核是一個獨立的職務，用以提供客觀的確認及諮詢活動，以提昇、改善組織的營運價值，協助機構透過系統化及紀律化方法，評估及改善治理、風險管理及控制程序之效果，以達成組織的目標。」

二、內部稽核由內部稽核人員執行，針對內部控制要素中的監督項目，加以

個別檢核與評估，並於每隔一段時間從全新的觀點去評估。

參　內部控制與內部稽核的關係

內部控制是一個企業的管理階層所採用的一切政策及程序，為協助其確保能達成管理的目標，盡其可行的範圍內，有系統的並有效的管理其營業，包括政策的可信度，資產的保護，舞弊及錯誤的防止與偵測，並適時的預備可靠的財務資訊。

內部稽核是一個獨立的職務，目的是檢測內部控制是否設計完備，並被適當地執行。內部稽核人員能夠評估內部控制制度在組織內部執行的情形，且在其負有的獨立功能下，向管理高層報告，以促使內部控制持續有效。稽核工作在「消極上」是防止弊端，在「積極上」是協助管理階層，以精進企業之管理體質。

例如公司有考勤辦法，用以規定員工請假出勤，是內部控制制度。內部稽核則是去檢查：

一、員工是否有依照考勤辦法來執行？是否有照規定請假、依規定時間上下班？

二、人事單位是否依規定統計考勤結果？是否依規定計算薪資或相關作業？

故知內部稽核與內部控制的關聯性－內部稽核之重要性乃在協助機關發揮內部控制之功能，亦即內部稽核扮演了評估控制制度之有效性的重要角色。

肆　風險(risk)

一、IAA 的定義：

「在稽核之下，任何事件或行動對組織產生危害影響的可能性。」

二、COSO的定義：

經由適當的控制所能減輕之企業個體達成其目標的威脅。

三、一般的定義：

變化性的衡量；欲達成某目標或結果時意外的變化，也就是任何可能影響企業達到其管理或控制目標的威脅或障礙。

伍　風險評估(risk Assessment)

一、IIA的定義：評估並整合有關不利的情況或事件的可能性，作專業判斷的一個系統化的過程。

二、中華民國內部稽核協會準則公報之「第二號公報－風險評估」第11條對

風險評估的定義：

「風險評估係依據風險因素對各種不利情況或事件做有系統之分析與評估，以判斷風險發生之可能性與影響程度。內部稽核單位可對風險因素賦予權數，以顯示其相對重大性。」

三、美國聯邦體制的定義：運用風險基礎(risk-based)的方法，於適當的稽核範圍內，衡量銀行作業的相關風險。

該定義之下，風險評估應具有四項特性：

(一)客觀而具體，可以量化的

(二)賦予彈性及專業判斷

(三)易於使用及瞭解

(四)共同適用於各個聯邦準備銀行

陸　各項風險

做風險評估之前須先瞭解各風險的定義，再對各風險因素進行評估與監控，免除或減低危害或損失，才能增進作業風險管理的效益。以下是美國紐約聯邦準備銀行對各風險的定義：

一、作業風險(Operational Risk)：由於人員或系統的不當、失誤或失敗的內部流程，或是外部事件所造成的內部流程、人員或系統的損害，以致對

聯邦準備體制產生直接或間接的損失或其他負面的影響。

二、金融風險(Financial Risk；含信用風險及市場風險)：在特定的業務流程中重大的財務(financial materiality)風險，及其對聯邦銀行或系統的潛在衝擊。因交易對手未能履行其財務義務(信用風險，Credit Risk)，或市場利率的不利變動(市場風險，Market Risk)，引發銀行遭受損失的可能性。

三、策略風險(Strategic Risk)：由於策略規劃流程，領導階層，或執行面，導致策略計畫不是完全有效，致使聯邦準備體制無法達成任務或目標的風險。

四、信譽風險(Reputational Risk)：聯邦準備體制因未能遵行現行法律或管理風險，或因外部事件，或聯邦準備體制未履行其職責，使聯邦準備真實地或感覺到可能降低本身的聲譽的風險。

五、固有風險(Inherent risk)：無法以其他相關內部控制預防或偵測錯誤發生的風險，亦即不存在內部控制之內，所發生的風險，比如會計人員將200元記錄成200萬元的風險。

六、殘餘風險/淨風險(residual Risk/Net Risk)：固有風險中無法由控制環境

來減輕的風險，稱之殘餘風險。能透過稽核控制環境[註](Control Environment)的測試，查看殘餘風險的等級。

註：所謂控制環境(Control Environment)：藉由營運/業務的管理得以消除或降低固有風險的一切活動；但風險的完全減輕並非必然的目標。

第二章　作業風險管理

金融機構之營運受其外部環境及內部組織、程序與步驟的影響，根據國際清算銀行（Bank for International Settlements；BIS）所屬之巴塞爾銀行監理委員會（The Basel Committee on Banking Supervision）資料顯示，銀行面臨的主要風險中，以信用風險(Credit Risk)所占比重最高，約為60%；次為作業風險(Operational Risk)，約占30%；市場風險(Market Risk)與其他風險，如信譽風險等則較低，各占5%。故銀行需將「作業風險」與信用風險、市場風險一樣，妥善地管理與監督。

本章首節就作業風險與作業風險管理之定義予以說明，再就美國紐約聯邦準備銀行(Federal Reserve Bank of New York；以下簡稱FRBNY)的作業風險管理分節介紹。

第一節　作業風險與作業風險管理之定義

隨著金融機構的合併、跨業經營及國際化，擴大了信用、市場及作業風險。巴塞爾銀行監理委員會乃於2001 年1 月16 日發布新巴塞爾資本協定建議（A Proposal for A New Basel Capital Accord，即 Basel Ⅱ），明確規範除信用風險與市場風險外，並將作業風險納入資本適足的計算，以期提升國際金融服務的風險控管能力，於是在新巴塞爾資本協定中，將銀行面臨的風險歸納為信用風險、

市場風險及作業風險三種。

何謂作業風險？在2003 年4 月新巴塞爾資本協定第三版諮詢文件（The Third Consultative Package，簡稱CP3），將作業風險定義為：「因內部作業、人員及系統之不當或失誤，或因外部事件所造成損失之風險」。此定義包含法律風險，但不包含策略風險及信譽風險。由於各銀行對作業風險有著不同的定義，因此巴塞爾銀行監理委員會認為各銀行應依據其內部不同目的，選擇適用於其機構之作業風險定義以健全實務運作。

作業風險之「管理」，顧名思義係指對作業風險的「認定、評估、監督以及控制或減緩」，所以作業風險管理是決策者用以降低或抵消風險的一種程序。進一步定義之：「作業風險管理 (Operational Risk Management；ORM) 是以系統化來辨識風險與利益，以助於在特定情況中做成最佳策略的決定，乃是一項決策性工具。其設計的用意在於使風險最小化，為求減低災難，保護資產，保障福利等，是一種保存資源的有效措施與程序。」

作業風險管理的目的，是藉由建立及有效執行健全作業風險管理機制，以降低銀行的作業風險，並達成銀行營運及管理目標。作業風險管理流程可分為風險辨識、風險評估、風險衡量、風險控管、風險溝通，是一個動態循環的過程，有規劃完善的管理流程，才能確保銀行具備完善的作業風險管理。以下將介紹

FRBNY的作業風險管理。

第二節　FRBNY 風險暴露與管理的發展

作業風險歷久以來一直是 FRBNY 的主要風險，近年來其風險管理的發展，依風險暴露的情況，可區分為下列三個重要時期：

一、2008-2010 年：全球金融危機(Financial Crisis)，引發的金融風險包含市場風險及信用風險，美國聯邦準備銀行緊急介入，宣布政府對金融市場的救援計畫，該項計畫被視為是美國史上最大的政府介入金融市場行動。於是聯邦準備理事會（Board of Governors）決定將金融風險列為必須揭露的風險，並且責成「風險監督委員會」(Risk Oversight Committee)專責研究疑難問題，另設立風控長(Chief Risk Officer)負責金融風險的分析與報告。所以金融風險的管理是當時的重點。

二、2011-2012 年：轉為強調端點到端點流程(end to end process)的改進，主要項目有三：

(一)建立優化業務流程(Business Process Excellence；BPE)計畫

(二)制訂新控制策略，先在一個區域學習應用，再適用於所有區域

(三)焦點包含終端使用者啟用的工具(例如：試算表)及臨時員工(contingent workers)。

三、2013-2014 年：著重於整合，其重點如下：

(一)建立風險小組(Risk Group)，設立在風控長之下，負責作業風險及金融風險。

(二)制訂風險表格列管風險，以發展風險管理紀律及銀行的核心功能。

(三)設立作業流程及控管的圖表框架，以評估並建立各活動階層的控制點，這項目前已在執行中。

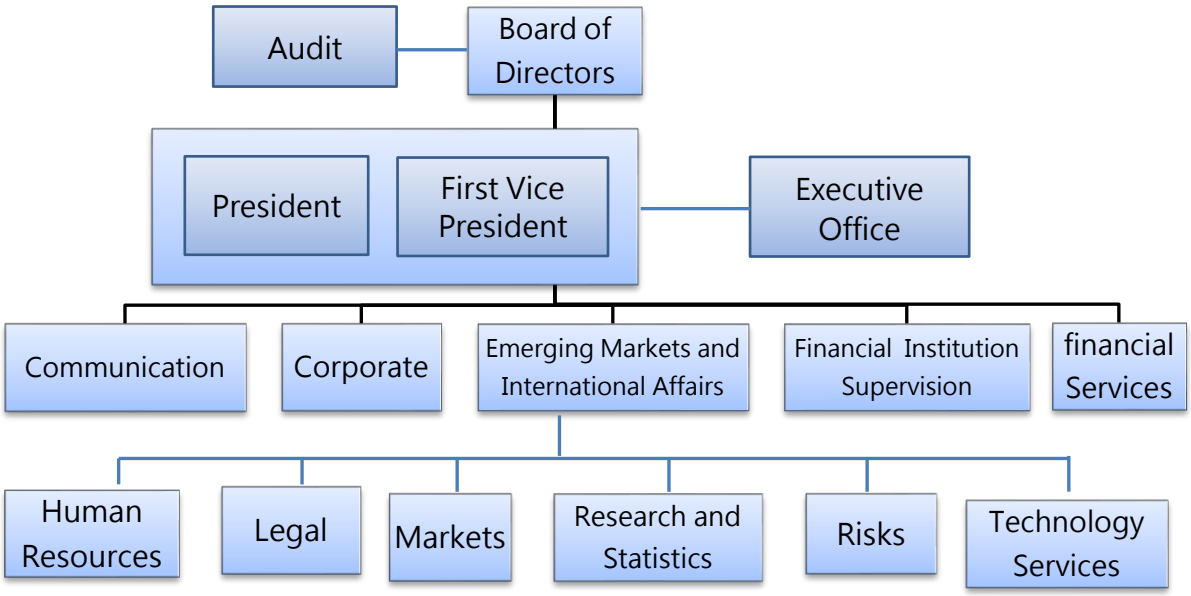
(四)為推動並落實銀行整體風險管理，將原來僅是監控金融風險的「風險監督委員會」(Risk Oversight Committee)，改為「稽核及風險管理委員會」(Audit and Risk Committee)，隸屬於銀行董事會(Board of Directors)，負責整合所有風險。

第三節 FRBNY的治理架構

FRBNY是由中央職掌作業風險管理，負責整體作業風險規劃，風險的監控，制定準則，整合風險分析(包括業務部門的自行評估，風險事件等)，整合風險概況等，定期做成作業風險報告，並且每半年將綜合風險概況，陳報風險委員會、管理委員會，稽核及風險管理委員會。有關其風險報告的發展將在下節介紹，本節先對FRBNY的治理架構做簡介。

FRBNY在聯邦準備體系之理事會(Board of Governors of the Federal Reserve System)的總監督下運作，理事會每年向國會報告兩次。FRBNY受數個屬稽核階層的委員會監督，另受美國審計總署與監察長辦公室(the Office of the Inspector General)的審查。

FRBNY設有董事會(Board of Directors)、政風室(Ethics Office)及內部稽核職能，且其財務報導每年由獨立的外部公司稽核。其員工大約有3000人，分為多個組和室，除了內部稽核為獨立的單位外，所有的業務部門均向總裁及第一副總裁報告，再由總裁及第一副總裁向銀行董事會呈報，其組織關係圖如下。



第四節 風險報告的發展與要項

壹　風險報告的發展

一、從制式化的資料到有意義的資訊

原本陳報的風險評估資訊是非常制式化的，業務單位只是將之視為檢查清單(checklist)處理，結果是錯誤率高，所具價值不大，而且風險清單中未附詳細的評註，無關風險管理。

現在陳報的風險評估資訊就較具意義了，業務單位能各按其需求去評估，對主要風險附有詳細的評註，包括敘事及風險分級，且增進各功能之間與小組之間的討論；起初雖然是錯誤率高，但持續半年適度的努力後，已產生相當的價值。

二、殘餘風險分級表格-主要由稽核及風險管理委員會決定

(一)提出關於風險分級在過去及未來的看法，和現行的評估。

(二)對每一個風險種類的殘餘風險分級的改變加上評註，等級是按主要業務類別(major business lines)區分，而非以功能式組織(functional organization)區分。

(三)促進跨功能和小組，以及風險委員會、管理委員會，稽核及風險管理委員會之間的討論。

(四)起初亦是錯誤率高，但持續一季的努力後，已是低錯誤、高價值。

三、作業風險概況報告及軌跡紀錄表

(一)辨識主要風險論題、趨勢及減緩活動計畫。

(二)主要資訊來源是業務部門風險評估。

(三)經由各風險委員會與稽核及風險管理委員會之間的共同討論。

貳　風險報告的要項

一、風險及控制自行評估

所有業務單位每年呈交的報告中，係依功能式組織[註]記載主要作業風險，所呈報的項目範圍如表一所列。

註：功能式組織（Functional organization）係企業組織結構中的一種類型，組織內部單位依據工作性質來劃分部門，強調專業性，適合具重複性的工作、例行性事務，但不適於動態、不確定性與複雜性高的專案。其特色是不同功能部門間的人員互動、溝通較差。

表一　風險報告項目一覽表

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(identified)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。

二、風險事件報告

FRBNY對於風險事件報告，界定四項報告方針：1.風險事件及嚴重程度(重大、中等、低、近乎零)；2.風險通知書及升級過程；3.風險分析及報告過程；4.必要的始末資料。另規定每位職員不管其任期，階級或職位都該對風險事件負責，但風險事件的報告中不提懲罰。

每季陳報風險事件的分析資料，以確認業務面及銀行全面的趨勢，由風險顧問覆審導致風險事件的起因及其性質。

三、業務風險及控制圖(Business Risk and Control Mapping)

(一)業務風險及控制圖的處理三步驟：1.繪製業務流程圖-包括不同業務部門之間的移轉；2.辨識及評估流程風險；3.擬定減緩風險策略及控制方案。

(二)業務風險及控制圖的功用如下：

1. 提供各項業務之風險及控制的端點到端點的概觀，以助於各項功能/業務風險之辨識及確認。

2.統籌目前風險報告、評估及控制之運用工具的架構，促進活動階層中作業風險及相關控制方法的評估。

3.加強在各階層中風險/控制文化，滲入組織中各個階層的從業人員。

4.統籌架構目前風險報告、評估及控制的工具，支源其他圖/風險/控制的計畫(例如：優化業務流程及資料處理)

5.提供在各功能或組別中可接受之剩餘風險的流程，藉以洞察直接從何處投資可以降低風險。

6.藉由業務風險及控制圖的異動管理，有助於辨識在流程改變之中可能有的風險。

四、目前持續改進之處

(一)目前作業風險報告向風控長陳報

-分別由不同人員負責金融風險及作業風險，但合併陳報。

(二)當金融風險減弱時，作業風險則躍居主要風險

-隨組織改變，給予我們重新探討何處應優先改進的機會。

-銀行近來所得的結論是要倡導一個強健的策略計畫，正尋求將辨識策略風險與作業風險計畫相結合的良機。

(三)統籌業務風險表格

-整合風險的概況。

-運用風險模型幫助確認應該控制之點(如：作業及法規遵行風險)。

(四)新規劃的業務風險及控制圖，是經由端點到端點的流程檢查，來確認風險並改進控制。

第三章　營運持續計畫（Business Continuity Planning）

近年來，隨著各項重大災難的發生，如美國 911 事件、東南亞大地震與海嘯，和 SARS 疫情等，除了造成許多人員傷亡外，更衝擊企業的營運作業，於是，營運持續管理的議題開始受到重視，企業期望藉由實施營運持續管理作業，將災害發生時所帶來的衝擊和中斷時間降至最低，同時讓營運持續能力提升至最大。

巴塞爾銀行監理委員會將作業風險損失事件型態分為七大類：即內部舞弊（Internal Fraud）、外部詐欺（External Fraud）、員工作業與工作場所安全（Employment Practices and Workplace Safety）、客戶、產品與營運作業（Clients, Products and Business Practices）、人員或資產損失（Damage to Physical Assets）、營運中斷與系統當機（Business Disruption and System Failures）和執行、運送與作業流程之管理（Execution, Delivery and Process Management）。

穩定全國金融是中央銀行的重要職責，那麼央行營運不中斷的重要性自不在話下，有鑒於此，本章特別就上述七類風險中「營運中斷」一項，簡述美國紐約聯邦準備銀行(Federal Reserve Bank of New York；以下簡稱FRBNY)的危機管理。惟營運持續管理的理念近年來在各界已廣受重視，在多處論著中亦有很多的探討，所以就不再此多作著墨，僅就FRBNY現行的營運持續計畫及危機管理稍做介紹。

第一節 FRBNY的營運持續計畫

美國聯邦準備銀行兼負維繫全美及全球金融穩定的重責，營運持續計畫對其尤顯重要。2012年颶風珊蒂(Sandy)重擊美國東岸，導致電力與交通中斷，許多網路資料中心的運作，都因為電力供應不穩定，或是動力中斷以及水患等問題受到影響，美國證券交易所也史無前例地陷入連續休市2天的窘境。美國東岸的無線基地臺陷入癱瘓，影響所有的無線通訊服務，包括通話、上網、數據傳輸等網路服務都因此面臨無法持續營運的挑戰，FRBNY因而更體認到加強銀行的營運持續計畫的重要，列出兩大必要主因是：

一、任務不中斷

(一)執行貨幣政策。

(二)透過對存款機構、市場及支付系統、最後放款者的監督，來維繫金融的穩定。

(三)提供金融機構、美國政府及外國中央銀行等金融服務。

二、營運持續計畫是作業風險計畫中的一部分

- 有效的營運持續計畫可以減輕營運中斷的影響，並降低整體的作業風險。

壹　營運持續環境中風險及危害的認知

在制定計畫之前，須先瞭解營運持續環境中的主要風險及危害的情況，才能研訂周全的計畫。

一、主要風險

(一)人為災害：1. IT 的威脅；2.恐怖分子的威脅；3.國內動亂；4.內部的威脅

(二)天然災害：1.氣候的威脅；2.全國性流行病

二、危害情況

(一)威脅的影響無法預測：

範圍是局部性或區域性？中斷時間是幾天、數月或幾年？這些或許可預期，也或許無法預測。

(二)危害發生情況：

FRBNY考量下列各種情況制定計畫：1.辦公大樓無法使用；2.無法通訊(如：電腦網路，電信)；3.職員無法工作；4.以上情況合併發生。

貳　制定營運持續計畫的依據

FRBNY依據國際清算銀行(Bank for International Settlements, BIS)所訂的金融機構高級營運持續原則(High-level Business Continuity Principles)，以及國際災難恢復協會(Disaster Recovery Institute

International；DRII)的專業實作要點，制定橫跨整個聯邦準備體系的營運持續計畫，並力求不斷改進，找出最佳實作規範。另設立四大策略營運團隊：1.營運持續專門小組 2.營運持續指導委員會 3.營運持續聯繫小組 4.外部合作者（External partners）。

參　營運持續計畫的內涵

一、營運持續計畫項目有下列九項：

(一)營業項目概述

(二)營業衝擊分析：管理階層分析機構資源喪失所造成的衝擊。

(三)關鍵性過程及其在其實際應用上的確認

(四)目標回復時間(Recovery Times Objectives) - 是指在故障或災難發生後，直到系統恢復運作所需的時間(可容忍的系統中斷服務時間)。

(五)目標回復時點(Recovery Point Objectives) - 災難發生前，最近一次資料備份/複製成功的資料時點(可容忍的資料損失)。

(六)必需的基礎設施及場地空間

(七)各部門或應用系統間的相依關係

(八)訊息溝通計畫

(九)意外事故備援地點

二、維護計畫及訓練

(一)維護計畫：每年審核及驗證營運持續計畫，以確定計畫是否適當、充足並有效，可以滿足持續性的需求，進而確保計畫的流程不會因時間而失效。

(二)訓練：

1.人員的安全為第一優先 - 以人員預先安排妥當為首要

相關的訓練有疏散程序及安全演練，全面電腦模擬訓練，印發全體職員緊急事故手冊，舉辦認知講習會及線上演練等；另以 9 月為全國預備月。

2.持續危機管理訓練及測試 - 技術準備狀態測試，桌面演練，危機管理情境演練等。

第二節 FRBNY的危機管理

首先清楚架構危機管理組員的角色與職責，再輔以文檔資料，形成最佳實作規範。危機管理組員分別有：1.第一線出動人員；2.緊急應變計畫指揮官；3.疏散協調員/消防員；4.緊急事故處理小組；5.危機處理官員/資深管理團隊；6.營運持續聯繫小組；7.外部合作者。

至於輔助的文檔資料內容則臚列如下：

一、危機處理職責與工作-確認主要人員知悉其在緊急事故中派定的職務與責

任。

二、全體工作人員的安全及可能的影響

(一)若是可能，在事件發生之前關鍵人員預先定位。

(二)建立緊急狀況中可能產生的人事相關問題之處理原則，如補償金等。

(三)確保可取得各種設備及支援，足供緊急事故期間待命的關鍵人員使用，例如：人員衛生保健物品，毛毯，雪鏟，食物及飲水等。

三、持續運作

(一)確保在異地營運，於延長期限時有足夠的容納空間；且當第一線出動人員/緊急處理組員無法立即得到支援時能自己自足。

(二)考慮與附近旅館或燃料供應商簽立契約或備忘錄，在緊急狀況中協助供給事宜。

(三)若在遠地備援時，確保人員有足夠設備，如手提電腦，連接網際網路，備用電源等。

四、通訊(外部及內部)

(一)在緊急事故之前覆審危機通訊協議及後勤工作。

(二)確保在緊急事故期間能有多種的通訊方式。

(三)確保銀行職員，客戶與其他相關單位間的聯繫是準確的，而且得到的是最新消息。

(四)預測客戶所需的資料。

五、協調與外部合作者的回應行動-建立/維持主要的危機溝通關係，如第一線出動人員，公共/健康安全小組，和州/聯邦管理機構，使這些關係在緊急事故中能夠統籌得宜。

第四章　優化業務流程

優化業務流程(Business Process Excellence；BPE)也稱為作業優化(Operational Excellence)，係運用業務流程管理系統(Business Process Management；BPM)，將BPE導入業務及資訊技術 (Information Technology；IT)，可快速並有效率地建立預警流程，提出業務面現行或未來將面臨的困難，使組織更有能力對營運環境的改變預作準備。

在過去，組織優先考慮的是工作效率和預測未來市場的能力。如今資訊時代，則強調對環境的快速回應能力，因而組織設計要求具有彈性。所以對組織活動的每一個單獨領域，重建並制定新的、有彈性的流程及架構是非常重要的。一個組織如果持續舊有不合時宜的實務作業及科技基礎架構(technology infrastructure)是不可能成長的。在微利與競爭激烈的現代，如何用最精簡的資源執行各項業務流程，能夠維持品質，同時又能達到風險控制的效果，乃成為企業所關注的焦點，因此業務流程的優化是現代企業不得不思考的問題。

所謂流程管理（process management），其核心就是流程，流程是任何企業運作的基礎，企業所有的業務都需要流程來驅動，一般認為流程管理是一種以規範化的構造端到端的優化業務流程為中心，持續的為企

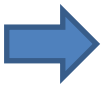
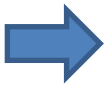
業管理和運營提供標準規範的操作。

第一節 FRBNY 優化業務流程的應用

優化業務流程(Business Process Excellence；以下簡稱 BPE)最初是由金融服務小組(Financial Services Group)提案，已被證實是一項使 FRBNY 的作業更有效率，決策更有彈性的重要因素。BPE 在 FRBNY 所應用的範圍如圖一。圖二則是 FRBNY 將 BPE 技術應用於風險管理，兩者相配合的情形。

圖一　BPE 在 FRBNY 所應用的範圍

圖二　作業風險管理與 BPE 的配合情形

作業風險管理 需要：		**BPE** 提供：
關鍵流程及活動的確認		運用端到端流程(End to End process) 查看並了解業務面
監控關鍵指標並警告潛在問題		統計製程管制(Statistical Process Control)[註]及流程管理(Process Management)
消除問題/看現行流程的績效		流程改進
以新流程預防問題		流程設計

在流程的優化中強調端到端流程(End to End process)，所謂「端到端流程」係指以客戶、市場、外部單位或機構及企業利益相關者，為輸入或輸出點的一系列連貫、有序的活動的結合。輸入端從客戶需求端出發，輸出端也是到滿足客戶需求端去。

註：統計製程管制(Statistical Process Control；SPC)，係指一套自製程中去蒐集資料，並加以統計分析，從分析中去發掘製程的異常，立即採取修正行動，使製程恢復正常的方法。

從企業整體來看，一個制度中往往制定了幾個細則或流程，或涉及兩三個部門，若只關注於局部流程的優化，不能解決根本的問題，無法實現全局的優化。以員工投訴獎金未及時發放為案例，單純強調獎金發放流程是不夠的，因還涉及獎金核算流程，所以必須從開始核算數額，到獎金發放到員工帳戶看成一個完整的端到端流程，才能有效地解決此問題。因此要整合起來分析，一旦整合流程後，很多工作可以並行處理，就能大大提高處理時效。

以下各節將介紹 FRBNY 如何在業務流程管理系統中，運用失效模式與效應分析風險評估工具(FMEA Risk Assessment Tool)，透過數據來瞭解並證實流程目前在效率、品質、風險控制面上的績效狀況，並找出流程問題的根本原因，進而提出改善目標與執行改善計畫，持續追蹤流程績效的變化，達成持續性的流程管理。

第二節 FMEA 風險評估工具(FMEA Risk Assessment Tool)

壹　何謂失效模式與效應分析

失效模式與效應分析(Failure Mode & Effects Analysis；以下簡稱 FMEA)，是一種預感式風險管理的作法，是一種由下而上的歸納式系統分析或流程分析方法，用來評估潛在性的錯誤，包含找出什麼會造成錯誤，以及會發生錯誤的方法(失效模式)，決定每個失效模式對系統的影響。分析的對

象是系統，與風險及控制評估(Risk and Control Assessment；RCA)不同，RCA 分析的是事件；亦即分析系統那裡會出錯，一旦出錯會多糟，那裡需要修正才能避免事故發生。至於 RCA 將在第七章中討論。

FMEA 是企業內推動各項改善活動的基礎工作，其目的可用來作為設計管制工具(Design Control Tool)、風險分析工具、風險管理工具等。

貳　FMEA 分析法之步驟

一、定義每個流程功能或風險類別，決定風險及其影響，並對影響程度評估等級。

(一)風險：在某一流程功能失效時，描述將發生何種錯誤，若沒有察覺並更正或移除，會引發衝擊的風險。(例如：遺漏訂單號碼)

(二)衝擊(Impact)：對客戶需求的影響-通常指計畫目標或最終交付物。(例如：延遲付款發票)

(三)衝擊度(Impact Rating；IMP)：對客戶影響的程度予以分級。(9=非常嚴重，7=很高，5=中等，3=很低，1=微小)

二、確認引發風險的所有因素並分配發生機率

(一)引發因素(Triggers)：導致發生風險的因素(例如：流程步驟未完成，印刷錯誤)

(二)發生機率(Probability；PROB)：以發生的可能性/頻率分級(9=非常高或 > 50%，7=高或 33%，5=中等或 13%，3=低或 5%，1=微小或 < 5%)

三、確認任何可能防止或察覺風險之減輕風險的行動，給予察覺的機率，將所有的機率相乘得到風險優先指數(RPN)。

(一)目前減輕情形(Current Mitigation)：在發生衝擊之前以系統化方式來防止或察覺風險或其引發因素，如自動化控制及偵測方法，包括稽核，檢查清單，檢閱，測試，訓練等。

(二)察覺(Detection；DET)：對如何能察覺風險已經發生的機率給與分級。(9=幾乎不可能，7=不太可能，5=中等，3=高，1=非常高)

(三)風險優先指數(Risk Priority Number；RPN)：做為風險分級的依據數目，RPN = IMP×PROB×DET。

四、確認建議減輕風險之行動及指派負責人員

參　FMEA 風險評估案例

FMEA 風險評估工具提供了有條理的方式來做風險評估，其設計的表單如圖一，圖二則為實例，係取自軟體開發流程之風險評估的一部分(見於本章末兩頁)。

第三節 業務流程管理系統帶給業務面的激勵

運用業務流程管理系統，能使企業迅速並且有效率地建立應用流程，去因應現行及未來的營運所面臨的挑戰，因而企業將更有能力隨營運環境的改變，適時去調整。

在業務面運用業務流程管理系統者很多，然其共同的主題都是作業優化及風險管理。綜觀業務流程管理系統為企業業務發展所帶來的激勵有以下幾方面：

一、獲得新的成長機會與創造能力：因看見並回應市場的改變，以及滿足客戶需要的變化，以更好更快的決策得著了新的成長機會與創造能力。

二、新的法規遵循與風險管理：因監督現行標準及政策的執行，隨時更新了新的法規遵循與風險管理。

三、滿足客戶的需求：因更快速地回答問題並解決爭議，使客戶的滿意度提高。

四、作業效率的壓力：藉著提升績效的能見度，促使作業成本降低，令作業更具效率。

FMEA 風險評估工具(FMEA Risk Assessment Tool)

■為風險評估提供一種有條理的方式

風險評估(risk assessment)

#	流程功能/風險種類	風險	衝擊	IMP	引發因素	PROB	目前減輕的情形	DET	RPN	建議淡化之行動	負責人員&目標日期
	審查程序步驟/風險種類為何？	風險是什麼？	如果風險發生，衝擊是什麼？	此風險對客戶的影響程度為何？	什麼是引發因素？	此風險發生的可能性？	防止此風險發生的現行控制與程序是什麼？	如何發現此風險已經發生？	IMP X PROB X DET	降低引發的可能性，或提高偵察的行動是什麼？	誰該對此行動負責，及目標完成的日期為何？
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											

■下表是取自軟體開發流程的風險評估的一部分

風險評估(risk assessment)

#	流程功能/風險種類	風險	衝擊	IMP	潛在失效因素	PROB	目前減輕的情形	DET	RPN	建議減緩之行動	負責人員&目標日期
	審查程序步驟/風險種類為何？	風險是什麼？	如果風險發生，衝擊是什麼？	此風險對客戶的影響程度為何？	什麼是引發失效因素？	此風險發生的可能性？	防止此風險發生的現行控制與程序是什麼？	如何察覺此風險已經發生？	IMP X PROB X DET	降低引發的可能性，或提高偵察的行動是什麼？	誰該對此行動負責，及目標完成的日期為何？
1	規定日期	「抄近路」以符合計畫期限	無法符合報告的要求	9	延誤附屬計畫	7	任務與職責表及品質的覆核流程	9	567	勤加訓練以確保執行稽核的品質計畫	CARS 計畫經理
2	規定日期	「抄近路」以符合計畫期限	無法符合報告的要求	9	對流程的重要性缺乏賞識	7	任務與職責表及品質的覆核流程	9	567	於高層樹立風氣(高職責及團隊配合)	Dave Rebich
3	規定日期	「抄近路」以符合計畫期限	無法符合報告的要求	9	對達成期限嚴厲的施壓	7	任務與職責表及品質的覆核流程	9	567	分享對計畫品質原則的確立包括：清楚地傳達品質比計畫表及不修改的目標更重要	EOG
4	管理	在第 3 錯誤階層(高)做決策	無法符合預算	5	無充分資訊或影子治理的流程	3	任務與職責表	5	75	在 R&R[註]文件中確立清楚的期望	CARS 計畫經理

註：R&R：Repeatability & Reproducibility(再現性與再造性)　　RPN：風險優先指數(Risk Priority Number)

第五章　風險評估方法

有別於前章所談的 FRBNY 在業務流程管理系統中運用 FMEA 風險評估工具，本章將談到美國聯邦準備體系(Federal Reserve System；以下簡稱 FED)中稽核所用的風險評估方法論(Risk Assessment Methodology；以下簡稱 RAM)。

風險評估是稽核規劃過程中的一項必要程序。為什麼要進行風險評估？主要是希望「錢要花在刀口上」，也就是將現有資源(成本)發揮最大的效益。而透過風險管理可以有效率地簡化業務，是以內部稽核計畫需要導入風險評估模式。

第一節 FED 風險評估方法

在第一章說明風險評估的定義時，曾提及 FED 對風險評估的定義，係運用風險基礎(risk-based)的方法，於適當的稽核範圍內，衡量銀行作業的相關風險；並且須具有客觀、量化、彈性、簡易通用等特性。

所謂的「風險基礎稽核」(Risk-based Audit)，其做法就是先找出稽核對象（ Auditee ）的所有相關風險，然後再為每項風險配對目前的控制點（ Key Control)，並衡量其控制是否足夠及有效。

FED 的風險評估方法聚焦於三點：1.集中在固有風險；2.強調人力資源風險；3.強調變化性及複雜性(新興風險)。至於風險評估的流程則是：1.訂定稽核範圍

及查核活動(auditable activities)；2.應用風險模型；3.年度風險評估與分級；4.依據風險分級、頻率指標、專業判斷訂定年度稽核計畫。下一節則就如何應用風險模型得到風險分級、查核頻率等指標，進而規劃年度計畫做說明。

第二節 風險模型的應用

壹　風險模型

風險模型可分為兩大主要部分-業務概況(business profile)及風險評估計分矩陣(Risk Assessment Scoring Matrix)來說。

一、業務概況 - 搜集風險資訊並分析、評估風險。

(一)記載稽核範圍內每個受查單位的風險評估，做成文件檔案供擬定中的稽核範圍所利用。

(二)風險資訊來源包括：稽核管理、銀行管理、最近的稽核範圍、作業風險管理計畫、異常事件、稽核與客戶端的聯繫關係等。

二、風險評估計分矩陣 - 將查核活動分列等級，以規劃整體稽核範圍，評分過程如下：

(一)預先訂定風險因素的加權數

(二)給予每個風險因素風險等級 1~4 - 4=高；3=中高；2=中；1=低

(三)計算風險因素的分數 - 加權數 X 風險等級

(四)加計所有風險因素的分數

貳　風險評估計分矩陣範例(部分節錄資料)

一、表一為風險評估計分矩陣空白表格；表二為風險評估計分矩陣案例(見於本節末兩頁)。

二、範例說明

(一)風險因素(risk factor)分四大類：

1.作業風險：(1)業務流程；(2)技術與資訊管理；(3)人力資源

2.金融風險(包括信用風險及市場風險)

3.策略風險

4.信譽風險

(二)查核頻率(audit frequency)：依據評分的高低訂定如下

風險分級	分數範圍	最高頻率
高	326-400	每年
中	251-325	3 年內
低	100-250	稽核長授權決定

註：高風險項目的稽核可視影響因素而延長至 2 年

(三)完成計分矩陣得到指標

1.固有風險分數：高、中、低

2.減輕風險因素指標：(1)計畫不變；(2)增加查核頻率；(3)減少查核頻率

3.規劃之建議：(1)立即；(2)每年一次；(3)兩年一次；(4)三年一次；(5)其他

(四)影響因素(influencing factors)不可忽略：

1.稽核人員對標示高或中高風險之特定程序或功能的說明

2.做稽核規劃時，應個別注意有關低風險因素項目的額外討論及考量

3.這些程序或功能足夠證明：

(1)需要比整個業務範圍的查核頻率更高

(2)採個別查核或集中在整體稽核範圍中

表一 風險評估計分矩陣(Risk Assessment Scoring Matrix)-節錄

風險因素 (risk factor)	加權 (weight)	風險等級(risk level) (H=4 M+=3 M=2 L=1)	分數 (weight X level)	先前分數 (prior score)
作業面(Operational)				
1.業務流程(Business Process)	20	0	0	
2.技術及資訊管理 (Technology and Information Management)	20	0	0	
3.人力資源(Human Resources)	20	0	0	
金融/重要性(Financial/Materiality)	20	0	0	
策略(Strategic)	10	0	0	
信譽(Reputational)	10	0	0	
合計	100		0	

固有風險分數頻率(Inherent Risk Score Frequency)：❑▼
影響因素(Influencing factors)：❑▼
建議頻率(Recommended Frequency)：❑▼

風險分級(risk rating)	固有風險分數(inherent risk score)	頻率(frequency)
高	326-400	每年但可依影響因素延至兩年(Each Calendar year but can be extended to two based on influencing factors)
中	251-325	每三年(Every three Calendar years)
低	100-250	稽核長授權決定(General Auditor Discretion)

其他稽核計畫考量要點：請確認本業務概況中列為高或中高風險的範圍，確認這些程序或子功能是否有助查核計劃步驟的執行，或者決定列在其他更直接顯示該風險的另項查核範圍。例如：假設在業務範圍中 IT 功能是複雜又顯示高風險，則 IT 功能的審查，可能就要比整個業務範圍的查核頻率更高；此例的解決方案可能是將這些 IT 功能列在 IT 專案稽核中。

上次查核日期：　　上次風險等級：
查核日期：　　風險因素總分：

表二 風險評估計分矩陣(Risk Assessment Scoring Matrix)-節錄

風險因素 (risk factor)	加權 (weight)	風險等級(risk level) (H=4 M+=3 M=2 L=1)	分數 (weight X level)	先前分數 (prior score)
作業面(Operational)				
1.業務流程(Business Process)	20	4	80	80
2.技術及資訊管理 (Technology and Information Management)	20	3	60	60
3.人力資源(Human Resources)	20	3	60	60
金融/重要性(Financial/Materiality)	20	2	40	40
策略(Strategic)	10	3	30	30
信譽(Reputational)	10	3	30	30
合計	100		300	300

固有風險分數頻率(Inherent Risk Score Frequency)：**中等**(Moderate)
影響因素(Influencing factors)：**增加查核頻率**(Increase Audit Frequency)
建議頻率(Recommended Frequency)：**2 年內**(Within 2 yers)

風險等級(risk rating)	固有風險分數(inherent risk score)	頻率(frequency)
高	326-400	每年但可依影響因素延至兩年(Each Calendar year but can be extended to two based on influencing factors)
中	251-325	每三年(Every three Calendar years)
低	100-250	稽核長授權決定(General Auditor Discretion)

其他稽核計畫表考量要點：請確認本業務概況中列為高或中高風險的範圍，確認這些程序或子功能是否有助查核計劃步驟的執行，或者決定列在其他更直接顯示該風險的另項查核範圍。例如：假設在業務範圍中 IT 功能是複雜又顯示高風險，則這些 IT 功能的審查，就要比整個業務範圍的查核頻率更高；此例的解決方案可能是將這些 IT 功能列在 IT 專案稽核中。

價格支撐小組(VST)風險評估最初是統合在貼現窗口風險評估，現在則是獨立評估，乃是根據起初對 VST 進行風險評估的結果是中等風險等級，我們遂決定查核頻率為每兩年一次(而非三年)。根據該區域/系統呈現之風險的危險程度，所有風險因素列為高、中高或中等。我們決定在 2014 年查核 VST。

上次查核日期： 03/29/2013　　上次風險等級： 中等
查核日期： 04/2014　　風險因素總分： 300

參　年度稽核計畫

內部稽核單位依評分高低篩選應該導入年度稽核計畫之稽核作業項目，其目的是要達到稽核資源之有效配置並擬定年度稽核計畫，並非所有作業項目、單位都要稽核，而是以風險評估結果之高低來考量，在有限的人力與時間內，提升稽核之品質及效率。在年度稽核計畫中應注意的要點如下：

一、通常將風險愈高者列為愈優先稽核。

二、年度稽核計畫中稽核的時間表應該是彈性的。

三、業務流程、風險等級及查核計畫至少每年要審查並修正一次。

四、在計畫各個稽核範圍時，應個別衡量風險因素的分級。

最後摘要以下五點結論：

一、RAM 規範於 IIA 準則中。[註]

二、RAM 適用於 FED 所有的業務活動

三、風險評估以固有風險為基礎

四、整體的風險評估流程有 4 步驟：

(一)確認整個聯邦銀行的查核活動

(二)完成業務概況檔案資料及評估與評分

(三)根據風險將稽核活動(auditable activities)予以分級

(四)根據風險評估之結果規劃稽核範圍

五、影響因素應列入考量，因查核頻率會受其影響。

註：2013 年 1 月 1 日起適用之「國際內部稽核執業準則修訂版」見於中華民國內部稽核協會之網站公告。

第六章　內部稽核能力模型

什麼是內部稽核能力模型（Internal Audit Capability Model；以下簡稱IA-CM）？可用以下三點做扼要的敘述：

一、傳達工具：適用於組織企業，用來建立有效的內部稽核，強調內部稽核之價值論點的一套工具。

二、評估的架構：提供可以評估能力，或自行評估，或外部評估的架構。

三、規劃圖：有明確的步驟，可供一步一步的遵循，來建立能力，並逐步提升。

有關IA-CM在美國內部稽核協會的研究基金會(The Institute of Internal Auditors Research Fundation)2009年出版的「Internal Audit Capability Model(IA-CM) for Public Sector」一書中，有詳細的解說，本章僅就其緣起，以及內部稽核能力模型矩陣作基本介紹。

第一節 內部稽核能力模型的緣起

2004年，公營部門委員會(Public Sector Committee；以下簡稱PSC)建議發展一套IA-CM，可以加強在公營部門中，內部稽核的監理能力及其權責的重要性。PSC發現內部稽核在不同國家中可能有極大的差異，因為管理實務、步驟程序及各個政府的文化各不相同，於是PSC認為建立一套通用的模型，讓公營部門的內部稽核活動，在做自行評估時可以運用，是有需要的；而且有一套工具可供用來評估

稽核活動的進展，並作為訓練、建立能力的依據，也是必需的。

美國內部稽核協會的研究基金會遂於2006年9月開始著手計畫發展IA-CM，提供全球政府部門或更廣泛的國營機關的內部稽核，在執行時有基本的依據，以強化其能力，建立有效並制度化的內部稽核。該計畫分兩個階段，第一階段是自2006年10月至2007年4月，第二階段是自2007年11月至2009年5月。兩階段的計畫內容如下：

第一階段：定義每一個階層的特性，內部稽核活動的要素，以及每個要素與每個階層中的關鍵流程領域（Key Process Areas；KPAs）。

第二階段：依據第一階段的結果，研擬制訂五個能力階層，並進而加以辨認、評估每一個階層對下一個階層的能力貢獻。

第二節 內部稽核能力模型矩陣

在IA-CM所定的公營部門有效的內部稽核所需的基本架構中，包含5個漸進的能力階層及6項基本要素。這5個階層分別為初始階段、基礎建構階段、整合階段、管理階段及最佳階段，每個階層各有其特性及其稽核活動能力。而內部稽核活動必須包含6項基本要素：1.內部稽核之角色與職務；2.人員管理；3.專業實務；4.績效管理與權責；5.組織關係與文化；6.治理架構。而內部稽核能力模型矩陣(Internal Audit Capability Model Matrix)則如圖一所示。

圖一 內部稽核能力模型矩陣

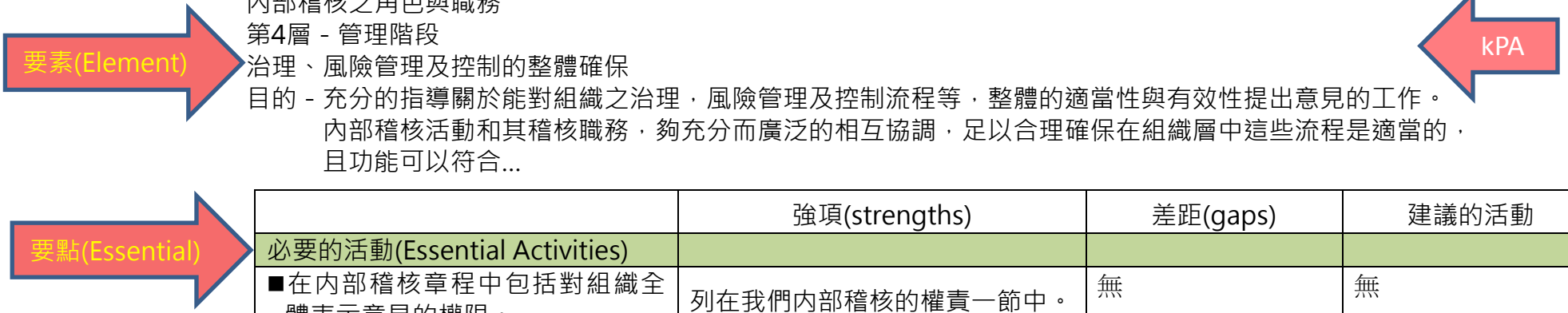
	內部稽核之角色與職務	人員管理	專業實務	績效管理與權責	組織關係與文化	治理架構
第5層-最佳階段	內部稽核被視為變革的主要推動者	▪領導者參與專業組織 ▪人力預測	▪專業實務之持續改進 ▪策略性內部稽核規劃	內部稽核成效的公開報導	有效性及持續性之關係	內部稽核活動之獨立性、權力及授權
第4層-管理階段	治理、風險管理及控制的整體確保	▪內部稽核促進管理發展 ▪內部稽核活動支持專業組織 ▪人力規劃	稽核策略影響組織的風險管理	績效衡量之質與量的整合	稽核主管的建議並影響高階管理	▪內部稽核活動的獨立監督 ▪稽核主管向高層主管報告
第3層-整合階段	▪諮詢服務 ▪績效/金錢效益稽核	▪建立團隊及稱職的能力 ▪具專業資格的人員 ▪人力協調	▪品質管理的基本架構 ▪風險導向稽核計畫	▪績效衡量 ▪成本資訊 ▪內部稽核管理報告	▪與其他覆核單位的協調 ▪管理團隊的整體要件	▪內部稽核活動的管理監督 ▪籌資機制
第2層-基礎建構階段	遵循法令稽核	▪個人專業能力發展 ▪辨識並招收具熟練技能的人員	▪專業實務及流程的基本架構 ▪稽核計畫以管理階層/利害關係人為優先作基礎的	▪內部稽核作業預算 ▪內部稽核業務計畫	內部稽核活動範圍內的管理	▪完整接觸組織之資訊、資產及人員 ▪既有的報告體制
第1層-初始階段	▪事前無系統的；▪覆核文件及交易的正確性及遵循法令與否或單一的稽核；▪產生的報告端視位居其位之人的技能而定；▪除了那些有專業學會協助者外，未建立專業實務；▪有籌資之需時，由管理階層核准；▪缺乏基礎結構；▪稽核可能是較大組織內一個單位的一部分；▪稽核員可能是大型組織中的一個單位；▪未建立專業能力；▪因此並無特定的關鍵流程領域					

在每一個階層中各包含了數目不等的關鍵流程領域 (Key Process Areas；以下簡稱KPAs)，所謂KPA是指內部稽核活動從某一階層進到下一階層之前，在該能力階層必需具備並持續改進的關鍵行動。每一個能力階層包含一個以上的KPAs，而KPAs均與內部稽核的6項要素相結合，KPAs是決定內部稽核活動之能力的主要建立領域，亦即在每一個階層中的KPAs，建立了實務作業及下一個階層能力的基礎。而每一個KPA則包含一項目的，必要的活動(essential activities)，結果及制度化之實務，此由下頁圖二的IA-CM中KPAs的應用範例，即可明白。

在某一內部稽核能力階層中的內部稽核活動，相關的KPAs必須非常熟練並且制度化，才可視為能力已到達該階層。然而每一內部稽核活動可以選擇維持在任一階層，使其內部稽核活動在該特定的組織及環境中，仍有最佳的表現。也就是說，可以選擇維持在第2層或第3層，而不渴求進升至下一階層，因為對該時期而言，現行階層的成本效益最好。

是以，此模型架構了一個可供遵循的漸進步驟，這些步驟分成五個進展能力步驟，經由許多細步的逐漸推進，來強化或提升內部稽核能力，使各機關能執行有效的內部稽核，達成機關監督體系的需求及專業的預期。

圖二　IA-CM中KPAs的應用範例



內部稽核之角色與職務
第4層 - 管理階段
治理、風險管理及控制的整體確保
目的 - 充分的指導關於能對組織之治理，風險管理及控制流程等，整體的適當性與有效性提出意見的工作。內部稽核活動和其稽核職務，夠充分而廣泛的相互協調，足以合理確保在組織層中這些流程是適當的，且功能可以符合...

	強項(strengths)	差距(gaps)	建議的活動
必要的活動(Essential Activities)			
■在內部稽核章程中包括對組織全體表示意見的權限。	列在我們內部稽核的權責一節中。	無	無
■確保內部稽核活動範圍包含組織的治理、風險管理及控制流程。	稽核章程中給予此項權利，可以查核公司治理，IT 治理，SIRA 及法規遵循。	無	無
■依照風險基礎稽核計畫，充分審核有關組織的治理、風險管理及控制流程等。	公司治理，IT 治理，SIRA 及法規遵循均列入稽核範圍，風險均依照稽核範圍去評估。	無	無
■稽核所提的整體意見是在一定期間的查核內(通常是一年)。	整體分級/意見列在 ARC 報告中，並和 AC 及 MC 討論過。	無	無
■對每個別查核的意見是在特定執行期間提出。	執行中	無	無
■對所提的意見要充分，並有相當的稽核憑據，是與準則的規定相符的。	執行中，經由 QA 計畫查證確定。	無	無
■必要時，可以執行年度性的組織治理稽核，以支持整體的意見。	公司治理，IT 治理，SIRA 及法規遵循均列入稽核範圍，風險均依照稽核範圍去評估。	無	無

第七章　稽核執行方法論

前面提過內部稽核單位應依風險評估結果擬訂年度稽核計畫，本章將以 FED 的做法為例，介紹稽核規劃的方法，並簡介整合式稽核的概念。

第一節　FED 稽核規劃方法

FED 稽核規劃方法是以計畫為中心(planning-centric)的風險基礎查核方法，而不是以實地查核為中心(fieldwork-centric)。近來 FED 的稽核執行方法有略做修正，其計畫階段所花費的時間約佔稽核時間的 20%，以往所花費的時間將近稽核時間的 60%。好的計畫不但可以充分確認對外的稽核工作，而且風險及控制評估的文件檔案可供日後參考；其修訂後的稽核周期(Revised Audit Lifecycle)如圖一所示。

壹　稽核規劃方法的重點說明

一、稽核規劃方法的重點有四：

(一)設計一個可供稽核人員於規劃稽核工作時的架構。

(二)規劃分兩個建議階段：

1.第 1 階段是關於擬訂策略及受查者背景資料分析(例如:聯繫工作)。

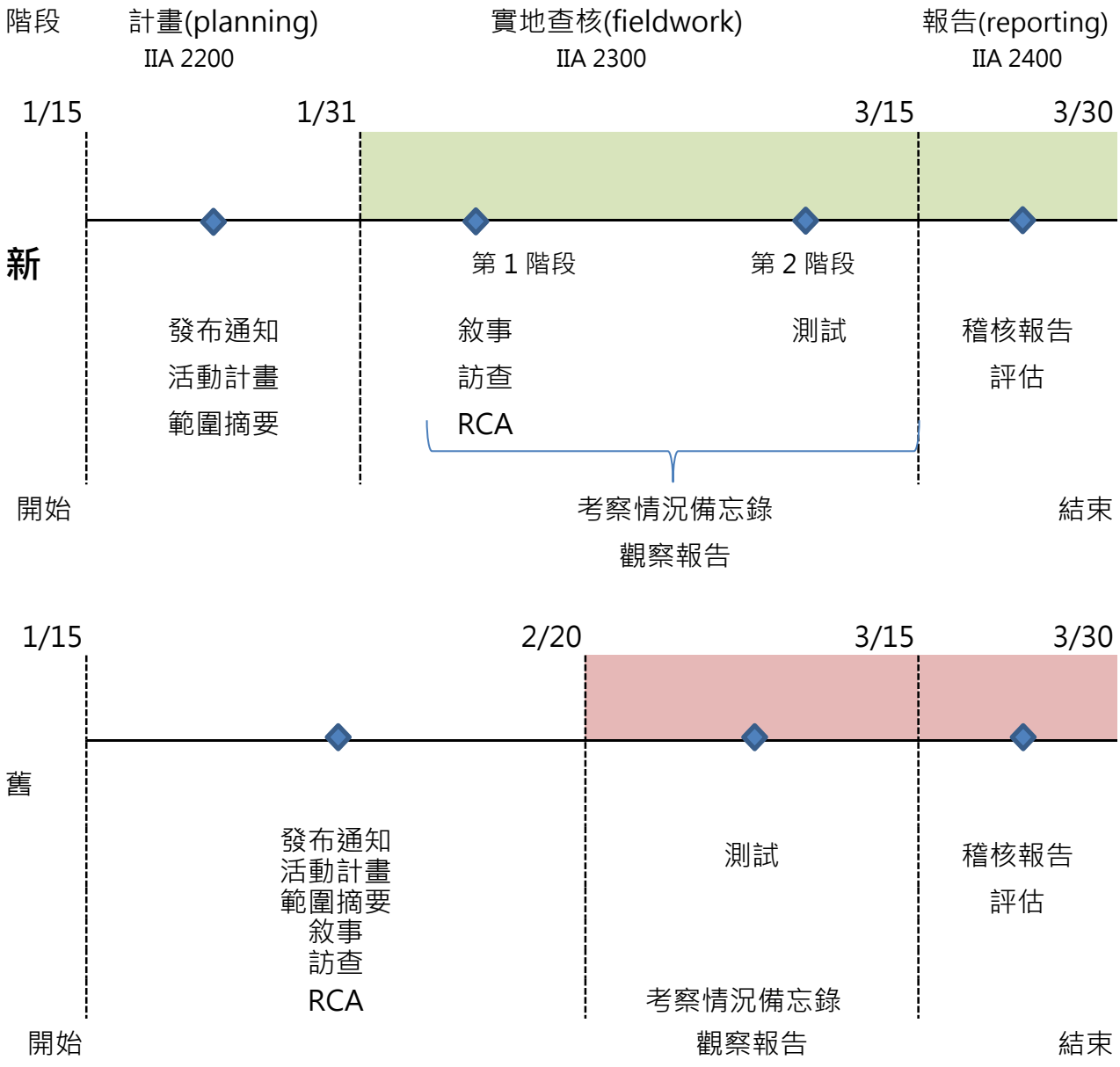
2.第 2 階段是關於固有風險、控制目標(預期的控制)，並與稽核對象(受

查者)預先討論。

(三)彙集資訊做成風險及控制評估(Risk and Control Assessment ; RCA)文件。

(四)過程中也應將稽核主管及稽核管理單位列入檢查點。

圖一 紐約聯邦銀行修訂後之稽核周期



二、風險及控制評估(Risk and Control Assessment；以下簡稱 RCA)

稽核周期中所稱的「RCA」，是取自業務流程中的固有風險，控制目標(預期的控制)及控制活動(實際的控制)，併同稽核人員對控制設計的評論，彙集而成的文件。實務上，RCA 分兩階段完成：

(一)初步的 RCA：是根據稽核人員的專業知識及自背景資料分析而得的資訊，提出風險的描述及控制目標，在規劃的初步階段擬訂，可供與稽核領導人員討論稽核作業時之依據。

(二)修訂後的RCA：根據實地訪查，並經由管理階層審查後，始完成修訂後的RCA。

三、稽核規劃之活動摘要

稽核規劃之活動摘要步驟如以下所列，並以圖二稽核時程表之範例，增進對稽核工作整體時程規劃之瞭解。

(一)選定稽核對象

(二)背景資料分析，並做成記述固有風險及預期的控制目標的初步 RCA 文件。

(三)規劃期間必需執行的工作摘要紀錄，亦即「活動計畫」與「範圍摘要」。

(四)發布通知給稽核對象

(五)啟始會議(Opening Meeting)

(六)詳細的實地訪查並更新 RCA，即將實際的控制目標及對控制設計的評估列入 RCA。

(七)發布考察情況報告給稽核對象，報告中將計畫階段所做的工作，初步的訪查結論，以及預備進行的實地查核做成摘要。

(八)執行實地查核

圖二 稽核時程表範例

貳　以計畫為中心之查核方法的優點

內部稽核的定位，已從傳統之事後的評估及確認，轉為以計畫為中心的

風險導向稽核，即注重事前的預防與評估，其優點如下：

一、在直接稽核之外，即做成風險控制評估，其資料來源有：先前的稽核，外部的審核，管理階層的自行評估，以及由業務聯繫與其他稽核同仁互動間取得的資訊。

二、在計畫階段，經由與業務單位管理階層的聯繫與討論所彙集的資訊，可作為日後稽核的參考。

三、藉助綜合性的風險評估，將查核目標專注於高風險項目；並有助於聚焦在控制面的考查，而非交易面。

四、可以減少實地查核階段中大量的稽核測試。

第二節　整合式稽核

「整合式稽核」(Integrated Auditing)並非是個新觀念，因現今風險管理已轉為處理企業之各類風險及整體風險，正因風險並非獨立，會互相影響，隨之控制亦是彼此相關，因此各類型之稽核有整合之需，遂認為整合式稽核是現今一個有效果兼具效率的稽核方式。

根據 2007 年公開發行公司會計監理委員會(Public Company Accounting Oversight Board；簡稱 PCAOB）訂定之第 5 號稽核準則(Auditing Standard No.5)規定：「對財務報導之內部控制的稽核，應與財務報表的稽核整合為一。」

整合式稽核的特點是：

一、將自動化及人工控制與相關風險，同時合併為一個單一稽核。

二、將作業流程，IT，及 COSO 所稱的 3 方面-財務報導、法規遵循及作業的效率與有效性，均整合在內部控制的稽核中。

三、合力將傳統稽核要點-金融面、作業面及資訊技術，集合為一個廣泛的稽核個體。

最後綜括整合式稽核的優點如下：

一、兼具效率和有效性。

二、評估企業之整體風險，有一致的看法。

三、能更有廣泛性的風險檢查。

四、充分使用不同的專業技術，增進稽核人員的技巧。

五、稽核團隊彼此間更密切合作，交換稽核發現之資訊，有更多的學習機會。

第八章　資訊科技安全管理與稽核

美國微軟總裁比爾．蓋茲說：「如同所有重大的改變一樣，資訊社會的好處必然伴隨著缺點而來。」資訊科技的進步也會衍生許多問題，如個人隱私、智慧財產、電腦犯罪、電腦與系統的安全等。傳統上所稱的「資訊安全(Information Security)」，焦點在於人，流程，及支援資訊與維持系統可靠、完整、即時的技術方法。現在隨著網際網路的普遍發達，資安攻擊手法不斷在翻新，新的威脅和安全弱點(Vulnerabilities)每天都在出現，危險大幅擴增，如今已改稱為「網路安全 (Cyber Security) 」。

本章先對資訊科技(Information Technology；以下簡稱 IT)安全風險管理做初步瞭解，再談 IT 稽核的趨勢。

第一節 資訊安全風險管理

資訊安全屬風險管理的一環，資訊安全風險不斷地在改變，用以管理這些風險的方法與技術也當不斷地隨之變化。資訊安全是一個管理過程，而不是一項技術導入過程，在 ISO 27002 標準中提到，「資訊安全是為了有效保護資訊不會受到各種威脅，實施各項適當的控制措施，以使企業能夠持續營運，將可能受到的損失降至最低，並獲得最大商機。」

壹　IT 的共同及新興風險

在執行 IT 安全風險管理及 IT 稽核之前，需先對 IT 的共同及新興風險有所認知，此類風險可分下列幾種：

一、網路安全

二、第三者風險

三、資訊安全管理

四、資料管理(DATA　Management) (安全，可用性，品質，法規遵循)

五、最新科技〔雲端運算(Cloud Computing)，虛擬化（Virtualization）〕

六、行動運算（Mobile Computing）

七、IT 資產管理

八、終端使用者的應用技術〔社群（social media），內部威脅管理，錯誤訊息〕

九、應用系統開發

十、持續營運/IT 備援

十一、法令遵循

貳　資訊安全管理計畫

為強化風險控制，一個成熟的資訊安全管理計畫應含括以下幾個方面：

一、架構：精簡，一致化，維持即時、安全及敏捷的系統平台與設計結構。

(一)降低駭客的攻擊面（Attack Surface），並且更迅速的回報系統中的漏洞(即弱點，Vulnerabilities)。

(二)預算考量-企業應當投入多少預算在管理資訊安全的風險，資安建設的建置成效如何等，均需評估考量。

(三)是否有高階管理階層的支持-導入資訊安全管理體系是否能為組織帶來實質效益，取決於組織管理架構的成熟度及調適能力。

二、弱點偵測(Vulnerability Testing)

駭客有組織的尋找資訊系統與網路結構中的漏洞來加以攻擊，要做到全面防堵幾乎是不可能的事情，此時，對攻擊手法要有更有效的傳導及反應，應採取端點到端點的安全測試管理。

三、人員(內部人員威脅)

企業管理階層應注意內部相關人員的背景經歷或職員保險，因內部相關人員對企業一次的破壞工作，會對企業經營團隊或對外的評價帶來很大的反效果，因此有賴防止、監視體制的維護，例如在工作場

所以外設置隱藏式監視系統。

四、外部服務提供商的可信度

(一)供應商安全保證計畫(審查、合約保證，及監控)

(二)持續監控或依規定提報資安事件

五、威脅情報：是否藉由多方面的情報來源，例如威脅情報交換平台，以縮短遭受攻擊到遏阻威脅之間的時間。

第二節 IT稽核的趨勢

壹 IT 稽核的新趨勢

現今 IT 稽核的趨勢如下：

一、企業風險管理

(一)企業觀點對照 IT 觀點下的風險比較

(二)將 IT 風險連結至組織目標

(三)端到端風險評估方法

二、增進與企業所有權人和非 IT 利害關係人的互動

三、與有保證的供應商合作

四、評估 IT 的管理活動

(一) 提升對策略目標的注意，以及法規的遵循和作業的問題

(二) 人事風險(權責劃分，人才挽留，技術能力)

五、檢查新興及其他重要風險

如：網路安全，第三者風險，最新科技，行動運算，社群

六、充分利用組織內外部的科技專業知識

七、聚焦於整合式稽核及 IT 專案/計畫審查

八、持續稽核與監控

貳　IT 稽核依循的標準

IT 稽核人員和風險管理專家做評估時，遵循的一些架構及標準如下：

一、資訊與相關技術控制目標(Control Objectives for Information and related Technology；COBIT)

二、資訊技術基礎架構庫(IT Infrastructure Library；ITIL)

三、內部控制專門研究委員會(Committee of Sponsoring Organizations；COSO)

四、國際標準組織(International Organization for Standardization；ISO)

五、美國國家標準及技術研究院（National Institute of Science and Technology；NIST）

六、沙賓法案（Sarbanes-Oxley；SOX）

茲以 COSO 標準中 IT 稽核的架構做說明，在 2013 年 COSO 架構中，新增 17 項原則分佈於五大要素之中，其中將「資訊的一般控制」列為「控制活動」項目之一，如下表所列；所以 IT 的控制是在組織的內部控制架構之中，目的是在確保資料的可靠性，正確性及可用性。

2013 年 COSO 架構新增 17 項原則分佈於五大要素之列表

控制環境	1.對誠正與道德價值表明承諾 2.執行監督之責任 3.建立結構、職權及責任 4.表明稱職的承諾 5.施行責任究問制度
風險評估	6.找出攸關/合宜目標 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
控制活動	10.選擇及建立控制活動 **11.選擇及建立資訊的一般控制** 12.制定相關政策及程序
資訊與溝通	13.使用相關資訊 14.內部溝通 15.外部溝通
監督	16.進行持續性和/或個別評估 17.評估及溝通缺失

IT的控制主要分為一般控制（IT general controls）和應用控制（IT application controls）兩大類，目的在於減輕IT風險：

一、IT的一般控制：對IT環境的一般性控制，例如異動管理，使用者及存取管理等。

二、IT的應用控制：是內建在個別作業程序的應用系統內，例如系統組態設定（System Configuration Settings）。

最後摘要 FRBNY 的 IT 稽核計畫如下：

一、結合 IT 流程，IT 基礎架構與組織單位。

二、植基於辨識及瞭解

(一)組織策略及業務目標：核心業務與 IT 策略間盡可能減少差異。

(二)主要業務流程：增進業務知識

(三)以模型支援 IT 稽核作業

(四)應用基礎架構：藉由資訊基礎架構瞭解整個業務流程的變更和相對風險。

三、IT 稽核執行的工作

(一)執行 IT 流程及基礎架構稽核

(二)參與業務流程的整體稽核

(三)專案審核

(四)新措施的諮詢

(五)持續聯繫活動

結論與建議

壹 內部稽核的新紀元

傳統的內部稽核重視財務稽核，是在交易發生之後才開始執行，以歷史交易及遵循度為查核重點，採用檢核表查核，偏重偵測及除弊，非以風險為考量。

現今的內部稽核範圍除涵蓋財務稽核外，亦包含管理稽核，要求更積極與有效的風險管理，並參與業務流程的設計，強調企業營運目標及創造企業價值。

IIA 理事長 Richard Chambers 在 2010 年一般稽核管理會議(GAM)裡的主題演講中重申了一點：「為了增加稽核的意義與價值...稽核需要了解昨天發生的事情，今天提供洞察營運上發生的原因，同時了解組織將在明天遇到什麼樣的風險。」

內部稽核的趨勢已從傳統稽核轉變為以風險為基礎的查核方式，稽核人員的角色已從檢察官的角色轉變為醫生的角色。現今的稽核被要求能夠辨識企業整體的風險，協助控制潛在風險，防止可能損失，也就是要增加稽核的價值。

是以內部稽核單位面對環境的複雜化，科技的日新月異，肩負著極具挑戰的稽核任務，亟需提昇稽核人員的專業素養及加強訓練，有鑒於此，個人謹提出以下建議：

一、增進業務知識：參與業務流程或引用業務上有實作經驗的人，例如 FRBNY 會將稽核人員暫調至業務部門學習。

二、充實新知：隨著金融商品不斷創新與複雜化，若未充分瞭解新金融商品的內涵，會缺乏稽核判斷能力，致使稽核虛有其表。

三、專業訓練：多方藉由查核技術訓練，及資深稽核人員的經驗傳授等，培養稽核人員執行稽核工作必須具備的重要職能。

四、招攬 IT 專業人才：面對高度資訊化的環境，文件電子化與業務應用系統不斷地擴增，稽核方式須同步做改變；又為因應隨時變化的 IT 風險，亟需增加具備 IT 專業的稽核人員，才能隨時注意新興風險，並更新稽核計畫，使 IT 稽核計畫具有彈性，不致僵化。

貳 稽核方式具彈性

按 IIA 的定義，內部稽核應採取「系統化和規範化的方法」，即應結合組織的具體情況，採取各種不同的方法。現今很多企業在學習如何

導入新的稽核技術，以協助組織有效率地應用在其稽核分析上的探討。

然而，並非每一個組織需要相同的內部稽核能力或成熟度，因為每個組織有不同的企業文化和組織結構，稽核方式應視其組織的特性與複雜化程度，以及組織所曝露的風險程度而定。所以在學習各樣稽核技術與模型後，必需要能夠彈性應用。

基於此，謹就傳統稽核與以風險為基礎的查核方式提出個人的建議：

一、對於某流程首次稽核時，採用傳統稽核方式：因為風險基礎稽核只查和風險相關的點，其他不相關之處，如人手安排是否合理，流程是否可以更有效率，在風險基礎稽核中可能不會考慮到；而傳統稽核方式，有助於對整個流程有詳細而深入的了解，較能增加查核的深度或密度。

二、對於複雜且無重大變動的流程，宜採用風險基礎稽核：因為對於例行性，低風險之業務，若用檢查表每年重複查核等傳統方式，可能容易因過度標準化，而造成稽核的機械化。反之，採用風險基礎查核，可依風險評估之高低，規劃稽核計畫，減少低附加價值的查核，使有限的稽核人力與時間，做最適當的方配。

參考文獻

國外資料：

1. COSO NEWS RELEASE.(2013)
2. Organization-about the New York FED. Available at: http://www.newyorkfed.org/aboutthefed/org_chart.html. Accessed August 2014.
3. Operational Documents-Operational Risk Management Policy. Black Sea Trade & Development Bank. Available at: http://www.bstdb.gr/about-us/key-documents/operational-documents/Porfolio_Risk_Management_and_Investments_policy.pdf. Accessed June 2014.
4. The Federal Reserve Bank of New York. The handouts of the Specialized Training Programs -The Operational Risk Management and Internal Audit course. (2014)
5. The Institute of Internal Auditors Research Foundation. (2009). Internal Audit Capability Model (IA-CM) for the Public Sector. Download PDF-Introduction.

國內資料：

1. 江美英(2007)。FRID 應用對企業內部控制影響之研究。國立政治大學資訊管理研究所碩士論文。資料引自 http://nccur.lib.nccu.edu.tw/
2. 李雲寧(2006)。作業風險管理(ORM)及安全管理體系(SMS)。開南大學空運管理研究所。資料引自 www.knu.edu.tw/air/doc/speech/

2006%20orm%20&%20sms%20(Capt.%20Lee).ppt

3. 許雅婷(2007)。營運持續管理標準化時代來臨。iThome。資料引自 http://www.ithome.com.tw/node/46305
4. 莊盛祺/ David Chuang(2014)。AACM 稽核分析能力成熟度模型-Audit Analytics Capability Model。資料引自 http://blog.uprofit-tw.com/?p=3616
5. 馮智偉(2013)。解決駭客任務！資安危機處理的八大關鍵。精誠資訊恆逸教育訓練中心電子報，第 553 期。資料引自 http://blogs.uuu.com.tw/ucomexpress/post/2013/12/09/第 553 期 gt
6. 楊素柳(2004)。Basel II 作業風險資本之計提對銀行業衝擊之探討。真理大學財經學術研討會。
7. 薛如倩、蔡亞珍(2014)。Heads Up - COSO 更新 2013 年的內部控制整合性架構。勤業眾信聯合會計師事務所企業風險服務部。勤業眾信通訊 2014 年 02 月號。資料引自 http://www.deloitte.com/view/tc_TW/tw/41932/46531/CCSA_CIA/2f11907acb504410VgnVCM1000003256f70aRCRD.htm
8. 張娜依(2010)。COSO 報告及對我國企業內部控制的啟示。企業研究論文。資料引自 http://big.hi138.com/gongshangguanli/qiyeyanjiu/201003/219505.asp
9. 失效模式分析研討(2008)。指導老師：張前偉，組員：廖建傑、吳政賢、林慧蘋、林宜倩、李俊明。國立臺北科技大學。
10. 行政院主計總處委託研究推動強化政府內部控制發展策略之研究(2012)。行政院主計總處。計畫主持人：鄭丁旺教授，共同主持人：許崇源教授，陳錦烽副教授，林宛瑩副教授，研究助理：潘俞自，鄭錦瑩。(P.64)。
11. 風險管理/危機管理。凱林國際教育股份有限公司。資料引自 http://caring.com.tw/02_tranning.html

12.健全政府內部控制(2011)。行政院內部控制推動及督導小組，工作分組。資料引自 http://funds.hs.ntnu.edu.tw/S_APSWEB/HTML/DOC/內控教材範例.pdf

13.電腦稽核(2010)。ISACA JOURNAL 摘譯文章，第 7 期，Vol 1 and Vol 3。資料引自 http://www.isaca.org/About-ISACA/History/Chinese-Traditional-/Documents/ISACA-Journal-Translation-No7-CT.pdf