行政院所屬各機關因公出國人員報告書

（出國類別：其他）

紐約聯邦準備銀行「風險管理與內部稽核」研討會出國報告

服務機關：中央銀行

姓名職稱：邱曉玲、陳佩瑜

派赴國家：美國、紐約

出國期間：113 年 5 月 26 日至 113 年 6 月 2 日

報告日期：113 年 8 月 14 日

摘要

內部稽核作為組織中的第三道防線，扮演著至關重要的角色。紐約聯邦儲備銀行（FRBNY）負責關鍵金融設施系統（如 FedWire 和 FedTrade）及其他重大業務（如公開市場操作）的運行，為確保該等關鍵業務不受干擾，FRBNY 遵循三道防線模型，設計一套全面、嚴謹的內部稽核流程以確保該行達成關鍵目標。為促進該行內部之間溝通及協調，FRBNY 稽核團隊導入一套聯絡模式（Liaison Model），期以透過稽核聯絡人角色，協助內部稽核工作順利進行，並提升稽核成效。

然而，即便擁有完善的內部稽核框架，內部稽核的成效仍依賴於具備專業的稽核人員，因此FRBNY 致力於培養優秀的內部稽核人才，以建立一支強大的稽核團隊。對此，FRBNY 除了提供的各項專業培訓，並鼓勵稽核人員持續學習專業新知與相關技能。FRBNY 稽核團隊表示，為應對創新科技與環境轉變所伴隨而來的風險與挑戰，下一代內部稽核必須具備一系列關鍵技能，包括中、高級數據分析能力、以全局視角評估風險的能力、創新思維與能力、靈活性與敏捷性、科技新知與 AI 應用技能等，才能更好地勝任工作。

目錄

壹、 前言

本次參加由美國紐約聯邦準備銀行（Federal Reserve Bank of New York，以下簡稱 FRBNY）於 113 年 5 月 28~31 日舉辦之「風險管理與內部稽核」（Risk management and internal audit）研討會，與會學員共 106 位，分別來自歐、亞、非及美洲等 57 個國家。

本次研討會議題包括 FRBNY 內部稽核流程、FRBNY 稽核範例介紹-Fed 公開市場操作帳戶（System Open Market Account，SOMA）與雲端運算專案計畫、營運韌性、人工智慧在風險管理的應用、強化網路安全的策略、新興詐騙風險的預防以及數位轉型經驗分享等。由 FRBNY 之稽核、風險及技術等團隊成員擔任講師，就前述各項議題進行簡報，並採用 FRBNY 設計的 APP 請學員當場作答，APP 當場同步統計與顯示結果，藉以了解學員想法與各國施行情況，再進一步對相關結果深入探討，亦安排小組討論進行經驗交流。

內部稽核在組織運作中扮演關鍵角色，作為第三道防線，其主要職責不僅在於保證業務正常運作，尚包括對內部控制措施或潛在風險提出建議與改進措施，以提升組織的運作效能。隨著新興科技的蓬勃發展並逐步導入組織，組織的運行模式與潛在風險亦隨之改變。尤其在人工智慧崛起與數據導向的時代，除了專業素養外，稽核人員更需要掌握數據分析以及應用人工智慧等關鍵技能，並靈活、敏捷地因應

外部環境所帶來風險與挑戰。

本報告分為七章，除此前言外；第貳章為內部稽核之三道防線模型；第參章為 FRBNY 內部稽核流程；第肆章與第伍章分別介紹 FRBNY 的兩個稽核範例- Fed 公開市場操作帳戶(SOMA)與雲端運算專案計畫；第陸章介紹下一代內部稽核；最後為結論與建議。

貳、 內部稽核之三道防線模型

一、背景

早期，許多組織採用內部稽核、品管人員、法規遵循主管和調查舞弊人員等專家來管理風險。雖然這些專家各具獨特觀點和特定技巧，對組織健全運作有其貢獻，但由於相關的風險和控制職責分散於多個部門，這可能導致重疊或缺口，並且缺乏一套系統化的方法來指派及協調風險管理職責。

為了解決這些問題，國際內部稽核協會（IIA）於 2013 年發布內部控制三道防線模型，包括：

- 第一道防線：業務單位的管理控制
- 第二道防線：由管理階層設置的風險控制和遵循督導職能
- 第三道防線：內部稽核提供的獨立確信

然而，面對快速變化的風險環境和組織日益複雜的背景，IIA 於 2020 年對 2013 年的模型進行了修訂。此次修訂融入了實務經驗和治理分析，並彙編了來自超過 2000 位個人或組織的專家意見，修訂模型主要改進以下三點議題：

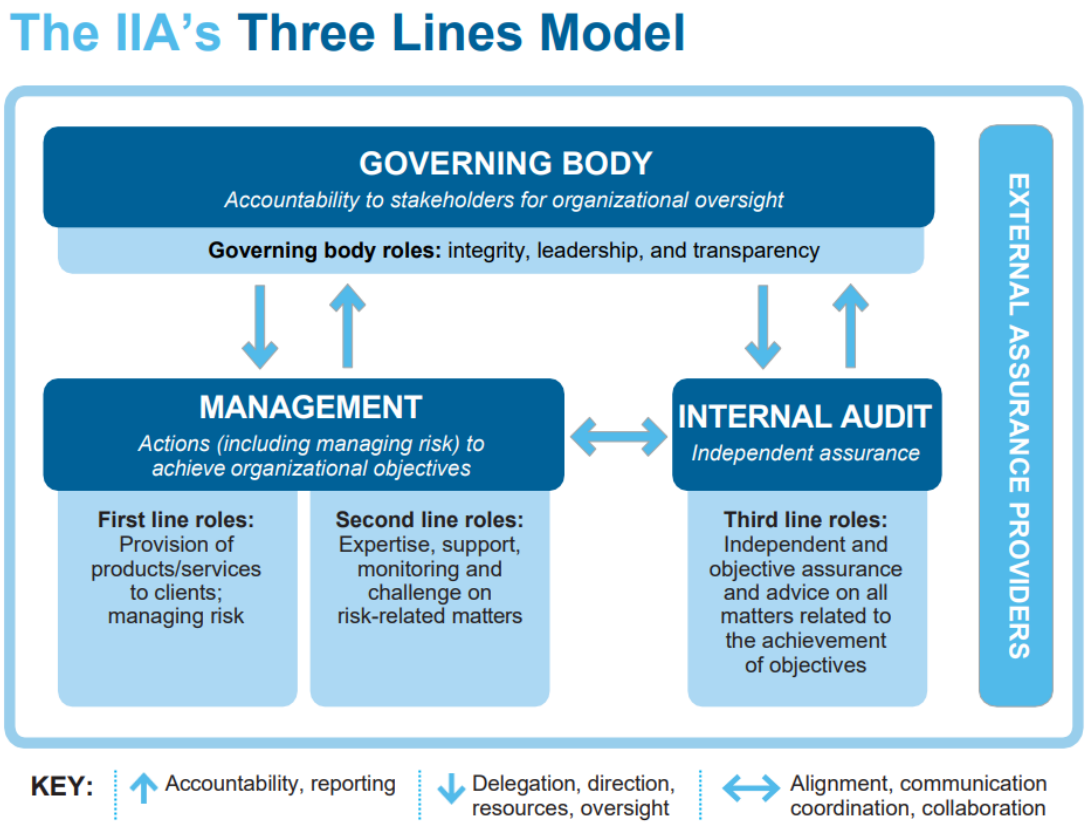
- 增強基本原則，強調風險管理框架的一致性
- 擴大模型範圍至創造和維護價值的整體視角
- 強調持續改進和動態調整的必要性

此修訂旨在使三道防線模型更具實用性和適應性，以應對當前複雜的風險管理挑戰。

二、內部稽核與三道防線模型

2020 年 IIA 發布之三道防線模型（圖 1），係基於六項關鍵原則，此模型明確界定治理單位、管理階層和內部稽核的角色和職責，亦可清楚了解內部稽核在第三道防線中之重要性和獨立性。茲說明六項關鍵原則如下：

圖 1、IIA 三道防線模型



資料來源:IIA

■ 原則一：治理

組織應建立適當的治理架構和作業流程:

✧ 治理單位的角色：以誠信、領導和透明的監督，並對利害關係人負責。

✧ 管理階層的角色：管理階層需透過風險導向的決策和資源運用，以達成組織目標之管理。

✧ 內部稽核的角色：獨立的內部稽核應透過嚴謹的調查和深入溝通，提供獨立的確信和建議，促進組織的持續改善。

■ 原則二：治理單位角色

✧ 治理架構的建立：治理單位需建立有效的治理架構和流程，確保組織目標與利害關係人利益一致。

✧ 授權：治理單位應授權並提供資源給管理階層，以達成組織目標，並符合法律、法規及道德期望。

✧ 監督內部稽核：必須建立及監督一個獨立、客觀且稱職的內部稽核功能，提升組織目標達成的信心。

■ 原則三：管理階層和第一及第二道防線角色

✧ 第一及第二道防線角色：第一道防線角色涉及直接提供商品或服務，第二道防線則專注於風險管理相關協助。由管理階層擔任第一道和第二道防線角色。

- ✧ 防線角色的運作：第一和第二道防線角色可以混合或獨立運作。第二道防線角色可能指派專家，提供第一道防線角色額外專業知識、支援和監控，也可能只專注於特定風險管理目標，如法律遵循、內部控制、資訊安全等。此外，第二道防線角色也可能擴展到企業風險管理(ERM)等更廣泛的範疇。

■ 原則四：第三道防線角色

- ✧ 內部稽核的獨立性與專業性：內部稽核應通過系統化、嚴格的流程和專業知識，提供關於治理和風險管理適當性及有效性的獨立且客觀的確信和建議。
- ✧ 報告責任：內部稽核應考量內外部確認服務，並直接向管理階層和治理單位報告查核發現，促進組織的持續改進。

■ 原則五：第三道防線的獨立性

- ✧ 獨立於管理職責：內部稽核必須保持獨立性，這對其客觀性、權威性和信譽至關重要。
- ✧ 維持獨立性的方法：內部稽核可通過直接向治理單位負責、不受限制地訪談所需人員、接觸資源和必要資訊，以及在規劃和執行查核時免於干擾和偏見來建立獨立性。

■ 原則六：創造和維護價值

✧ 合作與一致性：各角色應共同合作，確保所有活動與組織目標一致，以創造和維護價值。

✧ 資訊的可靠性和透明度：通過有效的溝通、合作和協調，確保風險導向決策所需資訊的可靠性、一致性和透明度。

這些原則有助於建立一個清晰的內部控制和風險管理架構，從而提升組織的治理效能和風險管理水平。

參、 FRBNY 內部稽核流程

一、 查核前置作業

FRBNY 內部稽核採用採取風險導向的方法，著重於風險之辨識、評估與管理，審慎評估各受查者風險以對其量身訂做查核活動及頻率，針對風險較高者投入較多查核資源，此與傳統查核對於不同風險項目採齊頭式之查核頻率及深度顯有不同。FRBNY 總稽核 Clive Blackwood 並強調，該行內部稽核首要職能在於協助受查單位事前防範風險的發生，而非事後發現受查單位的業務缺失。

在年度查核前，FRBNY 稽核團隊運用風險加權評分矩陣（Weighted Scoring Matrix）評估受查單位各項業務風險高低，作為制定查核計畫之參考。風險加權評分矩陣係由營運風險（Operational Risk）、財務風險（Financial Risk）及策略風險（Strategic Risk）三大面向，對各項業務進行風險評分，並依據評分結果決定稽核項目的優先次序與頻率。以下分別說明前述三類風險的定義及評估時考量因素：

(一)營運風險

營運風險係組織面臨不確定性因素可能影響正常營運之風險，此風險包含業務流程、科技及人力資源風險。常見的例如天災造成運作中斷、物料短缺或生產排程不當等因素產生作業停擺、網路資安風險、人員訓練不足等。評估此風險須同時考量流程的重要性、作業的複雜

度、法規的遵循等。

(二)財務風險

財務風險係組織受到國內外經濟、產業變化等因素，造成公司財務影響，例如利率或匯率波動及財務報導錯誤表達等。評估此風險須同時考量信用風險、流動性風險、市場風險等。

(三)策略風險

策略風險因經營策略失誤而產生損失之風險，例如客戶過度集中及企業併購。評估此風險須同時考量組織策略的重要性、治理架構等。

辨識上述風險後，將各風險因子給予不同計分權重，再乘以風險等級，最後計算總加權風險分數，風險分數高者（風險評等中等以上者）將列為優先稽核對象(如圖 2 所示)。

圖 2、風險加權評分矩陣

Risk Factor	Weight	Risk Level[1] (H=4, MH=3 M=2, L=1)	Score
Operational			
1. Business Processes	20	3	60
2. Technology & Info. Mgmt.	30	4	120
3. Human Resources	20	3	60
Financial/Materiality	20	4	80
Strategic	10	3	30
TOTAL	100		350
Risk Rating[1]		High	

Risk Rating	Score	Frequency of Audit Attention
High (4)	350-400	Up to two calendar years
Moderately High (3)	276-349	Up to three calendar years
Moderate (2)	200-275	Up to four calendar years
Low (1)	100-199	General Auditor Discretion

資料來源:課程講義

二、內部稽核程序

內部稽核程序主要分為查核規劃(Planning)、實地查核(Fielding)及報告(Reporting)三個階段，FRBNY 說明其各階段執行重點如下:

(一)查核規劃階段

稽核團隊首先研擬一份行動計畫(Plan of Action)，內容包括背景分析、風險評估摘要、查核目標和範圍和預算、查核預計時程表等。計畫擬定後由總稽核(General Auditor)發表一份查核聲明(Audit Announcement)，其內容包括規劃查核起迄日、查核團隊成員名單及召開啟動會議(Opening meeting)時間等。啟動會議係進入實地查核前重要項目，藉此會議向受查者介紹查核團隊、查核標的與方法、預計時程規劃情形、查核範圍與契約等。

(二)實地查核(Fielding)

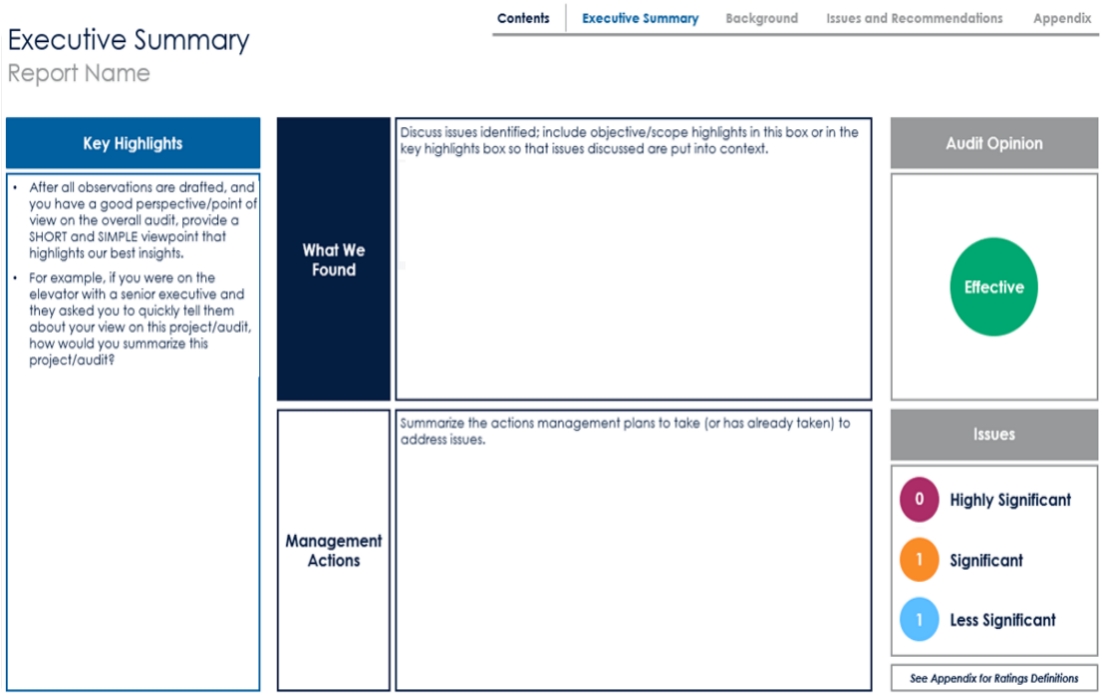
FRBNY 實地查核主要包含三個關鍵要素，穿透(Walkthrough)、測試(Testing)及結論。其中，穿透測試係指查核人員抽選一項特定業務，會同受查單位實際操作全部流程，藉以了解實際業務運作方式，並從中評估、測試其內部控制措施的有效性。此外，在稽核過程中，查核人員會出具內部稽核狀態報告(Internal Audit Status Report)來揭露查核最新狀態和時間表，此報告將列出逐項已完成查核項目或正在進行查核項目、出具報告目標時間等內容，讓稽核團隊每個人能夠隨

時掌握查核進度。

(三)出具稽核報告

FRBNY 要求稽核報告應力求簡單明瞭地傳達稽核結果及發現，於陳述過程應避免使用技術性名詞，以報告閱讀易於理解為最高原則。FRBNY 提供稽核報告模板（如圖 3 所示）分為五大部分，分別為標題頁、執行摘要、背景、問題與建議處理措施及附錄。其中，最重要為執行摘要，其內容包含關鍵焦點（Key Highlights）、查核發現（What We Found）及管理階層決策（Management Action）。在關鍵焦點部分，著重於提出一個簡短且簡單的觀點來總結全文，用以表達稽核團隊對於此次查核之整體意見。

圖 3、稽核報告模板



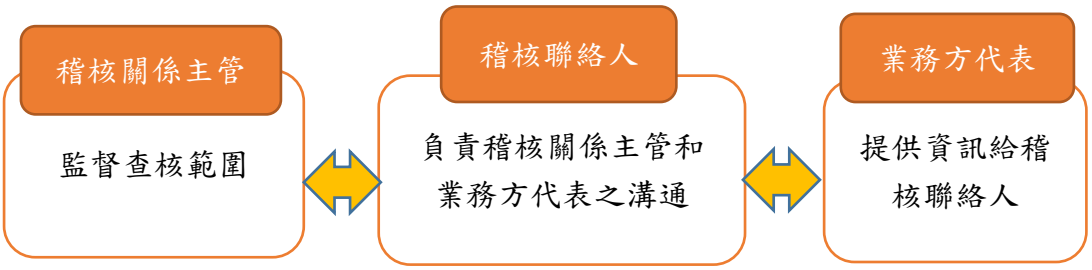
資料來源:課程講義

三、聯絡模式（Liaison Model）

(一)建立聯絡模式

內部稽核的成功與否，取決於稽核團隊與受查者良好溝通協調及合作關係。查核過程中，受查者往往對查核者易有防衛心態，不願詳盡說明，且雙方直接溝通可能面臨僵局。為了解決這些挑戰，建立一個緩衝、有效的聯絡機制是至關重要的。此機制可以由中間者居中協調，有效地傳遞訊息，從而使查核結果事半功倍。為此，FRBNY 內部稽核部門引入了一套聯絡模式，主要由稽核聯絡人（Audit Liaisons）、業務方代表（Business Area Representative）以及稽核關係主管（Audit Relationship Leader）構成（圖 4）。

圖 4、FRBNY 內部稽核聯絡模式



資料來源:課程講義

稽核聯絡人扮演了雙方溝通之關鍵角色，其職責如下:

1. 與業務方代表之溝通

透過業務方代表提供之訊息，稽核聯絡人先深入了解組織營運和相關風險，再依風險高低決定與各部門溝通頻率並出具聯絡會議紀錄

（Liaison Meeting Notes）。查核過程，與業務方代表持續建立有效關係並即時掌握組織有無重大風險變化。最後，將查核結果傳遞給相關部門，並提供建議或改善措施。

2. 與稽核關係主管之溝通

稽核聯絡人彙整各部門流程可能產生之風險及控制弱點，協助稽核團隊完成年度風險評估，以擬訂查核範圍、項目及加強重點。查核過程持續與稽核團隊討論，以提升查核效能。最後，對稽核團隊出具之查核報告提供建議並協助傳達給相關部門。

(二)聯絡模式之效益:

根據 FRBNY 經驗，持續使用該聯絡模式可能帶來以下效益：

1. 確保遵循內部稽核師協會（The Institute of Internal Auditors，IIA）第 1210 條規定
2. 增強稽核作為顧問的角色
3. 透過全面整合財務和資訊科技變化來增加價值
4. 減少重複且無效益之活動
5. 協助辨認新興風險
6. 提升稽核過程效率
7. 提供更為廣泛且有效率之確信範圍

四、大型專案計畫查核

大型專案計畫較複雜、具較高風險、辨識潛在問題難度較困難等特性，故須投入一段較長期間查核。雖大型專案計畫查核與一般查核程序大致相同，其主要目標係在查核期間能及時提供事前遠見，而非一般固定時點查核，通常只提供事後之建議。

(一)專案計畫查核要項

FRBNY 對大型專案計畫之查核聚焦在四大層面，分別說明如下:

1. 治理（Governance）方面：檢視人員組成、政策設立、資訊傳遞等治理框架，以驗證是否能達成該計畫既定目標。。
2. 管理（Management）：評估專案和專案管理活動之控制措施是否充分且適切。此外，大型專案會額外聚焦於專案之財務活動，包含預算編制、成本估計、財務預測及預決算比較等。
3. 解決方案（Solution）：從選擇供應商或開發者之過程，到評估產品的主要功能，以評估解決方案的品質和進展。
4. 執行（Implementation）：評估專案新服務之啟用，是否通過核准、遵循法律情形，以及專案後續監控。

(二)早期預訊訊號（Early Warning Signs）

依 FRBNY 過去實施大型專案計畫查核經驗，歸納出以下幾項早期預訊訊號可能導致最終專案失敗，包含:

1. 主要利益關係者（stakeholders）未參與大型專案計畫
2. 專案治理框架未符合規模(太複雜或太簡易)，無法提供有效支持
3. 未獲得高階管理者的支持
4. 資源未能充分投入專案計畫
5. 改變的控制程序是無效的
6. 專案團隊未具備適當技能和經驗
7. 估計專案計畫的執行時間及投入精力不切實際
8. 未能明確辨識該專案計畫與其他計畫或第三方（例如供應商）之關係

(三)關鍵成功因素

FRBNY 亦分享大型專案計畫是否成功的關鍵因素，包含:

1. 整個專案計畫執行過程，有主要利益關係者適當參與。
2. 高層主管支持專案計畫並協助提供策略。
3. 利害關係人了解專案計畫核心價值，並確保目標與企業策略一致。
4. 整個專案計畫執行過程，專案團隊具備適當職能並妥善運用資源。
5. 為了降低第三方相關風險，供應商須適當管理。
6. 有一套公認的程序，提供專案計畫執行時點及如何進行之指引，內容涵蓋治理和風險管理方法。

肆、 FRBNY 稽核範例- Fed 公開市場操作帳戶(SOMA)

一、Fed 公開市場操作帳戶(SOMA)概述

公開市場操作係央行於金融市場買賣證券，以調控準備貨幣與市場利率的操作機制。聯準會(the Federal Reserve System, Fed)的公開市場操作，係由聯邦公開市場操作委員會（FOMC）授權 FRBNY 負責操作。FRBNY 依據 FOMC 的貨幣政策目標，在市場上買賣證券以調節銀行體系準備金、聯邦基金利率及其他短期利率水準，該等證券存放於 Fed 公開市場帳戶（System Open Market Account，SOMA）。

二、SOMA 的投資組合內容

SOMA 投資組合可分為美元計價資產以及外幣計價資產兩大類，分別說明如下：

(一)美元計價資產

- 美國國庫券（Treasury Bills，T-Bills）；
- 美國中、長天期公債（Treasury Notes and Bonds，Notes/Bonds）；
- 美國浮動利率債券（US Treasury Floating Rate Notes，FRNs）；
- 美國抗通膨債券（US Treasury Inflation-Protected Securities，TIPS）；

- 聯邦機構債券（Federal Agency Securities），由 Fannie Mae, Freddie Mac and Federal Home Loan Bank 等 3 家聯邦機構發行；
- 機構房貸擔保證券（Agency Mortgage-Backed Securities，Agency MBS），由 Fannie Mae, Freddie Mac, and Ginnie Mae 等聯邦機構擔保發行。

(二)外幣計價資產

- 歐元計價資產，包括歐元定存、德國公債、法國公債與荷蘭公債；
- 日圓計價資產，包括日圓定存與日圓債券。

三、SOMA 的操作方式

SOMA 經聯邦公開市場操作委員會（FOMC）授權，由 FRBNY 的公開市場操作交易室（Open Market Desk）負責操作，操作方式說明如下。

(一)以美元計價資產執行國內公開市場操作(Domestic Open Market Operations)之交易，包括：

- 買、賣美國公債
- 買、賣機構房貸擔保證券
- 附買回、附賣回協議（repo and reverse repo agreement）

- 借券交易(Securities Lending)

(二)以美元計價資產執行國外公開市場操作(Foreign Open Market Operations) 之交易，包括：

- 外匯即期、遠期交易
- 歐元(存放在 BIS、德國央行及法國央行)與日圓定存(存放在日本央行)
- 買、賣歐元與日圓公債
- 第 3 方附賣回協議(Euro Tri-Party Reverse Repurchase)

四、稽核 SOMA 的流程與方法

查核 SOMA 的年度計畫係由 FRBNY 總稽核擔任總召集人，並指定資訊稽核與營運稽核共同查核。以下將分別說明查核 SOMA 的前置作業、擬訂計畫及實地查核等。

(一)查核 SOMA 的前置作業

首先，釐清 SOMA 查核範疇，包括 SOMA 各項操作(請參考 SOMA 操作方式)，以及公開市場操作交易室所使用的相關系統，例如交易平台。

隨後，查核人員藉由風險加權評分矩陣評估 SOMA 各項業務的風險高低，決定稽核項目的優先次序、頻率，並據此規劃、制定稽核計畫。

(二)擬訂 SOMA 的查核計畫

在擬訂 SOMA 的查核計畫階段，稽核團隊會邀請第一道防線與第二道防線的所有利害相關人共同參與，包括市場團隊資深主管以及負責 SOMA 內部控制人員、風險團隊的法規遵循小組、法律小組等，期以借重各方的專業，共同維持 SOMA 穩健運作。稽核團隊特別強調，內部稽核能否充分發揮第 3 道防線功能的關鍵是資料，因此查核人員需要取得充分資料以辨識 SOMA 業務的潛在風險。例如，前期資訊稽核報告、稽核聯絡人的工作紀錄、外部審查報告以及其他內部與外部涉及該項業務的相關文件或報告等(如表 1 所示)。

表 1、查核資料

資料類別	用途
前期資訊稽核報告	回顧前期稽核報告，瞭解過去查核的內容、範圍和結果，此有助於辨識哪些業務項目已經查核，哪些可能需要重新查核。 查核跟蹤之前報告中提及缺失或其他待改善的問題，進一步評估改進措施是否有效，以及是否有新的風險出現。
稽核聯絡人的工作紀錄	參考稽核聯絡人與各方利害關係人的討論內容或其他資訊，評估是否有任何議題需要進一步查核。
其他業務單位的稽核報告中涉及本項稽核的重要訊息	例如，Fedwire 資金移轉系統的稽核報告中提及 SOMA 操作的相關議題，評估是否列入日後查核的參考。
外部審查報告	例如，聯邦準備系統對 FRBNY 的查核報告，以及 FRBNY 的外部審計報告。
其他內部與外部相關文件、報告	例如，內部、外部其他機構對 SOMA 操作的相關報告、文件等。

資料來源：課程講義

(三)以整合式稽核方式實地查核 SOMA

整合式稽核（Integrated Audits）並非是一新興概念，由於現今風險管理範疇涵蓋組織內各類風險，而且各種風險之間的關聯性日益緊密且相互影響，因此整合不同類型稽核工作變得至關重要，並有助於提供更全面的評估，從而更準確且有效地識別潛在風險。透過不同專業領域的稽核人員共同合作，稽核人員不僅能夠共享專業知識和資源，同時避免對同一業務的重複查核，從而使整體稽核工作更有效率與深度，進一步增強對風險識別與管理的效果。

在實地查核 SOMA 時，稽核團隊便採用整合式稽核方式，由營運及資訊稽核共同執行穿透測試，由查核人員抽選一筆或數筆交易，偕同公開市場操作交易室的交易員完成該交易。經由穿透測試，稽核人員一方面可以實際觀察業務流程，從中更深入了解 SOMA 業務內容、運行方式與其控制點；另一方面，可以驗證控制措施是否適當，可以確保其在實際操作中能夠有效地識別與管理風險，藉此評估其內部控制措施是否有任何需要改進地方。例如，當交易員執行一筆外匯交易，營運稽核與資訊稽核同時查核以下控制措施：

■ 營運稽核

✧ 交易授權和驗證：確認交易是否經適當的授權，以及授權程序是否完整。

✧ 交易確認：交易完成後，是否經適當的確認程序，例如交易系統產生的確認紀錄。

✧ 交易記錄：確認交易記錄是否在規定時間內完整且準確地輸入記帳系統，包括交易日期、部位和交易對手等訊息。

✧ 法規遵循：交易是否符合相關的法規監管要求，以及內部規定。

■ 資訊稽核

✧ 系統的內部控制措施：如登入管理、加密、系統日誌監控等(如表 2 所示)。

表 2、SOMA 的資訊稽核項目與查核重點

資訊系統控制	稽核項目	查核重點
一般控制	1. 邏輯安全性(logical security)：系統的安全措施，包括用戶身份驗證、訪問權限與權限級別、加密、防火牆等。	查核系統的登入措施，如登入權限設定，確認是否有防止未經授權人員登入系統。
	2. 資訊變更管理(change management)：系統與應用軟體的更新、修改與汰換等管理。	查核有關更新與修改的記錄，並確保所有變更均經過核准與測試，不會對系統造成任何負面影響。
	3. 系統監控(logging and monitoring)：系統活動與相關紀錄的監控措施。	查核交易系統日誌記錄，確保所有重要的系統活動均有記錄，並能及時發現並應對異常行為。
應用控制	1. 自動編輯檢查(automated edit checks)：系統可以自動檢查輸入資料是否正確。	確認系統有自動檢查功能，能及時發現並糾正資料輸入錯誤。
	2. 數據傳輸測試(vendor interface monitoring)：測試系統之間的數據	測試系統的數據傳輸功能，確保數據在不同系統之間傳輸時不會出現遺失或發

資訊系統控制	稽核項目	查核重點
	傳輸是否準確與完整。	生錯誤。
	3. 數據品質管理(data quality management)：管理系統內儲存數據的品質。	檢查數據管理流程，確保數據品質，包括準確性與完整性。
	4. 自動對帳(automated reconciliations)：系統可以檢查相關數據是否一致。	檢查系統的自動對帳功能，確保帳戶數據沒有不一致的情況。
其他	1. 營運持續計畫：組織發生任何意外後，幫助其恢復正常營運的計畫。	查核前、中、後台的營運持續計劃，確保任何系統在發生故障後可以迅速恢復營運能力。
	2. 營運韌性：幫助組織靈活應對未來可能風險與挑戰的措施。	查核平時是否有模擬各種風險情境，研擬可能之應變準備及復原計劃，並且不斷由經驗中學習、改善，以強化因應外在衝擊之營運韌性。
	3. 終端用戶工具(end user tools)：用以檢查用戶端電腦的安全性與有效性的工具。	檢查用戶端電腦的安全設置，防止用戶端出現安全漏洞。
	4. 漏洞管理(vulnerability management)：用以識別、評估和修復系統和應用軟體中存在的安全漏洞。這些漏洞可能會被惡意攻擊者利用，從而導致系統遭受各種形式的威脅和攻擊。	查核是否有定期進行漏洞掃描，並及時修補已發現的漏洞，防止交易系統被攻擊。
	5. 數據保護與加密措施(encryption)：保護機密數據須經授權才能取得與使用。	檢查數據加密措施，確保機密數據在傳輸與儲存過程中是安全的。

資料來源：課程講義

之後，根據穿透測試的結果，對 SOMA 的業務流程、風險和控制措施進行綜合性分析，並根據評估結果，確認控制措施的有效性，或者提出改善建議。稽核團隊表示，以整合式稽核方式查核 SOMA 具備以下效益：

1. 稽核人員可以深入瞭解該業務流程運作，確保所有的控制點均能被充分辨識與查核。
2. 驗證不同角色與職能之間的職責劃分是否符合規定，並確保沒有不當權限分配。
3. 同時考量業務運作及 IT 設施的風險，可以提供全面的風險視圖。
4. 各類型的稽核人員共同查核，可降低對受查單位業務運作的干擾。

伍、 FRBNY 稽核範例-雲端運算專案計畫

一、 雲端運算介紹

雲端運算是指將資料、應用程式、平台或服務存放在虛擬網路空間中，替代實體硬體設備，而使用者只需透過網路連接遠端伺服器，即可獲得資料或服務(如圖 5 所示)。

圖 5、雲端運算運行概念

資料來源：課程講義

(一)雲端運算環境

雲端運算主要分為公有雲、私有雲以及結合前述 2 種的混合雲，使用者可依據原有的 IT 架構及基礎設施與業務需求，選擇適合的應用模式與服務(如表 3 所示)。

1. 公有雲

由第三方雲端服務供應商建構和營運的雲端平台，其主要優勢在

於成本效益高，而且能夠迅速擴展來應對工作負載的增長。在管理和維護方面，公有雲由雲端服務供應商負責相關設施的日常營運、安全性維護和災難恢復，因此使用者可以減輕在資訊設備的負擔。然而，公有雲也存在一些挑戰，如對雲端服務供應商的依賴性和網路安全性。

2. 私有雲

私有雲是專門為單一組織而建立和管理的，通常由該組織自行建構在自有數據中心，或第三方提供的 IT 設施。私有雲雖然提供最高安全性和隱私保護，但部署、維護成本較高，也缺乏公有雲的擴展性和靈活性。

3. 混合雲

混合雲兼具公有雲與私有雲的部分優勢。使用混合雲的組織可將作業分開處理，機密性較高的作業在私有雲運作、一般作業則透過公有雲進行。然而，公有雲與私有雲的整合不易，而且管理難度相對較高。

表 3、公有雲、私有雲及混合雲的優、缺點比較

類型	公有雲	私有雲	混合雲
優點	易取得雲端運算資源 初始成本低 容易部署	安全性高 雲端環境掌控度高	結合前兩者優勢 運算效率更高 擴張性佳
缺點	資訊安全性可能較低 雲端環境掌控度較低	維護成本高 資源無法快速擴張	管理難度高 整合難度高

資料來源：自行整理

(二)雲端運算服務模式

雲端運算分成三個主要服務模式，分別說明如下。

1. 基礎架構即服務（infrastructure as a service, IaaS）

使用者視其需求，向雲端供應商承租網路、伺服器或儲存空間等運算資源，而供應商須維持該等基礎架構之正常運行及安全性。例如，Amazon Web Services (AWS) 提供的 Elastic Compute Cloud (EC2)。

2. 平台即服務（platform as a service, PaaS）

由雲端供應商提供一平台環境，供使用者在該平台進行應用程式之開發、部署、維護與管理。例如，Google Cloud Platform 提供的 App Engine。

3. 軟體即服務（software as a service, SaaS）

使用者可藉網路連線方式使用雲端供應商授權之應用軟體，而無須安裝在使用設備；且雲端供應商負責該應用軟體之更新及維護等。例如，微軟的 Office 365。

(三)雲端運算優點

採用雲端運算有諸多優點，主要有調整彈性、成本效益、效能提升和靈活性，分別說明如下。

1. 調整彈性

雲端平台可以輕易地擴展以支援更多使用者或是大型工作負載

量，而無需擴增實體伺服器及網路設備。因此，組織可以快速調整資源，以因應各種變化的需求，而不會受到 IT 基礎設施的限制。

2. 成本效益

採用雲端運算可以降低 IT 營運成本。雲端服務供應商負責雲端設施的維護和更新，使組織可以減少在硬體設備和軟體升級的支出。

3. 效能提升

由於數據和應用程式可以在雲端資料中心中快速存取，藉此使用者可以享有更快的回應，因此雲端部署能夠提升應用程式的效能和使用者體驗。

4. 靈活性

雲端平台提供即時的資源調配能力，允許組織根據需求動態調整計算能力、存儲空間和網路頻寬，從而有效地支持創新科技的導入和實施。

二、 雲端遷移的策略

雲端遷移（Cloud Transformation）是指將內部部署的資料、應用程式和系統轉移到雲端平台的過程，主要有以下 4 種移轉策略：

(一)汰除或停用（Retire）

將過時的、不再使用的、或者功能重複的應用程式從現有的 IT 環境中移除或停用，毋須移轉至雲端環境。

(二)重新佈署（Rehost）

將現有的應用程式直接移至雲端環境上運行，無須修改應用程式。

(三)Re-platform（平台移轉）

此方法介於重新佈署和重新架構之間，僅對應用程式進行有限的修改，以便在雲端環境中更有效率地運行，但不會完全重新架構應用程式。

(四)重新架構（Rearchitect）

現有應用程式或服務架構進行重大修改或重新編寫，使其符合雲端環境運作的要求，並且進一步發揮雲端平台的功能。

三、採用雲端運算的主要風險

雲端運算雖有許多優點，但也伴隨著一些潛在風險。FRBNY 稽核團隊認為，採用雲端運算的風險，主要有以下 5 點：

(一)數據風險（Data Risks）

數據風險是指數據在存儲、處理和傳輸時產生風險，包括：

1. 數據洩露：因為雲端平台出現安全漏洞，導致儲存在雲端平台上數據被入侵、竊取；
2. 數據完整性（Data Integrity）：數據在傳輸、儲存或更新等過程中，未經授權被修改或刪除。

(二)操作風險

操作風險是指在雲端環境中營運、管理與維護時，可能遇到的風險，包括雲服務供應商的設備發生故障導致服務中斷；以及人為操作錯誤導致系統故障或數據丟失。

(三)雲端治理

雲端治理是指組織管理和保護在雲端環境中使用的資料、應用程式的一套管理實踐，包括安全性管理、符合法規、成本控制和風險管理等方面，確保組織在雲端中可以安全、有效率地運作。

(四)雲端服務供應商風險

雲端服務供應商風險是指過度依賴雲端服務供應商所帶來的風險，尤其是供應商鎖定（Vendor Lock-In）風險，亦即是對單一雲端服務供應商的過度依賴，導致組織面臨業務連續性風險。一旦該雲端服務供應商發生故障、遭受攻擊或變更其服務條款時，可能會對使用者產生重大的業務影響。其次，由於轉移成本過高，企業可能難以快速轉換到其他雲端服務供應商，進一步增加業務的脆弱性。因此，組織需要定期審查和評估現有的供應商契約和服務水平協議（SLA），才能確保及時發現、應對上述潛在風險。或是，亦可考慮採行多雲策略（Multi-Cloud Strategy）的應對措施，將部份工作配置在數個的雲端服務供應商，以減少對單一雲端服務供應商的依賴。

(五)雲端技術風險

在雲端環境中，使用特定的技術和工具可能帶來風險。其中包括多租戶架構，即多個客戶共享相同基礎設施和資源，可能導致數據安全風險；以及虛擬化技術的使用，這些技術本身可能存在漏洞，例如虛擬機管理程式的漏洞可能被利用來進行攻擊。

四、稽核雲端運算專案計畫

經評估與衡量後，FRBNY 內部高層與技術團隊均認為雲端運算較傳統伺服器作業具備更多優勢，而且有助於日後導入更多創新科技，因此決定採行雲端運算服務。由於採行雲端運算是一項跨部門的大型專案計畫，其成功與否直接影響到 FRBNY 多項關鍵業務的運作與管理，加上該專案計畫具有高度複雜性和風險，因此 FRBNY 稽核團隊認為對其稽核是必要的，以確保該項專案計畫中任何未被發現的潛在風險可以及時辨識和加以管理。

雲端運算專案計畫的稽核流程類似於一般查核流程，亦分為計畫擬定、實地查核及報告等階段。在前置作業時，FRBNY 稽核團隊與計畫領導人召開多次會議進行談論，以全面了解該專案計畫的運作模式、計畫時程及內容。隨後，對專案進行風險評估以鑑別其主要風險所在，按風險評估結果擇定稽核項目以及制定查核計畫。

在實地查核階段，FRBNY 稽核團隊採用專案計畫管理審查

（Program Management Review，PMR），查核雲端運算專案計畫。專案計畫管理審查（PMR）為一專案審查方式，用於評估和監控大型專案計劃的整體進展和成效，以確保相關管理和治理機制的有效運作。PMR 主要關注專案計畫治理(Program Governance)、專案計畫管理(Program Management)和專案計畫解決方案(Program Solutions) 等三大層面，其中審核項目與內容如表 4 所示，以確保整個專案計畫在過程中受到全面監督。

表 4、專案管理審查（PMR）介紹

審查項目	內容
專案計畫治理	1. 治理與監督框架：檢視專案計畫是否有效管理，以及是否可以支持專案計畫達成當初所設定之目標。 2. 角色與職責：確認專案計畫有明確定義所有利益相關者的角色與職責。 3. 利益相關者溝通：確認所有利益相關者之間溝通良好。
專案計畫管理	1. 風險管理：辨識、評估風險，以減少其對專案計畫的影響。 2. 問題管理：確認專案計畫的問題得到妥善處理。 3. 範疇管理：確保專案計畫的範疇明確。 4. 財務管理：確保專案計畫預算和財務績效受到控管。 5. 績效指標：追蹤專案計畫的關鍵績效指標，以衡量其成效。
專案計畫解決方案	1. 解決方案的品質：檢視解決方案是否符合專案計畫的需求。 2. 測試管理：檢視專案計畫解決方案是否經過嚴格的測試並具備可行性。 3. 解決方案採行管理：確認專案計畫解決方案順利部署與採行。 4. 變更管理：確認專案計畫以最小化方式進行變更，並且有效執行。

資料來源：課程講義

稽核團隊與雲端架構團隊（Cloud Architecture Team）以及其他參與該專案計畫者定期安排會議，檢視上述所有項目的審查結果，據此制定具體的改善或糾正措施。PMR 是一個循環學習和改進過程，經由每一次審查結果從中吸取教訓，持續提升專案計畫的成效和管理效率。此外，稽核團隊亦隨時掌握該專案計畫相關重要訊息，並向稽核委員會與該行高層報告。

五、採行雲端運算所伴隨其他新興風險

採用雲端運算雖然帶來眾多優勢，但也伴隨諸多新興風險，包括由第三方或第四方導致的風險、人力資源挑戰以及技術債務，分別說明如下。

(一)由第三方或第四方導致的新興風險

第三方風險指的是組織直接使用外部機構（第三方）的服務或產品時可能面臨的營運中斷風險。例如，若組織依賴某一雲端服務供應商，而該供應商發生系統故障或安全漏洞，將直接影響到組織正常運作。第四方風險則是指與第三方有業務往來的供應商（第四方）可能發生作業失誤或服務中斷，間接對組織的營運造成風險。

在上述情境中，FRBNY 認為，因第三方或第四方失誤造成的網路風險是目前最值得關注的新興風險。這些風險通常難以由終端使用者完全控制，且常常在突發事件中顯現，難以即時應對。例如，先前

微軟的資安供應商 CrowdStrike 發生軟體更新失誤，導致微軟提供雲端服務產品出現全球性的大規模故障，造成紐西蘭、澳洲、日本、印度等地區的微軟用戶電腦出現藍屏現象(Windows 系統遇到嚴重錯誤時顯示的藍色錯誤畫面)。因此，FRBNY 強調應對此類風險的重要性，包括加強供應商風險評估以及研擬可能之應變準備及復原計劃。

(二)人力資源的挑戰

由於雲端運算技術的快速發展，組織需要具備該項專業的技術人員來管理雲端運算服務。然而，人力市場上具備這些技能的專業人員供不應求，導致組織面臨人力資源的挑戰。對此，除了提供技術團隊員工相關的培訓課程之外，FRBNY 人力資源部門也制定有吸引力的人才招募、留用策略，降低專業人員不足的風險。

(三)技術債務（Technical Debt）

技術債務是指在開發應用軟體過程中，出於快速完成交付的考量而採用暫時性解決方案，惟該等暫時性方案可能在未來增加組織對系統維護成本與複雜性。因此，在開發系統時，組織應盡量安排足夠的時間和資源，才能確保相關系統架構的健全性和可擴展性。對此，定期審視和改進現有的技術解決方案，避免技術債務的積累，將有助於保持系統的穩健運作，並確保能夠應對未來的需求和挑戰。

陸、 下一代內部稽核

FRBNY 設計了一套嚴謹、完整的內部稽核業流程與聯絡模式，以確保組織的重要目標可以如期達成。然而，即使擁有良好的內部稽核框架，也需要優秀的稽核人員來執行，才能發揮最大的內部稽核效能。以下，將分別介紹下一代內部稽核需具備哪些關鍵技能、FRBNY 如何培養優秀的稽核人員以及提高稽核團隊凝聚力之策略。

一、 下一代內部稽核的關鍵技能

FRBNY 稽核團隊認為，在今日快速變化的商業環境中，內部稽核需要具備一系列技能才能成功適應與應對各種挑戰，包括專業的懷疑態度、良好的溝通技巧、深入了解業務運作的驅動力、批判性思維（critical thinking）、敏捷性與適應能力以及基礎數據分析能力(如圖 6 所示)。

圖 6、當前內部稽核的必備技能

資料來源：課程講義

然而，隨著科技的快速發展與外在環境的轉變，未來 10 年內部稽核必須進一步強化其技能組合(如圖 7 所示)，尤其是中、高級數據分析能力、以全局視角評估風險的能力、創新能力、靈活性與敏捷性及科技新知與 AI 應用技能，分別說明如下：

圖 7、下一代內部稽核的關鍵技能

資料來源：課程講義

(一)中、高級數據分析能力

在當前的金融環境中，如何即時蒐集所需資訊，以及善用數據分析獲取有價值之見解，已是稽核團隊的必修課題。考量數據分析已成為稽核人員必備的關鍵技能，因此 FRBNY 積極鼓勵稽核人員不斷精進此一技能，例如學習運用進階數據分析工具(例如 SQL、Python 及 Tableau)來辨識潛在風險與異常行為，以勝任日益複雜的稽核工作挑戰。

FRBNY 稽核團隊將稽核人員所需的數據分析技能分為三個等級(如表 5 所示)，每個等級都建立在前一級的基礎上，強調持續學習與

提升技能的重要性，並說明、解釋數據分析如何在內部稽核作業中加以應用。

表 5、數據分析等級

基礎	中級	高級
目標:理解數據的基本概念	目標:可以將數據轉化為有價值的洞見	目標：可以深入發掘數據的意涵
說明： 可以讀懂與解釋各種圖表與儀表板。 ✧ 了解數據的基本概念,如數據類型、收集與品質。 ✧ 了解數據分析的基本方法與流程，包括數據清理、整理與基本分析。 ✧ 了解數據視覺化對分析數據的重要性，並學習有效地建立與使用圖表。 ✧ 了解如何管理與治理數據，確保數據的準確性與完整性。	說明： 不僅能閱讀圖表與儀表板，更能進行數據分析。 ✧ 能夠靈活運用 MS Excel 或 MS Access 進行較複雜數據分析。 ✧ 掌握更多數據分析技能，如趨勢分析與迴歸分析。 ✧ 能夠創建圖表來展示分析結果。	說明： 可以進行高級數據分析及相關工具開發，成為內部稽核部門的數據專家。 ✧ 熟練使用 Power BI Desktop、Tableau、Deep Prep、Alteryx、SQL 與 R 語言等高級數據分析工具，進行數據探勘,發現隱含在數據中的模式或關聯。 ✧ 使用上述工具建立專業的視覺化圖表，幫助高層管理者快速理解與決策,提升稽核報告的價值。

資料來源：課程講義

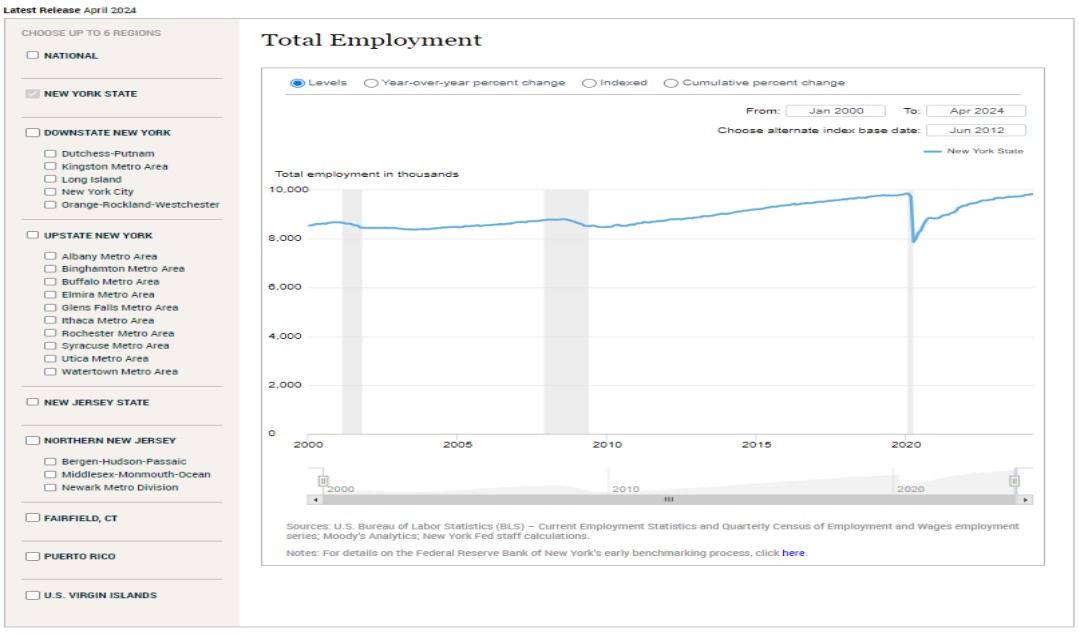
FRBNY 講師並表示，近幾年來 FRBNY 內部高度重視數據分析在各項業務的推行、應用，並設置數據分析辦公室（Data & Analytics Office，簡稱 DAO）、延攬業界優秀數據人才以及著手修改數據治理架構等。近來該行在其網站展示一系列資料視覺化成果，將量化的數據或質性的文字、圖片與聲音等轉為各類型分析圖表(如圖 8、9 所示)，

希望透過視覺化處理幫助外界對相關內容的理解。

圖 8、FRBNY 展示其網站上視覺化圖表

資料來源：FRBNY 網站

圖 9、FRBNY 展示其網站上視覺化圖表



資料來源：FRBNY 網站

(二)以全局視角評估風險的能力

以全局視角評估風險的能力是指，稽核人員能夠以全局的視角與思維來思考組織面臨的風險，不是僅專注於某項業務流程中細節，而是可以辨識影響組織長期發展的潛在風險，進而提出有價值的建議。例如，在查核某一業務時，稽核人員不僅要關注其內部控制流程是否符合相關法規和內部標準，還需考慮是否可以支持其他業務部門平穩運作，或是幫助組織達成關鍵目標。

(三)創新思維與能力

在稽核工作中，創新能力至關重要，包括在面對新興風險時，能夠運用創新思維，提出新穎的解決方案來應對。對此，FRBNY 稽核團隊中持續推動創新文化，鼓勵其他成員提出創新想法與稽核方法、保持對創新科技與新知識的學習熱情，以提升各方面的專業能力。

(四)靈活性與敏捷性

靈活性與敏捷性是指，稽核人員能迅速適應新業務需求或是工作環境的變化。例如，在新冠疫情期間，稽核人員需要快速適應遠程辦公的模式，靈活調整稽核計劃與工具，確保稽核工作順利進行；再者，稽核人員能夠運用敏捷式稽核方法(agile auditing)，例如迭代進程管理，以適應業務環境的快速變化與不確定性，確保稽核工作始終維持高效率與高品質。

(五)科技新知

FRBNY 稽核團隊強調，未來 10 年稽核人員的關鍵挑戰之一，即是創新科技導致組織面臨的營運風險型態不斷演變。因此，稽核人員須積極充實資訊科技新知，才能辨識其對組織所帶來之新興風險。FRBNY 稽核團隊進一步分享，為因應科技發展浪潮，FRBNY 於 2020 年啟動一項科技前瞻(TechForward)大型專案，進行組織數位轉型，以便更好地導入創新科技，例如雲端運算及人工智慧(AI)。隨著更多創新科技逐步導入，一方面提升該行的營運效率，另一方面也帶來許多新興風險與挑戰，例如第三方風險及新興詐欺風險，所以稽核人員必須具備相關科技新知，才能更好地評估創新科技導入對業務運作的潛在風險。

(六)AI 應用技能

稽核人員需要持續學習將科技新知應用於查核工作，尤其是 AI 應用技能，幫助提升查核的效率、準確性與全面性。根據本次研討會的線上調查，與會央行學員尚未開始使用 AI 技術協助查核工作，但多數均認同應用 AI 技術協助查核是未來趨勢。

二、培養優秀的稽核人員

為培養優秀的稽核人員，打造一支高素質、專業化的稽核團隊，FRBNY 除了提供多項內、外部培訓課程之外，同時也鼓勵稽核人員

取得專業證照，以增進自身專業知識與技能。以下說明 FRBNY 培訓稽核人員的方式，以及建議稽核人員取得那些專業證照。

(一)提供內、外部培訓課程

1. 知識論壇與專業訓練講習

FRBNY 內部定期舉辦知識論壇與專業訓練講習，以促進稽核人員知識分享與專業能力提升。例如，以舉辦知識論壇方式，邀請內、外部專家分享最新的稽核理論、實踐與新知，例如機器學習在內部稽核中的應用；或是舉辦各項專業訓練講習，如數據分析應用。透過這些方式，提升整體團隊的專業水準。

2. FRBNY 各項業務介紹課程

安排 FRBNY 各項業務介紹課程，幫助稽核人員認識、了解 FRBNY 的實務運作。再者，FRBNY 經常舉辦大型國際研討會，內容大都是與央行核心業務相關主題，並邀請各國央行人員共同參與、交流。FRBNY 稽核人員可以經內部安排參加，從中了解核心業務內容與運作流程。例如，稽核人員透過參加支付清算研討會，可以幫助理解支付清算流程及相關基礎設施以及最新議題，該等背景知識有助於在稽核過程中可以更準確地辨識、評估潛在的風險，或是提出建設性的改進建議，幫助組織改進其內部控制與流程。

3. 外部培訓課程

FRBNY 每年提供補助，供稽核人員參加外部機構所舉辦稽核相關課程，學習最新的稽核查核方法、法規與專業新知等，來提升稽核人員的實戰能力與專業能力，使稽核團隊能夠有效地應對挑戰，並維持高品質的稽核成果。

(二)稽核人員的專業證照

FRBNY 鼓勵稽核人員取得稽核類專業證照(如表 6 所示)，希望稽核人員藉由參加證照考試過程，持續精進專業知識與技能，並在不斷變化與挑戰的稽核領域中脫穎而出。此外，隨著新興科技的發展，FRBNY 亦鼓勵稽核人員取得資訊類專業證照(如表 7 所示)，以便更好地評估新興科技對組織運作的影響與伴隨而來的新興風險。

表 6、稽核類專業證照

證照名稱	介紹	取得資格	取得難度
國際內部稽核師 (Certified Internal Auditor, CIA)	由美國內部稽核師協會（The Institute of Internal Auditors, IIA）頒發，是全球公認的內部稽核領域核心認證。	具備學士學位或同等學歷，並擁有至少兩年的內部稽核工作經驗；或是具備碩士學位，並擁有至少一年的內部稽核工作經驗。	中等至高，考試範圍廣泛且需要深入理解內部稽核的原則與實踐。
舞弊稽核師 (Certified Fraud Examiner, CFE)	由美國舞弊查核師協會（Association of Certified Fraud Examiners, ACFE）頒發，專注於欺詐預防、偵查與調查等領域。	需要具備學士學位或同等學歷，並有至少兩年的欺詐檢查相關工作經驗。	中等，考試內容涉及多個領域，包括財務與法律。
國際電腦稽核師 (Certified Information Systems Auditor, CISA)	由國際電腦稽核協會(ISACA)頒發，為電腦稽核、控管、確認與安全等專業領域中全球公認的資格標準。	需要具備至少五年的資訊系統稽核、控制或安全相關工作經驗，或符合部分豁免條件的工作經驗。	中高，考試涉及資訊系統理論與實務經驗
美國註冊會計師 (Certified Public Accountant, CPA)	由美國各州自訂各州的會計師考試資格以及核發執照。CPA 主要針對財務與會計工作，但對內部稽核工作同樣重要。持有 CPA 認證表明持證人具備財務報表審計、稅務、財務管理與法規等專業。	需要具備學士學位或同等學歷，並達到一定會計課程學分要求。	中高，考試內容廣泛，需要深入理解與應用財務與會計知識。

資料來源：課程講義、上述認證機構網址

表 7、資訊類專業證照

證照名稱	介紹	取得資格	取得難度
AWS 認證 (AWS Certified Solutions Architect)	由 Amazon Web Services 頒發，專注於 AWS 雲端的技能。	需要具備雲端計算的基本知識與至少一年的 AWS 使用經驗。	中等，考試內容為 AWS 雲端的專業知識。
Alteryx 認證 (Alteryx Designer Core Certification)	由數據分析公司 Alteryx 頒發，專注於使用 Alteryx 平台進行不同程度數據分析的專業技能。	需要具備基本的數據分析知識與使用 Alteryx Designer 的經驗。	中等，著重實際操作技能與 Alteryx 熟悉度
資訊系統安全專業人員(Certified Information Systems Security Professional, CISSP)	由國際資訊系統安全認證聯盟（(ISC)²）頒發，是資訊安全領域公認的專業認證。持有 CISSP 認證意味著持證人具備設計、實行與管理資訊安全計劃的能力。	需要具備至少五年的資訊安全相關工作經驗，或者具有四年的工作經驗並擁有資訊安全或相關領域的學士學位。	高，考試內容涉及多個資訊安全領域。
SAFR 認證 Security Assurance for the Federal Reserve (SAFR) Certification	FRBNY 為員工設計的專業認證，專注於金融相關系統的資訊安全實踐。	申請者需參加 FRBNY 內部培訓，並通過網路安全管理、風險評估、控制措施以及安全事件處理等考核。	中等

資料來源：課程講義、上述認證機構網址

三、促進稽核團隊合作與凝聚力

稽核團隊合作對於提升稽核工作效率與品質至關重要。在新冠疫情期間，FRBNY 稽核團隊中約三分之一的成員是新加入，加上遠距辦公，導致部分稽核人員未曾進過 FRBNY 辦公室，或是與其他團隊成員有共事經驗。在疫情結束後，FRBNY 則採取混合辦公模式，員

工每星期中有 2 至 3 天可以選擇遠距辦公，因此成員之間彼此見面機會甚少。為促進團隊成員對彼此的了解，培養信任感，促進整個團隊的合作與凝聚力，FRBNY 採取以下方式：

(一)促進團隊成員之間的聯繫

1. 增加員工見面、互動機會

由於混合辦公模式使成員間見面、互動機會變少，因此稽核團隊定期安排一些實體聚會，例如稽核人員早餐會，讓成員在共進早餐之時，可以面對面交流、互動，以提高成員的團隊參與感與歸屬感。

2. 安排社交聚會與團隊活動

稽核團隊不定期舉辦社交聚會與團隊活動，使成員在輕鬆愉快的氛圍中加強彼此的聯繫，從而提升團隊的凝聚力與工作滿意度。

活動範例 1：

在疫情期間，稽核團隊設計類似爐邊談話的線上交流平台，讓成員自由參加。參加者可以輕鬆分享成長經歷或其他有趣話題，藉此增進團隊成員之間了解，並讓新進與資深成員之間建立更緊密的聯繫。

活動範例 2：

由稽核團隊設計一個尋寶活動，由實體與遠距辦公的成員共同合作進行，地點包括 FRBNY 辦公室與曼哈頓市區景點。這種遊戲形式的團體活動不僅有助於團隊合作，也讓新進成員能夠快速融入團隊，

並對 FRBNY 內部及周遭環境有更好的了解。

活動範例 3：

由稽核團隊邀請成員共同參與社區服務與志工活動，例如清理公園與籌款活動，藉此不僅能夠回饋社會，還能使成員在工作之外建立更深的友誼，有助於提升團隊凝聚力與士氣。

(二)調查工作意願與安排輪調

為提高稽核人員的工作滿意度，稽核團隊盡力使每位成員的興趣與專長能夠與其工作相匹配。對此，FRBNY 稽核團隊採取以下措施：

1. 年度工作意願調查

在每個新的年度開始之前，稽核團隊進行一次工作意願調查，以了解每位稽核人員的職業規劃、專長與興趣，並納入日後工作分配考量之中。

2. 安排工作輪調

稽核團隊主管根據年度工作意願調查，適時安排工作輪調，以增進每位稽核人員志趣與工作經驗。

3. 適時調整工作分配

稽核團隊定期舉行內部會議，除了討論業務外，也同時了解每位稽核人員的工作情況，並根據需要調整工作分配，確保每位稽核人員在合理工作量下發揮最佳表現。

綜上所述，面對快速變遷的環境與科技進步所帶來的挑戰，FRBNY 稽核團隊透過持續提升稽核人員的專業知識與技能，以及促進團隊合作與凝聚力，不僅提升了稽核效能以應對未來的不確定性，同時為該行的長期發展提供堅實的支持，確保其關鍵目標的達成。

柒、 結論與心得

本次研討會，FRBNY 總稽核 Clive Blackwood 多次強調，該行內部稽核首要職能在於協助受查單位事前防範風險的發生，而非事後發現受查單位的業務缺失。稽核團隊與風險團隊之間定期交流，經常討論可能存在的潛在風險；而業務單位對內部控制有任何疑慮，亦可以尋求稽核團隊的意見、幫助。因此，不同於過去內部警察角色，該行稽核人員更多是扮演為組織增加價值的顧問角色，並與第一道防線、第二道防線維持良好合作關係，共同維持組織的健全運作。再者，隨著新興科技快速發展，FRBNY 已逐步導入新興科技優化各項業務。因此，稽核團隊鼓勵成員充實科技新知、增強數據分析等關鍵技能，期以增強內部稽核職能，並更好地應對創新科技與環境轉變所伴隨而來的風險與挑戰。

期望通過此次研討會的學習經驗，能為本行提供有價值的參考，並提出建議如下：

一、 鼓勵稽核人員充實科技新知，以應對新興科技的挑戰

隨著更多創新科技開發並逐步導入組織，稽核人員需充實資訊科技知識，掌握新型查核方法，才能有效辨識及應對該等創新科技的風險。本次研討會中，香港金融局代表透露，該行正致力於開發一套生成式人工智慧系統供內部使用。如何有效稽核該 AI 系統的運用，並

辨識與之相關的潛在風險，已成為該行稽核人員當前面臨的主要挑戰。

因此，建議稽核人員在平日廣泛增進資訊科技新知，既可以提升查核技能和敏銳度，增強內部稽核工作的成效，也可以更好地因應創新科技所帶來的挑戰。

二、 鼓勵稽核人員精進數據分析技能，以提升工作效率

FRBNY 稽核人員分享其團隊在近幾年的主要變化之一，即是使用更多數據分析執行稽核工作，以便更有效地識別潛在風險與異常行為。許多央行學員紛紛表示，其內部不僅積極運用數據分析提升稽核效能，更進一步鼓勵稽核人員學習高階數據分析工具，如 Python 與 Tableau。因此，建議稽核人員充實數據分析能力，以提升查核效率與洞察力；另一方面，建議行方日後或可參考英文培訓班的方式，辦理數據分析培訓課程，供有興趣學習的同仁參加。

三、 鼓勵參與國際研討會，增進稽核知能

本次研討會中，馬來西亞央行稽核主管 Marina Abdul Kahar 表示，該行稽核團隊除積極參與國際研討會之外，亦經常參訪美國、英國、澳洲、新加坡、泰國及印尼等國央行，針對特定議題進行交流，藉此優化其內部稽核制度、方法及使用工具等。其他央行學員，如義大利、智利與英國等，亦經常參加國際研討會，藉此與其他央行建立良好情誼，相互交流。因此，為持續增進稽核知能，建議鼓勵同仁參與稽核

相關國際研討會及交流活動，藉此增加本行內部稽核之深度與廣度，提升稽核品質及效益。

為持續增進稽核知能，建議鼓勵同仁參與國際稽核相關研討會及交流活動，藉此增加本行內部稽核之深度與廣度，提升稽核品質及效益。

參考資料

1. 王良允（民 111），參加「美國紐約聯邦準備銀行風險管理與內部稽核」線上課程視訊報告。
2. 鄭碩易（民 112），參加「美國紐約聯邦準備銀行風險管理與內部稽核」出國報告。
3. Chan, Amy, Craig, Lauren, Hoagland, Patrick, and Cheng, Emily (2024), "Auditing Cloud Migrations," Central Banker Programs, Federal Reserve Bank of New York.
4. Mason, Ryan, Tracey, Robert, Thomas, Kimdolyn, Murtha, James (2024), "Auditing Mission Critical Services," Central Banker Programs, Federal Reserve Bank of New York.
5. Lewis-Hyles, Janis, Diji, Bunmi, Garcia, Kaili, Lange, Cary (2024), "Internal Audit at the New York Fed: Key Processes and Components," Central Banker Programs, Federal Reserve Bank of New York.
6. Khan, Saniya, Sullivan, Alexandra, and Star, Lauren (2024), "The Next-Generation Internal Auditor," Central Banker Programs, Federal Reserve Bank of New York.
7. Pieger, Robert (2024), "Cybersecurity Risk Management Strategies," Central Banker Programs, Federal Reserve Bank of New York.
8. Yacono, Anita (2024), "Digital Transformation Journey," Central Banker Programs, Federal Reserve Bank of New York.
9. The IIA's Three Lines Model：An update of the Three Line of Defense.