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：鄭碩易/辦事員

派赴國家：美國、紐約

出國期間：112 年 5 月 20 日至 112 年 5 月 27 日

報告日期：112 年 7 月 17 日

摘要

一、美國聯邦準備體系分為聯邦準備系統理事會、聯邦準備銀行及聯邦公開市場委員會三部分，主要目的係執行貨幣政策、監督金融體系及維護金融穩定，確保國家貨幣供應穩定與金融體系之正常運作。

二、紐約聯邦準備銀行稽核小組之主要任務係執行內部稽核，並於稽核結束後向受查單位提出建議改進事項，以合理保證受查單位可辨識潛在風險並加以改進。

三、新興風險可能對傳統之管理方法造成影響，機關內部若未能即時對該類風險做因應，調整自身之營運策略，可能產生巨大損失。

四、資料治理將持續發展和演進，以因應數據快速增長及日益複雜之技術環境，然而隨著對數據價值之重視，好的資料治理將成為機關成功之關鍵要素。

目錄

壹、前言

內部稽核於機關中扮演至關重要之角色，身為機關中的第三道防線，不僅要就受查單位之業務運作透明化與合規性提出合理保證，也要針對缺失提出建議改進事項，藉由改善缺失以提高機關營運之效率及效能。然而，科技日新月異，隨著各種新興科技導入，機關的管理模式與潛在風險也隨之改變，內部稽核人員面對這些新興科技影響所帶來的新議題，也必須有一定程度的瞭解，以強化對機關提供諮詢及確信服務角色之價值。

在當今不確定且快速變化之商業環境，風險管理已是機關中不可或缺的一部分，好的風險管理不但能幫助機關應對各種挑戰及風險，亦能為機關提供更穩健且持續之發展。另外，在大數據時代下，探索與存取數據（Data）[1]之管道比以前更加多元及便利，但也伴隨著數據品質參差不齊、數據來源是否可靠及資料安全性等問題，因此各產業開始關注並發展資料治理，期望能透過資料治理提升數據品質及可靠性，同時對數據傳輸或共享過程中能提供適當保護，以防止數據洩漏或損壞。

本次研討會，主要介紹美國聯邦準備體系、紐約聯邦準備銀行（Federal Reserve Bank of New York，以下簡稱 FRBNY）之內部稽

[1] Data 係指「數據」或「資料」，兩名詞因翻譯習慣用法，於本報告中交替使用。

核流程、新興風險之因應及資料治理之未來趨勢等議題，俾供未來業務上參考。該研討會為 FRBNY 於 2020 年 COVID-19 疫情爆發後，首次舉辦實體課程，課程日期 5 月 22 號至 25 號為期四天，除本行外，有來自日本、韓國、加拿大、澳洲、瑞士等 33 國，共 44 名學員參與；講師則是由 FRBNY 總稽核-Clive Blackwood 先生所率領之稽核團隊擔任，並就前述各類議題進行簡報，同時針對學員所提出問題，進行說明及經驗分享，整體內容相當充實豐富。

本報告分為六章，除此前言外；第貳章為美國聯邦準備體系概述；第參章介紹紐約聯邦準備銀行之內部稽核；第肆章為新興風險之因應；第伍章說明資料治理之未來趨勢；第陸章為結論與建議。

貳、美國聯邦準備體系概述

1913 年美國通過聯邦準備法（Federal Reserve Act）後，建立聯邦準備體系（Federal Reserve System，以下簡稱 Fed），該體系為美國中央銀行系統，其目的係執行貨幣政策、監督金融體系及維護金融穩定，確保國家貨幣供應穩定和金融體系可正常運作。Fed 由以下三部分所組成：

一、 聯邦準備系統理事會（Federal Reserve Board）

由 7 名理事組成，其成員需透過美國總統提名並經參議院同意後任命，任期為 14 年。理事會負責制定貨幣政策，並監督其他聯邦準備銀行之運作。

二、 聯邦準備銀行（Federal Reserve Banks）

Fed 體系共計分為 12 個區域，每個區域都設有 1 家聯邦準備銀行（分布詳圖 1），全美 12 家聯邦準備銀行負責執行理事會所制定之貨幣政策及提供金融服務予其他商業銀行或金融機構，暨負責收集區域經濟數據及提供貨幣政策制定之意見。12 家聯邦準備銀行中以 FRBNY 規模最大，員工人數約 3,000 餘人，主要承擔公開市場操作及調節美元外匯市場等重大任務，且該行擁有全世界規模最大的地下金庫，提供各國央行及國際組織寄存及保管黃金之服務。

圖 1 美國聯邦準備銀行及其管轄區
資料來源：研討會講義

三、 聯邦公開市場委員會（Federal Open Market Committee，簡稱 FOMC）

該委員會由聯邦理事會主席及聯邦準備銀行總裁組成，主要職責為控制及監督美國貨幣供給量和利率，並透過調整聯邦基金利率和其他貨幣政策工具來影響經濟活動及金融市場，以實現物價穩定、降低失業率以及提高經濟成長率等目標。FOMC 通常每 6 周會舉行 1 次會議，基於經濟數據、就業情況及通膨預期等因素，討論並決定是否調整聯邦準備利率及是否需要修正其他貨幣政策。

Fed 透過前述三大機構互相合作，以確保美國本土金融穩定外，其在全球金融體系中也扮演重要角色，Fed 制定之貨幣政策及行動會對全球金融市場及經濟產生重要影響，故許多國家央行會與 Fed 保持緊密聯繫，以確保全球金融體系穩定。

參、紐約聯邦準備銀行之內部稽核

FRBNY 稽核小組之主要任務係執行內部稽核，審查銀行業務運作、會計及資金管理、法令遵循和風險管理，並於稽核結束後向受查單位提出建議改進事項，以合理保證 FRBNY 可辨識潛在風險並加以改進。

FRBNY 行內各業務單位須先向總裁、副總裁進行業務報告，再彙報董事會；稽核小組則是直接向董事會任命組成之稽核及風險委員會（Audit and Risk Committee）做報告，該委員會由被推薦之董事組成，主要係協助董事會評估稽核人員之獨立性、財務報表揭露之正確性及風險管理框架之有效性等事項。

有關 FRBNY 稽核小組功能及任務之執行簡述如下：

一、稽核小組於機關中扮演之角色

機關內部為了確保能平均分配風險管理及內部控制之責任，進而使風險能夠有效被辨識、評估及業務運作得符合相關法規和內部標準，普遍採用三線防禦（Three lines of defense）模型來協助機關提高整體風險管理能力及內部控制效能，目前三線防禦模型將機關劃分成營運單位管理、風險管理及內部稽核等三道防線，詳細劃分如圖 2 所示。

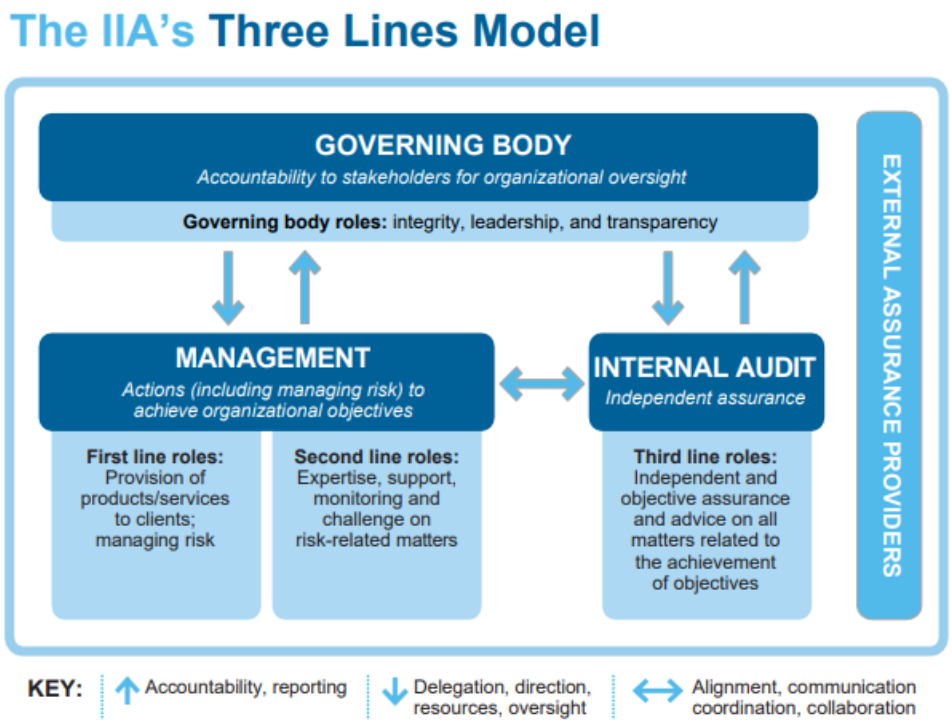


圖 2　內部控制三線防禦模型

資料來源：The IIA's Three Lines Model：An update of the Three Line of Defense

內部稽核係機關中第三道防線，主要係確認 FRBNY 第一道及第二道防線可確切辨識及管理風險，並提供機關客觀且獨立之諮詢及確信服務[2]，而根據北美內部稽核師協會（The Institute of Internal Auditors North America）公布之指引，機關內部第三道防線須具備下列特質，以確保內部稽核效能可充分發揮作用：

（一）向高階管理階層與董事會提供第一道及第二道防線工作之確信認證。

（二）內部稽核部門主管不承擔內部稽核以外之營運責任，以保護其

[2] 確信服務（Assurance services）是由具有相關專業知識和經驗的專業人士提供的一種服務，旨在評估、檢查和評價特定信息或情況的可靠性、合規性和有效性，該服務有助於提供相關利益相關方對機關或業務的信心，並為決策提供有價值的信息和建議。

客觀性及機關獨立性。

（三）有單獨向董事會報告稽核結果之管道，且第三道防線主要功能是提供確信服務而非業務管理，這是他與第一道及第二道防線最大的不同。

（四）按照公認的國際內部稽核準則來執行稽核工作。

二、 查核前置作業

FRBNY 稽核小組於進行實地查核前，會先釐清查核對象及範圍，接著針對查核標的進行風險評估程序，目前 FRBNY 使用加權評分矩陣（Weighted Scoring Matrix，圖 3）來評估受查單位所屬各項業務風險高低，該矩陣將整體風險分為營運、財務及策略等三大計分權重， FRBNY 對前述三類風險定義如下所述：

（一）營運風險

係指機關在日常業務運作中所面臨各種不確定性及潛在損失之風險，像是人力配置不當、網路病毒攻擊、業務因颱風、地震等天災被迫中斷，都是機關中常見之營運風險，另 FRBNY 將營運風險進一步細分成業務流程、科技及人力資源等三類風險。

（二）財務風險

係指機關在財務營運過程中面臨可能導致損失之風險，例如：利率波動、債務人信用破產等不利因素，除了外在環境變化外，機關

內部之財務報表不實表達，也有可能是產生財務風險的因素之一。

（三）策略風險

係指機關在制定和實施策略目標時所面臨之不確定性，可能導致設定目標無法實現或產生重大影響之風險，這些風險通常涉及機關內外部環境變化，可能對機關競爭優勢及長期發展產生重大影響。

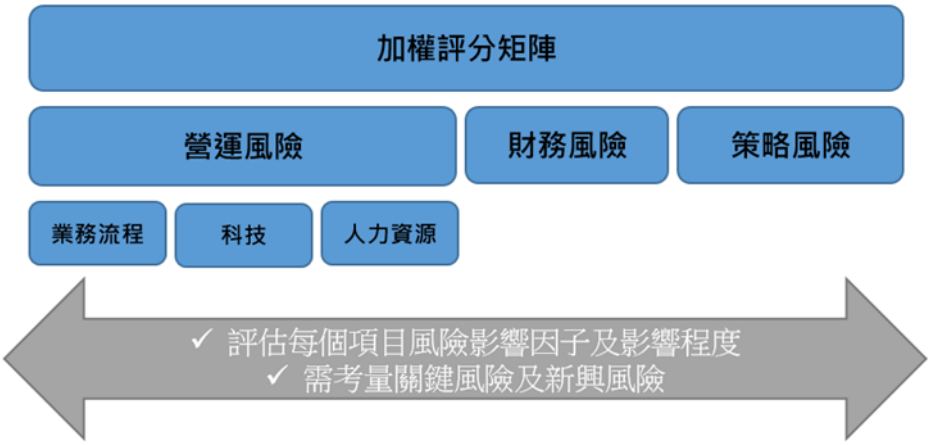


圖 3 FRBNY 風險評估加權評分矩陣
資料來源：研討會講義

在完成風險鑑別與分析後，稽核小組依照加權評分矩陣之風險分類及權重對各項查核標的進行風險評估，評估分數大小與風險高低為正向關係，接著按照評分結果來決定稽核優先次序及稽核頻率，以作為訂定年度稽核計畫之參考。

三、 查核流程

FRBNY 之內部稽核流程可分為計畫擬定（Planning）、實地查核（Fielding）及報告（Reporting）三個階段，在實地查核前，稽核團隊會與受查單位先召開一場啟動會議（Opening meeting），以下將逐

一介紹每個階段。

（一）計畫擬定

完成風險評估程序後，開始進入計畫擬定階段。稽核團隊須擬定一份行動計畫（Plan of Action），內容包括受查單位業務流程摘要、情境分析、風險評估結果及查核目標與範圍等項目，讓主管能快速瞭解此次查核目的及範圍。計畫擬定完成後，由總稽核（General Auditor）發布查核聲明（Announcement），聲明內容包括查核預計起訖日、查核小組人員、啟動會議日期等資訊。

實地查核開始前，稽核團隊會與受查單位召開啟動會議，該會議主要係介紹稽核團隊成員、查核標的與方法、預計時程表、查核期間聯絡管道以及最後出具報告之格式等，希望於查核前與受查單位充分溝通，讓後續實地查核能夠更順利進行。

（二）實地查核階段

總稽核發布查核聲明且與受查單位召開啟動會議後，查核小組便能進入實地查核階段。目前 FRBNY 查核小組普遍使用穿透（Walkthrough）測試，評估受查單位特定業務流程，及其所設計之內部控制或風險控管措施是否確實採行及效益為何。查核人員參與部分或全部計畫，例如抽選一筆交易，與受查單位一同完成交易程序，透過穿透測試，可以幫助稽核團隊深入瞭解流程運作模式，

有機會發現潛在之風險及問題，即時向受查單位提出看法或建議。而在查核過程中，查核人員會出具內部稽核狀態報告（Internal Audit Status Report，詳圖 4），隨時記錄已完成之查核標的、稽核中項目及完成時間等資訊，讓稽核團隊能夠隨時掌握查核進度。

圖 4　FRBNY 內部稽核狀態報告格式
資料來源：研討會講義

（三）報告階段

FRBNY 要求稽核報告應清晰、簡明地傳達稽核結果及發現，於陳述過程中應避免使用過於專業或技術性之名詞，以不影響報告閱讀者理解為最高原則。此外，報告中所出具之建議改進事項，需確保受查單位能如期改善，因此查核小組於出具建議改進事項前，需與受查單位充分溝通。

目前 FRBNY 報告分為標題頁、執行摘要、稽核背景、問題與建議改進事項及附錄等五大部分。課堂講師認為，撰寫執行摘要是最重要的，需以合適之排版及簡單扼要之文字來陳報各章節要項，幫

助報告閱讀者在短時間內，對本次查核範圍及結論有基本概念。

圖 5 為 FRBNY 稽核報告中執行摘要之格式，主要由關鍵焦點（Key Hightlights）、查核發現（What We Found）及管理階層決策（Management Action）組成。在關鍵焦點部分，著重於提出一個足以總結全文之簡要觀點，以彰顯稽核團隊對於此次查核之見解，並提供閱讀者有價值之訊息，使幫助他們在短時間內瞭解受查單位之潛在風險，而稽核單位主管也會先閱讀關鍵焦點部分，來判斷是否有必要閱讀全篇報告。另外，於查核發現及管理階層決策兩欄，則分別記錄已發現之問題及為解決所發現問題，建議管理階層可採取之措施。

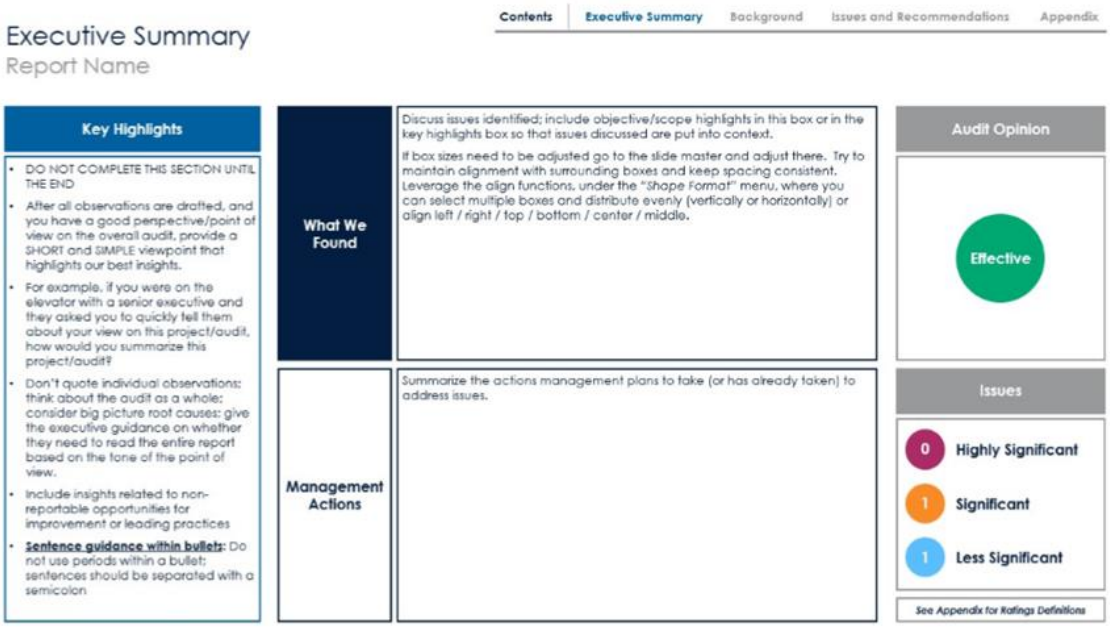


圖 5　FRBNY 稽核報告-執行摘要格式

資料來源：研討會講義

全美 12 家聯邦準備銀行皆設有總稽核及稽核小組，平常相互交

流查核上所遭遇的問題，同時也能調閱其他聯邦準備銀行之內部稽核報告，作為自身查核之參考資料，為免各銀行報告用語不一，易造成理解上之錯誤，聯邦準備銀行建立專門資料庫（Library），標準化風險與控制措施項目分類及用詞，以減少溝通上之誤會。

四、 內部稽核聯絡模式

稽核團隊與受查單位間之溝通協調順利與否，係內部稽核能否有效運作之重要因素，若查核人員堅持己見或是受查單位配合低落，則查核過程時將面臨層層阻礙，為解決前述問題，FRBNY 於內部稽核部門導入聯絡模式（Liaison Model），該模式之核心價值在於建立有效的聯絡人角色，促進機關內不同部門之溝通、合作及協調，目前已廣泛運用於各產業中。

FRBNY 內部稽核聯絡模式架構如圖 6 所示，分別由稽核聯絡人（Audit Liaisons）、稽核團隊領導人（Audit Relationship Leader）及業務方代表（Business Area Representative）等三方組成，稽核聯絡人主要任務係擔任稽核及業務代表兩方之溝通橋梁，負責傳遞查核過程中所發現之重要資訊並提出有效之建言。

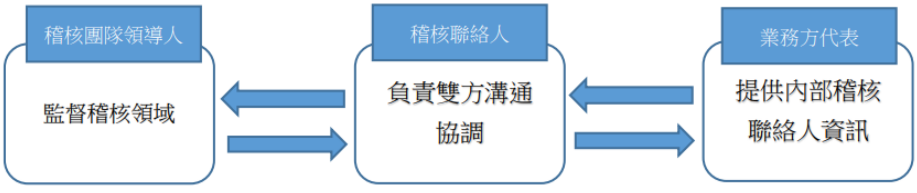


圖 6　FRBNY 內部稽核聯絡模式
資料來源：研討會講義

稽核聯絡人職責如下所述：

（一）內部稽核相關事務之溝通：稽核聯絡人於機關內部擔任稽核相關事務之聯繫點，並促進不同部門間的溝通與協調，聯絡人可能需要回答問題、提供指導及協助解決稽核相關問題，而每次與業務方代表之協調均會出具聯絡會議記錄（Liaison Meeting Notes），以便其他相關人員了解會議討論內容及結果。

（二）內部稽核計畫之協調與管理：稽核聯絡人可協助稽核團隊領導人確定查核範圍、確保稽核資源有效分配及協調查核工作時間表。

（三）稽核報告結果之傳遞：稽核聯絡人負責將查核報告及結果傳遞給相關部門，並解釋查核結果及提供建議改進措施。聯絡人於必要時也須協調不同部門間合作，以解決查核過程中所發現之問題。

透過建立聯絡模式，可以確保機關內部稽核職能運作順利，查核訊息之傳遞及處理也能更加迅速和準確，同時能促進不同部門間之合作與協調。FRBNY 認為，若確實且持續使用內部稽核聯絡模式，則產生以下效益：

1. 確保機關遵循內部稽核師協會（The Institute of Internal Auditors）

準則第 1210 條[3]。

2. 強化稽核做為顧問角色之價值。

3. 減少重複且無益之業務活動。

4. 協助辨認新興風險。

5. 提升稽核過程之效率。

6. 提供更為廣泛且效率之確信服務。

五、 大型專案計畫稽核

大型專案計畫係指於特定期間內，由多個相關活動組成之大規模計劃，該類專案通常需橫跨多個部門進行合作，並可能耗費大量之資源、時間及預算，其執行成果通常會對機關經營成敗有重大影響。通常大型專案規劃較複雜，本身固有風險（Inherent Risk）[4]也較高，因此 FRBNY 認為，針對該類型計畫進行稽核有其必要性，以辨認未揭露之潛在風險。

大型專案計畫稽核流程與一般查核相同，分為計畫擬定、實地查核及報告等三階段。稽核團隊於初始評估後，與計畫領導人進行訪談，確定專案計畫時程及內容，接著進入風險評鑑程序，以鑑別專案主要風險，並依據訪談內容及風險評估結果來擬定查核計畫。實地查核期

[3] IIA 準則 1210 是關於「技能專精」的標準。該標準強調內部稽核人員須具備執行其個別職責所需之知識、技能及其他能力；內部稽核單位整體須具備或取得履行其職責所需之知識、技能及其他能力。

[4] 固有風險（inherent risk）指的是在考慮內部控制或風險緩解措施的影響之前，存在於一個流程、活動或機關中的風險水平。

間，稽核團隊會進行穿透測試，持續尋找專案計畫中隱藏之問題及風險，同時考量內部控制之有效性，俟查核結束後，稽核團隊會出具稽核報告並針對專案計畫缺失提出建議改進事項。以下將介紹 FRBNY 實地查核大型專案計畫之稽核要項及計畫早期預警訊號（Early Warning Signs）與關鍵成功因素（Key Success Factors）：

（一）實地查核稽核要項

實地查核階段，FRBNY 將查核重點聚焦於計畫治理（Goverance）、管理（Management）、執行（Implementation）、解決方案（Solutions）等四部分，其查核架構如圖 7 所示，以下將逐一介紹各部分之稽核要項：

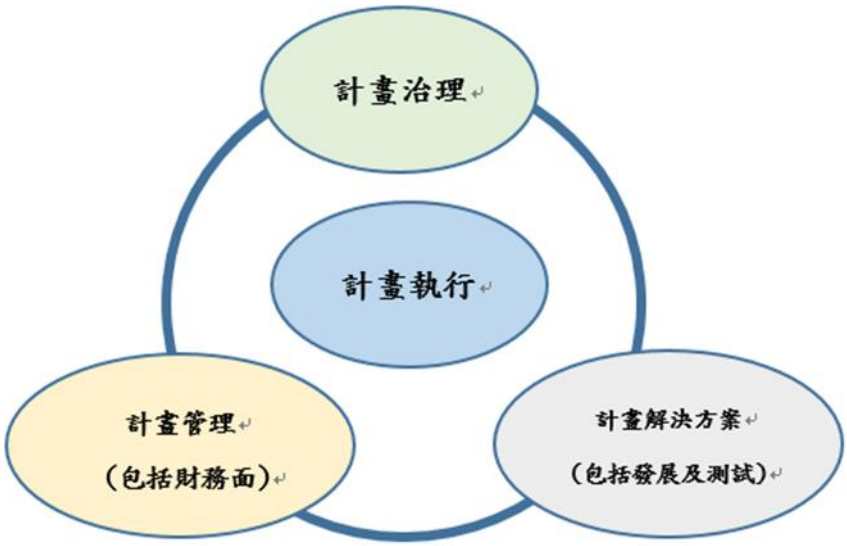


圖 7 專案計畫查核架構
資料來源：研討會講義

1. 治理：檢視專案計畫治理框架，包括計畫參與人員、人力配置、政策及資訊蒐集等，以確認是否可支持專案計畫達成當初所設

定之目標。

2. 管理：評估專案計畫管理活動及控制措施之妥適性，包括資源管理、風險管理及品質管理等，此外還會審視專案計畫之財務（Financial）活動，例如預算編制、成本預估、費用支出許可及預決算比較等，是否有異常或違反控制程序之情形。
3. 執行：評估專案計畫執行活動之合理性，例如：新服務或新工具之啟用是否通過核准、法令遵循、是否制定訓練計畫或使用手冊及計畫後續進度追蹤等。
4. 解決方案：從機關選擇之供應商或系統開發人員及產品主要功能，來檢視計畫解決方案之品質及進展情況。若專案計畫解決方案涉及資訊系統技術領域，則會另外進行開發（Development）及測試（Testing）兩項作業評估。
   （1）開發：評估各項發展活動之控制措施合理性，例如程式碼管理、品質管理流程及軟體開發過程所使用之理論和工具，並確定發展過程中是否遵守安全開發措施（Secure development practices）[5]。
   （2）測試：評估各測試階段之控制措施是否合理，例如系統測

[5] 安全開發措施（secure development practices）是指在軟體開發過程中採取的一系列方法和措施，旨在確保軟體的安全性和抵抗潛在的安全風險。內容通常包括安全需求、安全設計、安全編碼、安全設計及安全培訓等。

試、使用者認證測試、回歸測試及整合測試等，並確認測試計畫及弱點追蹤之妥適性。

（二）早期預警訊號

依照稽核團隊經驗，在查核過程中如有以下現象，可能係造成專案計畫執行成效不彰之早期預警信號：

1. 關鍵利害關係人未參與專案計畫。
2. 計畫團隊未具備足夠技術與經驗。
3. 預估計畫所需時程以及產出效益不切實際。
4. 機關資源未充分投入至專案計畫。
5. 計畫未獲得高階管理階層充分支持。
6. 未明確辨識該計畫與其他計畫或是第三方（例如：供應商）之關係。

（三）關鍵成功因素

一項大型專案計畫能順利完成，通常具備下列關鍵成功因素：

1. 利害關係人參與（Stakeholder Involvement）-專案計畫執行過程中有適當之利害關係人參與。
2. 管理階層支持（Executive Support）-高階主管支持專案計畫並協助提供策略規劃。
3. 清楚的業務目標（Clear Business Objectives）-使利害關係人理解

專案計畫核心價值並確保目標與策略相符。

4. 熟練地運用資源（Skilled Resources）-計畫團隊須具備專業知識且須妥善分配計畫資源。

5. 第三方/供應商管理（Third Party/Vendor Management）-供應商須經適當管理以降低第三方風險。

6. 正規方法（Formal Methodology）-針對計畫流程及管理模式繪製流程圖，內容包括計畫治理及風險管理等。

整體而言，稽核團隊須充分理解整個專案計畫之運作模式，並隨時與計畫團隊溝通，以便隨時更新相關資訊，查核過程中以計畫四大領域（治理、管理、執行及解決方案）為查核方向，並從中辨識計畫之關鍵成功因素及是否存有早期預警訊號。此外，專案計畫稽核時程較一般查核長[6]，因此稽核團隊除了於查核結束出具查核報告外，也會於查核前中期出具查核報告，FRBNY 認為，若能在查核中前期提供有效資訊或建議改進事項供計畫團隊參考，除了能提高專案計畫成效外，也能提高稽核人員做為顧問角色之價值。

[6] 依 FRBNY 稽核團隊經驗，通常一項大型專案查核需耗費半年至兩年才能完成。

肆、新興風險之因應

新興風險（Emerging Risk）係指相對較新且可能對經濟、社會或環境造成重大影響之風險，而這些風險通常與新興技術、市場或趨勢有關，並可能對傳統之管理方法造成影響，機關內部若未能即時對該類風險預為因應，調整自身之營運策略，則可能產生巨大損失。FRBNY 認為目前機關中常見之新興風險與人工智慧（Artificial Intelligence，AI）、網路（Cyber）及第三方管理（Third-Party Management）等三大領域有所關聯，以下將逐一做說明。

一、 人工智慧風險

人工智慧係指系統或機器能模擬和執行類似人類智能之能力，目前經過數十年發展與研究，AI 之應用已迅速擴展至各領域，例如自動駕駛、機器翻譯、醫療診斷等，其在改善工作效率、創造新的商業模式及解決複雜問題方面具有重要潛力，已逐漸成為我們生活中不可或缺的一部分。現行 AI 應用領域架構如圖 8 所示。

FRBNY 認為，中央銀行若能妥善運用 AI 技術，可協助機關於風險管理方面提供更強大之工具與技術，例如利用大數據和機器學習技術分析歷史數據，建立模型預測金融市場風險；亦可運用 AI 監控金融市場或支付系統之即時數據，即時檢視異常活動及潛在金融不穩定因素等。雖然導入 AI 技術能強化央行內部管理效率，但同時

也面臨許多挑戰，例如員工缺乏相關知識，導致難以駕馭 AI 所產生之人為風險，或 AI 系統初始演算模型設置錯誤，致後續演算結果產生偏差之模型風險（Model Risk），甚至會有些惡意攻擊的 AI（Adversarial AI）被用來從事不法行為。

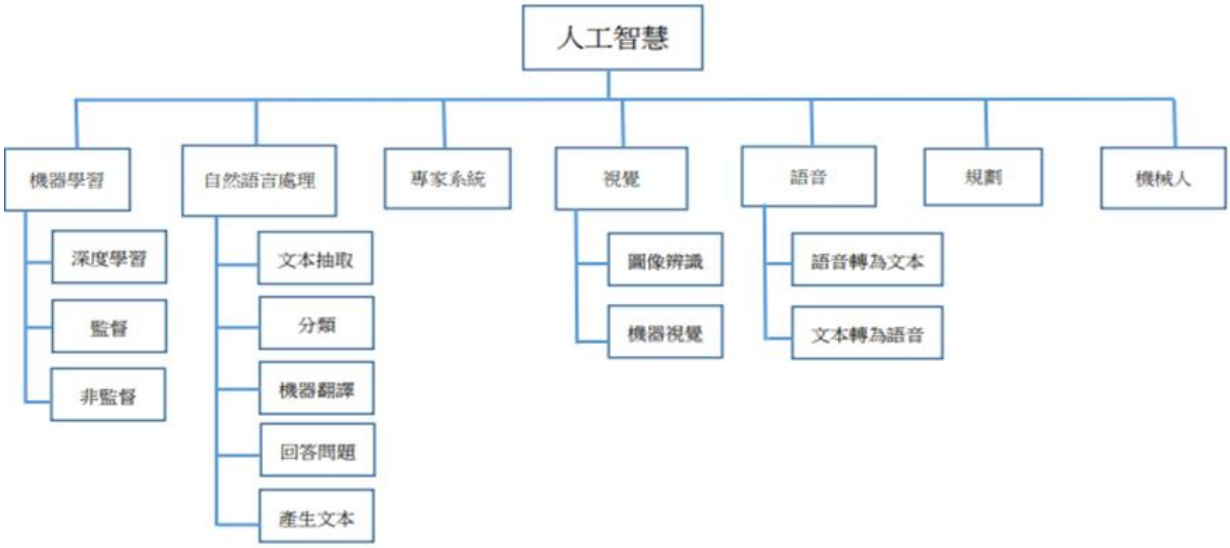


圖 8　人工智慧應用領域架構
資料來源：研討會講義

依據 FRBNY 稽核團隊經驗，提供機關內部人工智慧風險之辨識方式：

（一）檢查模型開發過程：內部稽核人員可審視人工智慧模型之開發過程，包括數據收集、特徵選擇、驗證等步驟，以確保模型建立之過程符合相關法規規定，及是否存在偏差或不公平之情形。

（二）檢核模型運行情況：內部稽核人員可以檢測人工智慧模式的運行情況，確保模型之正確型及穩定性，例如利用穿透測試，實

際抽取一筆交易帶入系統實際運作，觀察模型是否出現不當行為或錯誤決策之情況。

（三）評估風險管理措施：內部稽核人員應評估機關對人工智慧風險之管理措施，包括風險評估、監控及應對策略之妥適性，並檢查機關是否有適當之政策或控制措施來預防人工智慧風險之產生。

（四）專業培訓與知識分享：內部稽核人員可參加相關專業培訓或研討會，持續更新對人工智慧風險之瞭解與知識，聯邦準備銀行也會定期舉辦相關研討會，提供稽核人員互相交流之機會。

二、 網路風險

網路風險係指機關使用網路或物聯網，潛在攻擊或數據洩漏之風險，包括未經授權之訪問、操縱、或破壞訊息系統及數據資料庫。該風險可能多個來源，例如駭客的惡意活動、軟體漏洞及人為錯誤等，對機關可能產生重大財物損失或聲譽損害，甚或要承擔相關法律責任。依據 FRBNY 提供統計資訊，美國企業平均一年需花費 13 萬 3 千美元處理勒索病毒攻擊所造成之損害，另外每年平均需耗費 50 個工作日處理惡意軟件攻擊，耗費金額高達 260 萬美元，可見網際網路風險已對企業營運效率產生重大影響。

（一）近年來網路風險日漸增加，主要可歸納下列原因：

1. 不斷演進之威脅環境：駭客及惡意攻擊者的技術與手段不斷進化與改進，使其得以更複雜且隱蔽之方式進行攻擊，例如釣魚信件、勒索病毒等，加上人工智慧技術興起，讓有心人士於撰寫惡意軟件或程式碼較以往更為便利，這些不斷演進之威脅環境，使得機關更容易遭受攻擊。
2. 日益複雜之技術環境：近年來企業依賴各種複雜技術和系統來支持業務營運，包括雲端計算、大數據，及物聯網等。這些技術環境複雜性，使得攻擊者有更多機會找到漏洞與攻擊入口。
3. 頻繁的數據交換與共享：企業於日常業務營運中需要頻繁地與內部或外部單位進行數據交換與共享，無形中潛在數據遭未經授權讀取或洩漏之風險，特別是在資料傳輸或是存取的過程更容易發生。
4. 人為失誤與內部威脅：內部人員自身疏失或不當行為，可能導致網路風險增加，例如：誤觸釣魚連結、無意間洩漏敏感資訊、未即時更新系統軟體等。依據統計，美國企業一年平均約有45%員工曾經誤觸釣魚信件連結，無形中使機關暴露於風險之中。

（二） 檢視或預防網路風險之方法：

1. 進行風險評估及審核機關安全策略：內部稽核人員應對機關

之安全策略進行風險評估，以確認系統流程中是否存有潛在風險及漏洞，除了使用 AI 技術檢測系統弱點外，亦與 IT 部門合作，協助稽核人員瞭解及評估機關內部安全措施及系統配置。

2. 檢視系統權限管理：內部稽核人員可以檢視機關系統權限管理程序，例如帳戶管理、密碼策略、用戶權限等，以確保只有授權用戶可以存取敏感資源及數據。

3. 監控安全事件及異常行為：內部稽核人員可以分析安全事件[7]與系統之異常行為，例如檢查安全事件日誌之監控工具紀錄，並分析用戶行為模式，即時檢測及應對相關之威脅。

4. 進行員工教育訓練：內部稽核人員可建議機關推動員工訓練或培訓，提高其對網路風險之認知，同時也可以檢視機關之培訓計畫與教育資源，評估所擬定之訓練計畫是否有達成預計成效。

三、 第三方管理風險

第三方管理風險係指機關與外部單位進行業務往來、資源共享或提供服務時所面臨之風險，該風險存在於機關與外部單位的相互依賴與資源共享，機關可能委託第三方處理數據、提供技術支援、管理

[7] 安全事件是指在計算機系統、網絡、應用程序或數據資源中發生的任何意外事件或活動，可能導致資訊安全受損、資料泄露、系統中斷、服務中斷或未經授權存取等問題。

基礎設施或提供其他服務，由於機關無法直接控制或監控第三方之管理，這種相互依賴關係無形中亦為自身營運帶來不少風險。所謂第三方除了與機關有直接往來之供應商、承包商等有業務合作之企業外，與第三方有業務往來之企業或是稱第四方，也有可能對機關營運產生影響，第三方管理風險之分層架構詳圖 9 所示。

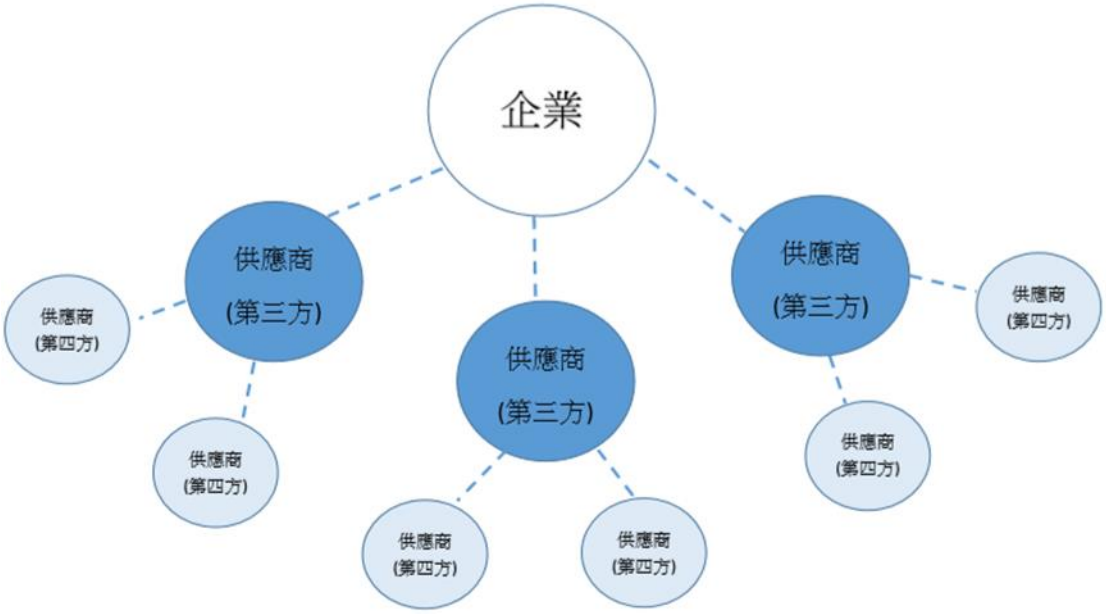


圖 9 第三方風險分層架構
資料來源：研討會講義

因應第三方管理風險，美國國家銀行監察署（Office of the Comptroller of the Currency）提出了第三方風險管理生命週期，主要係描述機關與第三方進行業務往來期間，從風險評估至監控審查之一系列活動與措施，期望透過實施完整的第三方風險管理生命週期，機關可以更容易識別、評估及管理與第三方合作之相關風險，並有助於保護機關資訊或資源，降低潛在第三方風險影響。該生命週期分為辨識與評估、合約與監控、監測與警報、審查與更新、終止與移轉等五

階段：

（一）辨識與評估：首先機關會對潛在之第三方風險進行評估，包括第三方風險管理能力、法令遵循等，通常會採用發放調查問卷之方式來進行。

（二）合約與監控：機關與第三方簽訂合約並制定明確之合作協議，內容須包括安全需求、風險管理措施、保密協議及法規遵循等，另外還須建立監控機制，以確保第三方按照合約執行，並定期評估其安全及合理性。

（三）監測與警報：機關需持續監測第三方之安全事件，以辨識任何異常或潛在之風險，通常可透過日誌分析及漏洞掃描等方式來實現，同時建立警報機制，以即時因應突發狀況發生。

（四）審查與更新：定期審查第三方風險管理措施之有效性與合規性，例如定期舉辦安全演習或測試，以驗證第三方之風險管理狀態和應對能力。同時依據評估結果，來判斷是否需更新合約及控制措施。

（五）終止與移轉：當與第三方終止合作時，機關需確認敏感訊息已安全移轉或銷毀，並解除合約與授權，以確保內部資訊不會再流漏至第三方。

FRBNY 認為目前最常見的新興風險係第三方產生網路風險，該

風險由於發生在第三方，無法完全由機關掌控，且往往事出突然，讓機關無法即時因應，進而導致機關承受不必要之損失，例如：知名車輛共享業者-Uber 於 2022 年 12 月與其合作之 IT 資產管理軟體供應商-Teqtivity 遭駭客攻擊，導致程式原始碼、IT 資產管理報告、網域登入名稱等內部資料外洩，當中更包含 7.7 萬名 Uber 員工姓名及電子信箱等個人資訊。

依據全球知名 IT 研究與顧問諮詢公司-Gartner 於 2022 年所出具之報告，目前由第三方產生之網路風險逐漸增加，僅 23%企業能即時因應第三方網路風險所產生之損害，該報告預測至 2025 年止，約 60%企業會將第三方網路風險列為風險控管之首要目標。為了因應第三方所產生之網路風險，機關採用第三方網路風險管理（Third-Party Cyber Risk Management，簡稱 TPCRM）來分析、監督以及減輕各種由第三方所產生之網路風險，包括制定內部控制程序、緊急應變措施及定期對第三方進行風險評估等。

有鑑於第三方網路風險逐年增加，TPCRM 也成為 FRBNY 內部稽核團隊之查核重點，並會透過下列標準來評估機關第三方網路風險管理之有效性：

1.是否與相關利害關係人（第三方或是與機關有業務往來之關聯企業）充分溝通。

2. 機關是否制訂 TPCRM 治理準則。

3. TPCRM 框架是否定期透過網路測試來評估檢核，以測試框架之有效性。

4. 除了第三方外，是否評估其他與第三方有間接或直接關係之公司（例如：上下游供應商）有產生網路風險之可能性。

5. 是否使用人工智慧來協助機關做第三方風險評估。

綜上，第三方之網路風險管理是機關確保與第三方業務合作安全之重要措施，透過有效之評估、監控及管理，機關方能降低與第三方合作產生之網路風險，並保護敏感訊息及業務運作之安全。

伍、資料治理之未來趨勢

資料治理係指機關於管理及使用資料時所遵循的一套原則，旨在確保資料之品質、可靠性、安全性與合規性，同時發揮資料之最大價值，減少資料錯誤和不準確性對機關之負面影響。而近代社會資訊量愈來愈大，機關取得資料之管道及方法更多元及方便，資料治理之重要性也日漸提高，以下將介紹 FRBNY 如何做資料治理。

一、 成立資料分析處

為了加速並活化企業對於商業決策、政策建議、研究等進階分析以及增加機關之資料資產價值，FRBNY 成立了資料分析處（Data&Analytics Office，簡稱 DAO）來管理資料，期望能提高機關營運效率並協助 FRBNY 業務推動順利。該部門主要有以下職能：

（一）資料治理與質量管理：建立資料治理政策和程序，以確保資料之完整性、安全性及合規性，包括定義資料標準、資料分類以及資料隱私等措施，另外 DAO 也會定期透過資料清理、驗證以及監控，藉此確保資料之質量。

（二）資料的分析與整合：從機關內外各來源，包括資料庫、系統和外部資料供應商來蒐集資料。

（三）商業智能及決策支援：提供商業智能平台，使業務單位能夠自行分析資料。這項功能允許相關利害關係人獨立使用或探索資

料，進一步創建特定報告並做出資料驅動的決策。

總而言之，資料分析處於FRBNY之資料治理中扮演重要角色，它為 FRBNY 資料治理提供框架及流程，並確保資料有效管理及使用，以協助機關達成目標，同時達成保護資料價值與安全性之效果。

二、 資料治理之方法

目前常見資料治理分成資料倉儲（Data Warehouse）、資料湖（Data Lake）及資料網格（Data Mesh）三種方法，以下將逐一介紹。

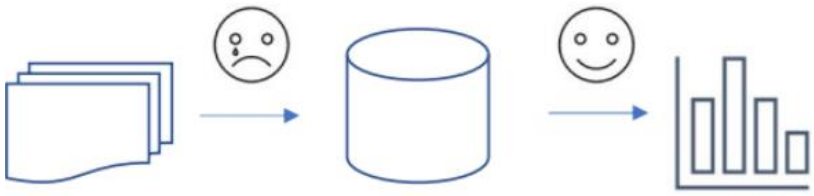
（一） 資料倉儲

係指從不同之源系統[8]中提取、轉換及加載數據，接著將其組織成易於查詢與分析之格式，並將處理完之數據儲存於單一資料庫（Warehouse）中，形成一個統一的數據儲存系統，供用戶隨時提取想要之資料，該管理方式有以下缺點，可參考圖 10：

1. 複雜性：從不同的源系統中提取和轉換數據，並確保數據的一致性和準確性是一個相當複雜的過程，因此資料倉儲之建設及維護需要高度技術與專業知識。
2. 數據一致性問題：資料倉儲需要從多個源系統中提取數據，並進

[8] 源系統（Source System）是指機關或企業中用於生成、收集或存儲原始數據的各種應用程序、資料庫或系統。這些源系統可以包括企業內部的各種應用系統、第三方應用系統、外部數據供應商等。

行轉換和整合，這可能導致數據一致性的問題，例如數據不準確、重複或缺失等。



資料倉儲預先建立一致且嚴謹之資料庫。
建構資料庫困難，資料提取容易。

圖 10 資料倉儲缺點
資料來源：研討會講義

（二） 資料湖

運作概念與資料倉儲類似，將從各源系統中提取之數據儲存於單一資料庫中，供使用者存取想要之資料，但資料湖於源系統提取資料時，可以接受不同結構及格式之數據，代表資料庫中能存放各種類型之資料，然而此管理方式有以下缺點，可參考圖 11：

1. 數據品質：資料湖中的數據通常是原始、未處理的，可能存在數據品質問題，如重複、缺失或錯誤的數據。在資料湖中進行數據分析和提取洞察時，需要投入額外的努力來處理和清理數據。
2. 安全性及隱私：由於資料湖中存儲了各種類型和格式的數據，其中可能包含敏感信息，因此需要采取適當的安全措施來保護數據的安全性和隱私。

資料湖保留數據原始格式，交由使用者自行處理。
建構資料庫容易，存取資料困難。

圖 11 資料湖缺點
資料來源：研討會講義

（三） 資料網格

資料網格是一種新興之資料治理模型，旨在解決傳統集中式架構，例如前面所提到的資料倉儲及資料湖，所面臨的一些挑戰。該治理架構如圖 12 所示，主要特色是將數據視為機關中之產品（Data Product），並將其所有權下放至相關業務單位，每個單位都有自己負責之數據領域，以自主的方式設計、開發及管理數據產品，提高數據資源之可靠性及靈活性。

該管理模式相較於資料倉儲及資料湖，具有以下特點：

1. 去中心化：資料網格模型將數據的所有權下放到各業務單位，避免集中式之數據管理結構，讓數據資源應用更具靈活性。
2. 自主管理：每個業務單位負責自己的數據領域，以自主的方式設計、開發和管理數據產品。這樣做可以提高團隊對數據的理解和責任感，並更符合業務需求。
3. 彈性與擴展性：資料網格模型使用現代化的數據基礎設施和技術，

如雲端儲存等，使該管理模式能應對數據的增長和變化，並支持數據產品快速開發和交付。

4. 標準化與共享性：資料網格模型鼓勵各單位採用標準化之數據結構、定義和使用規則，確保不同數據產品之間一致性，並促進各單位間之數據共享。

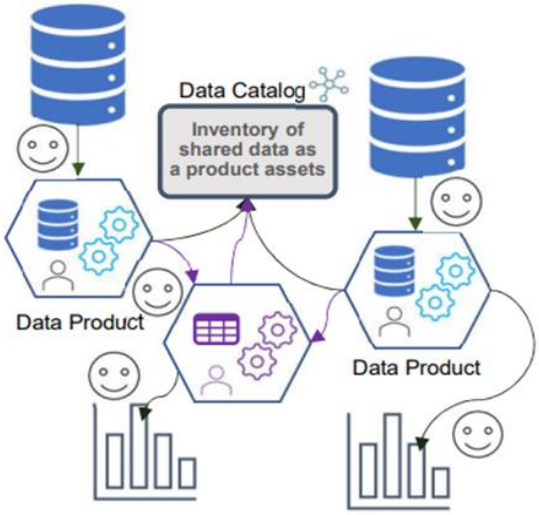


圖 12　資料網格架構
資料來源：研討會講義

目前 FRBNY 使用資料網格來管理數據，將數據視為機關中之產品，並採用分權管理，將數據產品所有權下放之各業務單位，並制定標準化之作業程序，以增加數據共享性。

三、 資料治理今昔差異

隨著科技日新月異，數據之取得相較過去也方便許多，這也連帶影響機關資料治理之方式，以下將分為「數據創造、傳遞及維持（數據產品生產者）」及「商業使用者體驗（數據產品消費者）」兩部分來說明資料治理之今昔變化，詳如表 1 及表 2 所述。

表 1　資料治理今昔比較（1）

數據創造、傳遞及維持（數據產品生產者）	
過去	現在
1.數據品質未透過統一系統做管理,需要透過數個團隊手動進行干預。	數據品質透過統一系統或專責單位做管理，減少手動交接及維護。
2.數據來源雜亂不一,所存取之數據不一定為有用資訊。	數據來源具有可追溯性並通過單位核準，以確保數據可用性。
3.資料治理責任權責劃分不明確。	由資料分析處來擬定資料治理相關事宜。

資料來源：研討會講義

表 2　資料治理今昔比較（2）

商業使用者體驗（數據產品消費者）	
過去	現在
1.使用者不容易探索或取得想要之數據。	可透過統一之管道來獲得數據，例如資料倉儲、資料湖、資料網格等。
2.數據來源或品質參差不齊,影響到使用者數據分析結果之準確度。	可透過可靠之資料治理確保取得數據符合目的，且數據品質是可信任的。
3.使用者無法得知數據之狀態，例如：年限、準確度、批准用途等。	透過現代化之數據處理架構，以實現高效、及時且準確之數據分析,讓使用者隨時掌握數據狀態。

資料來源：研討會講義

整體而言，資料治理在未來將持續發展和演進，以因應數據快速增長及日益複雜之技術環境，機關需要隨時注意數據之品質、安全性及可靠性，同時強化治理框架，隨著各單位對數據價值之重視，好的資料治理將成為機關成功之關鍵要素。

陸、結論與心得

本次研討會，除了介紹 FRBNY 內部稽核流程、大型計畫專案稽核外，還介紹了新興風險之因應與資料治理等伴隨外部環境變化所出現的新議題。基於人工智慧技術導入、網路攻擊逐年增加及資料治理概念興起，已經對各產業之營運模式產生影響，所面臨之新興風險也隨之增加，如未能及時做出因應，亦能造成難以估計之損失，FRBNY 近年也逐漸重視由人工智慧、第三方所產生之新興風險，並擬定應對措施做因應。

除了新興風險之衝擊，FRBNY 也強調機關內部溝通之重要，期望透過稽核聯絡人之建立，強化稽核團隊與受查單位之合作，不但能使查核計畫順利進行，也能幫助稽核團隊瞭解受查單位業務運作，協助機關即時覺察新興風險並做回應，聯絡人之概念目前也廣泛應用於各產業中。茲就本次研討會之討論議題提出以下心得供參：

一、 建立稽核聯絡人，強化內部稽核溝通職能

稽核團隊於進行查核時，除了本身必須具備一定之專業知識，溝通技巧也是影響查核成敗的重要因素，若查核人員堅持己見，甚至與受查單位產生衝突，那原本擬定之稽核計畫也將會窒礙難行，而內部稽核身為機關中第三道防線，若未能有效發揮其職能，機關暴露於風險之機率也將大幅提高。

為減少稽核方與受查方於查核期間所遭遇之溝通阻礙，似可參考 FRBNY 設立稽核聯絡人，擔任稽核團隊與受查單位兩者間之溝通橋樑，除能提高溝通效率、協助查核計畫之擬定外，還能進一步提高內部稽核人員作為顧問角色之價值，確保機關第三道防線能充分發揮效用。

二、 鼓勵員工補充新知，以因應科技所帶來之新興風險

隨著人工智慧、區塊鏈及雲端計算等新技術之導入，機關內部的營運風險也隨之改變，查核人員於擬定稽核計畫時，也必須將這些因科技所產生之新興風險納入考量，而根據勤業眾信於 2018 年發表之「內部控制 3.0」提到，隨著機關內部流程自動化機器人（RPA）、人工智慧（AI）之導入，內部稽核部門除了引進跨領域專家外，查核人員應利用工作之餘，參加相關課程補充資訊技術新知，以提高自身查核敏銳度，內部稽核人員具備資訊技術基本概念後，可協助機關檢視現有之內部控制制度，是否可因應新興風險所帶來之衝擊，也可以進行潛在風險評估，研擬防範措施，進一步達成事前預防之效果。

三、 針對第三方風險評估及因應

機關基於成本或人力資源之考量，有部分業務委託第三方廠商合作辦理，以提高經營效率及效能，但同時也帶來了第三方風險，

若未來第三方出現違約、資訊洩漏等不當行為，可能對機關造成嚴重影響，為避免或減少這些風險帶來的損失，宜提早做好因應措施是至關重要的。本行委外辦理之重要資通相關業務，似可參考美國國家銀行監察署所提出之第三方風險管理生命週期，從與第三方簽約前至合約結束期間，建立嚴格的監控機制、明確的合作協議及安全審查等措施，能讓機關更容易應對潛在之第三方風險，以降低損失並確保業務持續運作。

參考資料

1. FRBNY 研討會課程講義。
2. 蘇雅玲（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。
3. 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。
4. 勤業眾信會計事務所（2018 年），內部稽核 3.0-內部未來的關鍵即是現在。
5. 內部稽核協會報告（IIA position paper），2013 年 1 月
6. The IIA’s Three Lines Model：An update of the Three Line of Defense.
7. Fintech News , The 2020 Cybersecurity stats you need to know.
8. Gartner, Third Party Risk Management（TPRM）.
9. Gartner Press Release, Garner Unveils the Top Eight Cybersecurity Predictions for 2022-23.
10. Office of the Comptroller of the Currency, Third-Party Relationship.