出國報告（出國類別：其他）

參加美國紐約聯邦準備銀行「風險管理與內部稽核」課程

服務機關：中央銀行

姓名職稱：劉家偉 副科長

課程期間：112 年 5 月 22 日 至 5 月 25 日

報告日期：112 年 8 月 1 日

摘 要

本次奉派參加美國紐約聯邦準備銀行(Federal Reserve Bank of New York, FRBNY）舉辦之「風險管理與內部稽核」訓練課程。FRBNY 職責在維持金融穩定並有效控管金融風險，藉由運用三道防線模型，並透過內部稽核方式，以有效控管風險。課程內容（涵蓋中央銀行之主要風險管理及內部稽核實務）包括 FRBNY 主要面臨交易對手之風險、稽核小組運用三道防線模型作為風險管理框架、內部稽核程序與方法、數據治理，以及探討面對新興風險之應變準備等議題。本報告謹就相關議題分別加以說明，並研提下列建議事項供參：

一、透過模擬風險情境桌面演練，以強化業務同仁專業知能

值此瞬息萬變時代，同仁須面對各項風險挑戰，身為風險控管之第一線，應培養獨立思考與解決問題之能力。透過模擬風險情境桌面演練，有助激發同仁活化思維，並訓練即時解決問題之能力。本行業務單位可就經評估須面對較高風險挑戰之業務，定期舉辦桌面演練或類似研討，以提升專業知能及風險應變能力。

二、培養內部稽核人才，持續精進金融專業及數據分析能力

隨著科技發展浪潮，各單位大量運用人工智慧等科技於業務場域，惟同時具備資訊及業務專業之人力短缺，組織可能面臨新興風險，因此，培育跨領域專業人才儼然已成為組織發展之顯學。面對外來新興挑戰，同仁應持續精進金融專業知識並積極學習數據分析能力，以落實風險管理與內部稽核。

目 錄

壹、前言

職奉派於 112 年 5 月 22 日至 25 日參加美國紐約聯邦準備銀行（Federal Reserve Bank of New York, FRBNY）舉辦為期 4 天之「風險管理與內部稽核」訓練課程，參加人員除本行外，尚有來自德國、瑞典、瑞士及日本等共計 46 名學員。講師均為 FRBNY 內部稽核人員，藉由講授課程及分享美國金融風險管理與內部稽核等相關經驗，作為各國與會學員借鏡及參考。

本次課程主要探討 FRBNY 面臨之各項金融風險挑戰，以及如何運用三道防線架構有效控管風險。在內部稽核方面，稽核人員運用數據分析進行實地查核後，將稽核報告提供管理階層參考，同時協助第一及第二道防線及早採取預防措施，以有效控管風險。

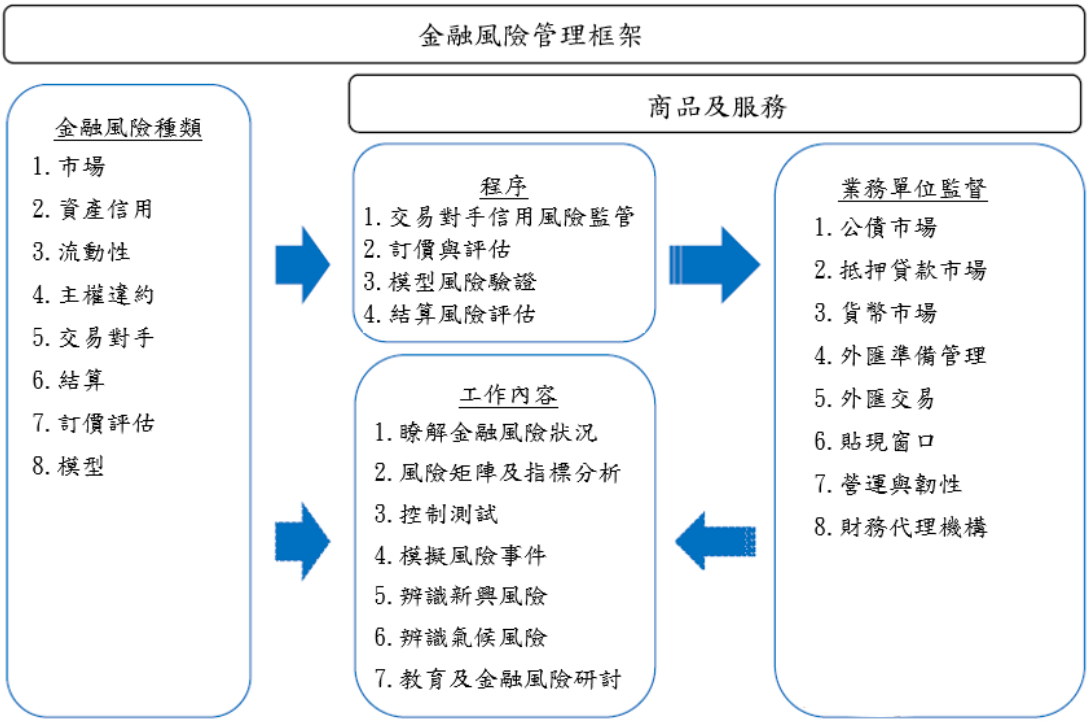
隨著資訊科技發展及後疫情時代來臨，同仁使用網路與應用軟體之機會及頻率增加，組織面臨系統遭受第三方惡意軟體攻擊（malware attack）之網路風險亦隨之提高。根據 FRBNY 調查指出，2021 年美國企業遭受惡意軟體攻擊之平均損失為 260 萬美元，而處理時間平均長達 50 天。為有效控管風險，FRBNY 預擬各項風險情境並訂定應變措施，以強化其因應風險之韌性。

本報告共分為柒章，第壹章為前言；第貳章介紹 FRBNY 面臨交易對手之風險；第參章為內部稽核與三道防線模型；第肆章為 FRBNY 內部稽核程序與方法；第伍章為數據治理及應用；第陸章探討新興風險下之應變準備；第柒章為心得與建議。

貳、FRBNY 面臨交易對手之風險

FRBNY 主要透過國內公開市場操作（包括購買國庫券、抵押擔保證券及附買回交易等）及貼現窗口提供市場資金，以穩定金融環境。在金融風險控管方面，作為第二道防線，負責對銀行承擔之金融風險進行獨立評估及監督；另訂定金融風險管理框架（Financial Risk Management Framework）（圖 1），並提出基本風險類別及監督指引供第一道防線遵循。該框架因應其面臨之各項金融風險擬訂監督方案（包括專注於交易對手風險監督、擔保品折價及訂價評估等），以有效控管金融風險。

圖 1　FRBNY 金融風險管理框架



資料來源：課程講義。

一、交易對手之風險

FRBNY 之交易對手涵蓋存款機構、初級市場交易商、貨幣市場基金、國營事業及金融週邊服務事業等。於提供市

場充足信用之過程中，FRBNY 進行下列交易時，可能面臨交易對手未能履行義務之風險：

(一)為促進支付清算系統效率，對存款機構提供無擔保透支。

(二)透過貼現窗口向存款機構提供隔夜（overnight）或有擔保短期貸款。

(三)為將資金利率維持在聯邦公開市場委員會訂定之目標範圍內，FRBNY 進行附買回交易（repurchase agreements），以及向公債交易商或抵押擔保證券金融機構提供貸款。

二、交易對手信用風險監督方法

為有效控管信用風險，FRBNY 採用三道防線模型作為管理交易對手信用風險之方法（Counterparty Credit Risk Oversight Program, CCRO），說明如下：

(一)第一道防線

首先對每個交易對手進行風險評估並給予信評等級，區分交易對手財務穩健程度，決定後續 FRBNY 與交易對手之策略（包括提供短期信用及擔保借款）。當交易對手信評較差時，將僅能獲得短期擔保貸款（通常為隔夜拆款），此類貸款在 FRBNY 監督管理下，適用更高之擔保品折價率。

(二)第二道防線

負責對金融機構之交易對手進行監督。首先確認第一道防線已準確評估交易對手之信用風險，對於信評較差之對手採取適當風險控管措施，以降低交易對手違約時遭受之損失，另提供金融機構專業知識與建議，強化其對交易對手之風險控管。

(三)監督方式

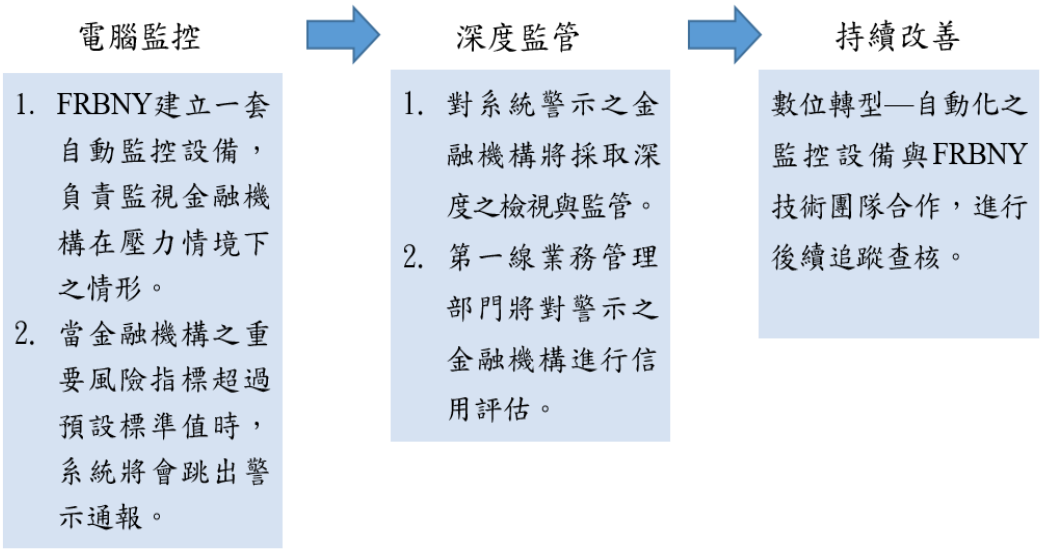
1.個別機構監督

FRBNY 開發評估各類型機構（涵蓋存款機構、初級市場、貨幣市場基金及金融週邊服務事業等）之方法，因應個別機構之特性調整監管方法，以適當評估交易對手之信用風險。

2.資料監管與電腦自動監控

CCRO 採用季報公開數據、監管機構對存款機構評估及信評機構等資訊，作為評估交易對手風險之參考。另為因應日益龐大之交易對手，CCRO 開發評估財務指標之自動化篩選工具（圖 2），聚焦在壓力情境下，自動篩選出超過關鍵財務指標之交易對手，將進行後續風險評估及查核行動。

圖 2　FRBNY 自動篩選流程圖



資料來源：課程講義。

三、FRBNY 扮演信用提供者角色

(一)作為最後貸款者

FRBNY 在經濟恐慌時作為最後貸款提供者(lender of last resort)，藉由交易對手交付抵押品為擔保，提供緊急貸款。

(二)提供充足信用

FRBNY 指出在 2008 年金融危機期間，提供信用並增加流動性具政策有效性。相較於 2007 年初之信用，2021 年底銀行及金融控股公司總計高出約 50%，透過提供寬鬆之信用水準，確保金融機構具有足夠資金以因應外部衝擊。

(三)更具包容性

近幾年 FRBNY 採取包容性（inclusive）態度，修正放寬交易對手之合格標準，以確保交易對手確實執行政策並促進公平競爭之市場；另一方面，放寬交易對手資格，係鑒於一些新交易對手因規模小致籌資能力較弱，可能造成市場額外負擔。FRBNY 認為採取包容性態度可能提高整體交易對手之風險，應作好風險控管以降低損失。

四、擔保品折價與評價

為提供市場充足流動性，健全市場發展，在執行附買回交易與貼現窗口抵押貸款時，央行持有之擔保品將存在市場風險[1]及訂價評估風險[2]。考量擔保品作為央行風險緩衝之重要性，合理評價擔保品以避免跌價損失至關重要。

(一)擔保品折價（haircut）

指央行評估交易對手提供之擔保品，經評價後給予一定

[1] 指由於市場價格之反向變動而導致財務損失之風險。

[2] 指供應商評估抵押品時，產生無法準確評估市場公允價值之風險。

之折價率，因此提供之貸款金額=（1-h）*擔保品價值，且 0<h<1（h 為折價率）。

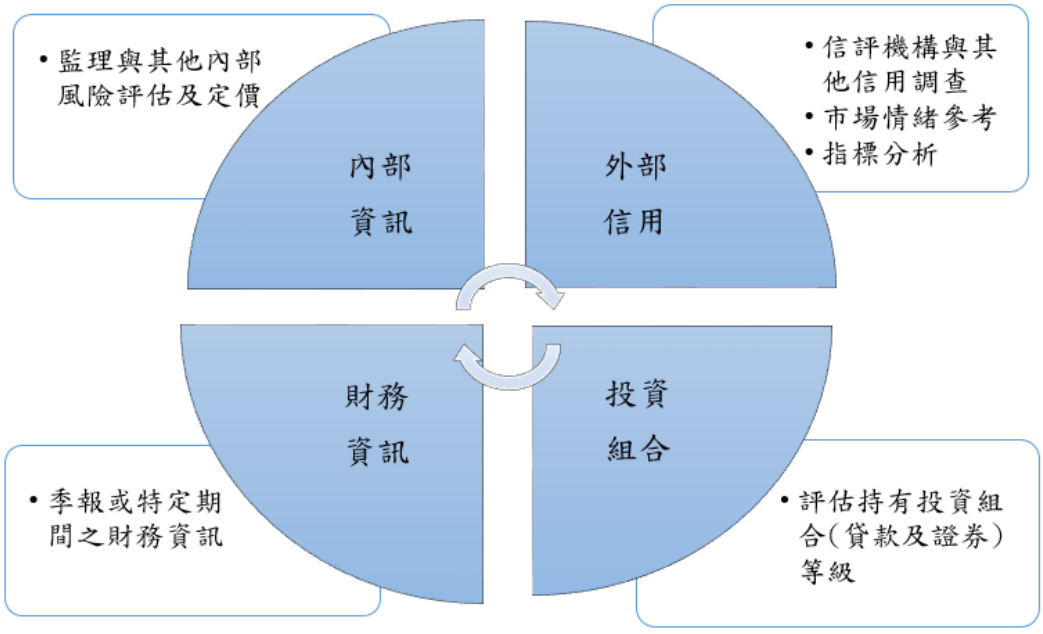
(二)影響折價率之因素

包括資產類型、信用評等及擔保品之流動性等，均影響折價率評價。

(三)擔保品評價（collateral valuation）

評價方式（圖 3）主要考量各種擔保品之歷史市場價格波動，給予合理之折價估值；至於在次級市場無法交易之擔保品，因無實際成交價格供參，故改採內部訂價機制（例如詳盡調查供應商之情況評估風險、設定訂價門檻及執行價格評估計畫等策略），以估算合理之價值。

圖 3　擔保品評價方式



資料來源：課程講義。

(四)緊急融通

由於 FRBNY 為最後貸款提供者，因此提供貸款給交易對手時，即使在金融危機期間，通常不致因市場壓力而調高折價率，確保交易對手能順利取得緊急融通。

參、內部稽核與三道防線模型

依據「國際內部稽核執業準則」[3]（International Standards for the Professional Practice of Internal Auditing, IIA Standards）對內部稽核定義，係提供獨立客觀之確認性及諮詢服務，增加組織價值及改善營運。內部稽核單位利用有紀律及系統性之方法，評估及改善風險管理流程，協助組織達成目標。

一、內部稽核與風險管理關係

(一)內部稽核目的

內部稽核在協助內部控制[4]、改善風險管理及監理之過程，以達成組織營運目標。隨著組織規模擴大與營運活動之複雜度提高，內部稽核之有效運作將提供有價值之風險評估報告供決策單位參考。

(二)內部稽核與風險管理關係

在追求營運目標下應做好風險管理，並透過訂定相關之管理程序，將風險控制在可控之範圍內；而內部稽核旨在協助評估管理程序之有效性，並適時予以修正，將修正建議連結於整體風險管理，確保組織營運目標與風險管理措施一致。

二、國際內部稽核協會簡介

國際內部稽核協會（The Institute of Internal Auditors, IIA）成立於 1941 年，為全球內部審計行業公認之權威、倡導者與主要教育者。IIA 提供指導原則供全球內部審計專業人士遵

[3] 準則之制定與發布為一項持續之過程。國際內部稽核協會在發布執業準則前，會進行廣泛諮詢及討論，其中包括透過準則草案向全球公開徵詢意見，最終彙整修訂並發布，供全球內部稽核執業人員遵循。

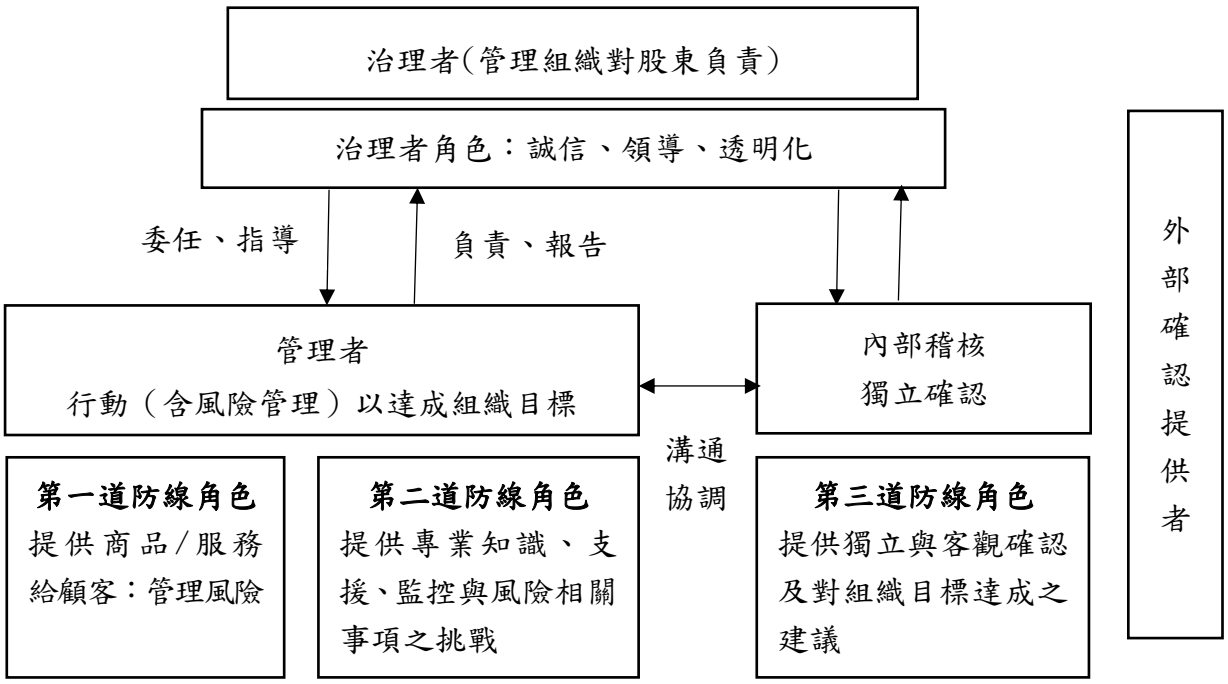
[4] 內部控制係一種管理過程，由組織之董事會、管理階層及其他成員負責執行，以確保達成營運目標，適用於財務及非財務層面之自行評估及監督工作。

循，內容包括核心原則、IIA Standards、職業道德規範及相關指引等規定。

三、IIA 三道防線模型

IIA 認為營運單位主要由一群具有相同目標者組成，包括利害關係人（stakeholders）、治理者（governing body）、管理者及內部稽核。為確保其營運目標符合利害關係人之利益，IIA 頒布三道防線模型，分別賦予治理者、管理者及內部稽核明確之權責範圍（圖 4），說明如下：

圖 4　IIA 三道防線模型



資料來源：IIA 出版（2020）。

(一)第一道與第二道防線

皆隸屬於管理者並受其監督，且由管理者定期向治理者負責及報告。

1.第一道防線：主要為確保組織能維持正常營運並提供商品及服務。

2.第二道防線：主要透過風險管理協助第一道防線正常運作，亦包括專家提供專業知識、支援及監控特定目標之風險管理（包括內部控制、品質管理、資訊安全、法令遵循、企業永續發展等），雖然主要業務為全方面風險控管，惟第一道防線仍具管理風險責任。

(二)第三道防線

第三道防線為內部稽核，主要協助董事會及管理者從事查核及評估，依據擬訂之職能架構（圖 5），提供前兩道防線管理，確保組織營運目標與風險管理政策一致，因此，內部稽核扮演角色至關重要。

圖 5　第三道防線職能架構圖

資料來源：課程講義。

(三)管理階層及董事會角色與責任

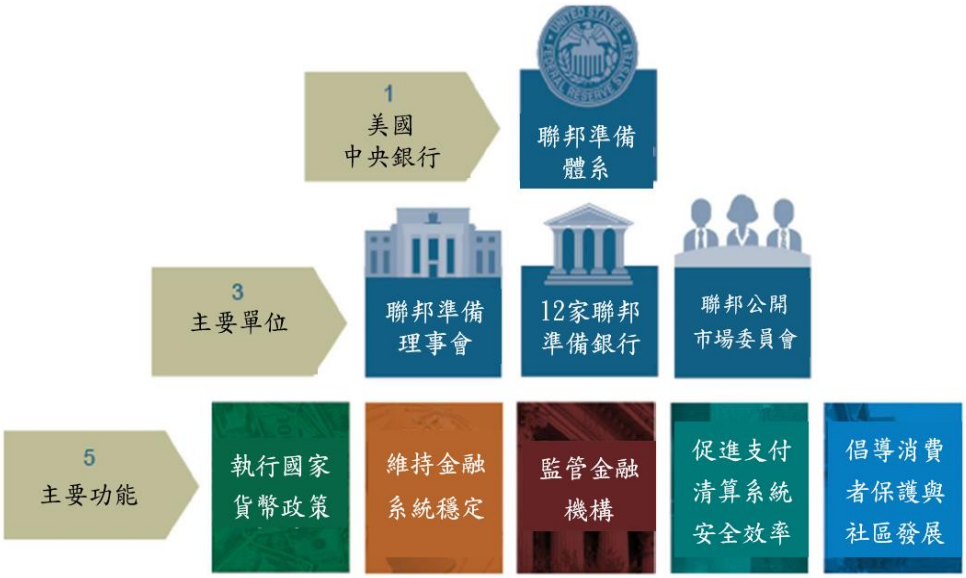
1.管理階層：金融機構執行長及高階管理者應負責建立治理文化，並將其文化推展到組織每個角落，藉由有效溝通及堅實之激勵措施，建立誠信與道德價值等正向控制環境。

2.董事會：制定組織總體營運策略及管理政策，由高階管理者執行其制定之目標、方向及內部監控政策，並對董事會負責。因此，高效能之董事會應對組織整體營運發展有確切遠景藍圖與方向。

肆、FRBNY 內部稽核程序及方法

聯邦準備體系（Federal Reserve System, FRS）為美國中央銀行體系（圖 6），主要由聯邦準備理事會（Federal Reserve Board

圖 6　美國聯邦體系圖



資料來源：課程講義。

of Governors）、聯邦公開市場委員會（Federal Open Market Committee, FOMC）及 12 家聯邦準備銀行（Federal Reserve Banks）組成。其中聯邦準備理事會為主要管理機關，委員會之 7 名成員由美國總統任命，負責監管聯邦準備銀行。FRBNY 為聯邦準備銀行之一，12 家銀行皆獨立營運。就內部稽核而言，實務上各聯邦準備銀行之稽核主管均定期討論及分享實務案

例，以強化聯邦準備體系之韌性，並確保稽核報告具備一致性標準。

一、內部稽核程序與方法

FRBNY 於年度查核前，依據前一年度評估受查單位加權評分矩陣（weighted scoring matrix）（表 1）之分析結果，計算受查單位總風險高低，作為本年度執行稽核計畫之參考。評估內容主要以受查單位之作業風險、財務重大風險及策略風險作為計分權重，其中作業風險依作業流程、科技與數據管理及人力資源評估可能產生之風險因子，權重乘以風險等級（1～4），最後計算加權風險分數，風險分數高者（風險評等中等以上者）將作為優先稽核計畫之名單，據以訂定本（2023）年度應執行之稽核計畫。

表 1　加權評分矩陣

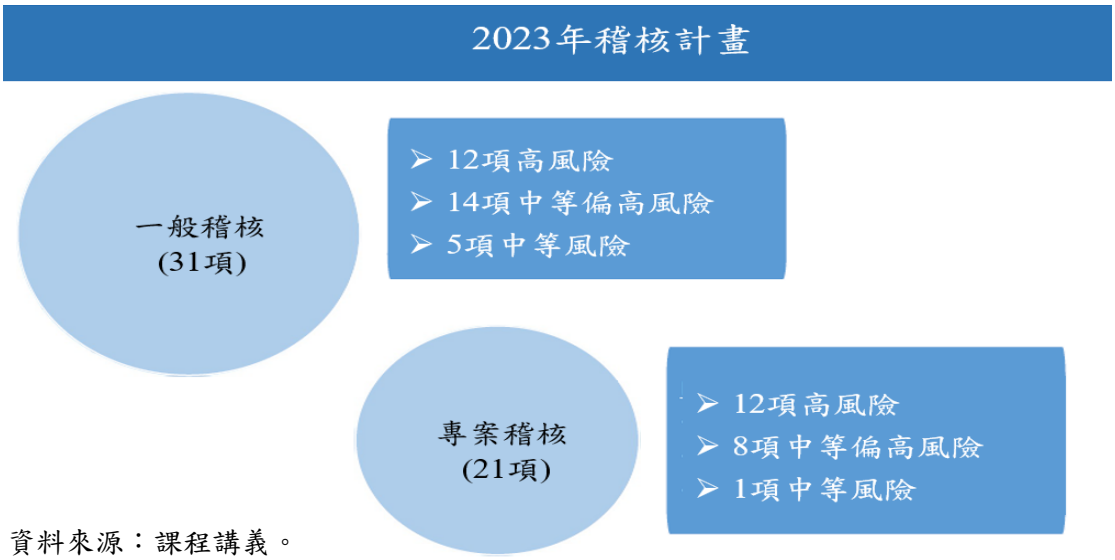
風險因子	權重	風險等級 (高、偏高、中、低)	分數
作業風險			
1.營業流程	20	3	60
2.科技及數據管理	30	4	120
3.人力資源	20	3	60
財務/重大風險	20	4	80
策略風險	10	3	30
總計	100		350
風險評等		高	

風險評等	風險分數	稽核頻率
高(4)	350-400	每 2 年 1 次
中等偏高(3)	276-349	每 3 年 1 次
中(2)	200-275	每 4 年 1 次
低(1)	100-199	一般審計自由裁量權

資料來源：課程講義。

依據加權評分矩陣分析結果，列出本年應執行之內部稽核計畫（圖 7），包括一般稽核 31 項及專案稽核 21 項，FRBNY 主要將內部稽核程序劃分為計劃、實地查核及報告 3 個階段，分述如下：

圖 7　2023 年稽核計畫圖



資料來源：課程講義。

(一)計劃階段（Planning）

1.公告備忘錄（announcement memo）

正式查核前以電子郵件通知受查主管本次查核範圍及目的如下：

(1) 查核範圍：包括規劃、預定實地查核日期、業務啟動會議日期、預定訪談日期、稽核主管及助理稽核名單、最後查核日期及查核風險等級。

(2) 查核目的：就查核範圍提供獨立之意見，協助組織在各項營運活動中作好風險控管。

2.範圍分析（scope analysis）

(1) 與受查單位人員面對面溝通，確認受查單位固有風險概況。

(2) 瞭解各業務程序風險之主要控管點，以執行設計

有效性評估及控制。

(3) 透過風險矩陣圖列出可接受之殘餘風險並評估風險管理。

(4) 列出經評估後實地查核前應查核之主要風險。

(二)實地查核階段（Fielding）

1.啟動會議

包括介紹稽核團隊、稽核目標及方法、時間排程、報告意見之方式、範圍及預期報告結果等。

2.查核及分析

(1) 依分析階段（包括紙本及數據分析）列出業務流程重要控管點，進行有效性測試及查核。

(2) 按各業務階段與受查單位人員密切溝通，確認各控管點有效性。

(3) 依控管點缺失及原因與相關業務主管討論確認。

(4) 與受查單位管理階層確認改善方案之可行性及預定完成日期。

3.文件及確認

彙整查核期間搜集之文件（包括相關業務表單、收據、受訪人員文字及照片佐證資料等），作為擬訂確認查核報告之依據。

(三)報告階段（Report）

1.提出稽核報告

稽核報告中應說明整體風險評等、主要風險之發生原因、影響及經討論後之改善承諾。

2.查核報告評等

就受查單位風險控管程序設計內容及執行情形，依其有效性分別給予足夠、待改善、有限或不足等 4 級評比，

並由業務單位依規定於目標日期前改善。

3.缺失改善追蹤與確認

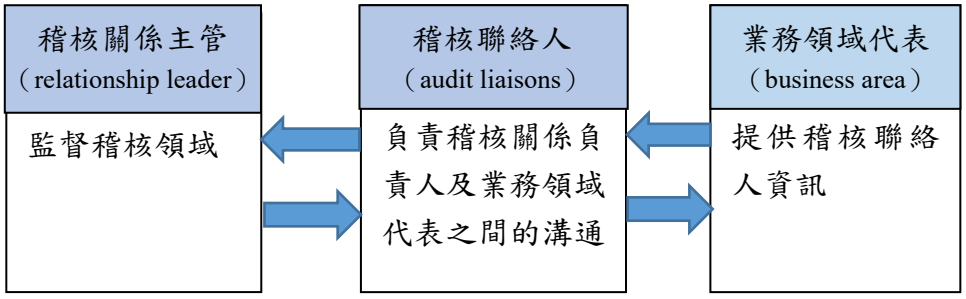
內部稽核部門應就查核所提缺失意見，經業務單位修正後進行追蹤與管控，並由稽核單位覆核改善情形。

二、溝通聯繫模式

(一)聯繫目的

業務複雜之稽核專案（例如營運、財務及資訊部門），為避免不同稽核人員對專案報告之表達產生重大差異，需要稽核聯絡人（audit liaisons）負責稽核關係主管與各業務領域代表之溝通管道，整合意見並確保稽核品質具一致性（圖 8）。

圖 8　liaison 溝通模型架構



資料來源：課程講義。

(二)稽核聯絡人之責任

1.瞭解組織營運風險：從組織各部門（包括財務及資訊部門）之角度，瞭解並整合相關風險。

2.擬訂稽核專案：彙整組織各部門風險後，評估重大變動對組織營運之影響，並擬訂查核專案。

3.與業務人員溝通或訪談：依風險高低決定與各部門人員溝通之頻率，並就查核文件重點與相關人員討論。

4.持續與業務代表溝通：就組織重大事件可能導致相關風

險、議題及科技發展應用，持續與各業務代表溝通，評估組織整體風險。

5.提供稽核計畫意見：彙整各部門流程可能產生之風險及控制弱點，提供總稽核擬訂每年稽核流程項目及重點。

(三)稽核聯絡人對組織之效益

1.確保稽核作業符合 IIA Standard 1210 規定[5]。

2.強化稽核人員作為價值顧問之功能。

3.整合財務與資訊部門因業務變動影響稽核範圍之情形。

4.提供更廣泛及有效率之確認服務。

5.有助於辨識新興風險。

6.減少重複且冗長之訪談程序，促進稽核流程之效率。

三、對大型銀行採取專案稽核

(一)重新檢視專案

大型專案隱含具有較大之風險，包括財務風險、投入資源風險及因作業流程改變所造成之變動風險。此外，因專案流程較為複雜，可能造成查核失誤之隱含風險，因此，稽核人員應提早參與稽核計畫之規劃與執行，以預先辨識上述風險並降低可能造成之損失。

(二)專案稽核流程

與一般稽核流程大致相同，FRBNY 將專案稽核流程分為計劃、實地查核與撰寫稽核報告 3 部分，分述如下：

1.計劃階段：主要透過與大型專案聯絡人連繫，獲得專案有利資訊，擬訂以風險為基礎之專案計畫。

2.實地查核：執行專案風險評估及辨識主要風險，並擬訂專案之預定完成時間，將專案執行期間切割為不同區間，

[5] 內部稽核人員須具備執行個別職責所需之知識、技能及其他能力，惟欠缺前述專業時，內部稽核主管須取得適當之專業外部服務協助。外部服務提供者可以是組織或個人，包括會計師、估價師、經濟學家、統計分析人員、資訊科技人才、稅務及法律專業人才等。

有效掌握稽核進度。

3.撰寫稽核報告：每一稽核區間提出稽核報告，風險報告須包括專案可能面臨之主要風險及新興風險，專案完成後應提出最終稽核報告。

(三)專案早期預警訊號（early warning signs for programs）

由於大型專案查核較為複雜，可能耗費半年至 2 年才能完成，故及早發現專案可能面臨之問題將至關重要。FRBNY 列出 7 項預警訊號，包括主要利害關係人未參與專案、高階主管不支持專案、專案經理未獲得充分授權、專案資源未充分配置、無效率改變控制流程、專案團隊缺乏適當技術與經驗及過度倚賴其他專案成員（如特定供應商）等，作為執行專案之參考。

(四)主要成功之因素

由於專案涉及利害關係人數眾多與耗費人力及時間成本等因素，造成專案失敗率高，因此，FRBNY 歸納 6 項執行大型專案之成功要素（圖 9），俾確保專案順利執行。

圖 9　大型專案成功之要素

資料來源：課程講義。

伍、數據治理及應用

數據治理是資料管理流程之核心部分，其作業涵蓋整個資料生命週期，包括前端作業系統、後端業務資料庫至終端數據分析，對數據蒐集、儲存、存取、應用、監督及控管，經由人員、技術及作業流程三者間之交互合作，以管理組織重要數據資產，並藉角色分工、訂定標準、制訂架構與運用數據等過程，確保數據具標準化、完整性、安全性及有效性，並與營運目標一致。

一、數據治理架構

數據為組織重要之資產，惟大部分資料未經標準化。此外，由於各部門交易數據良莠不齊，組織無法確定品質優劣，數據治理即成為提供組織進行決策分析之重要工作。以下簡要說明數據治理步驟：

(一)定位角色職能

數據治理主要核心工作係透過組織團隊將數據整理並應用於治理框架，因此，賦予角色定位為治理第一步，通常包括數據治理委員會、管理委員會及治理工作小組，負責執行數據治理業務。

(二)訂定政策標準

治理委員會成員通常由財務及各業務部門高階主管擔任，負責推動並監督資料治理政策與架構；管理委員會（由數據治理負責人、相關業務及資訊專家組成）依據擬訂之政策標準，訂定工作流程及實施步驟；治理工作小組負責執行治理業務，小組成員包括資料所有者、資料品管人員、架構師及分析師等。

(三)落實數據管理

良好數據管理應確保數據具標準化、完整性、安全性及有效性，俾供管理階層作為決策分析參考，分述如下：

1.標準化：數據管理最大挑戰之一為數據格式多樣化，例如訂單系統、銷貨系統及客戶服務系統內散布各樣業務流程數據，因此，企業如何建立一套機制，訂定數據標準並加以整合，確保數據之可用性，將攸關數據品質關鍵。

2.完整性：每項業務之數據資產須有專屬人員保管，確保數據資料具完整性，因此，數據治理之成敗不僅仰賴治理工作小組人員合作，更須業務單位配合提供高品質且連續性之資料，確保數據完整可用。

3.安全性：以明確之數據等級及權責劃分，阻絕未經授權內部人員存取或外部駭客攻擊及惡意滲透；透過儲存安全、網路安全及存取安全之制度與作業，確保數據之安全性，達到安全控管數據與快速應用，以發揮數據價值。

4.有效性：數據治理系統需要持續監控與修正，確保系統能有效提供彙整數據；另業務單位應持續提供意見反饋，協助團隊釐清治理框架並達成組織目標。

(四)重視數據倫理

數據治理有助於提供高品質資料供決策者使用，惟若控管不佳，可能造成數據外洩等個資問題，因此，應控管數據之使用權，限制並監管不同層級對數據之存取權及使用權限，避免被有心人士濫用。

二、數據分析辦公室

(一)數據分析辦公室（The Data & Analytics Office, DAO）

主要負責監督及評估數據風險，有助於採用重要數據與分析作業組織，建立最佳框架與標準指引，涵蓋數據治理、商品辦公室、數據管理、進階數據分析及數據策略共 5 個項目，以提升數據資產潛在價值，強化組織根據數據分析評估相關風險。

(二)即時數據之應用價值

DAO 與業務單位溝通、評估、擬訂優先順序及交付資訊商品等流程，將資訊應用程序傳送雲端服務，並將業務解決方案及最終用戶資訊載入企業數據與分析工具集（enterprise data and analytics toolset），俾利業務單位使用即時資訊商品以評估風險，提升其對業務單位價值。

(三)數據網格（Data Mesh）

數據網格係一種嶄新之設計、開發及數據管理方法（圖 10），將數據視為產品所有權之概念，數據生產者提供開放標準與互通性（interoperability）商品，為數據消費者提供創新服務並提升數據使用價值。數據網格主要具備下列 4 項主要特性：

圖 10　數據網格圖

資料來源：課程講義。

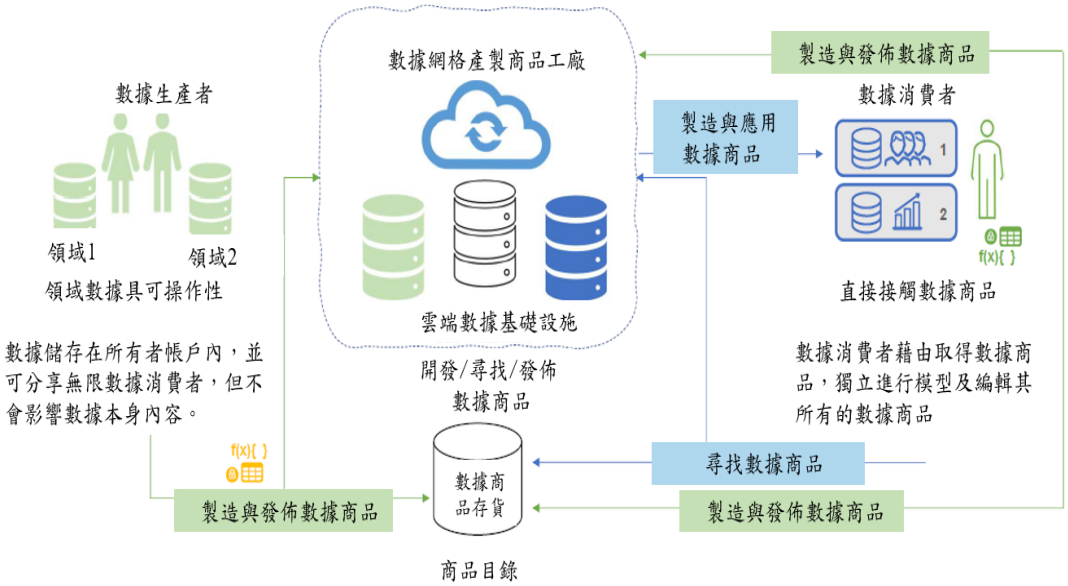
1.數據即商品：具有領域知識（domain knowledge）之業務單位擁有數據資料，扮演數據消費者角色（圖 11），能更即時使用、定義並瞭解數據歷史流程，同時因應市場營運變化，有效運用數據以滿足瞬息萬變之市場需求。

2.數據生產者：即數據之所有者。生產者最瞭解其創建之數據，包括結構、用途及價值，而創建目的即是為提供消費者操作分析使用。

3.數據運用互通：業務單位可直接使用數據商品，並自行治理、應用與維護數據，無須資訊單位耗費人力及物力支援，有效降低維運成本。

4.創新性：有別於以往數據僅集中儲存於資訊中心資料庫，數據採分散方式存放於各領域業務單位，數據所有者可直接對數據品質進行維護、使用及更新儲存，具有創新數據管理之特性。

圖 11　數據商品流程圖

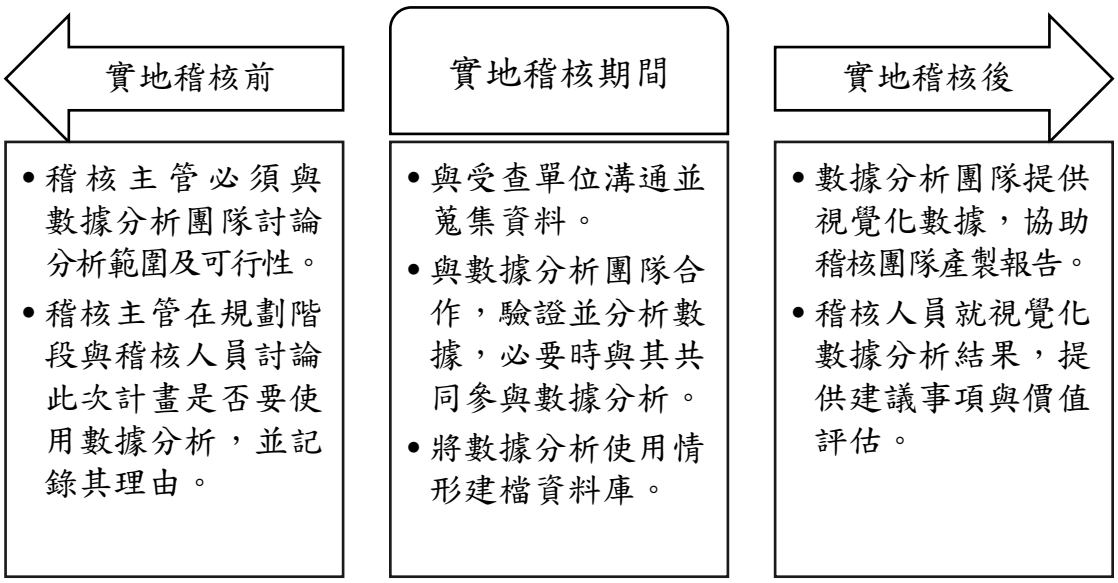


資料來源：課程講義。

三、導入數據分析稽核流程

根據全球調查，2021 年數據治理已成為組織面臨最大風險之一。稽核人員檢視組織數據治理之架構與過程，並提供確認之意見，有助組織運用數據並做好決策。此外，稽核團隊將數據治理導入稽核流程（圖 12），在實地查核前、期間及查核後與數據分析團隊充分討論，運用分析團隊提供之數據於實地查核，有助於節省稽核時間並聚焦高風險之業務流程，以提升稽核品質。

圖 12　導入數據分析之稽核工作流程圖



資料來源：課程講義。

陸、新興風險下之應變準備

新興風險係指短期可能包含高度不確定性，雖不至於對單位營運造成嚴重影響，長期卻可能對單位構成潛在威脅，主要包括下列 3 項風險：

一、網路風險（cyber risk）

網路風險指資訊系統故障或軟體遭受攻擊，導致組織財務或聲譽遭受損害之任何風險（圖 13），其產生原因如下：

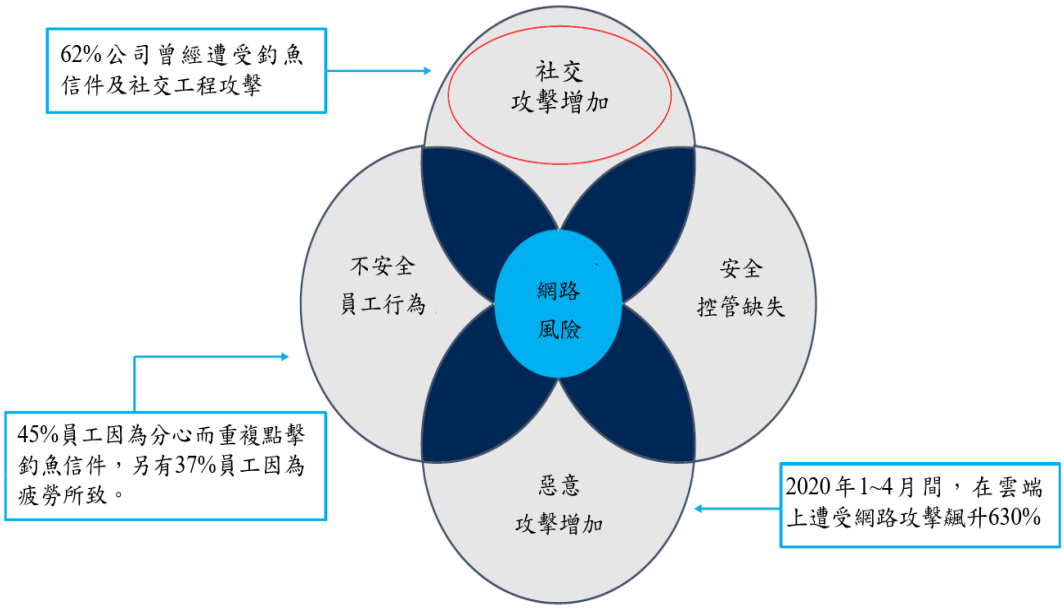
(一)第三方惡意潛入組織未經授權之安全漏洞，以獲得進入其內部系統之權限。

(二)企業本身系統安全性及完整性較差。

(三)人員疏忽點擊釣魚信件或遭受社交工程攻擊。

為降低風險造成之損失，組織應於平時強化系統安全及加強員工教育訓練。

圖 13　網路風險示意圖



資料來源：課程講義。

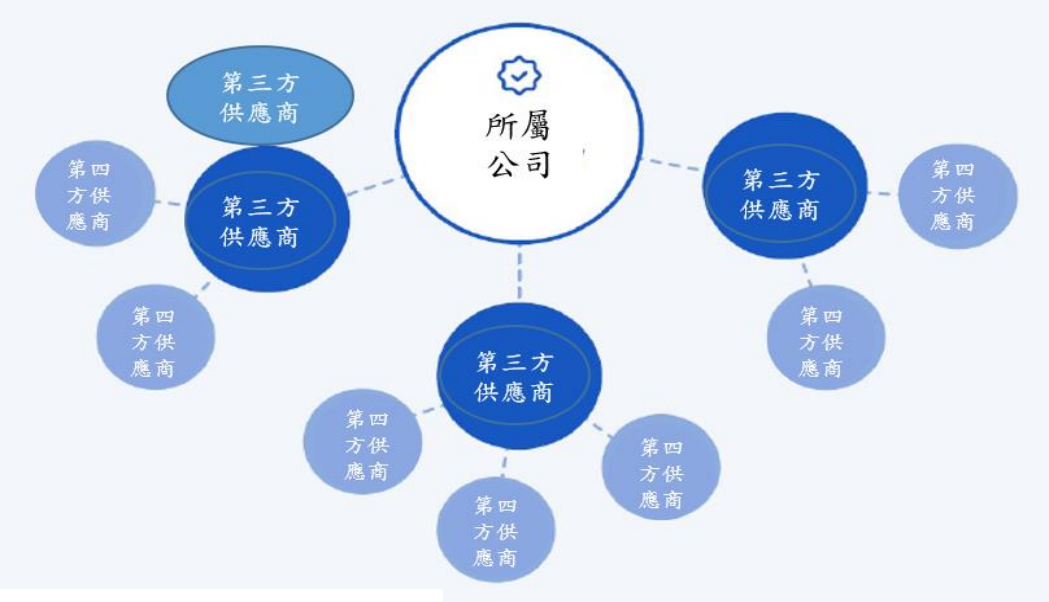
二、第三方風險（third party risk）

第三方風險指網路犯罪集團透過找尋與組織合作之第三方服務供應商（圖 14），間接從中找到橫向入侵組織之攻

擊路徑，導致組織遭受損失之風險，此類攻擊方式廣泛存在於各項產業（包括生產製造、系統、軟體及委外服務等）。

為降低組織可能面臨之損失，宜進行第三方風險管理（third party cyber risk management, TPCRM），以實地考查、訪問及問卷調查方式，辨識供應商之實際營運情況，分析、監督及管理第三方風險之流程。

圖 14　第三方風險示意圖



資料來源：課程講義。

三、人工智慧風險（artificial intelligence risk, AI risk）

人工智慧風險係指組織使用人工智慧解決各項工作內容時，可能因惡意軟體入侵或缺乏人員控管，致發生財務損失或資訊外洩風險。FRBNY 指出，AI 可提供自動化控管流程、提升風險管理效能及安全性管理等優點；惟亦面臨私人隱私外洩、安全性管理疑慮及人員操作不當等新興風險，因此，人員培訓與應用課題將為未來 AI 發展一大挑戰。

四、網路勒索風險（cyber ransomware）

網路勒索風險係指惡意第三方藉著使受害者之加密設備上文件無法使用，脅迫其提供贖金以獲得重新使用加密文件之可能。

(一)支付贖金原因：包括為解密遭勒索者惡意加密數據、防止其破壞加密金鑰及避免惡意勒索者外洩內部數據等。近幾年惡意勒索日趨猖獗，鎖定目標多為美國地方州政府及其關鍵基礎設施，藉以勒索更多報酬，惟諸多案例顯示，即使受害者已提供贖金，仍無法使用遭加密或破壞之數據。

(二)因應方案：除上述勒索風險外，由於後疫情時代促使行員工作型態轉變，居家或遠端辦公比例增加，使用網路信箱交換資訊頻率提高，致遭受網路釣魚攻擊（phishing attacks）風險隨之大幅增加。為有效控管風險，必須持續訓練行員對風險事件警覺性，透過建置系統自動偵測功能及模擬釣魚信件，藉以強化行員風險意識並提高組織風險辨識能力。

五、強化韌性（resiliency）

(一)韌性

韌性係指為因應外在衝擊之準備及適應能力。由於 FRBNY 負責關鍵基礎設施系統（例如 FedWire 及 FedTrade）正常運作，為避免新興風險可能造成銀行重大損失，平日應模擬風險情境並制訂綜合風險評估計畫，強化因應外在衝擊之韌性。

(二)制定綜合風險評估計畫

目前 FRBNY 已模擬約 150 個風險情境，制訂具預防性

之後續復原計劃，藉由持續監控威脅因子，動態調整風險情景，以評估對整體金融環境之影響及預擬各項因應措施。

(三)桌面演練（tabletop exercises）

桌面演練係指因應風險模擬情境，研擬可能之應變準備並進行實地演練。FRBNY 分享桌面演練技巧，主題為符合時效性與相關性之最新國際發展趨勢，例如中小型銀行擠兌危機或網路勒索風險等議題。透過演練有助於參與者重新釐清風險各種面向，藉由指派各種利害關係人參與討論，俾由演練中得到反饋，以強化組織營運韌性。

柒、心得與建議

良好風險管理有賴三道防線密切合作，三道防線雖各司其職，惟實務上若於第二或第三道防線始發現缺失時，恐已付出龐大成本。因此，應由業務單位首先在執行控管點或控制機制實施前，即具有專業判斷能力；繼而後二道防線於平時能提供諮詢與建議性之協助，有效提升業務單位自我管理之風險意識。

隨著金融科技發展，數據治理愈形重要，經由人員、技術及作業流程間之合作，確保數據具標準化、完整性、安全性及有效性，俾利稽核人員運用數據分析聚焦於風險性業務查核，不僅節省取得資料時間成本，更有助後續核心業務資料分析，以提升稽核品質。謹就本次課程研提下列建議事項供參：

一、透過模擬風險情境桌面演練，以強化業務同仁專業知能

以國庫業務為例，各業務單位除每年度修正業務 SOP 作為依規辦理之憑據外，每年底另評估並提交年度內部控制作業自行評估表，以落實業務控管；會計單位亦按月辦理各業務單位

之主要業務查核，並提供諮詢意見，以提高業務單位風險意識。前述作業程序實質上已具備三道防線控管精神。

業務單位為風險控管之第一線，負責內控制度設計與實施，惟控管流程恐因業務人員更迭頻繁或不熟悉風險因子，致無法充分評估風險。透過模擬風險情境桌面演練，供各業務人員重新審查相關工作內容，釐清正確觀念及思索可能面臨之風險，藉由跨單位間之反饋機制，可激發不同思維，並訓練同仁即時解決問題之能力。建議業務單位可就經評估須面對較高風險挑戰之業務，定期舉辦桌面演練或類似研討，透過意見交流，以提升同仁專業知能及風險應變能力。

二、培養內部稽核人才，持續精進金融專業及數據分析能力

國庫業務為因應國際金融環境及永續發展趨勢，除指派同仁參加本行金融科技工作小組外，並成立研究發展小組，適時就國內外主權綠色債券與永續發展、數位資產等相關新興金融議題進行翻譯研究分析。

隨著科技發展浪潮，促使國內各單位投入大量資源於人工智慧開發與應用場域，以因應時代發展趨勢，相關人力需求因而大增，惟專業人力之育成存在時間落差，尤以兼具資訊與金融方面之跨領域人才培訓不易，組織可能面臨新興風險挑戰。此次分組討論稽核成員分享職涯時，多數同時具備金融及資訊相關專業，並有跨部門協作與培訓課程，俾利精進各項新興風險管理之專業知識。建議同仁持續精進本身金融專業知識並積極學習數據分析能力，以落實風險管理與內部稽核。

參考文獻

1. FRBNY 訓練課程講義資料。
2. 王良允（2022），「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，中央銀行，8 月。
3. 林雅欣（2021），「參加美國紐約聯邦準備銀行（Federal Reserve Bank of New York）「風險管理與內部稽核（Risk Management & Internal Audit）線上課程視訊報告，中央銀行，8 月。
4. 李素慧（2021），「參加美國紐約聯邦準備銀行訓練課程『風險管理與內部稽核』出國報告」，中央銀行，8 月。
5. 王志源（2020），「參加法國央行舉辦之『內部稽核與內部控制研討會』訓練課程出國報告」，中央銀行，2 月。
6. IIA（2013）“IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control”, Jan.
7. BCBS（2021）“Principles for Operational Resilience”, Mar.
8. Ashraf Khan and Majid Malaika（2021）“Central Bank Risk Management, Fintech, and Cybersecurity” IMF Working Paper, Apr.