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：李佳芷/辦事員

派赴國家：美國、紐約

出國期間：114 年 4 月 26 日至 114 年 5 月 3 日

報告日期：114 年 6 月 11 日

摘要

一、美國聯邦準備體系於 1913 年設立，為美國中央銀行體系，負責制定與執行貨幣政策、監管金融機構並維護金融穩定。紐約聯邦準備銀行具核心地位，其政策對全球經濟與金融市場具有重大影響力。運用「三道防線」模型提升風險治理，透過業務單位、風險控制部門與內部稽核合作，強化風險辨識與控制。實施制度化協作與科技工具，提升資訊透明與應對效率，展現跨部門協作在風險管理中的關鍵價值與挑戰。

二、紐約聯邦準備銀行積極運用人工智慧偵測異常、經濟預測及風險治理。面對模型黑箱風險與數據偏誤挑戰，強調建立可信賴、透明且負責的治理框架，推動跨部門合作與持續監控。未來將聚焦風險為本策略、強化模型驗證、培養風險意識及國際監理合作，確保人工智慧在金融穩定中發揮最大效能。

三、紐約聯邦準備銀行在資訊安全領域，建構涵蓋技術、資料、營運、人員與供應商的多層防護機制，核心為四大資安韌性能力：預測、承受、復原與調整。為提升風險透明度，該行建立關鍵風險指標體系，涵蓋弱點管理、存取控管、內部行為監控、應變速度及釣魚偵測等項目，並為各指標設定風險容忍值，超出即啟動改善行動。該行於 2024 年第 4 季風險報告顯示整體風險維持可控，並已針對超標項目迅速調整控管措施，確保資安持續強化與穩定。

四、內部稽核在金融機構中扮演策略角色，透過稽核聯絡模型、風險評估與即時整合稽核，加強風險管理與內部控制。案例中展示動態稽核計畫與跨部門合作，未來建議強化資料分析、跨領域能力與稽核建議落實，提升治理效能與前瞻價值。

目錄

壹. 前言

作為中央銀行的一員，深知在當前金融環境中，風險管理與內部稽核對金融穩定與機構運營的重要性。隨著全球金融市場的變動與複雜度日益增加，提升相關領域的專業知識與實務能力，對於制定和執行有效的政策、監控風險以及保障機構運行的健全性，具有極其重要的意義。近年來，隨著新興科技的迅速發展，內部稽核的職能面臨新的挑戰與機遇。面對數據與科技浪潮的來臨，若內部稽核人員能夠掌握並善用數據，將能在風險評估、監控與決策制定中，擁有顯著的優勢。因此，對於相關技術及其在風險管理中的應用，具有深刻理解與實務操作能力，已成為現代內部稽核人員不可或缺的核心素養。

職奉准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 114 年 4 月 28 至 5 月 1 日，為期 4 日，舉辦之「風險管理與內部稽核」（Risk management and internal audit）訓練課程，由 FRBNY 選派之各部門專家擔任講座，具備高度專業理論及多年實務經驗。計有來自各國央行共 73 位學員參加，分別來自內部稽核部門、風險管理部門，及檢查監管部門等。本研習課程進行方式係由講師簡報課程內容及學員提問進行雙向意見交流，並結合理論與實務，以增進學員對風險管理與內部稽核之瞭解，期能增進風險管理知識，並借鏡 FRBNY 內部稽核作法。

本報告分為六章，除此前言外；第貳章介紹美國聯邦準備體系之三道防線；第參章說明人工智慧與風險管理；第肆章說明資訊安全治理與關鍵風險指標體系；第伍章說明內部稽核在計畫管理中的策略角色；最後，第陸章為結論與建議。

貳. 美國聯邦準備體系之三道防線

一、聯邦準備體系概述

作為全球最具影響力的中央銀行體系，美國聯邦準備體系（Federal Reserve System）的政策動向對國際金融市場具有重大指標性作用。其制定的聯邦資金利率不僅直接影響美國國內的貸款、房貸與投資成本，更對全球資本流動與貨幣政策具有示範效果。除了經濟與金融面的政策影響，也逐漸將金融包容性、永續金融與科技創新納入其考量範疇，如對金融科技（Fin Tech）業者的監管態度調整、對綠色金融風險的研究，顯示其在面對 21 世紀新興挑戰時，正持續演進並扮演更廣泛的政策制定者角色。總而言之，美國聯邦準備體系不僅是美國經濟穩定的中樞機構，更已成為全球金融秩序與貨幣政策協調中的關鍵力量，對全球經濟的穩定與發展具有深遠而持續的影響力。

(一)聯邦準備體系成立背景

美國早期曾設立第一與第二銀行作為中央銀行雛形，但因政治爭議與地方權力對抗而相繼解散。1837 年至 1863 年間進入「自由銀行時代」，缺乏中央金融管理導致體系混亂。1907 年金融危機後，社會呼籲建立穩定的中央機構。1913 年，美國國會通過「聯邦準備法」（Federal Reserve Act），正式設立聯邦準備體系，以統一貨幣政策與維護金融穩定。

(二)聯邦準備體系的三大主體

1. 聯邦準備理事會（Federal Reserve Board of Governors）：位於華盛頓特區，由總統任命的 7 名理事組成，負責制定貨幣政策指導原則並監督金融體系。
2. 聯邦準備銀行（Federal Reserve Banks）：分布於全美 12 個地區，提供區域性金融服務並執行政策。
3. 聯邦公開市場委員會（Federal Open Market Committee，簡稱

FOMC）：由 12 名成員組成，負責執行公開市場操作，調控資金供應與利率，以促進經濟成長與穩定物價。

(三)紐約聯邦準備銀行：FRBNY 是唯一在 FOMC 中具永久投票權的地區銀行，並執行主要貨幣操作，如管理公開市場帳戶（System Open Market Account, SOMA）、買賣政府證券等。此外，也負責金融監理、支付系統與外匯操作，是聯邦準備體系中最具影響力的機構。

二、三道防線模型概述

在當前金融體系日益複雜且高度監管的環境中，有效的風險管理框架對於機構穩定性與信任至關重要。美國聯邦準備體系中「三道防線模型」（Three Lines Model）的實務應用，特別聚焦於如何透過強化三道防線：第一線業務單位、第二線風險與法遵部門、第三線內部稽核之間的協作，以提升整體風險識別、緩解與回應能力。以下分析各道防線間的合作方式，並透過 FRBNY 實務經驗，並探討其對風險管理效率與監督成效之實際影響，及如何透過制度化的協作機制，共同強化組織韌性。

(一)第一道防線（First Line of Defense）：業務與經營單位，負責日常業務運作，並承擔初步風險識別與控管責任。其作為風險發生的前線，對風險事件的即時性回應至關重要。

(二)第二道防線（Second Line of Defense）：風險管理與法遵單位，為風險政策制定者與監控者，負責建立整體風險管理框架，並對第一線的控管措施進行監督與輔導，確保其合乎法規與內部政策。

(三)第三道防線（Third Line of Defense）：內部稽核，具備高度獨立性，主要執行對整體控制機制與風險管理程序的評估與稽核，並向董事會或監督機構提出改進建議。

三、三道防線協作模式

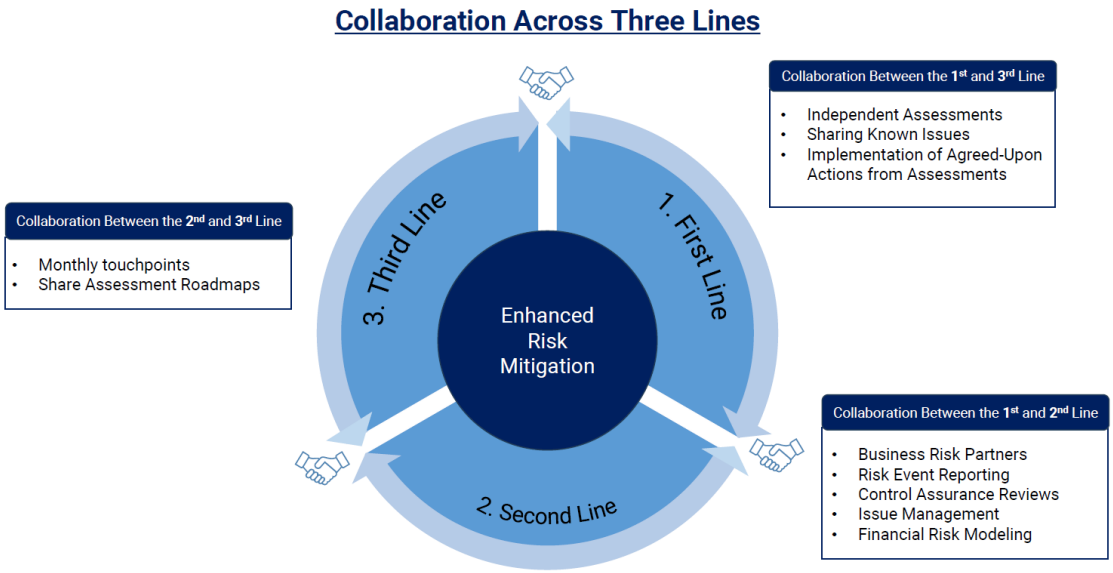


圖 1 FRBNY 三道防線間的合作機制

資料來源：研討會講義

(一)第一道與第二道防線之協作

在現代企業風險管理體系中，業務風險夥伴制度、風險事件通報、控制確認與檢視，以及議題管理等四大機制，構成了組織有效辨識、監控與回應風險的核心架構。

首先，透過業務風險夥伴制度（Business Risk Partners），企業能在各業務單位中設置專責人員，協助第一線即時了解公司風險政策，辨識潛在風險，並提供操作上的建議與應對方案，使風險管理不再僅是後端監控，而是前線作業中的一環。其次，風險事件通報（Risk Event Reporting）制度的建立，讓員工能即時回報任何潛在或已發生的風險事件，包括操作失誤、系統故障、內控缺失或法規違規等，確保相關單位與管理階層能在第一時間掌握風險動態並啟動應對機制，有效防止問題擴大。第三，為確保日常控制措施的有效性與執行力，企業會定期進行控制確認與檢視（Control Assurance Reviews），藉由檢視程序、資料與紀錄，確認控制作業是否落實，同時找出潛在的制度缺口並提出改善建議，進一步強化內控體系的完整性與可持續性。最後，當稽核或風險

評估中發現問題時，透過議題管理（Issue Management）機制，可整合跨部門資源進行共同行動，從確認問題根本原因、指定負責單位、設定改善時程，到後續追蹤與議題關閉，建立完整的管理與回饋機制。

上述風險管理制度環環相扣，形成一套具前瞻性、即時反應與持續優化能力的風險控制框架，不僅提升了組織對內部與外部風險的應變能力，也進一步鞏固營運穩定性與法規遵循的治理基礎。

(二) 第一道與第三道防線之協作

在企業風險治理與內部控制體系中，稽核部門的角色至關重要，而「獨立評估」、「資訊共享」與「同意後實施行動」三項機制則共同構築了有效的稽核管理與風險回應流程。

首先，獨立評估（Independent Assessments）是稽核部門的核心職能，透過與業務部門保持適當距離，對第一線作業與控制流程進行客觀、公正的檢視，不僅能發掘潛在的風險與制度漏洞，也有助於評估既有控制措施的有效性與落實程度。其次，為了提升稽核工作的完整性與效率，企業推動資訊共享（Sharing Known Issues）制度，鼓勵各部門主動揭露已知的風險事件、操作缺口或控制不足，使稽核人員能更精準聚焦關鍵風險點，避免資源浪費，並強化內部的透明文化與信任機制。最後，當稽核作業完成後，將稽核發現轉化為實質改善，仰賴同意後實施行動（Implementation of Agreed-Upon Actions）的有效落實。此一機制強調由稽核單位與被稽核單位共同釐清問題、訂定可行的改善方案，並明確責任歸屬與執行時程，確保改善行動真正被執行並追蹤至完成。

這三項機制不僅強化了稽核工作的專業性與效能，也促進組織內風險意識的提升與制度化的持續改善，對於打造穩健、透明

且可持續的公司治理體系具有深遠意義。

(三)第二道與第三道防線之協作

在整體風險管理與內部監控體系中，建立跨部門協作與資訊整合的機制至關重要，其中「月度接觸」（Monthly Touchpoints）與「共享評估藍圖」（Share Assessment Roadmaps）兩項作法，有效促進風險管理工作的連貫性與資源配置的效率。

首先，透過月度接觸機制，風險管理部門與業務單位、稽核部門或其他相關部門能夠定期進行會議或交流，藉此同步最新的風險趨勢、監控指標與控制措施落實進展，並及時回應環境變化或新興風險議題。這種常態化的溝通機制不僅提升資訊透明度，也有助於建立部門間的信任與協作文化，進一步強化風險管理行動的整體一致性與時效性。其次，為提升稽核與風控工作的協調性，企業推動共享評估藍圖制度，即風險管理部門與內部稽核部門共同協調與整合年度工作計畫，明確界定各自責任範疇，避免重複稽核與資源浪費。透過計畫共享，雙方可更精準配置人力與時間資源，同時在發現重大議題時能快速形成合力，提升問題處理效率。

這兩項制度的落實不僅提升了風險管理流程的協同性與反應速度，也有助於打造一個系統性、主動性與高效率的風險治理架構。

四、效益與挑戰

(一)主要效益

在現代企業風險管理與內控體系中，跨部門協作與制度整合已成為提升治理效能的關鍵手段，透過系統化的合作機制，企業得以在風險識別、控制一致性與資源運用等層面取得顯著成效。首先，風險識別與回應更即時（Faster Risk Response），藉由建立跨部門的溝通與通報機制，能夠快速掌握潛在風險來源與異常徵

兆，並即時啟動風險應變措施，縮短從風險發生到處理的時間，進而有效降低風險對營運與聲譽的影響。其次，控制架構一致性提升（Consistency in Control Frameworks），透過整合各部門在流程管理、內部控制與監督上的標準與做法，不僅能避免重複作業與資源浪費，還可確保各單位遵循一致的制度與原則，強化整體組織在制度落實與稽核準備上的整合力。最後，資源有效分配（Optimized Resource Allocation）則透過資訊共享與職能協調，使企業能清楚掌握各項風控與稽核工作的重點與進度，避免資源重疊投入，讓人力、預算與時間等有限資源能更精準地用於高風險區域或策略性項目，提升整體風險管理的效益與策略對齊程度。

總體而言，這三項效益相輔相成，透過結構性合作與資訊透明，企業得以建構一套更靈敏、更一致、也更高效的風險治理架構，提升整體營運的穩定性與組織韌性。

(二)潛在挑戰

儘管跨部門協作在風險管理中能帶來高度的整合效益與執行力，但在實務推動過程中仍存在若干潛在挑戰，若未妥善處理，反而可能削弱制度運作的穩定性與效率。首先，角色混淆（Role Blurring）是一項常見問題，當多個部門共同參與風險識別、控制執行或應變決策時，若各自的職責、權限與責任界線不夠清晰，容易導致工作重疊、盲點或責任不明的情況發生，進而影響整體執行力與風險應對的連貫性。因此，必須透過明確的職責分工、標準作業流程以及持續的溝通協調來加以化解。其次，資訊管理壓力（Information Overload）亦是一大挑戰，隨著協作的擴大與資訊共享的頻繁進行，部門間流動的資料量大幅增加，若缺乏明確的資訊處理流程與過濾機制，將容易產生資料重複、錯誤遺漏或傳遞失真，進而造成決策延誤或風險判斷偏差，因此亟需建立一套有序的資訊管理架構，確保資料的準確性、即時性與可用性。

最後，部門信任建立不易（Trust Gap Between Lines）也是推動跨部門協作時不可忽視的隱性障礙，不同部門之間可能因文化背景、作業慣性或歷史經驗存在隔閡，若彼此缺乏理解與信任，將削弱協作的意願與效率。因此，除了制度設計外，更需要透過長期的互動、持續溝通與共同目標的凝聚，來強化彼此間的信任關係與合作默契。

雖然跨部門協作是提升風險管理品質與效率的關鍵策略，但也必須同步關注並積極管理其衍生的制度風險與執行挑戰，方能實現風險治理架構的真正落實與永續發展。

五、風險胃納與容忍度

在全球化與科技快速演進的今日世界，風險不再僅僅是一項應避免的負面因素，而是策略決策中不可或缺的一部分。組織若要達成其使命與目標，勢必需要在追求機會與控管風險之間取得平衡。風險胃納（Risk Appetite）與風險容忍度（Risk Tolerance）即協助組織理解、管理並最終承擔風險的兩項核心工具。

風險胃納指的是一個組織在實現策略目標的過程中，願意接受的風險總量與類型。它代表著高階管理層對於風險報酬的態度與哲學，是整體風險策略的核心。舉例而言，一家新創科技公司可能選擇高風險胃納，以快速進軍市場並測試創新產品；反觀一間監管嚴格的金融機構則可能採取較低風險胃納，避免觸犯法規或影響信譽。而風險容忍度則是更具體與操作化的定義，描述組織在特定目標或程序中，所能接受的波動範圍。例如，一家銀行可能設定其不良貸款率不得超過 2%，即為其信用風險的容忍度指標之一。此指標提供第一線管理人員與中層主管在執行過程中可依循的實際標準。這兩者雖性質不同，但卻密不可分。風險容忍度須在風險胃納的總體方向下運作，否則將導致執行上的矛盾或效率低落。

風險胃納的核心目的，並非僅在於限制風險或降低損失，而是協助組織在風險可控的情況下，有效實現策略與價值創造。它應作為引導業務發展的方針，而非設限工具。一套健全的風險承擔架構，能夠在組織內部建立共同理解，使成員清楚可接受的風險邊界，進而避免因認知落差造成資源錯置或責任不清。此外，它也為高層提供衡量風險與績效的依據，提升治理透明度與問責機制。藉由設立清晰的容忍指標，管理者得以即時監控與調整執行策略，增強組織的營運韌性。

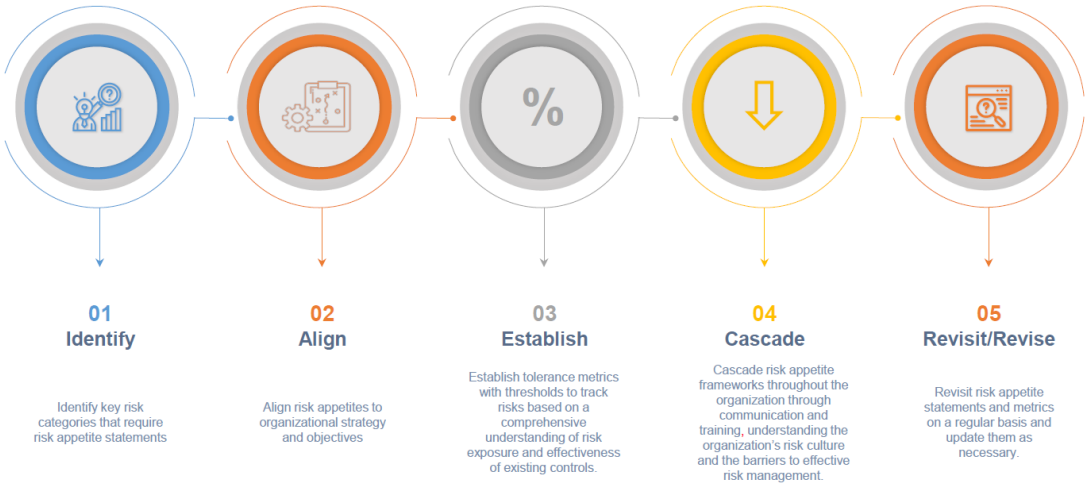


圖 2 FRBNY 風險胃納制度分為五個步驟

資料來源：研討會講義

風險胃納的制度化可依循五個步驟（圖 2）。首先，組織需針對自身營運特性辨識主要風險類別，例如法律、財務、營運與聲譽風險等。以跨國製藥公司為例，其面臨的關鍵風險包括藥品研發失敗、法規變動及產品召回。接下來，風險胃納須與策略目標緊密結合，確保風險偏好與組織使命及中長期發展方向一致。第三步是設定具體、可量化的風險容忍指標，並與關鍵績效指標 Key Performance Indicators，KPI）連結，例如某國有銀行即針對詐騙風險設定異常事件比例上限，超出則自動觸發稽核程序。第四，透過內部溝通與訓練將風險管理理念向下傳遞，藉由政策修訂、工作坊與模擬演練，促使風險語言成為各部門共通語彙。最後，

組織須定期檢視風險聲明與容忍標準，隨著市場變化與內部條件調整制度內容，以維持風險管理架構的彈性與應變能力。

風險胃納制度能否落實，關鍵在於風險文化的成熟度。風險文化反映的是組織整體對風險的態度、價值觀與行為模式。當風險被視為可辨識、可管理且具潛在價值的資產時，組織能更主動掌握機會與應對挑戰。強化風險文化可從高階主管的示範帶頭、明確的獎懲制度、將風險納入績效考核，以及推動跨部門訓練與溝通著手。根據普華永道（PricewaterhouseCoopers，PwC）的研究，擁有高度風險文化成熟度的金融業者，其營收成長率平均高出同業 16%，顯示文化建設對組織績效具有明確助益。

儘管風險胃納制度具備策略價值，但在實務導入上仍有挑戰。數據取得不足常使風險暴露與控管效果難以量化，造成容忍指標難以精準設計；部門間協調不易也導致風險觀點與業務績效目標產生落差。加上風險文化多需長時間培養，在傳統產業尤為明顯。針對上述困難，組織可循序漸進地引入專業風險顧問、發展視覺化分析工具，並設立跨部門風險小組，在具代表性的重大專案中先行試點，以建立制度基礎並推動文化落地。

六、FRBNY 實務經驗與成效

FRBNY 的實務經驗顯示，跨部門協作對提升風險管理效能至關重要，其透過制度化會議、共享計畫與公司治理、風險管理及法規遵循（Governance, Risk and Compliance，GRC）平台進行稽核追蹤，成功平衡了監督獨立性與執行效率。為解決常見協作挑戰，企業應從三方面著手：一是制度化協作流程，透過政策明確劃分角色與責任，並設立監督與評估機制；二是善用科技工具，如 GRC 平台整合風險資料與追蹤行動，提升資訊共享的即時性與透明度；三是建立跨線文化，透過聯合訓練與部門輪調，增進信任與理解，促進跨部門凝聚力。這些策略相互補強，能有效強

化「三道防線」架構的整合運作，並提升風險監督的精準度與回應速度。未來金融機構應持續朝向制度化、科技化與文化整合發展，實現協作導向的風險管理模式，確保組織長期穩定運行。

參. 人工智慧與風險管理

在當代數位轉型的浪潮下，人工智慧（Artificial Intelligence，AI）逐漸滲透到金融體系的各個角落，並在資料處理、預測模型與決策支持等領域中發揮關鍵作用。尤其對中央銀行這類具系統性風險監管職責的機構而言，AI 的應用不僅有助於提升效率，更可能改變傳統的風險管理方式。然而，同時伴隨著一系列技術性與治理層面的挑戰，包括模型不透明性、資料偏誤、決策責任歸屬問題等。在此背景下，結合 2025 年由 BIS 風險管理顧問小組（Consultative Group on Risk Management）所發表的報告，以及 FRBNY 等先進實務經驗，進行多面向的議題式分析，探討 AI 在央行風險管理中的發展背景、應用實例、模型風險、治理挑戰及未來應用策略，並試圖描繪出「風險為本」的 AI 發展藍圖，協助金融監理機構在創新與穩定間取得平衡。

一、人工智慧在風險管理中的興起與發展背景

人工智慧的核心能力包括模式辨識、機器學習與自然語言處理等，這些技術最早被應用於商業數據分析與推薦系統中。近年隨著運算能力的提升與大數據的普及，AI 在金融產業中的應用亦日益廣泛。尤其在 2008 年金融危機後，市場對於更早期、精準的風險預警機制需求上升，進一步推動了 AI 在監管科技（Regulatory technology，RegTech）與風險控管上的發展。

在中央銀行層級，AI 的角色不再限於輔助性工具，而逐漸轉化為系統性分析的核心技術之一。舉例來說，許多央行開始使用 AI 技術進行系統性風險識別、宏觀經濟預測、支付系統異常監測等任務。這不僅改善了資訊流通速度，也有助於提升政策制定的

即時性與準確性。

此外，生成式 AI（如大型語言模型）更為風險治理帶來全新契機。過去由人工撰寫的風險政策文件，現可透過 AI 草擬初稿，節省大量時間並確保語言一致性，進而提升風險文化的傳遞效果。

二、FRBNY 導入 AI 的應用實例

FRBNY 在 AI 的應用上呈現多樣化趨勢，選取三類具有代表性的案例進行說明。

首先，在「異常偵測」領域，FRBNY 的抵押品估值模型中導入了孤立森林演算法[1]與分群技術，藉此辨識貸款抵押品中價格偏離常態的情形。透過 AI 輔助的模型，分析人員能更快速地鎖定潛在問題資產並進行後續調整，有效強化整體金融安全網的穩定性。

其次，在「經濟預測」方面，AI 被用於 GDP 即時預測與通膨走勢分析。相較傳統模型，AI 能更靈活處理非結構化數據（如新聞、社群媒體、央行聲明等），大幅提升預測的靈敏度與準確率。

最後，生成式 AI 則應用於「風險治理文件與溝通」上。透過大語言模型，FRBNY 的風險管理團隊能快速產出與產業標準一致的風險治理草案，或針對內部培訓、FAQ 與案例研究建立互動式教材，進而深化員工的風險文化認知。

三、AI 風險管理挑戰與模型風險

雖然 AI 技術為風險管理帶來諸多優勢，但同時也產生新的風險形式。其中最主要的是「模型風險」（Model Risk），即模型的輸出結果可能與實際情況偏離，並進一步導致錯誤決策。

AI 模型的高度複雜性、資料依賴性與黑箱特性，使得其驗證難度遠高於傳統統計模型。現行如 SR11-7[2]等風險管理框架提供

[1] 孤立森林演算法(Isolation Forest)：是一種非監督式異常偵測演算法，透過隨機選取特徵並切分資料，建立樹狀結構。異常值較容易被孤立，因此在樹中的深度通常較淺，演算法即透過平均分割深度來判斷資料點是否異常。

[2] SR11-7 是美國聯邦準備系統與貨幣監理署共同發布的模型風險管理指導原則，旨在協助銀行機構有效管理其使用量化模型帶來的風險，特別是在金融決策過程中可能出現的錯誤或誤用情況。

初步的指導，但在實際運用上仍面臨以下挑戰：模型定義與分類不明確，導致治理流程不一致；缺乏針對 AI 的驗證指標與門檻；人機協作角色模糊，影響問責機制。

此外，AI 模型的更新與維護也需耗費大量資源。每次重新訓練、變更參數或轉移平台，都可能產生新的誤差或漏洞，甚至觸發潛藏的系統性風險。因此，建立一套持續監控、跨部門合作且可回溯的 AI 模型生命週期管理機制，是當前中央銀行面臨的重要任務。

四、AI 治理與風險框架建構

根據 2025 年 BIS 風險管理顧問小組報告，各國央行應共同建立一套以「可信賴性、透明性與責任性」為核心的 AI 治理框架。該框架主要建議包含：建立 AI 政策準則與應用門檻、釐清模型責任歸屬與人為介入權限及導入產業最佳實務如 COSO ERM[3]進行風險對照分析。

並強調「結構性對照分析」的重要性，即在 AI 導入後，組織應系統性地比對現行風險管理架構與 AI 應用後的流程差異，並據以調整內部治理政策。舉例而言，若 AI 模型決策無法被充分解釋，則不應用於高敏感度的金融監理行動中，否則將衍生監管風險與信任危機。

治理框架的成功推動還需仰賴跨部門合作，包括科技部門、風險管理部門與法規遵循部門共同參與治理流程設計，確保每一項 AI 應用符合道德規範、數據保護法規與公共利益原則。

五、風險導向的 AI 應用之道

人工智慧已無可避免地成為金融風險管理的重要工具。對各國央行而言，如何在發揮 AI 效益的同時，有效控管其風險，成為

[3] COSO ERM（Committee of Sponsoring Organizations of the Treadway Commission 提出的 Enterprise Risk Management）：是全球廣泛使用的企業風險管理標準之一，協助組織識別、評估、管理並監控風險以實現目標。2017 年發佈新版，強調風險管理與企業策略和績效的整合。

當前治理改革的核心挑戰。FRBNY 認為未來 AI 風險管理的關鍵方向應包括：

(一) 建立「風險為本」的 AI 應用策略，優先導入於低風險與高資訊透明度領域；

(二) 強化模型驗證與監控能量，提升模型生命週期的可控性；

(三) 培養跨部門風險意識，讓科技與風險治理對話常態化；

(四) 推動國際監理機構合作，制定 AI 風險共通標準與監理沙盒機制。

總結而言，人工智慧的發展固然迅速，但其應用於風險管理時，必須更為謹慎與周延。唯有如此，方能在保障金融穩定的同時，開發 AI 技術的最大潛能。

肆. 資訊安全治理與關鍵風險指標體系

隨著資訊科技高度發展與全球營運環境日益複雜，企業面對的風險型態與衝擊程度亦顯著提升。企業韌性（Enterprise Resilience）與資安治理（Cybersecurity Governance）因此成為組織治理的重要支柱。透過 FRBNY 實務經驗案例，探討企業如何透過制度化的韌性策略與資安治理架構，提升對營運中斷、網路攻擊、內部威脅等風險的預防與應變能力。結合策略性預警機制、關鍵風險指標（Key risk indicators，KRI）、治理協議與領導行為的協調，可有效提升組織在動盪環境中的存續力與競爭優勢。

現代企業面臨的挑戰不再僅限於市場競爭或資源配置問題，更必須應對來自外部環境如自然災害、疫情爆發、地緣政治、以及最具潛藏威脅的資安風險。根據世界經濟論壇（The World Economic Forum，WEF）發布的全球風險報告，資安事件已成為企業最關切的長期風險之一。為了提升整體抗風險能力，企業須建構橫跨人員、流程、技術與策略的綜合防禦體系，即所謂的「企業韌性」。

以下說明企業韌性與資安治理如何互為補充，並建構一套可

衡量、可追蹤、可改進的風險管理機制，提供具體指標與實務策略，以協助企業在動態風險環境中持續運作與成長。

一、企業韌性的概念與構成及資安治理架構與發展趨勢

企業韌性可視為企業在面對危機或干擾時，所具備的預警、承受、復原與調適等四大能力。其核心不僅是災後復原，更在於災前預防與持續改善。

資安治理是一套橫跨組織治理、策略規劃、風險評估與資源配置的整合性框架，其目的在於保護資訊資產不受外部入侵與內部濫用。有效的資安治理需涵蓋政策制定、執行標準、關鍵績效指標、關鍵風險指標、以及高階管理層參與的決策流程。

在資訊安全領域，FRBNY 建構了涵蓋技術、資料、營運、人員與供應商的多層資安防護機制。其核心為四大資安韌性能力（Cyber Resilience Capabilities）：

(一)預警（Anticipate）：

此階段強調情報收集與風險預測，組織須建構早期預警機制，包括資安監控系統、威脅情報平台（Threat Intelligence）、以及情境模擬（Scenario Planning），以便提前偵測異常事件並部署資源。

(二)承受（Withstand）：

在風險發生時，組織必須具備持續營運能力（Business Continuity Capability），此包括關鍵任務系統之備援機制、資料備份策略、與第三方風險管理制度，以確保營運不中斷。

(三)復原（Recover）：

復原階段的重點在於災後快速重啟營運功能，縮短停機時間。透過事件回應流程、災後檢討與改進計畫，組織可從每次危機中提煉經驗、優化流程。

(四)調適（Adapt）：

調適意指透過組織學習與制度演化回應內外部變化。此過程

包含風險評估重整、政策更新、與人員訓練等，目的是使組織具有自我修復與成長能力。

二、資安治理的實務構面與指標設計

在企業韌性逐漸被納入組織核心戰略架構的當下，資安治理成為支撐整體韌性能力的關鍵支柱。治理的實施不應僅停留在政策層面，而必須延伸至具體制度、流程、指標與行動層級，才能真正對抗日益複雜且多變的網路威脅。

(一)資安治理框架的採用與調適

資安治理的基礎是建立在成熟的治理框架上，常見的國際標準包括：

1. NIST 網路安全框架（National Institute of Standards and Technology Cybersecurity Framework，NIST CSF）：由美國國家標準與技術研究院[4]（National Institute of Standards and Technology）制定，其核心由治理、識別、保護、偵測、回應、與恢復六大功能構成。
2. ISO/IEC 27001 資訊安全管理標準（Information Security Management System, ISMS）：為全球廣泛應用的資訊安全管理制度，其強調風險導向與持續改善。
3. COBIT（Control Objectives for Information and Related Technologies）：側重於資訊科技治理與控制領域，強調企業整體資訊科技治理結構的對齊性與監督。

組織在導入上述任一架構時，應評估其適用性，並針對自身業務特性與營運模式進行調整與細化。例如，FRBNY 選擇以 NIST CSF 為主架構，並搭配自身金融監理角色與高敏感度系統需求，加強第三方供應商管理（Third-Party Risk Management）與特權存取控制（Privileged Access Control）機制。

[4] 美國國家標準與技術研究院（National Institute of Standards and Technology，NIST）：是美國聯邦政府的一個機構成立於 1901 年，其核心職責是制定和推動測量、標準與技術創新，以提升美國的經濟安全與產業競爭力。

(二)資安營運的關鍵構面與能力成熟

FRBNY 實務顯示，資安治理需涵蓋實務構面（Operational Domains），各領域相輔相成，構成全面性的防禦體系：

1. 身份與存取管理（Identity and Access Management，IAM）：掌握誰有權限存取哪些系統或資料，是防止內部濫權與外部滲透的核心機制。
2. 弱點管理（Vulnerability Management）：對所有系統與應用進行定期掃描與漏洞修補，是資安營運成熟度的基本指標。
3. 事件回應（Incident Response, IR）：建立快速應變機制、通報程序、與事故後的分析與報告。
4. 內部風險管理（Insider Risk Management）：識別因疏忽、惡意或誤用行為而導致的內部風險，常結合行為分析（Behavioral Analytics）與稽核追蹤（Audit Logging）。
5. 資料保護與加密（Data Protection and Encryption）：涵蓋資料傳輸、儲存與備份過程的全方位保護。
6. 特權存取管理（Privileged Access Management）：嚴格控管對敏感系統的管理性權限，避免不當存取。
7. 供應鏈風險管理（Third-Party and Supply Chain Risk Management）：對外部合作廠商實施資安條件要求與審查，確保系統整體韌性。
8. 安全監控（Security Monitoring）與分析：部署持續性監控工具，如安全資訊與事件管理系統（Security Information and Event Management，SIEM）與端點偵測與回應系統（Endpoint Detection and Response，EDR），可即時掌握威脅、快速應變，並執行主動威脅獵捕（Threat Hunting），強化整體資安防護。

上述每一項構面皆可設計對應的指標與度量方式，成為組織持續改進（Continuous Improvement）的依據。

(三)指標設計：風險與績效的整合導向

資安治理若欲落實到實務層面，必須透過可衡量、可追蹤、可改善的指標體系予以監控與引導。此體系主要分為兩大類：

1. 關鍵績效指標（Key Performance Indicators, KPI）

KPI 主要衡量治理執行層面的效率與效能，例如：身份與存取管理（IAM）帳戶建立與刪除作業平均完成時間、系統更新後漏洞修補完成率、事件處理時間中位數、員工資安訓練完成率，及這些數據可用以評估治理機制的運作品質，並向管理階層回報執行成效。

2. 關鍵風險指標（Key Risk Indicators, KRI）

KRI 則關注風險本身之變動趨勢，具預警功能，常見指標包括：外部釣魚郵件點擊率、特權帳戶未使用超過 30 日比例、攻擊事件未於預期時限內回應之比例、未完成第三方資安審查的供應商占比、空密碼保管庫（Empty Password Vaults）數量，及漏洞未於規定天數內修補之比例（例如高風險漏洞 14 天內未修補）

這些指標多以「容忍區間（Tolerance Range）」方式呈現，若超出容忍範圍，即需啟動調查與改善行動。

(四)關聯指標與治理決策之互動

為發揮指標之治理效能，各項指標須與組織風險容忍度（Risk Appetite）連結，並嵌入治理決策流程中。，在 FRBNY 的應用中，每季彙整指標報告交由資安風險討論小組（Cyber Risk Discussion Group, CRDG）審議，若有指標長期超標，則需逐項進行：成因分析（Root Cause Analysis）、風險說明與補救建議（Risk Remediation Plan），及提升資源或修訂政策之提案（Policy or Resource Escalation）。並強調由各領域「召集者」（Conveners）與「參與者」（Participants）形成共識，再由「決策者」（Deciders）拍板定案。此決策紀錄皆需書面化存檔，作為未來事後審查依據。

(五)指標設計原則

一個成功的資安指標系統，應符合以下原則：

1.關聯性（Relevance）：與組織核心資產與風險緊密連結。

2.可衡量性（Measurability）：資料可取得，指標易於解釋與分析。

3.可行性（Actionability）：能驅動具體改善行動。

4.可理解性（Clarity）：能被高階主管與非技術人員理解與採納。

5.動態調整性(Adaptability)：能隨風險變動或策略改變調整容忍門檻。

三、FRBNY 案例分析：資安治理與韌性實踐

FRBNY 作為美國金融體系的樞紐，其資訊系統與數據資產面臨高度敏感與高攻擊價值（High-Value Targets）。在資訊安全與營運持續性的雙重壓力下，其資安治理與韌性實務展現高度制度化與可衡量性。以下從風險觀測、報告機制、與情境模擬三大面向進行分析。

(一)風險觀測機制與指標趨勢

FRBNY 建立了多項風險容忍指標（Risk Tolerance Indicators），每季針對各治理構面執行監控並呈報結果。例如，在 2024 年第四季（Q4 2024）：所有 37 項風險指標中，有 10 項超出容忍範圍（Out of Tolerance）；多數超標指標集中於事件回應（Incident Response, IR）、身份管理（IAM）、弱點管理（Vulnerability Management, VM），這些結果促使單位立即採取補救行動（Remediation Activities），如提高修補效率、加強裝置加密、移除無效特權帳戶等。

(二)報告與決策支持機制

針對監控結果，資訊安全團隊會製作「資安治理執行摘要報告」（Cybersecurity Governance Executive Summary），交由治理會議（Cyber Governance Forum）審議。報告內容包括：指標趨勢圖（Trend Charts of KRI and KPI）、趨勢異常說明（Anomaly Justifications）、預期風險預測（Anticipated Risk Forecast），及改善計畫摘要（Remediation Summary）。決策者依據報告所揭示之風險

態勢（Risk Landscape），決定是否啟動進一步資源調度、政策修訂或人員訓練計畫。

(三)資安情境模擬與預測分析

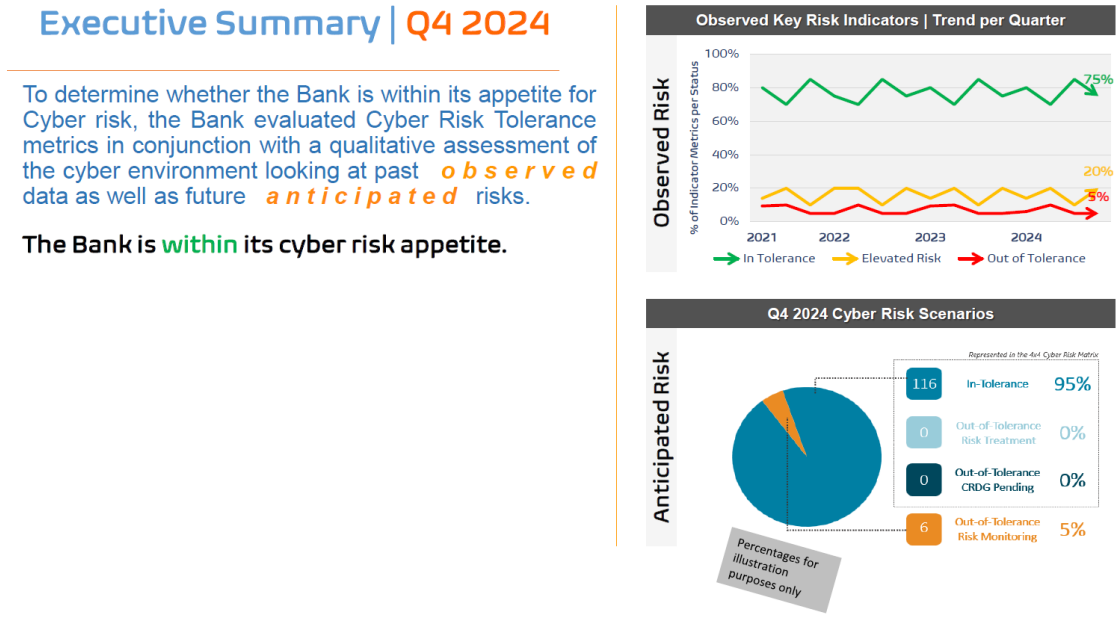


圖 3 FRBNY2024 年 Q4 預警模型

資料來源：研討會講義

FRBNY 建構了一套結合威脅情報（Threat Intelligence）與資安情境模擬（Cyber Risk Scenario Simulation）的預警模型。在 2024 年 Q4 期間，模擬揭示：勒索軟體（Ransomware）攻擊行為日益精緻，攻擊者善於迴避偵測、惡意 AI 工具（Malicious AI Tools）之濫用快速擴散，及有攻擊者聲稱竊得銀行資料，實際為誤導行為（False Flag）。透過這些模擬，可提前調整風險評估與應變策略，並與供應商同步提升防禦機制。

四、治理模式與領導行為：從個人決策到集體治理

(一)網狀治理架構（Distributed and Networked Governance）

FRBNY 導入一套網狀治理模式[5]，重點在於：所有資安風險決策須透過「資安風險討論小組」（Cyber Risk Discussion Group,

[5]網狀治理模式（Distributed Governance Model）：是一種非等級化、去中心化的治理架構，常見於多方協作、生態系統管理和跨部門合作中。這種治理模式常用於現代公共政策制定、區塊鏈組織管理、城市治理等領域。

CRDG）形成共識；決策參與角色分為召集者、參與者、決策者；所有成員必須明確表態（Explicit Concurrence），不得沉默代表同意。此一制度避免傳統治理中由單一主管拍板所造成的風險落差與責任模糊問題。

(二)領導行為與決策文化（Required Leadership Behaviors and Governance Culture）

成功的資安治理離不開領導層的主動參與與責任承擔。FRBNY 明文規定高階領導者必須：積極參與風險會議、不得獨斷決策、若不同意，必須提出強制升級機制[6]，及對所有決策過程進行紀錄（Documented Decision Trail）。這些行為要求建構了一種「決策即責任」（Decide and Own）的治理文化，有助於形成可追溯、具問責力的治理系統。

五、當前挑戰與改善建議

儘管各國央行已具備高度成熟的治理制度，但在快速變動的資安環境中，仍面臨多重挑戰，例如：

(一)第三方風險控管困難：外部供應商不易全面受控，成為資安攻擊破口。

(二)人力資源有限：具備資安專業且熟悉監理金融背景的人才稀少。

(三)威脅態樣變化快速：AI 與社交工程攻擊日益難以預測。

(四)指標與策略整合困難：部門間可能出現目標偏差與指標爭議等困難。

FRBNY 亦對此提出幾點改善建議：

(一)建置第三方資安履歷平台：供所有單位即時查詢外部單位風險歷史。

(二)強化紅隊演練與模擬測試：提升資安事件應變成熟度。

(三)導入 AI 威脅分析系統：即時預測與識別未知攻擊樣態。

(四)推動 KRI/KPI 制度化：將指標納入年度目標與預算審查流程。

[6] 強制升級機制（Mandatory Escalation）：指的是在處理某個問題或事件時，如果在預定時間內未獲妥善解決，系統或組織將依照既定規則，自動將事件提交（升級）給更高層級的負責人或部門，以確保問題獲得更快或更有力的處理。

伍. 內部稽核在計畫管理中的策略角色

在金融體系日益複雜化與科技快速演進的背景下，內部稽核不僅扮演著監督與查核的角色，更是企業治理、風險管理與內部控制三大支柱的重要一環。對於中央銀行及其他金融機構而言，有效的稽核流程能夠確保制度運作的合規性與透明性，同時強化組織對潛在風險的應對能力。涵蓋從稽核關係模型、風險評估程序，到即時整合稽核計畫的實施與具體操作細節。以下為 FRBNY 提升整體稽核效能與治理品質所使用之稽核規劃與執行框架。

一、稽核關係與聯絡模式

稽核工作的有效性，在很大程度上依賴於稽核部門與被稽核單位之間良好的溝通與協作。為了提升協同效率與信息透明度，聯絡模型（Liaison Model）成為稽核流程中的關鍵結構之一。

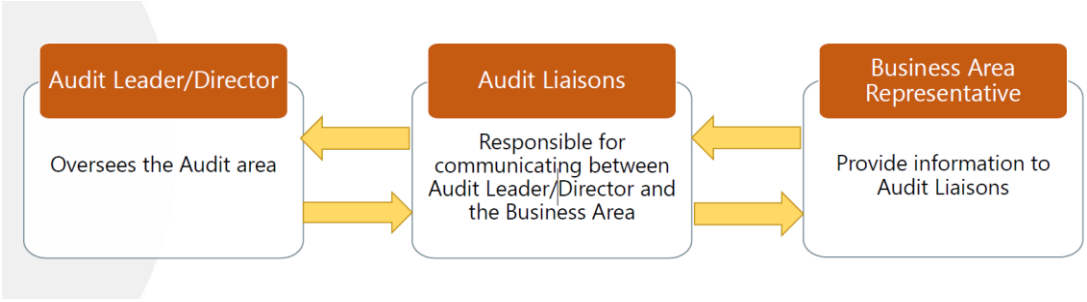


圖 4 FRBNY 聯絡模型（Liaison Model）

資料來源：研討會講義

圖 4 模型的核心在於建立「稽核聯絡人」（Audit Liaison）制度，使得稽核人員與業務部門之間能夠建立穩定的聯絡管道。每一個可稽核的實體（Auditable Entity）通常會指派一位主要聯絡人（Primary Liaison）與若干支援聯絡人（Supporting Liaisons），以確保稽核相關事宜能夠準確傳達並即時回應。

在資訊科技部門（Information Technology Department，簡稱 IT）方面，也設有類似的聯絡機制。IT 稽核主管（IT Audit Leader）負責主導技術面的稽核，並與 IT 部門主要聯絡人密切合作，以整合營運與技術層面的控制環節。這種橫跨多部門的協作模式，有助

於稽核部門在整體性上獲得更全面的資料支持與風險評估依據。

聯絡活動不僅限於稽核期間，是常態性進行，透過定期會議、協作平台與報告機制，維持長期資訊對稱。其最大優勢在於能夠讓稽核部門提前掌握潛在風險、理解業務變化，並減少冗餘的重複稽核工作，進而提升效率與價值。

總體而言，聯絡模型不僅是一種溝通機制，更是一套制度性的安排，其目的在於將稽核職能嵌入組織運作流程中，從而強化其顧問式角色與前瞻性價值。

二、風險評估機制

風險評估（Risk Assessment）是稽核規劃中不可或缺的環節，其目的在於識別與分析可能對組織目標產生負面影響的潛在風險，並依此決定稽核資源的分配與稽查頻率。透過系統性與週期性的評估作業，稽核部門能夠確保其工作聚焦於最具風險性與關鍵性的業務領域。

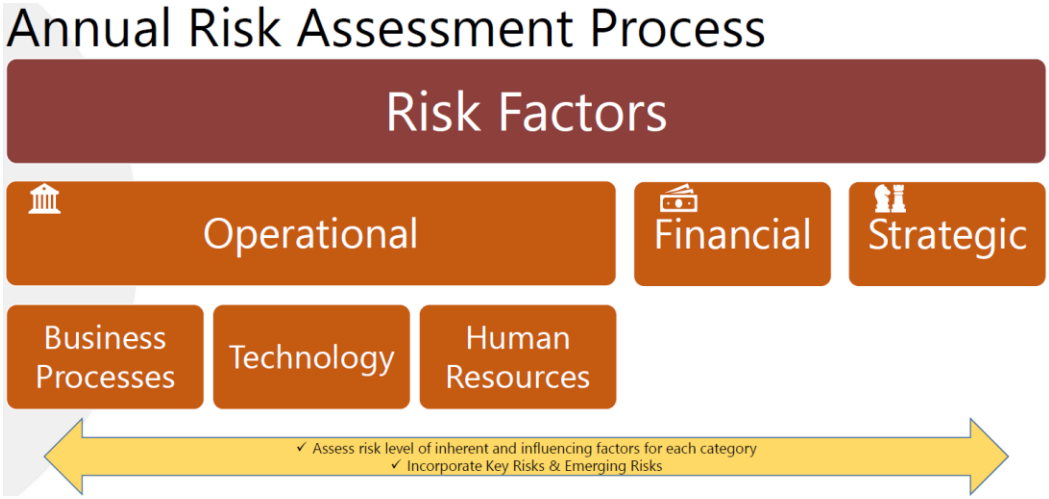


圖 5 FRBNY 年度風險評估過程

資料來源：研討會講義

在實務操作上，風險評估通常以年度為單位進行，並針對各可稽核實體進行風險分級。評估涵蓋多個面向，包括營運風險（Operational Risk）、財務風險（Financial Risk）與策略風險（Strategic Risk）等三大類別，並進一步依據業務流程、科技應用、

人力資源狀況、治理結構及外部法規要求等因素，進行綜合判斷。

其中，營運風險強調業務流程本身的風險性，如作業複雜度、關鍵性與法遵風險；財務風險則包含財務報表失真、流動性與市場風險等考量，而策略風險則涵蓋目標錯配與治理架構薄弱等潛在問題。科技應用則關注資訊系統的穩定性與自動化程度；人力資源狀況則與組織架構、職責明確度與員工能力培訓等相關。

風險評估程序的實施，通常由內部規劃小組主導，先進行內部會議收集資訊，並結合歷年稽核紀錄與外部風險趨勢，形塑整體風險輪廓。評估結果會產出風險等級（如高風險、中高風險、中等風險等），以作為決定年度稽核計畫的依據。

此程序不僅有助於稽核部門制定優先順序，也強化其與整體組織策略的一致性。更重要的是，透過納入相關風險的分析，稽核部門能及早調整方向與方法，強化稽核工作的預防性與前瞻性。

三、即時整合性稽核

即時整合性稽核（Point-In-Time/Integrated Audit）是一種結合特定時點觀察與橫向整合稽核的方法，目的是在限定時間內，同步檢視業務流程與資訊科技兩大面向的風險與控制狀況。這種稽核方法反映出現代組織面臨的高度複雜性與數位依賴性，並強調稽核過程的及時性與全面性。

即時稽核著重於在明確界定的期間內，對特定流程、控制或活動進行深入檢視。這與傳統以年度或季度為單位的定期稽核不同，更適用於需要快速反應或高度變動的作業環境。而整合性稽核則進一步結合營運與技術兩方面的稽核，透過跨部門合作，評估流程中控制設計的完整性與執行的有效性。

在操作層面，即時整合性稽核通常從風險導向出發，依據年度風險評估結果選定審查對象，並由稽核團隊與 IT 稽核人員共同制定稽核計畫。稽核內容不僅涵蓋手動與自動化流程，也包含資

料管理、資訊安全、系統設定與應用邏輯等項目。此種稽核形式特別適用於如付款處理、資料傳輸、資訊安全稽核等高度仰賴技術的作業環節。

這類稽核安排在一年內的任意時間點展開，而非固定於特定時段，有利於稽核單位根據實際情況彈性調整資源配置，提升稽核回應速度與效果。其同時也能揭露業務與技術間潛在的落差與風險交集，使稽核結果更具整體性與實務參考價值。

即時整合性稽核反映了現代稽核向顧問角色演進的趨勢，不僅止於問題揭示，更重視流程優化與控制設計的改善建議。因此，其執行品質與跨部門合作深度，已成為衡量稽核效能的重要指標之一。

四、稽核流程各階段

稽核流程的設計目的在於確保稽核工作能夠系統化、有效率地推進，並產出具洞察力與建設性的結果。整體流程可分為三個主要階段：規劃（Planning）、實地作業（Fieldwork）與報告（Reporting）。

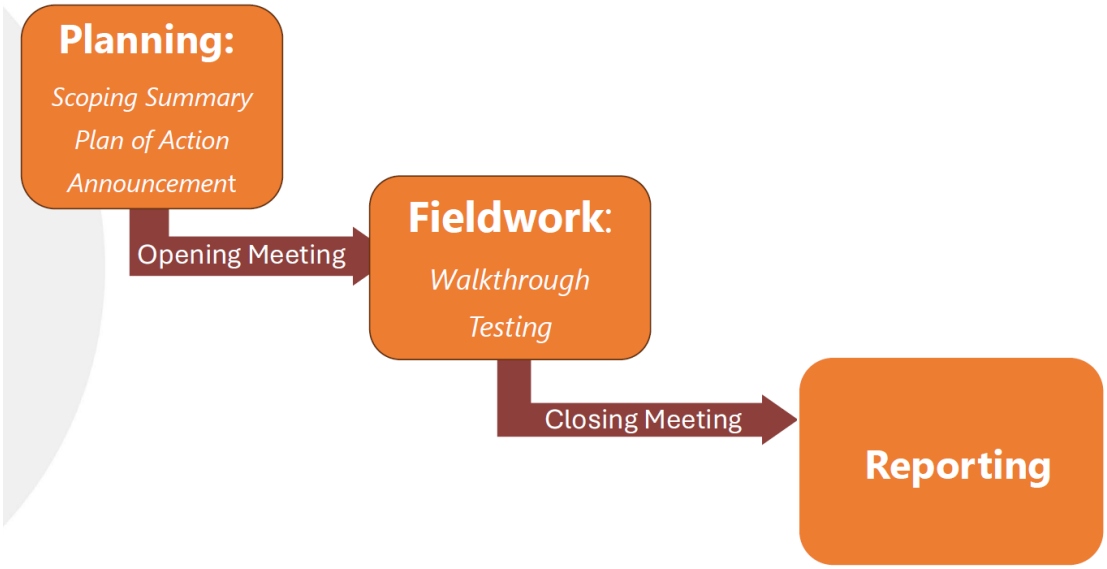
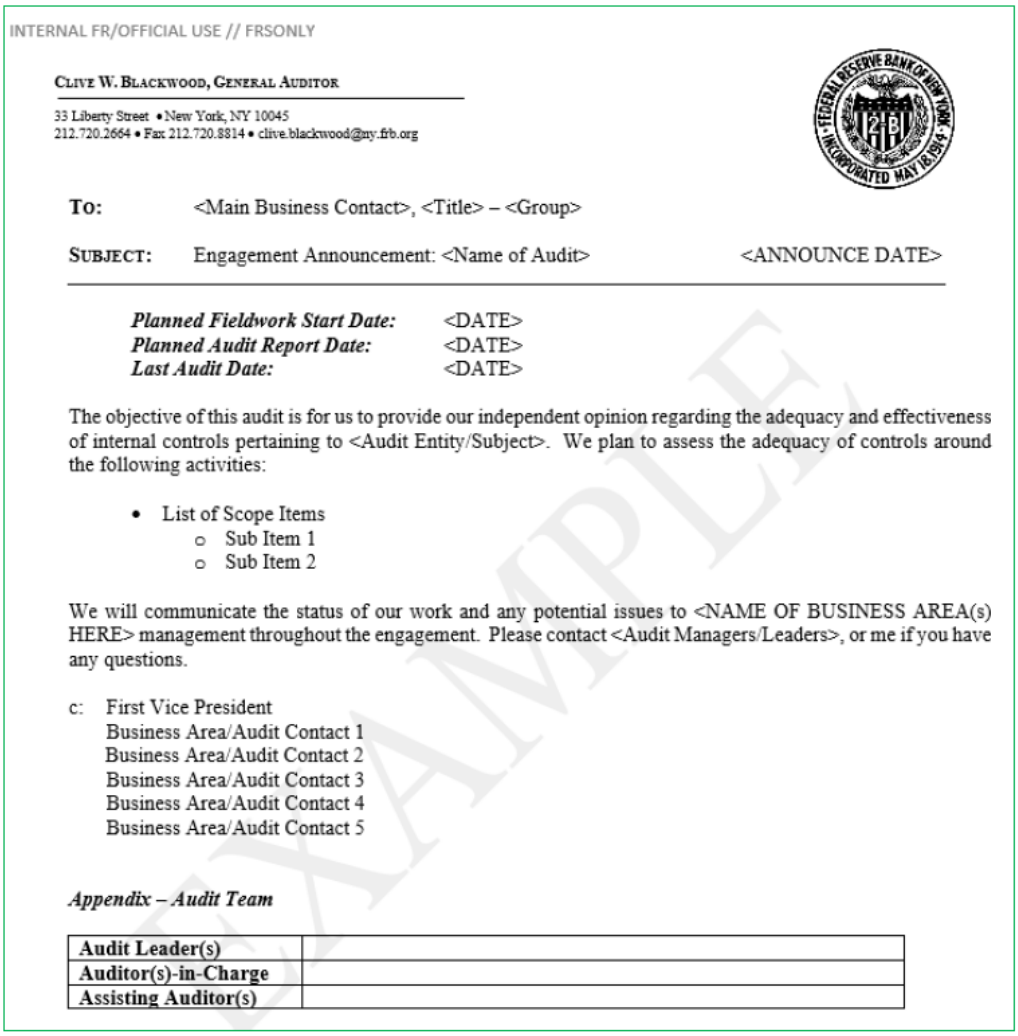


圖 6 FRBNY 稽核流程三階段

資料來源：研討會講義

在規劃階段，稽核團隊會先進行範疇界定（Scoping Summary），釐清稽核目標、重點風險區域與關鍵控制點。這一過程需要參考過往稽核紀錄、當前營運背景、風險等級以及受查單位的組織與系統架構。稽核計畫書（Plan of Action）在此階段成形，並透過正式的稽核聲明（Audit Announcement）通知受查部門。



INTERNAL FR/OFFICIAL USE // FRSONLY

CLIVE W. BLACKWOOD, GENERAL AUDITOR

33 Liberty Street • New York, NY 10045
212.720.2664 • Fax 212.720.8814 • clive.blackwood@ny.frb.org

TO: <Main Business Contact>, <Title> – <Group>

SUBJECT: Engagement Announcement: <Name of Audit> <ANNOUNCE DATE>

Planned Fieldwork Start Date: <DATE>
Planned Audit Report Date: <DATE>
Last Audit Date: <DATE>

The objective of this audit is for us to provide our independent opinion regarding the adequacy and effectiveness of internal controls pertaining to <Audit Entity/Subject>. We plan to assess the adequacy of controls around the following activities:

- List of Scope Items
  - Sub Item 1
  - Sub Item 2

We will communicate the status of our work and any potential issues to <NAME OF BUSINESS AREA(s) HERE> management throughout the engagement. Please contact <Audit Managers/Leaders>, or me if you have any questions.

c: First Vice President
Business Area/Audit Contact 1
Business Area/Audit Contact 2
Business Area/Audit Contact 3
Business Area/Audit Contact 4
Business Area/Audit Contact 5

Appendix – Audit Team

Audit Leader(s)	
Auditor(s)-in-Charge	
Assisting Auditor(s)	

EXAMPLE

圖 7 FRBNY 稽核聲明範本

資料來源：研討會講義

實地作業階段始於開場會議（Opening Meeting），此會議的目的是與被查單位建立共識，說明稽核目的、範圍、方法與時間表。在會議後，稽核人員會進行作業流程的走查（Walkthrough），以確認流程設計是否合理，控制措施是否存在。接續進行的測試則是為了驗證控制措施實際執行的有效性與一致性。整個過程中，稽

核團隊與管理階層持續保持溝通，以即時澄清資訊與修正理解。

最終階段為報告階段。稽核團隊根據實地作業所得資訊，整理出稽核發現與建議，並撰寫正式報告。此階段亦包括結束會議（Closing Meeting），在會議中向管理階層說明主要問題、控制缺失與風險等級，並討論改善計畫。報告中會註明各項問題的嚴重程度與潛在影響，提供受審部門作為後續改進的依據。

整體而言，稽核流程的每一階段都強調透明溝通與風險導向，並透過制度化的操作程序，確保稽核工作具備一致性、可追溯性與專業性。此種標準化流程不僅提升稽核效率，也加強其在組織治理中的影響力。

五、稽核角色與溝通機制

有效的稽核工作不僅取決於技術方法與流程設計，更需仰賴清晰的角色劃分與暢通的溝通機制。稽核部門的專業角色，在當代企業與公共機構治理架構中已日益從監察者轉型為顧問與風險管理的夥伴，這也促使溝通方式的演進與組織文化的調整。

在角色劃分方面，稽核團隊內部通常由稽核主管（Audit Leader/Director）負責主導整體工作，並協調各項資源與決策；聯絡人（Audit Liaison）則是稽核與業務部門之間的橋梁，負責日常溝通、資訊提供與進度追蹤。在科技層面，IT 稽核主管與 IT 聯絡人承擔相似的溝通與技術分析職責，確保資訊科技相關控制得以正確評估。

溝通機制的設計強調常態性與制度性。稽核團隊與受審部門定期舉行會議，並使用協作工具（Collaboration Tools）進行文件交換與任務協調。這些會議不僅限於正式的開場與結束會議，還包括過程中的工作會議與問題澄清會議。透過持續對話，雙方可就稽核進度、初步發現、控制效果與潛在風險保持一致理解。

為了制度化這些交流，稽核部門也開發出會議記錄模板

（Meeting Notes Template），藉由標準格式記錄會議摘要、責任歸屬與後續行動，提升整體透明度與可追溯性。此舉對於後續的問題追蹤與改善建議執行亦具關鍵作用。

這樣的溝通安排不僅提升了稽核效率，更進一步增強了部門之間的信任與合作關係，使稽核能夠從傳統的查核角色，逐漸轉型為具有洞察與策略性建議功能的業務夥伴，並在組織治理中發揮長遠影響。

六、案例分析與年度稽核計畫

為了強化風險導向的稽核策略，FRBNY 稽核部門會依據風險評估結果制定年度稽核計畫（Annual Audit Plan）。此一計畫並非靜態的文件，而是一套依循風險變動與業務優先順序而動態調整的稽核藍圖。於 2025 年稽核計畫，稽核部門預計執行 30 項稽核任務，以及 21 項計畫管理檢討(Program Management Reviews)，顯示其對風險密集領域的重視。

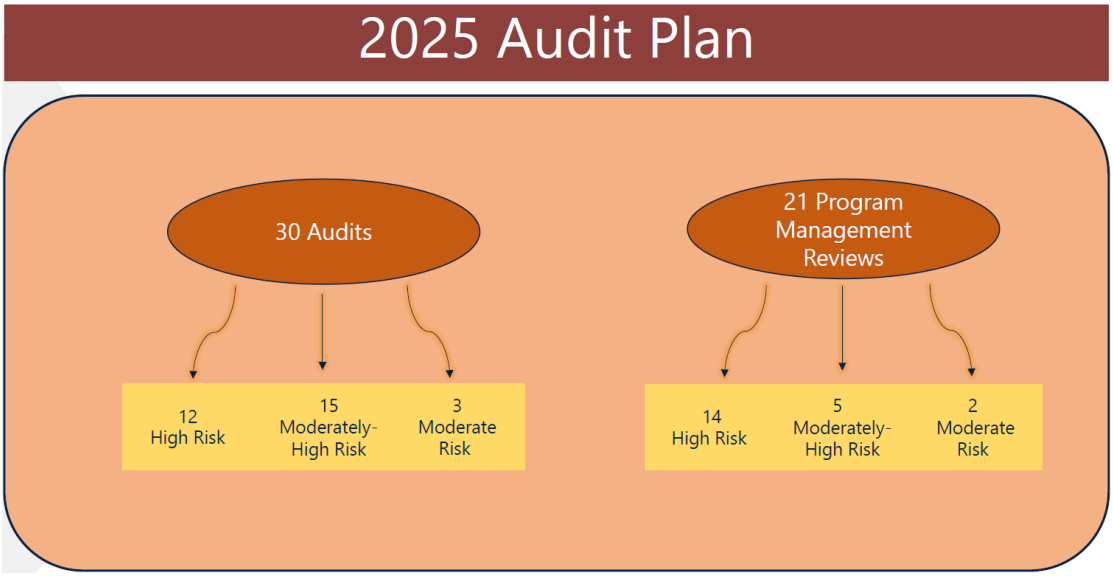


圖 8 FRBNY2025 年稽核計畫

資料來源：研討會講義

這些稽核任務根據風險分級進行排序，包括 12 項高風險（High Risk）、15 項中高風險（Moderately High Risk）及 3 項中度風險項目（Moderately Risk）。透過這種分級方式，稽核部門得

以將資源集中於對組織運作最具影響力的區域。此舉亦顯示出稽核部門不僅關注內部控制缺失，更注重於如何預防潛在風險，並對組織治理提供前瞻性支持。

風險分級的判斷並非單一因素決定，而是綜合考慮業務重要性、流程複雜度、過往問題紀錄、法規遵循壓力以及管理變動等多元要素。此外，稽核部門會根據不同受審實體的性質，分別安排即時稽核或期間性稽核（Period-of-Time Audits），並輔以日常聯絡與監控機制（Liaison & Monitoring Activities），形成一套完整的稽核保證體系（Audit Assurance Coverage）。

從 2025 年的計畫配置來看，可見稽核策略正逐步從事後查核轉向事前預防，並以資料驅動與風險導向的方式深化其治理角色。這樣的安排不僅有助於提升稽核成效，也增強了其與組織整體風險管理系統的連結性，成為推動穩健經營的重要力量。

陸. 結論與建議

本次研討會由 FRBNY 實務經驗出發，揭示金融機構在高風險與高科技環境中的應對策略，強調風險治理制度化與科技應用整合的必要性。核心理念包括：明確制度化風險胃納與容忍度，以平衡營運效率與風險控制；資安治理應融合關鍵風險指標（KRI）與營運韌性，加強跨部門協作防禦；AI 應用須強化模型驗證機制與倫理治理，確保決策透明與公平；而內部稽核則應轉型為策略夥伴，積極參與專案治理與風險預警，維護整體金融穩定與信任基礎。

FRBNY 提出現代稽核的轉型方向，涵蓋流程設計、角色分工、風險評估與科技導入。內部稽核已從傳統監督角色升級為風險控制與策略顧問的雙重角色，需建立跨部門溝通與聯絡模型，集中資源於高風險領域，並導入即時整合稽核方式以提升監控效能。強調稽核規劃與執行的一致性與透明度，確保成果落實。面對風

險環境日益複雜，稽核未來發展應朝向數位化、專業化與策略化，透過強化制度設計、人力資源與技術工具整合，發揮治理核心功能，支撐金融機構的永續經營。茲就本次研討會之討論議題提出以下建議供參：

一、主動精進技能，迎戰金融科技風險

隨著金融科技快速發展與數位化轉型加速，內部稽核部門的角色正從傳統監督者轉變為主動風險管理與策略支持者。面對 AI 等新興技術帶來的新型風險，稽核人員需持續精進專業技能，方能有效辨識並因應複雜多變的風險挑戰。參與國內外專業研討會與培訓活動，有助於掌握最新趨勢與實務做法，並透過與業界交流拓展視野，提升對科技風險的理解與判斷能力。

此外，稽核主管應積極投入人才培育，透過工作輪調、導師制度與持續回饋機制，強化團隊整體專業素養與風險應變能力。培養具備科技素養與跨領域知識的稽核人才，不僅能提升稽核效能，也有助於提出更具前瞻性與建設性的建議。總體而言，主動學習與持續專業發展將是稽核人員在金融科技時代保持價值與競爭力的關鍵。

二、強化 AI 風險識別，提升內部稽核效能

在數位化轉型與 AI 技術推動下，金融機構的業務流程與風險樣貌正迅速改變，對內部稽核工作帶來前所未有的挑戰。稽核人員不僅需關注傳統合規與流程控管，還需具備對 AI 技術風險的理解與因應能力。AI 雖提升效率，卻也可能因數據偏誤或演算法不透明導致不公平決策，甚至引發資安漏洞與數據外洩等問題。因此，稽核人員需結合數據分析工具與專業判斷，對 AI 應用進行有效監督，並在人機協作下維持風險控制的準確性與合規性。

同時，稽核角色亦應轉型升級，從制度監督者走向治理價值創造者。內部稽核部門需積極導入科技工具、提升資訊安全稽核

能力，並培養具備科技素養的專業人才，以因應不斷變化的風險結構。唯有結合科技、專業與策略視野，稽核部門才能在數位轉型中發揮預警、防範與改善的關鍵作用，確保組織在面對新興風險時具備足夠的應對力與韌性，實現「稽核即治理」的核心目標。

參考資料

1. FRBNY 研討會課程講義。
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. 全球內部稽核準則（Global Internal Audit Standards），2024 年。
4. The IIA’s Three Lines Model：An update of the Three Line of Defense.
5. Pieger, Robert (2024), “Cybersecurity Risk Management Strategies,” Central Banker Programs, Federal Reserve Bank of New York.
6. Yacono, Anita (2024), “Digital Transformation Journey,” Central Banker Programs, Federal Reserve Bank of New York
7. Gartner, Third Party Risk Management（TPRM）.
8. Gartner Press Release, Garner Unveils the Top Eight Cybersecurity Predictions for 2022-23.