金融監督管理委員會因公出國人員出國報告

（出國類別：其他－訓練）

參加美國聯邦準備理事會「2024 年訓練及活動計畫—風險管理與內部控制」

服務機關：金融監督管理委員會銀行局
姓名職稱：洪禎憶專員
派赴國家/地區：美國華盛頓哥倫比亞特區
出國期間：113 年 8 月 3 日至 113 年 8 月 11 日
報告日期：113 年 11 月 6 日

摘要

美國聯邦準備理事會及聯邦準備銀行為促進與其他國家中央銀行與銀行監理機關間之聯繫，開設國際培訓計畫並邀請各國中央銀行及銀行監理機關人員參與。本次奉派參加由美國聯邦準備理事會及聯邦準備銀行(Federal Reserve Banks)所舉辦之「2024訓練及活動計畫」，訓練課程主題為「風險管理與內部控制」。

本次課程期間為113年8月5日至113年8月8日，為期四天，訓練地點於美國華盛頓哥倫比亞特區聯準會訓練中心。課程目的在於使參與人員深刻理解內部控制與風險管理對銀行運作的重要性，並學習如何將內部控制與風險管理之評估納入整體銀行評級系統中。課程內容涵蓋介紹美國聯邦準備體系(Federal Reserve System, Fed)的監理職責、風險導向之金融監理、風險管理四大支柱、各類風險類型及相應之管理方式等內容，並透過案例研討與各國學員分組互動，幫助參與人員掌握課程重點。期望透過本次學習經驗，落實於本會金融監理實務工作。

本報告共有參章節，第壹章為前言；第貳章為課程內容摘要；第參章為心得與建議。

目錄

壹、 前言

一、 課程介紹

美國聯邦準備理事會(Federal Reserve Board of Governors，下稱聯準會)及聯邦準備銀行 (Federal Reserve Banks)為促進與其他國家中央銀行與銀行監理機關間之互動與聯繫，創設國際培訓計畫(International Training and Assistance, ITA) 。透過提供培訓和技術支持，ITA 計畫旨在幫助國際金融機構之監理機關提升其監管能力和業務運作。該計畫涵蓋各種課程、研討會和合作方案，主題涉及金融監管、風險管理及金融科技等。

今(113)年度聯準會及聯邦準備銀行所舉辦之「2024 訓練及活動計畫」，共設有五項實體課程，每項課程為期約四日至五日，課程主題分別為信用風險分析、金融監理機構之有效溝通、風險管理與內部控制、問題銀行處理及流動性風險管理。

二、 課程內容及目的

本次奉派參與之課程主題為「風險管理與內部控制」，課程期間為 113 年 8 月 5 日至 113 年 8 月 8 日，為期四天，訓練地點於美國華盛頓哥倫比亞特區聯準會訓練中心。課程參與者來自約 16 個國家，包括巴哈馬、香港、菲律賓、韓國、亞塞拜然、貝里斯、盧安達、尚比亞、馬拉威、獅子山共和國、迦納、約旦、克羅埃西亞、庫拉索、瑞士及我國，總計約 35 位參與者。課程 6 位主講者分別為聯準會國際培訓計畫之團隊負責人，以及來自克里夫蘭聯邦準備銀行(Federal Reserve Bank of Cleveland)、芝加哥聯邦準備銀行(Federal Reserve Bank of Chicago)、舊金山聯邦準備銀行(Federal Reserve Bank of San Francisco)、紐約聯邦準備銀行(Federal Reserve Bank of NY)、亞特蘭大聯邦準備銀行(Federal Reserve Bank of Atlanta)之監理官。

課程目的是使參與人員深入理解內部控制與風險管理對銀行運作的重要性，並學習如何將內部控制與風險管理之評估納入整體銀行評級系統中。課程內容涵蓋介紹美國聯邦準備體系(Federal Reserve System, Fed)的監理職責、風險導向之金融監理、風險管理四大支柱、各類風險類型及其管理方式等內容。透過主講者的簡報講解及分組案例研討，參與人員互相分享經驗和交流意見，有助於快速融入團體及掌握課程重點。

貳、 課程內容摘要

一、 美國聯邦準備系統與金融體系監理架構

(一) 回顧美國金融危機與金融監理制度發展

在美國聯邦準備體系(Federal Reserve System, FED)成立之前，金融恐慌事件頻繁發生，並對美國國內生產總值(GDP)產生重大影響：

- 西元[1]1873 年恐慌：導致美國經濟衰退，銀行倒閉，隨後經歷了四年的經濟蕭條。
- 1893 年恐慌：再次引發美國經濟衰退，銀行接連倒閉。
- 1896 年恐慌：造成美國經濟嚴重衰退。
- 1901 年恐慌：美國經濟衰退，導致北太平洋鐵路公司爭奪財務控制權。
- 1907 年恐慌：引發美國嚴重的經濟衰退，促使美國進行銀行監理改革。

1929 年至 1939 年間的經濟大蕭條(The Great Depression)是第二次世界大戰前全球經濟面臨最嚴重的危機，導致大量銀行倒閉和失業率飆升。因此，美國金融監理體系進行了大規模的改革， 以下為關鍵的改革措施和立法：

1. 格拉斯-斯蒂格爾法案(Glass-Steagall Act, 1933)：該法案又稱 1933 年銀行法(The Banking Act of 1933)，分離商業銀行與投資銀行業務，禁止銀行同時從事商業銀行業務(如存款、貸款)和投資銀行業務(如證券交易和承銷)，旨在降低金融體系風險，避免銀行過度投資。
2. 成立聯邦存款保險公司(Federal Deposit Insurance Corporation, FDIC)：於 1933 年成立，負責為銀行存款提供保險，保護存款人資金，防止銀行擠兌風險再度發生。
3. 成立證券交易委員會（SEC, Securities and Exchange Commission）：於 1934 年成立，負責監督證券市場，確保交易的透明度和公平性，防止欺詐及市場操控行為。
4. 銀行控股公司法案(Bank Holding Company Act of 1956)：旨在監督銀行控股公司，允許其在符合 FED 監理原則下跨州擁有多家銀行及相關業務。
5. 存款機構解除管制和貨幣控制法案(Depository Institutions Deregulatory and Monetary Control Act of 1980)：該法案逐步放寬銀行和儲蓄機構的利率管制，並要求所有存款機構遵守準備金要求。
6. 1980 年代末與 1990 年代初的儲貸(S&L)危機和銀行危機的相關法規。

[1] 以下內文所提及年度均為西元年。

7. 格拉姆-里奇-布萊利法案(Gramm-Leach-Bliley Act,1999)：又稱 1999 年金融服務現代化法案，廢止了部分 1933 年格拉斯-斯蒂格爾法案中對銀行、證券和保險業務間分業經營的限制，允許金融機構可同時經營投資銀行、商業銀行、證券公司和保險公司，該法案加速了金融市場整合和多元發展。

(二) 美國聯邦準備體系 FED 之組成和職責

FED 是美國的中央銀行，依據美國國會於 1913 年通過的聯邦準備法案(Federal Reserve Act)而創立，並受美國國會的監督。成立背景係為了避免再次發生 1907 年的金融大恐慌事件(The Panic of 1907)。FED 的組織架構主要包含三大主體：

1. 聯邦準備理事會(Board of Governors of the Federal Reserve System)[2]：位於華盛頓特區，由 7 位成員組成，包含主席和副主席，成員均由美國總統任命，並經參議院確認。
2. 聯邦準備銀行(Federal Reserve Bank)：在美國主要城市設有 12 個聯邦準備銀行，分別位於波士頓(第一區)，紐約(第二區)，費城(第三區)，克里夫蘭(第四區)，里奇蒙(第五區)，亞特蘭大(第六區)，芝加哥(第七區)，聖路易(第八區)，明尼亞波利斯(第九區)，堪薩斯城(第十區)，達拉斯(第十一區)，舊金山(第十二區)，銀行各自獨立運作。

圖 1：美國聯邦準備銀行分布區域(資料來源：課程簡報)

3. 聯邦公開市場委員會(Federal Open Market Committee, FOMC)：負責制定美

[2] 聯邦準備理事會所管轄的金融機構範圍包含：州立會員銀行(State charterted Member Banks)、銀行控股公司(Bank Holding Companies)、外國銀行分行及辦事處(Branches & Agencies of Foreign Banks)、Edge Act 公司(Edge Act Corporations)。

國的公開市場操作政策和實施貨幣政策。

FED 五大功能包括：執行國家貨幣政策、維持金融體系穩定、監管金融機構、促進支付和結算系統的安全與效率，以及促進消費者保護和社區發展。

圖 2：美國 FED 組成主體和監理職責(資料來源：FED 官網公開資訊 https://www.federalreserve.gov/aboutthefed/files/the-fed-explained.pdf)

二、 風險導向之金融監理

(一) 綜合監理(Consolidated Supervision)

綜合監理係 FED 監理的基礎，又稱為傘式或集團監理(Umbrella/Group wide Supervision)，由 FED 統籌金融控股公司的合併監理，而各主要銀行主管機關則負責監理金融控股公司旗下的銀行，至於其他非銀行子公司，則依其業務性質由各該目的事業主管機關負責監理。FED 作為傘式監管機關，將更專注於金融控股公司的綜合風險管理流程及整體資本充足性，以確保其財務狀況不會威脅到子公司存款機構的穩定性。

(二) 2008 年後美國銀行監理目標

1. 多德-弗蘭克華爾街改革與消費者保護法案(Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, DFA)：
   (1) 強化了 FED 的監督職能，並擴大其監督和金融穩定的職責。
   (2) 提高 FED 對金融機構的監理和審查標準，能夠根據個案或組織具體情況量身訂制適用的標準。
   (3) 防止金融機構過度承擔風險。
2. 第 12-17 號監理信函「大型金融機構的綜合監理架構」(Supervision and Regulation Letter, SR12-17 Letter)[3]：
   (1) 建立對大型金融機構的綜合監督框架。
   (2) 加強個體(microprudential)審慎監理。
   (3) 納入總體(macroprudential)審慎監理，以降低對美國金融體系穩定性相關的風險。
3. 綜上所述，DFA 和 SR 12-17Letter 的兩個關鍵監理重點在於：
   (1) 提高韌性：確保組織與其核心業務能在內外部壓力下存活，透過維持足夠的資本和流動性實現財務韌性，並透過有效的公司治理、風險管理和復原計劃實現營運韌性。
   (2) 降低對金融機構和經濟的影響：在組織發生失敗或出現重大弱點時，減少並最小化對金融系統和經濟的影響。

(三) 美國銀行以風險為導向之檢查

1. 檢查原則：

[3] 監理信函又稱 SR 信函，提供金融機構安全和穩健原則的指導，無法律規定之強制執行效果，按主題或年份排序。SR12-17 Letter 係 FED 於 2012 年發布，旨在提高大型金融機構的穩定性和透明度。

(1) 根據組織的規模和業務複雜性，決定監理或檢查工作的深度和持續監理的方式。

(2) 依賴其他外部監理機關之前的監理行為，或組織內部的稽核制度。

(3) 鼓勵並依賴銀行強大的風險管理策略，即風險四大管理支柱：董事會和高階管理層監督/公司治理、政策和作業程序、管理資訊系統(MIS)與內部控制。

2. 美國銀行監理或檢查模式(含在場或非在場的監理模式)：

(1) 橫向審查：同時對多家機構進行審查，涵蓋公司特有風險的監理和跨公司視角的發展，並由具跨領域經驗的團隊執行，如綜合資本分析和檢查(Comprehensive Capital Analysis and Review，CCAR)[4]，及復原與清理計畫(Recovery and Resolution Planning, RRP)審查。

(2) 特定公司審查(針對特定目標和時間點)與持續監測活動：針對特定目標和時間點的專案性檢查；持續監測活動，包含與組織管理階層的會議、分析內部 MIS 報告、市場指標及其他資訊。

(3) 依賴其他監理機關的資訊和評估：

甲、聯邦準備系統參與跨機構資訊共享和協調，以促進全面性且有效率的監理，避免重工。

乙、監理機關(OCC, FDIC 及州監理機關等)進行正式和非正式討論，以解決組織主要風險及協調監理策略。

丙、聯邦監理報告提供有關財務狀況的全面性資訊(如通知報表 Call Reports 或統一營運績效報告 Uniform Bank Performance Report, UBPR)[5]，供所有監理機關使用。

(4) 依賴內部審查和內部控制功能：旨在減少重工，確保檢查以風險為導向，簡化流程及監理負擔，並聚焦於高風險領域。

3. 針對不同金融機構類型之監理方式：

(1) 大型機構監理協調委員會監督之金融機構(Large Institutions Supervision Coordinating Committee Firms, LISCCs)[6]和大型金融機構(Large Financial Institutions, LFIs)[7]：

---

[4] CCAR 源自於 2009 年監理資本評估計畫(Supervisory Capital Assessment Program, SCAP)首次將壓力測試作為監理工具使用，第一輪 CCAR 係於 2011 年進行，初期目的在於提高大型銀行控股公司的風險應對能力，全面評估各項業務和資產的抗風險能力。

[5] UBPR 係為銀行監管、檢查及管理目的而設計之全面性分析工具，反映銀行管理決策及經營狀況對銀行績效及資產負債表之影響。

[6] LISCC 係指最大、最複雜且會對美國經濟構成最大的系統性風險的美國和外國金融機構。

[7] LFIs 包含大型銀行組織(Large Banking Organizations, LBO)和大型銀行外國組織(Large Foreign Banking

甲、配置全職且專注於特定風險領域之審查員和兼職監控風險之合作夥伴(Risk Partners)。

乙、強調持續監控及專案檢查，注重與風險相關的收益。

(2) 大型區域銀行機構(Large Regional Banking Organizations, Large RBOs)[8]：依賴銀行報告的分析；定期每季與管理階層召開會議；採持續監控；進行專案檢查或及年度滾動式評估等。

(3) 社區型銀行機構(Community Banking Organizations, CBOs)[9]和小型外國銀行機構(Small Foreign Banking Organizations , FBOs)[10]：每年度進行實地全面性檢查；針對近期問題或新興議題進行監理；與管理階層定期每季召開會議；持續追蹤 FBOs 總行所在國家的議題或事件。

4. 檢查流程：

(1) 檢查前：瞭解受檢機構現行概況並擬定年度監理計畫；評估持續的監測報告；制定初步風險評估概況(Risk Assessment Profile, RAP)；準備檢查備忘錄(Scope Memorandum)並發出檢查通知信函(Entry Letter)予受檢機構。

(2) 檢查時：進行實地或非實地審查，並填寫檢查意見工作底稿。

(3) 檢查後：擬定檢查結果和發現；修改風險評估結果；與受檢機構管理階層召開溝通會議；函送檢查報告；更新下年度監理計畫。

Organizations, Large FBOs)，其中 LBO 係指總資產超過 500 億美元且非 LISCC 的國內銀行和儲蓄貸款控股公司；而 Large FBOs 係指總資產超過 500 億美元且非 LISCC 的外國銀行組織。

[8] 大型 RBOs 係指總資產在介於 100 億至 500 億美元之間的本國銀行。

[9] CBOs 係指總資產規模低於 100 億美元以下之本國銀行。

[10] 小型 FBOs 係指總資產低於 50 億美元以下之外國銀行機構。

三、 風險管理四大支柱

對於銀行而言，固有風險係指在缺乏內部控制之情形下，某事件或行動可能對特定業務範圍產生潛在的不利影響，而風險管理的目的在於確保金融機構能夠事先識別潛在風險，並進行分析和採取預防性措施，以減輕固有風險帶來的負面效果。因此，風險管理的核心即是將固有風險轉為剩餘風險，並對其進行有效的控制和管理。

在金融機構風險管理過程中，依據剩餘風險的程度(高、中、低)及風險趨勢(增加、穩定、減少)，可以評估其風險管理架構的品質(強健、適當、弱)，以及是否能有效降低固有風險(程度分別為高、中、低)。一個有效的風險管理架構應能將高固有風險降低至適當範圍。風險管理架構包含下列四大支柱：

(一) 公司治理/董事會與高階管理層之監督

公司治理的缺陷往往導致銀行面臨問題、負面消息或財務危機。隨著銀行產品和業務活動複雜性不斷增加，加上市場多樣性及機構投資者影響力的提升，金融領域的整合使得全面監督變得更加重要。

經濟合作與發展組織(OECD)於 2004 年修訂的公司治理原則指出，公司治理涉及公司管理層、董事會、股東及其他利益相關者之間的關係。因此，銀行董事會應維護股東、員工、社會大眾等各方權益，不僅應清楚掌握業務面臨之各種風險，亦應參與制定風險策略和管理流程，以確保這些策略與銀行的整體目標及風險承受能力一致。此外，董事會可根據銀行規模，設置各類功能性專門委員會，以健全決策功能並強化管理機制。銀行董事會也應定期審查風險報告，確保風險管理流程有效運作，並根據市場變化作出調整，以確保銀行在可接受之風險範圍內穩健營運。因此，董事會對於建立和維持適當且有效之內部控制制度負有最終責任。

同時，銀行高階管理層應全面瞭解所有業務活動之風險架構，並依循董事會所通過之公司治理原則、風險策略及偏好，制定並實施各項風險管理程序或規範。銀行高階管理層應清楚向員工傳達內部控制之重要性，促進員工遵守相關法律和規範，以確保內部控制系統有效運作。

(二) 風險管理政策、作業程序與限額

銀行風險管理政策應與其營運策略一致，透過風險管理政策、作業程序與

限額，可以瞭解董事會和高階管理層的目標、風險偏好及容忍度，以及在營運活動中所建立的監控方式。

風險管理政策係指預先確定的指導性行動，旨在確保銀行營運符合其業務目標和策略。風險管理政策的制定要素應包含「3W」與「3H」六大要素，分別為：由誰負責(WHO)、允許範圍(WHAT)、風險限額範圍(WHAT)、報告方式(HOW)、控制方式(HOW)及驗證控管措施的方式(HOW)。

主管機關在銀行日常監理過程中，可以從下列項目判斷銀行風險管理政策之有效性：1.董事會是否批准並定期修訂風險管理政策；2.是否設定足夠的風險限額或額度；3.是否存有監督權責、授權層級及責任歸屬之缺失；風險管理政策是否與銀行實際營運活動一致。

風險管理作業程序係指將政策付諸實施之具體方式，為員工在日常營運中提供清晰且具體之執行方法，明確內部職責和分工權限，並指引與營運活動相關的重要決策與行動。銀行董事會制定適當的風險管理作業程序時，應注意避免權責和分工不明確、與內部控制或與風險管理政策不一致，這些情況恐影響政策之有效執行。

風險限額則是銀行董事會和高階管理層設定之風險參數，用以指導員工管理和降低風險的行動。風險限額會納入風險政策和作業程序，並透過管理信息系統(MIS)來測試其有效性。風險限額的制定應與銀行規模、業務性質和複雜性一致，並確保能有效防止銀行承擔額外的風險。

在日常監理中，主管機關可由以下幾個方面判斷銀行風險限額之有效性：1.是否有違反相關法令規範之情事；2.風險限額是否與風險評估結果一致；3.風險限額的設置是否妥當；4.銀行的營運活動是否在風險限額範圍內進行。

(三) 風險措施、監控與管理訊息系統(Management Information Systems, MIS)

風險管理訊息系統(MIS)是銀行董事會或高階管理層在制定決策時，用以提升整合性之系統，銀行應建立完善的風險管理資訊系統，確保能夠及時且準確地向董事會反映銀行整體狀況及相關風險資訊等，以提升風險管理的效率。

MIS 的組成要素包含下列項目：1.使用標竿測試(Benchmarking，或稱基準化分析法)將自身的表現指標與同業最佳指標進行比較；2.透過不同情境分析(Scenario Analysis)，評估潛在風險對銀行營運的影響；3.定期透過風險控制自

我評估(Risk Control Self Assessment, RCSA)檢查業務流程中的風險與控制措施是否有效，並進行改進；4.訂定關鍵風險指標(Key Risk Indicators, KRI)來監測風險事件發生的可能性或暴險程度；5.訂定關鍵績效指標(Key Performance Indicators, KPI)來衡量營運績效和風險管理的結果。

銀行訂定各類型指標，旨在有效監控、管理並優化其營運和風險控制。如流程指標用於衡量和評估特定業務流程的運作情況；暴險指標用來監控銀行在特定時點的風險暴露程度；控制效果指標則衡量銀行現有風險控制措施之有效性；績效指標則用於評估銀行在達成業務目標及績效方面的表現(如系統實際停機時間與既定系統復原計畫之差距)。

其中，KRI 和 KPI 兩者都是用於衡量機構表現的重要工具，二者差異主要在於 KRI 係用於監控和預測潛在風險，確保風險控制措施之有效性，而 KPI 則幫助銀行觀察業務活動的成效是否符合經營目標。有關 KRI 的特性包含下列各項：

1. 準確性：數據應來自可靠且具可識別性的來源。
2. 及時性：指標應能及時提供資訊，以便在必要時點採取糾正措施。
3. 關聯性：指標應與損失事件和控制環境惡化相關。
4. 簡單易懂：指標說明宜簡潔，且便於各業務單位瞭解。

在日常監理中，主管機關可由以下幾個方面判斷銀行 KRI 指標和 MIS 之有效性：1.KRI 是否與報告、分析和糾正行動的方法整合；2.KRI 是否能持續反映可接受的風險容忍程度和當前處理環境；3.風險監控和 MIS 報告是否涵蓋所有重大風險；4.用於監控和衡量風險的關鍵假設、數據來源、模型和程序是否適當，且是否持續測試其可靠性；5.報告是否能反映組織活動的複雜性、風險暴露程度，並符合風險限額和政策，並且比較實際表現與預期表現之差異；6.報告是否可準確、及時且充分的揭漏和傳達資訊，協助銀行識別任何不利的趨勢並評估當前面臨的風險程度。

(四) 內部控制與內部稽核

依據美國 COSO 委員會(Committee Of Sponsoring Organizations of the Treadway Commission)所發布的「內部控制-整體架構」報告，內部控制的定義是由銀行董事會、管理階層和其他成員設計並執行的一套過程，旨在實現三大目標：營運之效果和效率、銀行財務報導之可靠性，以及相關法令之遵循，該

內部控制架構包含五大要素：控制環境、風險評估、控制活動、資訊與溝通、監督。COSO 五大要素內容摘要如下：

1. 控制環境：控制環境係其他組成要素之基礎，塑造組織的文化並影響員工法遵意識與行為。包括員工的道德操守、董事會參與程度、高階管理階層的經營風格、公司治理結構、內部控制流程、以及職權分責方式和員工培訓等因素。
2. 風險評估：識別、分析和評估因營運環境變化、組織結構調整、人員異動、引入新興技術或開發產品所帶來的潛在風險。
3. 控制活動：設立完善的控制架構及訂定各層級之控制程序，如保護資產安全、最小化和監控利益衝突、職責分工和輪調、提升員工專業能力等具體措施。
4. 資訊與溝通：有效的內部控制制度應建立良好之溝通管道，透過 MIS 及時蒐集、彙整、紀錄、分析和產製報表，並將資訊傳遞內部相關部門，以便於決策。
5. 監督：持續監督和改進內部控制之有效性，並將所發現之內部控制缺失即時向適當層級通報。

內部稽核制度是對內部控制措施、風險管理架構和公司治理流程進行獨立評估的機制。銀行內部稽核單位是內部控制的第三道防線，以獨立、公正的精神協助董事會和高階管理層，查核與評估業務單位(第一道防線)及第二道法遵與風險控制部門(第二道防線)內部控制及風險管理制度之運作情形，並適時提供改進建議。FED 於 2013 年發布之第 13-1 號監理信函(SR13-1 Letter)，提供了金融機構在內部稽核獨立性、公司治理、稽核流程和改進機制等方面的指導原則，內容涵蓋增強內部稽核的實務經驗、稽核職能特徵、董事會或高階管理階層對於內部稽核委外的監督責任、獨立會計師的公正性指導，以及對金融機構內部稽核職能的監督評估。

在日常監理中，主管機關可由以下幾個方面判斷銀行內部稽核之有效性：1.稽核專責人員數量是否足夠，且是否具備足夠的專業能力；2.內部稽核的範圍是否全面涵蓋業務活動的風險；3.內部稽核流程是否完整且有效；4.是否有效監督公正第三方進行的委外稽核功能；5.稽核評估結果是否與各部門有效溝通並進行究責。

四、 各種風險類型與管理

(一) 作業風險

根據新巴賽爾資本協定對於作業風險的定義為：「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。」銀行可參酌新巴賽爾資本協定的規範，就其內部作業風險進行適當且明確之定義。作業風險管理包含以下五大核心循環要素：

1. 辨識：識別所有工作環境及日常營運中，可能直接或間接對銀行構成威脅的作業風險。
2. 評估：根據風險可能造成的損失程度和發生機率進行分析與量化。
3. 報告：定期向董事會、高階管理層和各業務單位報告作業風險暴險情況，並進行縱向或橫向聯繫；確保作業風險管理報告內容充分揭露且妥善保管。
4. 管理：對已識別和評估的作業風險，訂定相關風險管理政策及程序，以最小化負面影響或減少風險發生機率。
5. 監控：建立監控作業風險狀態及暴險程度的流程，並持續監控和調整策略，以應對不斷變化的風險環境。

作業風險管理架構應包含下列項目：1.公司治理架構應訂定明確的報告流程及職責分工；2.風險評估工具與方法；3.訂定作業風險之容忍度；4.作業風險報告和資訊管理系統(MIS)；5.使用一制性的用詞和標準化的分類；6.訂定作業風險對應政策和程序；7.獨立審核和驗證的流程和執行單位。

主管機關在銀行日常監理過程中，可從下列項目判斷銀行作業風險管理之有效性：

1. 是否建立妥當的作業風險管理架構，且董事會和高階管理層參與風險管理決策。
2. 是否有足夠的工具和方法進行風險評估，如：情境分析和壓力測試。
3. 是否建立健全的風險監控和報告機制，定期監控並生成相關報告，並向董事會和高階管理層呈報。
4. 是否定期進行獨立的內部稽核或委外審核。

(二) 信用風險

信用風險係指借款人或交易對手未能履行其契約義務而產生之違約損失風險。銀行信用風險管理是一個持續識別、衡量、監控及控制的過程。信用風險管理的重大要素分別為：

1. 董事會和高階管理層監督：董事會負責建立公司的信用文化，根據銀行經營目標制定與信用風險相關的管理策略和報告機制，並確保高階管理層能有效執行，對於建立及維持適當有效的信用風險管理機制負有最終責任；而高階管理層依據董事會核准之信用風險管理策略建立相關政策和程序，並於銀行所有營運活動中落實執行。
2. 政策、作業程序和限額：(1)核貸標準、(2)監控信用狀況和擔保品品質、(3)授信文件和例外准駁情形、(4)風險辨識過程：授信審查、預警名單及信用評等制度、(5)授信損失準備之提列方法(當期預期信用損失 Current Expected Credit Loss，CECL)及(6)債權回收程序。
3. 管理訊息系統(MIS)：系統建置應注意準確性、即時性及完整性，並包含放款預警或監控功能、壞帳機率預測功能及授信產品定價功能。
4. 內部控制：針對信用風險所建立的內部控制措施應包含：(1)職責明確劃分，如徵信、授信、覆核等作業應分別獨立、(2)雙重控制機制，防止由任何一任獨自控制整個授信過程，且重大授信作業執行時須由至少兩名經授權者進行核准、(3)授權和限額設定及(4)內部信用覆核機制。

主管機關於銀行日常監理過程中，可從下列項目判斷銀行管理信用風險之有效性：

1.管理階層重視擔保品而非償債能力；

2.風險定價不足。

3.超逾授信能力。

4.授信部門及審核作業人力不足。

5.無法對問題放款量、評等降級與例外准駁情形究責。

6.無視授信審核、覆核及稽核結果。

7.獎勵制度之設計導致承擔過多風險。

8.員工不瞭解授信政策內容。

9.自利交易(Self Dealing)[11]。

(三) 市場風險

市場風險係指銀行資產負債表內和表外項目(如資產、負債和損益)價值因市場價格(如利率、股價、匯率或商品價格)變動可能造成之損失。FED 於 2010 年所發布第 10-1 號監理信函(SR10-1 Letter)強調，金融機構對於利率風險

[11] 又稱自我交易，指負有信任義務者為個人利益而非為他人利益所從事的交易行為。

(interest rate risk, IRR)暴險程度，是監理機關評估金融機構對利率變動的敏感性和資本充足性的關鍵因素。市場風險管理的五大要素分別為：

1. 董事會監督：董事會負責核准市場風險管理策略和風險容忍度，確保市場風險管理機制適當且與銀行經營策略及管理階層的執行能力一致；對於所建立的市場風險管理機制負有最終責任。另可授權資產負債管理委員會(Asset/Liability Committee, ALCO)[12]執行部分權責，而被授權之 ALCO 須定期向董事會提交報告。
2. 高階管理層監督：依據董事會核准之市場風險管理策略建立相關政策和程序，確保銀行全體員工清楚瞭解並遵循相關作業程序，並確認被授權員工具有足夠能力和專業知識於營運活動中落實執行。
3. 政策、作業程序和限額：銀行應具備獨立之市場風險管理機制，明確風險管理職責，確保風險管理流程包含市場風險之辨識、衡量、控制、監督及報告，均能符合所定之政策和程序。
4. 管理訊息系統(MIS)：市場風險管理資訊系統應確保跨部門、跨交易與跨產品之間的衡量方法及資料來源一致，並有效掌握整體暴險部位，提供適當之風險衡量結果，以支援市場風險管理機制落實執行。
5. 內部控制：核心內部控制措施應包含建立有效的內部控制系統，切實執行職責分離，並定期向董事會和高階管理層匯報風險報告，以便其及時做出決策。此外，內部稽核單位應獨立審查市場風險管理架構之有效性，並提出改進建議。

主管機關於銀行日常監理過程中，可從下列項目判斷銀行管理市場風險之有效性：

1. 員工職責是否已分離。
2. 風險衡量模型是否符合其業務性質、範圍和複雜度。
3. 是否定期對風險衡量模型進行驗證，以確保在各種情境測試和壓力測試下之準確性和可靠性。
4. 風險衡量模型使用資料數據輸入、假設、參數設定和方法是否完整且準確。
5. 是否定期向董事會和高階管理層呈報風險報告。

(四) 流動性風險

[12] 較大型或產品較複雜之銀行可能成立 ALCO 負責設計與推行銀行利率風險管理制度及資金流動性風險管理制度，並管理與利率風險及流動性風險相關資產和負債部位。

流動性風險係指銀行因自身財務狀況或整體安全穩健性而無法履行其義務可能造成之影響，主要可分為下列三種類型：

1. 錯配風險(mismatch risk)：銀行在特定時間內因現金流入和流出無法匹配，導致無法獲得足夠的現金流以履行正常經營業務之義務。
2. 或有流動性風險(contingent liquidity risk)：因突發狀況導致銀行無法獲得足夠的資金以履行其義務之風險。
3. 市場流動性風險：銀行在處分資產(不會顯著降低市場價格)或取得金融場資金來源時，遭遇市場限制(如市場深度不足或市場運作干擾)之風險。

銀行應建立流動性風險管理架構，根據其風險容忍度，辨識、衡量、監督和控制流動性風險，並制定適當的風險管理策略和內部作業規範，運用流動性壓力測試及緊急應變計畫(contingency funding plan, CFP)[13]等流動性風險管理工具，定期檢視風險管理架構之有效性。流動性風險管理的重大要素分別為：

1. 董事會和高階管理層的監督：銀行董事會應依據自身經營目標核定和定期檢視流動性風險管理政策，並建立明確的職權分工機制，以便管理階層有效執行相關風險管理政策。此外，董事會和高階管理層應定期審視銀行緊急資金計劃，並了解子公司或關係企業之流動性風險狀況。
2. 政策、作業程序和限額：有效的流動性風險管理策略和作業規範應能辨識資金來源和運用，並能應對不利的業務情境，並根據自身流動性風險容忍度設定風險限額。
3. 管理訊息系統(MIS)：銀行可根據其經營資金策略、業務複雜性和風險投資組合調整風險管理報告的類型。對於規模較小且業務單純的銀行，可使用簡單的期距缺口分析或現金流報告來識別延續性或錯置性風險；至於規模較大且業務複雜的銀行，應建立更健全的管理訊息系統，如：
   (1)現金流預測：積極管理日間流動性部位和風險，預測流動性資產流入和流出時間點，並規劃日間資金取得之方式。
   (2)分散資金來源：建立有效分散資金來源和期限的投資組合。
   (3)流動性資產緩衝(Cushion of Liquid Assets)：持有足夠、高流動性且未受限制的流動性資產以因應各種壓力情境。
   (4)壓力測試：辨識潛在的流動性壓力來源。
4. 內部控制：確保流動性風險管理政策經董事會核准，並能有效讓管理階層

[13] CFP 係客觀、有系統且具即時性的手段，以因應潛在資金流動性危機，且應隨銀行業務性質及規模調整。

落實執行，同時監控流動性風險暴險程度在風險容忍度範圍內。

前開流動性風險管理政策和作業程序應涵蓋緊急應變計畫，該計畫旨在確保銀行於日常營運面臨各種緊急流動性事件時，能有充足之流動性資金來源以因應。緊急應變計畫應包含下列因素：

1. 依流動性壓力測試結果制定內容：銀行應依壓力測試結果提供前瞻性之風險評估，並制定有效的緊急應變計畫內容，以因應在各種緊急流動性事件下採取可行且即時的措施。
2. 訂定明確的職責分工：明定董事會、各管理階層和部門間之職責範圍，確保於緊急流動性事件發生時，各部門能各負其職並迅速執行。
3. 適時審視與更新作業規範與法規：確保緊急應變計畫內容符合最新的相關法規要求。
4. 定期測試：銀行應模擬各種緊急流動性事件，以測試所制定之緊急應變計畫是否能有效執行及發揮作用。

(五) 法律、法令遵循及名譽風險

在銀行日常營運中，該三項風險往往相互關聯，當其中一項風險發生時，極有可能引發另外兩項或其他風險。例如：若銀行未遵守法令規範，可能面臨主管機關裁罰以及新聞媒體負面報導，進而損害銀行名譽或引發其他法律訴訟。此外，該三項風險通常難以量化且容易涉及主觀判斷，一旦發生即可能影響社會大眾觀感或監理機關之監理態度，因此須綜合評估與管理。風險定義如下：

1. 法律風險：因銀行涉及不利的法律行動(如訴訟、無法履行合約、法律制裁或處分等)而可能對財業務狀況造成負面影響。
2. 法令遵循風險：指銀行因未遵守法令規範而面臨主管機關裁罰之風險。
3. 名譽風險：又稱為道德風險，指銀行因不當的商業行為或不實的負面報導等因素，造成客戶信任流失、市場地位降低和收入減少之風險。

銀行應依自身業務規範和複雜性採取適當的作業程序，當業務活動涉及不同類型之金融商品、境外客戶或跨國交易時，應綜整考量整體業務所適用之法令規範及國外監理機關之當地法規，以加強作業程序之適法性。

主管機關於銀行日常監理過程中，可從下列項目判斷銀行管理法律、法令遵循及名譽風險之有效性：

1. 所銷售之產品類型：是否有複雜結構性商品。

2. 服務提供範圍：客戶是否涵蓋不同國籍的個人、政治人物、律師事務所、非營利組織及高淨值人士等，銷售市場是否涵蓋稅務不合作國家(non cooperative jurisdictions)、避稅區(tax havens)及國外政治總部辦公室等。
3. 銀行經營策略：經營目標是否過於激進、信貸業務審核及洗錢盡職調查是否過於寬鬆、是否建立遵法合規的企業文化等。
4. 日常業務活動：是否涉及大眾關注之訟訴案件或大量客戶陳情、是否發生擾亂金融市場秩序或不符合其他法令規範之情事等。

(六) 第三方風險

銀行基於營運需求，而將部分日常業務或直接管理責任委託無關聯之第三方服務提供者或關聯企業(affiliate)處理或進行相關業務合作，以提升服務品質，然而，這樣的作法同時也可能帶來額外的管理風險，因此管理階層對於委外((outsourcing)作業之相關風險管理負有責任。

美國監理機關允許銀行可以將所有業務委外，涵蓋關鍵任務、內部控制和客戶端應用程式，而銀行委外範圍包含資訊科技、稽核、業務流程或非核心業務(如薪資處理、會計、人力資源等)，並就作業委外所可能衍生之風險提供指導原則供銀行遵循。第三方風險管理架構要素摘述如下：

1. 董事會和高階管理層責任：董事會和高階管理層應確保委外作業之安全性與合規性，並核准供應商管理政策，並制定完善的作業程序以降低委外風險。
2. 風險管理程序：應以風險為導向，且監督和控制應與風險程度相當。風險管理計畫與委外關係重要性、複雜性、共享數據數量和類型，以及委外重要業務數量高度關聯性。
3. 向董事會報告：定期向董事會報告管理委外作業的政策。
4. 整合風險管理：將第三方風險管理整合至公司整體風險框架。

銀行應謹慎分析及管理重要委外作業所附隨之風險，制定風險管理程序時應包括下列各項：

1. 訂定風險評估及策略計畫：依照經營策略目標、成本效益和風險建立確認程序，風險評估項目應包含績效標準、內部控制、報告機制及契約要件等，並針對委外作業終止建立適當的策略和緊急應變計畫。
2. 受託機構遴選原則：銀行依委外作業項目和業務複雜度，訂定受託機構之遴選原則，項目應包含受託機構的財務簽證報告狀況、公司及負責人聲譽、

管理資訊系統及內部控制環境之妥適性，以及應對偶發事件之營運持續或災難復原應變計畫等。

3. 契約明訂權利義務關係：

(1)確認雙方權利義務範圍，明確商品或服務提供之內容、形式或頻率，以及報酬費用計算方式和賠償條款等。

(2)訊息提供及接收責任：取得報告之方式、頻率及類型，確保資訊可及時且正確提供予銀行，並保障資訊傳遞過程之機密和安全性，包括偶發事件之應變程序和通報機制。

(3)稽核權利：銀行應有權查核受託機構(或其轉包商和供應商)及檢視績效之執行情形，並可選擇自行查核或委託第三方獨立稽核單位辦理。

4. 委外作業監督：指派適當人員定期檢視受託機構之財務狀況、內部控制和稽核情形、服務品質及履約情形等報告文件。

主管機關於銀行日常監理過程中，可從下列項目判斷銀行管理第三方風險之有效性：

1. 銀行所建立之內部作業制度和程序是否遵循主管機關相關法令規定。
2. 是否要求受託機構遵循相關消費者保護法、資安防護法及個人資料保護法等相關法規。
3. 是否於網站設置合作之第三方服務提供者專區供客戶查詢、或於契約中告知客戶相關條款及委外事項。
4. 是否提供消費者消費爭議之申訴管道等。

(七) 資訊科技風險

因應資訊科技(IT)和數位經濟發展，金融機構積極將新科技導入業務領域，以推動金融服務之開放與創新，但同時挑戰銀行對於新型風險之管理模式。資訊科技風險係指銀行在使用資訊科技時，因系統故障、網路駭客攻擊、人為操作錯誤或資料外洩等因素，可能對銀行日常營運、財業務狀況、客戶資安或名譽造成負面影響。因此，銀行除應重視資安防護外，亦應提升資安作業韌性，並建立穩健之資訊科技風險管理架構。

銀行資訊科技風險管理之項目應包含資訊安全、網路安全、供應商風險管理、營運持續性或災難復原應變計畫、應用程式使用控制、變動管理、數據管理及資訊科技稽核涵蓋範圍。

主管機關於銀行日常監理過程中，可從下列項目判斷銀行管理資訊科技風險之有效性：

1. 管理流程：管理流程是否確保資訊系統與業務流程及經營目標保持一致。
2. 架構：自動化資訊系統之基礎設計和各項組件是否符合現行和長期組織目標。
3. 完整性：系統、應用程式或電腦程式等相關資訊流是否能滿足終端使用者之需求和期望。
4. 安全性：控制措施是否能確保資訊資產在產生、傳輸、處理、維護和儲存之過程中，免於未經授權之使用、修改、毀壞或洩漏。
5. 可用性：資訊是否可持續且及時傳送資訊，以支援業務流程和作成決策。

參、 心得與建議

本次課程是由來自不同城市的聯邦準備銀行資深監理官擔任主要講師，課程內容涵蓋 FED 監理原則和架構，以及銀行風險管理之核心要素。課堂中講師們不吝分享其多年的金融監理實務經驗，亦鼓勵參與者提問和交流意見，課程進行方式有助於融入團體及掌握課程重點，以及提升國際金融監理視野，獲益良多，期望能將所學運用於本會金融機構實務監理中。謹就本次參與課程提出以下心得與建議：

一、 持續深化風險導向之監理精神，以落實分級管理

美國金融監理體系採用以風險為導向之模式已實行多年，根據金融機構資產規模將其劃分為 LISCC、RBOs、CBos 及 FBOs 等類別。對於不同類別的機構，採取相應的監理方式。其中，針對資產規模較大且可能對美國經濟構成系統性風險的 LISCC，則採取高強度和高頻率之金融檢查，並要求其遵守更嚴格的規範，如資本適足率和流動性比率等指標。本會為促進系統性重要銀行(D-SIBs)之風險承擔能力，強化其資本適足性及增強其經營之強韌性，於 2019 年修訂發布「銀行資本適足性及資本等及管理辦法」，及指定 5 家本國銀行(2020 年再增加指定 1 家)為我國 D-SIBs，並採取相關強化監理措施及差異化管理措施。

為利本會達到金融監理目標，本會於 2021 年間發布「金融檢查指導原則」，秉持同樣的差異化監理原則，主要關注高風險機構及業務，並根據差異化之查核頻率和範圍來提升監理效能。另對符合財務健全且具備有效內部控制制度之本國銀行，本會提供可申請採行風險導向內部稽核制度的機會。此外，國際金融監理機關對於某些金融機構業務(如委外事項)之規範，採用以風險為基礎方法(Risk-Based Approach, RBA)作為核心監管原則，本會亦參酌 RBA 精神調整並修訂相關規範。

近年金融科技持續創新與發展，逐漸改變金融機構傳統營運模式，如純網銀或純網保的興起，也進而推動了新型金融服務業的發展，包括電子支付機構及外籍移工國外小額匯兌業者等，以及非屬金融機構之虛擬資產平台及交易業務事業(VASP)、第三方支付服務業及金融科技公司等。本會因應趨勢持續推動法規鬆綁，開放金融業務與商品，並促進金融機構與金融科技業者合作。同時，金融機構與監理機關也面臨衍生的風險挑戰，本會延續 RBA 精神，根據不同業務性質調整監理框架，並制定相應的監理政策和原則。

二、 持續關注金融科技發展趨勢及新興議題，以應對新興科技的監理挑戰

在數位化時代，金融機構近年著重加速數位化轉型，金融監理機關應重視金融創

新所帶來了新興風險，並採取因應措施及完善法規，以協助金融機構制定風險管理策略。為了鼓勵金融機構善用科技及應用可信賴的人工智慧(AI)，本會參考他國政府及國際組織發布之相關指引文件，於 2024 年 6 月發布「金融業運用人工智慧(AI)指引」，並持續關注金融業導入 AI 科技所面臨之挑戰及機會。

另針對金融創新活動所帶來的資訊科技風險，建構安全且金融服務不中斷的金融服務環境，是金融監理機關與金融機構共同努力的目標。本會於 2022 年 12 月發布「金融資安行動方案 2.0」，供金融機構依據自身業務屬性及規模，衡量實際資安防護需求及執行可達性，納入內部資安規範。同時，金融監理機關透過培養具有相關知識之資訊人才，加強金融機構應對資訊科技風險及資安防護量能。

隨著各地戰爭爆發和極端氣候事件頻傳，全球局勢不穩，銀行業辦理境外授信業務，應謹慎評估各地政治和經濟狀況，避免海外暴險部位過度集中特定區域。金融監理機關應關注銀行業境外授信之風險控管，同時，隨著加密與虛擬貨幣交易及新型金融交易態樣興起，金融監理機關應加強非傳統金融模式之風險評估，並運用數據分析和監理科技等工具，提升監理效率。

三、 持續強化監理人員之專業知能，以提升我國監理效率及水準

鑒於金融科技迅速發展及金融環境持續變遷，促進金融機構經營態樣改變，金融監理機構人員的專業知能必須與時俱進，以便及時發現問題並提出適當的應對和監控措施。金融監理機關應評估市場發展情形及產業實務需求，定期進行相關監理措施和法令規定之滾動式檢討，確保金融體系穩定與安全。

為強化金融監理機關之監理量能，本會積極參與國內外培訓、論壇和研討會，並與其他國內外監理機關、金融機構和學業界單位建立合作關係，如簽署合作備忘錄或協議，建立正式的交流機制；或邀請學界及業界專家分享最新市場動態和專業知識等，進行多方資訊交流，以掌握最新市場發展趨勢，應有益提升與其他國家金融監理機構之聯繫，以及有助我國監理架構結合實務並接軌國際。

參考文獻

1. 本次訓練課程簡報資料。
2. 參加美國聯邦準備理事會「風險管理與內部控制課程」出國報告，張思捷，112年11月。
3. 中華民國銀行商業同業公會全國聯合會「銀行流動性風險管理自律規範」，113年2月。
4. Federal Reserve Board of Governors (2010), “SR 10-1: Interagency Advisory on Interest Rate Risk”, Jan.
5. Federal Reserve Board of Governors (2012), “SR 12-17/CA12-14: Consolidated Supervision Framework for Large Financial Institutions”, Dec.
6. Federal Reserve Board of Governors (2013), “SR 13-1/CA13-1: Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing”, Jan.