2025 資產管理金融新知暨法遵系列研討會

「金融業 AI 應用實務與資安風險管理」

活動實錄

金管會 施宜君副處長

證基會 王牲副總經理

資誠風險 張晉瑞董事長

隨著 AI 技術快速發展，金融業廣泛應用於投資、反洗錢及客戶服務，提升效率與精準度，但也面臨資安與合規風險。國際監理機構如 IOSCO 與歐盟已提出 AI 監管指引，我國金管會亦於 2024 年發布「金融業運用 AI 指引」，如何在推動創新同時強化資安防護與監理配套，為金融業持續發展的重要課題。

為深入探討金融業運用 AI 的監管面向、應用實務與資安風險管理，特舉辦本研討會，邀請主管機關與實務專家擔任講席，提供專業及實務交流。

「金融業 AI 應用實務與資安風險管理」議程

日期：6 月 26 日(四) 14:00-17:00

地點：台北花園大酒店國際廳

時間	主題	講席
14:00-14:10	主辦單位致詞	王牲 副總經理 證券暨期貨市場發展基金會
14:10-15:00	專題演講 1 金融業運用 AI 指引與監理趨勢	施宜君 副處長 金管會 金融市場發展及創新處
15:00-15:10	意見交流	
15:10-15:30	中場休息	
15:30-16:50	專題演講 2 AI 於金融業之應用與風控實務	張晉瑞 董事長 資誠智能風險管理諮詢公司
16:50-17:00	意見交流	

主辦單位首長致詞

證基會 王牲副總經理

王副總經理首先感謝所有與會貴賓的蒞臨，並指出人工智慧(AI)技術的快速發展，已為金融業帶來革命性的影響。例如：納斯達克交易所(Nasdaq)透過生成式 AI 加強市場監視系統，使監管機構能有效地監控並發現潛在的市場濫用行為。而根據我國金管會今年 4 月份的調查結果，臺灣已有超過 100 家金融機構導入 AI，範圍涵蓋前、中、後台作業流程，顯示 AI 在提升金融服務效率、品質及競爭力的巨大潛力。

然而，AI 技術創新的同時也伴隨資安與法令遵循風險。在國際監理進展方面，歐盟 AI 法案於 2023 年 8 月正式生效，旨在確保歐洲開發和使用的人工智慧完全符合歐盟的權利和價值觀；日本金融廳於 2024 年 3 月發布了針對傳統 AI 與生成式 AI 所面臨的挑戰與業界應用實踐的討論文件；美國商品期貨交易委員會(CFTC)則於 2024 年 12 月針對註冊機構在監管市場使用 AI 提出建議並強調合規的重要性；而我國金管會亦於 2024 年 6 月發布「金融業運用 AI 指引」，提供金融機構導入、使用及管理 AI 的重要參考。

今日安排兩項重要議題，首先邀請金管會金融市場發展及創新處施副處長，解析「金融業運用 AI 指引與監理趨勢」；接著由資誠智能風險管理諮詢公司張董事長，分享「AI 於金融業之應用與風險控管實務」，以 AI 應用實例進行經驗分享與交流。

專題演講 1：
金融業運用 AI 指引與監理趨勢

金管會金融市場發展及創新處 施宜君副處長

一、金融業應用 AI 的效益、挑戰及實際應用情形

施副處長指出，人工智慧(AI)在金融業的應用日益普遍，並帶來顯著優化與效率提

升。首先，AI 可實現服務自動化，提供投資、保險、支付、存款與貸款等各類金融服務。在防詐與安全保障方面，AI 能透過模式識別與異常偵測，有效協助識別潛在詐騙行為，強化金融交易的安全性。AI 技術亦能辨識客戶的情緒與情境，透過提供高度客製化的服務，精準滿足個別客戶需求並提升滿意度。而在內部作業效率上，AI 能快速進行資料蒐集、整理與分析，例如：查詢各國法規趨勢可先由 AI 進行初步篩選，節省大量人力與時間。另外，AI 也能協助優化營運流程，透過數據分析促進減碳，展現其在綠色金融與永續發展的應用潛力。

施副處長進一步指出，人工智慧雖為金融業帶來諸多效益，但導入過程仍面臨多項挑戰。首先，金融機構需建立完善的治理架構，確保 AI 應用符合法規與政策，並兼顧資料隱私與資安。技術層面則面臨新舊系統銜接困難、資料格式不一與高額升級成本等整合難題，增加導入 AI 的複雜度。而在人才方面，AI 技術高度專業化，金融機構需積極培育具 AI 開發與管理能力的人才，以確保系統部署與持續運作順利。

根據金管會今年 4 月的調查，全台 383 家金融機構及周邊單位中計有 126 家已導入 AI 應用，占比約 33%，銀行業與保險業的導入率較高，分別為 44%與 46%，證券及期貨業則為 23%。AI 導入的主要目的包含提升作業效率與生產力(30%)、節省人力(18%)、提升客戶體驗(15%)等。在應用場景上，銀行業前三大應用領域為認識客戶及防範金融犯罪、智能客服及內部行政作業，而證券期貨業與保險業皆以內部行政作業為主。然而，在銀行信用分析、證券期貨業協助客戶交易與投資組合管理、保險業的核保理賠流程自動化等面向，考量 AI 生成內容不穩定及判斷易產生偏見等疑慮，故使用率較低。

值得關注的是，在已導入 AI 的機構中有 48%已進一步應用生成式 AI，主要用於內部行政(39%)、智能客服(15%)及教育訓練等用途，展現生成式 AI 在金融業實務推展中的潛力，但仍需面對 AI 幻覺、資料安全、隱私保護與合規性等問題。施副處長指出，超過半數機構計畫增加 AI 應用，預期未來研發重點包括：防詐、大語言模型及風險管理。今年 2 月成立的「金融科技產業聯盟」即以推動金融科技應用研發為目標，將去識別化的資料導入 AI 模型進行訓練、建構警示帳戶態樣與金流履歷，以達成金融同業聯防阻詐之成效。

二、國際監理趨勢

隨著 AI 在金融服務領域的應用日益增加，AI 治理已成為重要國際金融監理議題。各國及國際組織正積極著手訂定相關原則或指引，以建構能兼顧科技創新與風險治理的可信任 AI 發展環境。

(一)國際證券管理機構組織(IOSCO)：於今年 3 月發布「人工智慧在資本市場的應用、風險與挑戰」諮詢文件，指出證券業 AI 常用於客戶溝通、支持決策流程(如機器人理財、演算法、投資分析)、強化監控與合規功能、提升作業效率。常見 AI 風險包括惡意使用、模型數據問題與集中度風險。常見金融業治理實務為將 AI 治理納入既有風險管理架構，或建立專屬的風險管理制度，包括組成跨部門團隊、高階主管及專家參與，並關注資料、資安及第三方風險。

(二)國際清算銀行(BIS)：於 2024 年 5 月及 12 月發布「金融數位化」與「金融領域人工智慧之監管：近期發展與主要挑戰」等報告，指出關鍵數位科技包含：分散式帳本技術(DLT)、雲端運算、人工智慧與機器學習、開放金融與應用程式介面等，在監理措施上建議加強國際合作、促進監理機關和金融機構間對話、確保透明度並強化監理機關的 AI 專業知識和能力。

(三)國際保險監理官協會(IAIS)：於 2024 年 11 月提出「人工智慧監理應用文件」諮詢文件，強調治理與問責的重要性，擬定對抗網路攻擊、數據操縱和洩露的安全措施。IAIS 指出保險公司應能解釋 AI 系統產出的結果，特別是對顧客或償付能力有實質影響的決策，能解釋內容並符合不同利害關係人之需求，並建立足夠的申訴救濟機制，以維護金融信任。

三、金融業運用 AI 指引

金管會為協助金融機構有效利用 AI 科技優勢並管理相關風險，參照全球主要國家監理機關及國際組織的指導原則，並結合我國金融市場發展狀況及金管會的監理政策方向，已於 2023 年 10 月 17 日公布「金融業運用人工智慧(AI)之核心原則與相關推動政策」，並蒐集金融機構及國際知名科技公司等共 150 項意見，邀集金管會 AI 法制專案小組諮詢顧問、金融機構及公會召開諮詢會議，於 2024 年 6 月 20 日正式發布「金融業運用人工智慧(AI)指引」。施副處長表示，該指引為指導原則，非強制規範，旨在鼓勵金融業導入、使用及管理 AI。指引總則章首先針對 AI、系統生命週期與風險管理進

行定義說明：

(一)AI 定義係採用採用銀行公會「金融機構運用人工智慧技術作業規範」的定義，「AI 系統」指透過大量資料學習，利用機器學習或相關建立模型之演算法，模仿人類學習、思考及反應模式之系統；「生成式 AI」則是指可生成模擬人類智慧創造之內容的相關 AI 系統。

(二)金融機構在導入 AI 系統時，應依照 AI 系統生命週期劃四個階段：系統規劃及設計、資料蒐集及輸入、模型建立及驗證、系統部署及監控，落實風險評估與管理機制：

1. 風險評估考量因素：應綜合評估 AI 系統是否直接提供客戶服務、使用個人資料的程度、決策自主性、系統複雜性、對利害關係人的潛在影響以及是否具備完善的救濟機制。

2. 以風險為基礎落實核心原則：應依據風險程度分配資源，對高風險 AI 系統採取更嚴謹的控制措施，如紀錄留存、持續監控、內外部審核或定期評測等，確保核心原則落實。

3. 第三方業者之監督管理：評估第三方是否具備相關專業能力，並建立監督與管理機制；並應注意複委託約定內容，釐清責任分配，預先規劃終止合作時的應對措施。

施副處長接著介紹「金融業運用人工智慧(AI)指引」之六項核心原則：

(一)建立治理及問責機制：應設立清晰的 AI 治理架構，指派高階主管或委員會負責跨部門協調與管理，並提供相關人員充分資源與訓練，強化董事會與管理層對 AI 的理解與監督。

(二)重視公平性及以人為本的價值觀：避免 AI 決策造成歧視，尊重人類自主權並提供受不利影響者救濟機制，從設計到部署各階段，應納入偏誤檢視、數據多元性、模型驗證與結果監控等措施。

(三)保護隱私及客戶權益：應依資料最小化原則蒐集與處理資訊，確保合法合規並取得客戶同意；尊重客戶選擇是否使用 AI 的權利，並建立外洩通報與供應鏈監管機制，保障個資與系統安全。

(四)確保系統穩健性與安全性：應強化 AI 系統在壓力環境下的準確性與可重製性，並防範外部攻擊；各階段應設有風險評估、資料處理、模型驗證及部署後的持續監控機制，以維持系統穩定與資安合規。

(五)落實透明性與可解釋性：應清楚揭露 AI 運作邏輯與對利害關係人之影響，並依情境審慎控管資訊揭露程度；應更新服務條款、主動告知使用 AI 並提供適當解釋，增進市場信任。

(六)促進永續發展：應評估 AI 對環境與社會之影響，選用高能效設備、優化演算法以降低資源耗用，並兼顧社會公平與數位包容；同時應保障員工權益，提供轉型所需訓練與支持機制。

四、結語

施副處長總結，推動金融科技須兼顧創新發展與監理韌性，並強調金管會提出的「促進金融科技發展五策略」與「強化數位金融監理韌性」的重要性。五項策略包括：建立一致政策框架，提供穩定創新環境；加強跨部門與公私協力合作，匯聚創新能量；培育具科技與法規理解的人才，因應快速變遷；運用科技強化監管效率與風險辨識能力；以及透過國際交流因應跨國金融創新挑戰。透過上開策略，金管會期望擴大創新容錯空間、鼓勵產業共創並強化市場彈性，以強化數位金融監理韌性並確保金融市場穩定與安全。

專題演講 2：
AI 於金融業之應用與風控實務

資誠智能風險管理諮詢公司 張晉瑞董事長

張董事長首先界定 AI 相關概念之定義：機器學習(Machine Learning)是能從現有數據中學習並改進以做出決策或預測；深度學習(Deep Learning)是基於人工神經網路的機器學習技術，使用多層處理從數據中逐步提取更高層次的功能；而生成式 AI(Generative AI, GenAI)則是使用大量數據和

大型預訓練模型來生成新內容的演算法，例如 ChatGPT，可用於創作藝術、音樂、文字，甚至虛擬世界等各種應用。

張董事長指出全球各國正逐步推行法規與行政指引，例如歐盟的 AI 法案預計 2026 年全面生效，不慎違反的企業將面臨高達 3,500 萬歐元或全球營業額 7%的罰鍰。面對日益趨嚴的監管與審查，張董事長建議企業可考慮導入適用的風險治理架構，例如 ISO/IEC 42001:2023 旨在促進負責任之 AI 治理、倫理使用、避免偏見及風險管理等，而 ISO 23894:2023 提供將風險管理應用於 AI 系統之具體指南，強調於 AI 開發、配置、提供及使用過程中應用 ISO 31000 風險管理原則。企業在 AI 應用實踐上，能以資訊安全管理系統(ISMS)作為資安保護之基礎，將人工智慧管理系統(AIMS)融入 PDCA(Plan, Do, Check, Act)循環，從中擴展出 AI 必要之管控面向。

一、治理風險

治理風險源於 AI 技術的快速發展超越現有監管框架，導致治理機制應變不足，風險管理失效。張董事長列舉各項管理困境與相應之具體控制實務：

(一)治理失靈風險：建立明確治理架構與責任機制

面對 AI 技術發展超出既有監管框架的治理失靈風險，組織應明確界定職責與權限，指定高階主管或設立 AI 治理委員會，負責 AI 全生命周期的策略監督與風險控管，並整合 AI 風險管理於既有架構，將 AI 相關風險納入企業既有的整體風險管理、內控、資安與法遵機制中，避免治理斷層。

(二)資源分配與持續監控挑戰：推動風險基礎管理與差異化監控

高風險 AI 系統所需的評估與監控資源龐大且長期，實務上可透過推動風險基礎管理，根據風險高低分配監控資源，高風險 AI 模型應設有更頻繁、更嚴格的監控與審核以確保控管品質。

(三)定義與語義模糊問題：建立全面的文件紀錄

面對 AI 系統定義不一致與術語混用的問題，建議可建立全面性文件紀錄，統一模型版本、用途、輸入來源與風險評估結果等 AI 模型資料與管理規範，建立一致性的參考依據並確保透明度與可追溯性。

(四)法規碎片化與跨領域整合難題：強化獨立審查與稽核

面對全球 AI 法規多元化與跨國金融機構遵循的困難，企業除了建立內部審查與監測機制以外，可考慮委託具備 AI 專業的獨立第三方機構，對高風險 AI 系統進行審查與評估，提供客觀的反饋以提升整體合規效率。

(五)組織變革與文化阻力：由上而下推動文化轉型與技能重塑

推動 AI 導入所需的文化轉型與人員培訓，建議可自高階管理層發起 AI 治理文化，確保組織上下對 AI 系統有共同理解與共識；在內部人員培訓上可提供 AI 相關培訓課程，介紹 AI 基本概念、運作方式、潛在風險及倫理原則，從高層到執行團隊提升 AI 素養與風險辨識能力。

張董事長強調，有效之 AI 治理，需要各方利害關係者攜手合作，並建議組織可採納「3+1 道風險控制防線模型」建構 AI 治理模型：

(一)第一道防線：由直接參與 AI 系統應用與開發的團隊負責，如數據品質管理、AI 解決方案開發、AI 系統部署與運維、業務需求與應用創新團隊，確保系統規劃、數據品質、內部測試與記錄開發過程。

(二)第二道防線：由法遵、風控、資安及業務督導單位共同確保 AI 應用符合法規、保障資訊資產、識別與管理風險、並遵循道德原則。

(三)第三道防線：由內部稽核單位獨立客觀檢查與評估 AI 運作流程，而 AI 倫理委員會則專注於倫理和社會影響層面進行審查與指導。

(四)高階指導與外部控制：董事會為「最高審核官與價值守護者」，AI 治理委員會是「策略總指揮部」，第三方鑒證機構是「外部驗證師與公信力背書者」，事業主管機關是「規則制定與監督者」，透過組織內部高階指導與外部獨立審查，共同確保 AI 治理的健全與合規性。

二、創新風險

張董事長指出，過去一年全球已採用生成式 AI 的企業從 32%大幅增加到 83%，臺灣企業則從 14%增加到 58%，並且有超過三成企業因採用生成式 AI 增加獲利，顯見企業積極擁抱 AI 革命新浪潮。然而，僅有 5%臺灣企業高度信任生成式 AI，低於全球 33%，顯示 AI 衍生的信任議題仍是一大挑戰。張董事長接著列舉 AI 創新帶來的多方風險與因應措施：

(一)AI 決策黑箱導致信任風險：導入可解釋 AI 與強化管理機制

AI 模型欠缺可解釋性，恐導致如顧客貸款被拒卻無法得知原因、收到邏輯矛盾的投資建議等問題，有損顧客對金融機構的信任，也不符法規對透明度的要求。為降低此類風險，機構應依據風險等級導入可解釋 AI(XAI)技術，並建立涵蓋開發、驗證與監控等階段的模型風險管理與人工審核機制。

(二)技術創新引發倫理風險：藉由監理沙盒測試並強化控管

若在未成熟或缺乏管控的情況下導入新技術，可能引發營運中斷或倫理風險。例如：AI 生成的投資報告使用煽動性語言鼓吹高風險標的，或因 API 整合錯誤導致顧客資產數據顯示不實，皆可能損害顧客權益。企業可善用監理沙盒與內部實驗平台，於風險可控環境下測試應用，確保創新與風控平衡。

(三)資安邊界模糊化提升攻擊風險：強化 AI 資安偵測與保護

新興網路風險如 AI 偽冒的網路釣魚信件、透過 AI 模型數據污染攻擊(Data Poisoning)在訓練資料中注入惡意資訊、或 IoT 理財應用擅自存取顧客個資，皆使資安風險倍增。建議金融機構應建立 AI 驅動的威脅偵測系統，提升即時防禦力，並落實數據生命週期治理及零信任架構，強化從資料源到設備端的全流程防護。

(四)AI 錯誤決策引發責任歸屬問題：建立明確顧客權益保障機制

當 AI 服務涉及多方技術與外部供應商時，決策錯誤容易導致責任不清與顧客權益受損，例如：AI 錯誤生成假新聞引發市場恐慌，導致股價劇烈波動與投資人損失，卻因合約未釐清權責而求償無門。企業應明訂與第三方的合約條款，將責任與賠償路徑明確化，並設計能快速轉介人工處理的客服機制，加強風險揭露與用戶知情同意流程，保障顧客權益。

三、安全風險

世界經濟論壇(WEF)「2024~2025 全球風險報告」指出，虛假訊息傳播、網路間諜活動與網路戰爭列為近年主要風險前五名，AI 技術造成之不良後果列為長期風險第六名。常見的 AI 攻擊手法「提示詞注入(Prompt Injection)」，其通過精心設計的輸入操縱大型語言模型(LLM)可能導致未經授權的訪問、數據洩露和決策受損，例如使用

ChatGPT 時若瀏覽到有心人士刻意產生的網頁內容，就會直接被催眠、未經用戶同意即依照網頁指示對用戶 Github 帳號做出有害的設置。張董事長接著分享安全面之管理困境與具體控制實務：

(一)AI 詐騙與系統攻擊威脅升高：導入零信任架構

面對詐騙者利用 AI 生成釣魚訊息或操控模型進行攻擊之風險，建議應建構 AI 驅動的防禦機制，導入威脅偵測、零信任架構與權限控管，並加強模型加密、版本管理與安全測試，確保系統穩定與風險可控。

(二)敏感資料外洩風險增加：強化資料治理與內部控管

若員工私自使用顧客機敏資料於生成式 AI 恐有個資外洩之虞，建議應落實資料分類、加密、驗證與存取控管，建立資料流追蹤與異常行為監控，並加強員工資安意識與操作規範，降低洩漏風險。

(三)第三方供應商風險擴大：建立供應鏈風控與合約規範

AI 系統多由外部廠商建置或維運，若缺乏審查與監控，恐引入技術與法遵風險。建議應強化供應商盡職調查，明訂合約責任與資安要求，定期稽核 API 串接、資料交換與更新流程，確保供應鏈透明與可信度。

(四)AI 模型易遭竊用與濫用：強化資產保護與演算法防護

AI 模型和相關知識產權可能面臨未經授權的複製或竊取風險，建議應對模型加密儲存、限制存取權限與版本管理，並實施 AI 專屬漏洞測試與防逆向設計，建立 AI 資產保護框架。

四、責任風險

張董事長以實例說明金融業社會道德責任之兩難：當金融機構授信業務透過 AI 信用評分系統自動分析客戶資料並做出決策，不必親自審核每一筆貸款申請，僅在異常發生時由 AI 風險監控系統即時發出警報。然而，演算法可能無意間對特定族群產生偏見，例如缺乏傳統信用紀錄的年輕人或弱勢族群，AI 在投資決策中可能會為了短期報酬而忽視長期永續發展因素，可能損害金融機構的長遠利益與社會形象，這些看似技術的決策，實則反映深層的社會價值選擇。

面對 AI 技術引發之責任風險與挑戰，張董事長建議應在設計 AI 系統時應賦予人類足夠的代理權與監督權，必要時能介入控制、審查與最終決策以確保 AI 系統不會損害人類基本權利；針對演算法偏見與歧視問題，應使用多元化、具代表性之數據集，謹慎使用可能產生偏見之個人屬性資料，並可邀請跨領域專業人員參與 AI 評估過程；並且在 AI 應用的同時善盡永續發展責任，運用 AI 促進普惠金融數位轉型與降低數位落差。

張董事長強調：別為了一時的效率，而犧牲長遠之信任。打造負責任的 AI 並非一次性達成的目標，而是需要持續學習、反思和改進的旅程，透過多方協作與共創，平衡創新與責任。AI 治理基礎須結合適當的策略、客製化的風險管理架構、安全部屬的 AI 技術與接收相關培訓的員工，方能打造兼顧安全與合規之營運環境。