金融監督管理委員會因公出國人員出國報告
（出國類別：開會）

第 6 屆「金融服務與雲端」峰會

服務機關：金融監督管理委員會銀行局

姓名職稱：童副局長政彰、林緯政專員

派赴國家/地區：馬來西亞

出國期間：**113** 年 **5** 月 **27** 日至 **113** 年 **5** 月 **29** 日

報告日期：**113** 年 **6** 月 **29** 日

摘要

在馬來西亞吉隆玻舉辦之第6屆「金融服務與雲端」峰會係由國際金融協會(Institute of International Finance, IIF)、東南亞國家中央銀行(South East Asian Central Banks, SEACEN)研究與訓練中心，以及亞馬遜雲端運算服務公司(Amazon Web Services, AWS)合作舉辦。本會議共有來自11個國家約100位金融服務業及科技業相關者參加，包括各國之監理機關、金融機構及產業代表。

會議採實體會議辦理，主題聚焦於雲端服務於提供人工智慧(Artificial Intelligence，下稱AI)相關解決方案之角色，以及透過雲端使用AI之跨境監理制度設計等議題。

本次會議議題包含IIF之「人工智慧、資料和雲端—金融服務中的連結、創新和價值創造」報告、亞太地區金融業的AI應用及監管政策發展、AI在公部門與私部門應用之案例分享、使用雲端服務之集中風險及美國財政部對AI應用之監管政策等，對我國監管業務推展具參考價值。

其中，於「金融業使用人工智慧之新興監管框架(Emerging Regulatory Frameworks for AI Use in Financial Services)」場次，主辦方邀請本會銀行局童副局長政彰擔任講者，向與會者分享我國金融業AI應用情形、監管框架及國際政策趨勢等內容，並獲與會單位正面迴響。

本報告將就會議討論重點進行摘述，並據以提出心得與建議，做為未來相關政策規劃之參考。

目錄

壹、背景說明 3
貳、高峰會之演講及座談會 4
一、「人工智慧、資料和雲端—金融服務中的連結、創新和價值創造」報告 4
二、「生成式 AI、大語言模型與雲端的崛起」座談會 9
三、「展望亞太金融服務業的 AI 應用及其監管」座談會 10
四、「AI 的可及性和可用性」座談會 11
五、「利用 AI 工具於公共部門：監管科技、監管技術和數位政府」座談會 11
六、「全球背景下，亞太區在金融業 AI 監理的多元方法」座談會 12
七、「欺詐和新的風險向量：利用 AI 實現快速因應」座談會 14
八、「金融業的集中風險探討」報告 14
九、「透過雲端實現營運韌性、網路安全和風險緩解」座談會 15
十、「亞太區以外的政策實踐與見解」爐邊會談 16
參、心得與建議 18

壹、背景說明

「金融服務與雲端：與監理機關及金融機構高峰會(Financial Services and the Cloud: A Summit with Regulators and Financial Institutions)」係由 IIF 與 AWS 等單位籌辦之活動，會議主要係邀請亞太地區之金融監管單位與金融機構參與，就金融機構使用雲端服務相關議題進行探討。

本(2024)年度為第 6 次舉辦，於 2024 年 5 月 28 日假馬來西亞國家銀行(Bank Negara Malaysia)訓練中心之場地舉行，由 IIF、SEACEN 研究與訓練中心及 AWS 共同舉辦，本次主題係探討金融業使用 AI 及雲端服務相關監理議題。

本次會議計有來自 11 個國家約 100 名金融監管人員、金融業者及科技產業之代表參與，會議採邀請制閉門會議，以**查達姆研究所規則 (Chatham House Rule)[1]進行，意即參加會議參與者以自由使用討論中的資訊，但不得透露誰發表了任何特定評論，以促進討論的意見表達**。

[1] Chatham House(2024),Chatham HouseRule, available at https://www.chathamhouse.org/about-us/chatham-house-rule (last visited:2024.06.21).

貳、高峰會之演講及座談會

會議首先由 IIF 於會議分享所發布之「人工智慧、資料和雲端—金融服務中的連結、創新和價值創造(AI, DATA, AND THE CLOUD - Connectivity, Innovation, And Generating Value In Financial Services)」報告，再由各國金融監理官員及金融機構代表就擔任座談會之與談人，就金融業使用 AI 與雲端服務涉及之實務案例、風險控管、監理制度與資料治理等議題進行分享與探討。

本會銀行局之代表童副局長政彰擔任「全球背景下，亞太區在金融業 AI 監理的多元方法」座談會之與談人，就我國金融業 AI 發展現況及監理政策進行分享，並獲與會人員熱烈反響。

本會議之演講及座談會之議題整理如下：

形式	議題名稱
演講	「人工智慧、資料和雲端—金融服務中的連結、創新和價值創造」報告
座談會	生成式 AI、大語言模型與雲端的崛起:金融服務、開發人員和支援者
座談會	展望亞太金融服務業的 AI 應用及其監管:發展、部署和治理
座談會	AI 的可及性和可用性 - 雲端、資料可用性和複雜業務模式的角色
座談會	利用 AI 工具於公共部門:監管科技、監管技術和數位政府
座談會	全球背景下，亞太區在金融業 AI 監理的多元方法
座談會	欺詐和新的風險向量：利用 AI 實現快速因應
演講	金融業的集中風險探討
座談會	透過雲端實現運營韌性、網路安全和風險緩解
爐邊會談	亞太區以外的政策實踐與見解

以下摘要各場活動之討論內容，並配合本會議主辦方所要求用之**查達姆研究所規則 (Chatham House Rule)**，不揭露與談人之代表單位、名稱及職銜。

一、「人工智慧、資料和雲端—金融服務中的連結、創新和價值創造」報告[2]

(一) 報告之撰寫團隊、撰寫目的、研究方法

該報告由 IIF 撰寫，旨在剖析 AI、資料和雲端服務在金融生態系之價值，探討生成式 AI 對金融機構影響、AI 之開發、部署和治理所涉及之風險管理議

[2] IIF，AI, Data, and the Cloud – Connectivity and Value Creation in Finance，Available at https://www.iif.com/Publications/ID/5777/AI-Data-and-the-Cloud-Connectivity-and-Value-Creation-in-Finance

題，以及所衍生之政策和監管問題。研究方法包括對金融機構首席執行長(CEO)和高級經理人的訪談、整理相關監理文件，並引用 IIF 於 2023 年 12 月發布之「生成式人工智慧使用情況調查報告(Survey Finds Generative AI in 2023)」[3]，作為相關論述之補充。

(二) 金融產業 AI 應用之當前發展

金融業長期以來一直是 AI 技術的使用者。近年來，隨著 AI 工具之創新發展，以及使用情境擴展，使這項技術成為金融創新領域最具發展潛力之項目。另一方面，隨著 AI 模型的複雜性和成熟度提升，各界也更容易取得及使用相關技術及服務。以近期引發眾多關注的生成式 AI 工具為例，其通常提供易於使用的操作介面，使得使用者幾乎不需要電腦或統計知識，即能上手使用並產生一般大眾均可以理解的內容。

雲端服務是開發和採用 AI 的重要基礎設施，因為 AI 的訓練和開發需要強大的計算能力以及大量優質資料支持，只有少數專注於 AI 技術的大型科技公司有能力開發與建構可應用於各個產業的大型人工智慧模型（即所謂的基礎模型），基礎模型完成開發後，其他協力廠商可於此基礎上再行開發符合金融產業需求之 AI 應用，並提供金融機構使用。AI 模型之生命週期可以分為「開發和測試」、「部署和完善」及「使用和驗證」等階段，並可依執行者或執行情境再細分(詳見表格 1)。

表格 1：AI 模型開發生命週期

	步驟一 **開發與測試**	**步驟二** **部署與完善**		**步驟三** **使用和驗證**
動作	開發基礎模型	客製化基礎模型，使其適用於金融服務用例	模型微調	使用模型
執行者	大型科技公司 (如 AWS、微軟、Google、臉書等)	專注於金融服務的 AI 服務供應商 (部署者 1)	金融機構 (部署者 2)	金融機構員工

來源：IIF ，AI, Data, and the Cloud – Connectivity and Value Creation in Finance

依據相關法規及金融機構內部風險管理框架，金融機構應要求外部服務提供者之 AI 模型具有與內部開發模型有相同驗證等級。然實務上許多金融機構表示，在日益複雜的 AI 產業鏈中，其能掌握的資訊有限，故難確保達成相關監理要求。依據 IIF 於 2023 年進行調查，只有 3% 受調查金融機構表示有信心獲得生成式 AI 模型的必要資訊，以達到等同於傳統內部 AI 模型的驗證水準。

[3] IIF, New IIF-EY Survey Finds Generative AI Could be Revolutionary for Financial Services，Available at https://www.iif.com/About-Us/Press/View/ID/5611/New-IIF-EY-Survey-Finds-Generative-AI-Could-be-Revolutionary-for-Financial-Services

另 78%受訪金融機構表示，對內部人員使用生成式 AI 已設有相關限制，81%受訪機構表示規劃將生成式 AI 限制於內部使用，而不提供客戶端應用。

金融機構採用由協力廠商構建的 AI 模型之情形日益普遍，並透過對 AI 模型進行客製化以符合其實際應用需求。前述客製化過程可由金融機構自行完成，或由專注於金融領域之外部服務提供商執行。惟金融機構對於外部開發系統之掌握度及信賴度仍不足，故金融機構仍持續自行開發 AI 模型以執行須非常精確之資料處理工作，特別是涉及使用機敏性資料之工作。

(三) 底層基礎設施對金融領域 AI 應用之影響

開發生成式 AI 模型可能比傳統 AI 模型所需資料及運算能力大 10 倍至 100 倍，由企業內部自行開發生成式 AI 模型可能會面臨成本高昂或是效率不佳的問題。因應此問題，目前許多企業係採取雲地混合模式，將內部資源與雲端服務相結合，以提高資源運用效率。

同時使用多個公有雲服務(跨雲)也是一大發展趨勢，根據 AI 服務提供商 Snowflake 研究，同時使用三大公共雲服務(AWS、微軟及 Google)的企業或機構，數量在 2023 年增加 207%。

使用外部開發的 AI 模型，或在雲端訂閱服務進行 AI 模型的開發或運行，將給金融機構帶來第三方風險。雖金融機構有豐富的業務委外經驗，對管理第三方風險並不陌生，但 AI 供應鏈涉及多的階層及多階段之供應商管理，使得問題比以往複雜度提升許多，亦將對既有風險管理框架帶來挑戰。美國國家標準和科技機構（National Institute of Standards and Technology，簡稱 NIST）於 2023 年 1 月發布的「人工智慧風險管理框架(AI Risk Management Framework 簡稱 RMF)」指出，使用者對 AI 工具的管理訓練資料品質、偏見(bias)、虛假信息(disinformation)及軟體漏洞的能力感到顧慮[4]。

該報告指出，針對金融業所使用之 AI 服務，各角色在不同階段有不同的責任：

1. **開發階段**：開發人員應考量提高**透明度**(判斷演算法如何及為什麼得出特定結論或決策的能力)的方法。為使開發出的 AI 工具符合金融機構之期待，於此階段第三方提供商需要熟悉金融機構在管理和報告 AI 工具風險相關責任及監理機關之期望，以做出相應之調整及設計。
2. **部署階段**：此階段部署者(包含外部廠商及金融機構內部資訊人員)和使用者間的溝通將成為重點，因此時使用者將考量 AI 工具的透明度，以及何時以及如何最終使用 AI 工具。為使 AI 之使用擴散順暢，使用者教育將至

[4] AI Risk Management Framework – Section 3. National Institute of Science and Technology (NIST), Department of Com-merce of the United States. 2023. Available at https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF/Foundational_Information/3-sec-characteristics

關重要，隨著使用者熟悉 AI 工具，其辨識 AI 生成的內容和建議的能力也會成長。

由於 AI 服務涉及多個參與者，終端使用者難以完全瞭解 AI 服務的所有面向，因此須由各參與者的共同努力控管相關風險。該報告建議可參酌「**風險緩解責任應由最有能力緩解該風險的人承擔**」之原則，建立風險管理架構，例如 AI 模型開發人員更適合確保使用符合標準之資料進行模型訓練，並測試模型是否存在偏誤，而部署人員更適合設定使用者互動參數，以防止資料洩露。

(四) 政策考量

自 2022 年 11 月 Chat GPT 推出以來，金融機構和監管機關加強對 AI 之開發、部署和治理等議題之關注。然而 AI 政策涉及議題不僅限於金融監管部門，還包括國家安全機構、技術標準制定者和個人資料政策主管部門。

截至目前為止，全面性的 AI 監管法規仍很少見，但安全、透明、公平和問責等共同原則已廣為各國政府所採納，並出現在世界各國的政策文件中。該報告整理國際間 AI 相關監管宣言及政策文件，舉如「G7 AI Declaration」、「G77 AI Pledge」、「G20 AI statements， Digital Economic Partnership Agreements」及「Trade Agreements in 2021-present」，並歸納其所揭示的國際 AI 發展承諾的共通項目，詳見**表格 2**：

表格 2：國際 AI 發展承諾的共通項目

Combating discrimination and bias 打擊歧視和偏見	適當執行個人資料保護法規
	促進道德 AI (道德 AI仍未有廣泛被接受之定義)
	在政府採購中納入反歧視條款
	將減輕AI偏見納入監管政策
	分享資料治理最佳實踐
Enhancing Security 加強安全	將 OECD 關於政府獲取個人資料的原則納入貿易承諾
	促進 IT 環境的最佳實踐
	重新審視和修訂風險管理框架
	將隱私權準則納入國內標準
Promoting Accountability 促進問責	將美國的 NIST AI RMF 納入貿易承諾
	參照「 G7 人工智能行為準則」制定AI的雙邊協議
	評估使用AI模型在執法行動中的標準，保持透明
Explainable and Interpretable Results 可解釋和可理解的產出	合作制定技術標準和透明度要求
	利用G7發布之原則作為承諾的基礎
	致力於查核實務和評估方法的相互認可
Creating AI opportunity 創造 AI 發展機會	減少 AI 商品和服務之貿易壁壘
	建立 AI 人才專家網路
	合作制定國際 AI 標準
	分享資料治理最佳實踐

來源：IIF ，AI, Data, and the Cloud – Connectivity and Value Creation in Finance

此外，AI 模型的開發和部署經常跨越多個市場，因此「政策的互操作性」及「促進資料跨境傳輸」對於 AI 的發展至關重要。正因為跨境議題的複雜度，**AI 的有效監管更須取決於多個部門的共同努力**，各層面之利害關係人共同參與將是監管政策得以落實之關鍵。

再從 AI 的應用可能性來看，其應用領域廣泛，涉及之議題可能包括國家安全、個人資料等人權保護、消費者保護、經濟穩定、市場集中度及避免反競爭行為等，其監理制度之設計自然較一般科技困難，為各國金融機構及監理機構帶來嚴峻的挑戰，且僅依靠其既有之資源或執法權限恐難以達成，亟需跨領域/跨機關之合作。

考量鑒於 AI 監管之複雜度，目前許多國家政策制定者仍以瞭解 AI 及發展 AI 為優先選項，而非制定發展 AI 相關之治理原則和安全標準等規範性法規。此外，更有部分國家推動人工智慧發展戰略，以積極推動其國內 AI 產業領域的發展，這些戰略之共同特徵包括在確保資訊安全、隱私保護及避免歧視的同時，增加國內算力及促進資料流通。

在主要國家的監管政策進展方面，歐盟已經制定了「人工智能法案(Artificial Intelligence Act)」，為目前國際間採取相對較為嚴格之管理做法。該法案將 AI 應用區分為 4 個風險級別，分別為最低風險或低風險、有限風險、高風險、不可接受風險，分別適用不同強度之規範以管理相關應用和開發。其中高風險及不可接受風險活動是該法案所主要規範對象，舉如「用以審核信貸及保險服務案件之 AI」屬於該法案所定義之高風險活動，其應遵循透明性之要求及事前審慎評估等。

中國大陸的國家互聯網信息辦公室於 2023 年 8 月 15 日發布施行「生成式人工智慧服務管理暫行辦法」，規範向中國大陸境內公眾提供生成式 AI 服務之行為，並制定生成式 AI 服務提供者在法律上應遵循事項，包括與註冊使用生成式 AI 之使用者簽訂服務協議，明確雙方權利義務，採取有效措施防範未成年人用戶過度依賴或者沉迷等[5]。另中國大陸民眾無法直接國內使用 ChatGPT 或 Google Gemini 等生成式 AI 服務，需藉由虛擬私人網路（Virtual Private Network，縮寫 VPN）或是中國大陸內境之代理商，方得使用該等服務。

美國目前監管部門未就 AI 訂有規範性法規，係制訂 AI 開發標準，同時為 AI 使用者提供自願性風險管理框架。例如美國 NIST 於 2023 年 1 月發布的「人工智慧風險管理框架 (RMF)」[6]，就 AI 之採用提供可參考標準，包括：

[5]國家互聯網信息辦公室，生成式人工智慧服務管理暫行辦法，來源：http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/zhengceku/202307/content_6891752.htm

[6]AI Risk Management Framework. National Institute of Science and Technology (NIST), Department of Commerce of the United States. 2023. Available at: https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF/Foundational_Information/3-sec-characteristics

- 評估 AI 工具的風險，包括服務提供商、軟體、硬體和資料相關風險。
- 根據所參與的 AI 價值鏈階段，瞭解並採取不同的風險控管措施。
- 定義風險容忍度(risk tolerance)，其意涵為「為實現目標而承擔風險的準備」，並應注意「對企業或社會可接受的風險水準，與背景環境及具體應用情境高度相關」。
- 優先關注可能產生高風險的 AI/ML 使用案例，並應建立得以停止 AI 模型的探索、開發或部署的「安全的方式」，使風險得到充分管理。
- 建立並維持適當的問責機制、角色區分和職責、文化和激勵結構，使風險控管措施得以落實。
- 追蹤新興和潛在風險。

因建構 AI 模型需使用大量且高品質的資料，對於資料流通之監管法規將影響 AI 產業發展。擁有大量資料及負責任的資料共享框架的國家，有利於 AI 技術快速發展。該報告發現亞洲地區的資料在地化(限制資料等不得跨境傳輸或儲存)及個資保護政策相對嚴格，可能為 AI 發展帶來挑戰。

(五) 結論

生成式 AI 的出現，迅速改變人們對如何開發、使用和治理 AI 的看法，並驅動許多國家進行相關監管活動。綜觀近期各國監理政策之變化，可看出 AI 相關監管活動之政策高度多訂於國家戰略層面，且其執行並非僅由金融監管機關負責。金融業在資料管理、技術監督和風險管理方面，較多數產業採取更高標準，金融機構作為 AI 產業之重要利害關係人，在政策討論和標準制訂過程中扮演重要角色。

考量 AI 價值鏈的複雜性，金融業及金融監管機關需拓展其互動的對象，邀集更多利害關係人共同參與相關政策及技術標準之討論，以確實落實風險管理。此外，為充分發揮金融領域 AI 創新的潛力，金融業之資料管理政策、雲端服務政策、AI 安全政策以及負責任的治理和監督方法需更緊密的連結，以確保相關政策發展時能保持一致。

二、「生成式AI、大語言模型與雲端的崛起：金融服務、開發人員和支援者」座談會

(一)生成式 AI 的優勢及金融應用

生成式 AI 與傳統機器學習模型不同之處在於，可利用大量未標記資料，無需人工標記[7]即可訓練模型。這使得金融機構得以使用內部資料來建立自己的生成式 AI 應用。生成式 AI 可應用在客戶溝通、行銷廣告、法令遵循調查等多個領域，例如可回應更複雜的客戶問題，提供個性化理財建議。在一些

[7]資料標記是將原始資料 (影像、文字檔案、影片等等)進行識別，並新增一或多個有意義與資訊性的標籤來提供內容的過程，讓機器學習模型可從中學習。舉例來說，標籤會顯示相片中是否有鳥或車子，指出一段錄音中會說出哪些字詞，或者一張 X 光片中是否有腫瘤，機器透過有標記的資料尋找共同特徵，以用於對新資料進行預測。

使用情境下，使用生成式 AI 創作內容，能將廣告轉換率提高 90%，縮短法令遵循調查時間，減少誤判率 25%。

(二)金融機構面臨的挑戰及因應

儘管生成式 AI 帶來許多機會，但金融機構在推動相關應用時仍面臨挑戰，因技術尚未完全成熟，需投入研究人員以掌握最新發展並制定指導方針。監理機關對生成式 AI 仍存有疑慮，金融機構須先在內部實驗、評估風險及偏見，確保應用於外部環境時風險無虞。對於跨國金融機構而言，需思考因各國資料在地化要求及個人隱私法規差異之應對策略。因目前各方正在制定不同的生成式 AI 規範，缺乏統一之指引架構，有待進一步統合。

(三)生成式 AI 未來展望

整體而言，生成式 AI 正推動金融服務創新，為產業帶來變革契機。生成式 AI 能將重複工作自動化，使人力投入在更有價值的工作。透過個性化建議及溝通能力優化，生成式 AI 將有助於提升客戶體驗，增強客戶服務。金融機構亦可利用生成式 AI 優化內部作業流程，降低成本並創造新商機，提高效率及收益。預期生成式 AI 將持續影響金融業發展，相關監管架構亦將逐步建立，金融機構應積極部署及調整策略，及早掌握這波浪潮。

三、「展望亞太金融服務業的AI應用及其監管：發展、部署和治理」座談會

(一)金融機構資料與 AI 應用之發展歷程

泰國金融機構約在五年前開始重視核心業務資料管理，制定相關政策框架，並逐步建立資料分析應用。隨資料管理機制日趨成熟，內部開始思考如何利用 AI 創造更大價值。銀行業者由於長期以來落實內部控制管理，已累積良好資料文化基礎，有利於轉型應用 AI。現階段需思考如何由傳統「規則主導模式」AI，轉移至機器學習模式[8]，但同時兼顧透明性、公平性和解釋力。

(二)AI 應用於客戶體驗與風險管理的策略方針

金融機構 AI 應用著重資料品質管控，瞭解資料來源並確保完整性，尤其關注邊緣群體是否被遺漏。評估資料偏差並採取措施修正，且需告知高層主管獲取認同。監控指標和跨部門問責機制也是關鍵，如發現偏差須及時修復資料。與談金融機構表示其發展 AI 強調透明度和人工干預，應避免 AI 演算法變成人類無法理解之黑箱，並致力維持客戶對金融機構資料處理的信任感。對內部而言，透過培訓課程提高員工資料素養。對外則採取不同溝通管道，讓客戶瞭解金融機構相關資安與隱私保護政策。

[8]「規則主導模式（rule-based model）」又稱專家模式，由人類寫出規則再交由電腦執行，優點為邏輯清楚可見，易於檢視修正，但 AI 之潛能限於人類專家的能力；「機器學習模式」則係由數據自動歸納出輸入與輸出的關係，沒有外部給定之具體規則，人類不易理解內部運算方式，係目前 AI 技術開發之重點。

(三)金融機構 AI 創新應用與願景

金融機構正運用 AI 改善客服中心的自動化作業，透過自然語言處理減少人力查詢產品資訊的時間，預計可節省約 18%的工時。同時也努力整合多項保險理賠系統於單一大型應用架構，透過 AI 預測推薦附近醫院和保險福利等資訊，優化客戶體驗。在未來 12 至 18 個月，與談金融機構期望 AI 能在提升營運效率和改善客戶體驗方面有所突破。未來將關注將生成式 AI 與現有機器學習模型互補應用，用不同視角解決相同的問題，例如貸款審核、貸款條件設定、貸款收回等議題。

四、「AI的可及性和可用性 - 雲端、資料可用性和複雜業務模式的角色」座談會

(一)AI 在金融業的應用與挑戰

雲端服務主要優勢包括可用性(accessibility)、全球資料中心協作，以與創新生態系統的緊密關係，有助於金融業者利用雲端服務部署 AI 應用。然而，金融業在部署 AI 時仍面臨許多挑戰，如資料優化及使用者濫用自動化的風險，教育使用者瞭解 AI 運作原理至關重要。使用 AI 之挑戰還包括遵守跨境資料轉移和隱私法規、資料不易追溯來源、資料清理、人才缺乏等。

(二)AI 治理相關措施

要妥適治理 AI 應用，包括許多面向，如資料治理、AI 演算法及使用者之控管等。在資料治理方面，相關措施包括建立資料所有權與問責機制、資料品質及法令遵循監控。在 AI 演算法之控管方面，可成立跨學科團隊來評估 AI 應用之風險並制定風險緩解措施，另設有獨立驗證團隊，在 AI 部署前進行符合公平透明原則的審查。對於使用者之控管，可建立使用 AI 模型的集中化權限控管，確保使用者明瞭責任及義務。最後，應與相關利害關係人積極合作，制定負責任的 AI 使用規範與標準。

(三)整合 AI 之挑戰

將 AI 整合至既有基礎設施時，需處理既存系統與流程之調適。關鍵在於瞭解 AI 可能帶來的風險，從法令遵循之角度給予指引。藉由法令遵循團隊及相關單位意見，權衡解決方案的配置性及在不同司法管轄區的限制，選擇適當替代方案，促進各部門之間的協作與模型分享，讓 AI 的運用更臻成熟。同時也應重視監理機關在 AI 治理之相關政策，雙方應保持良性互動，共同推進 AI 的負責任發展。

五、「利用AI工具於公共部門：監管科技、監管技術和數位政府」座談會

(一)AI 在金融監理機關之應用

金融監理機關積極運用 AI 技術，如澳洲監理機關以利用機器學習處理投訴資料、偵測詐騙案件，並開始探索生成式 AI 的應用。菲律賓監理機關則長期使用傳統機器學習模型進行預測、識別異常行為，並著手於整合自動化監

理流程，引入 AI 和區塊鏈分析技術。國際清算銀行(Bank for International Settlements，簡稱 BIS)則發佈報告，列舉央行在總體經濟分析、支付系統監管、金融穩定性的 AI 應用案例，同時該單位正進行多項 AI 專案。總結來說，許多監理機關已導入 AI 技術在其監理業務，並已有初步成效。

(二)AI 監理面臨挑戰與因應之道

AI 監理面臨的主要挑戰包括跨境資料轉移法令遵循、資料來源難以追溯、資料清理、吸引專業人才等。相對應對之作法包括識別 AI 風險並利用公開標準進行風險管理、制定相關指引、採用第三方驗證等機制。對於採用類神經網路技術之 AI 有不易解釋之問題，可藉由人為監督併同其他驗證方式因應。整體而言，現有 AI 一般性原則可作為相關政策之基礎，未來持續視產業需要推出高階治理原則和監理指引。

(三)AI 人才培育與監理規畫

金融監理機關普遍面臨 AI 人才缺乏的困境，相較民營機構，公部門在薪酬福利上難以競爭，因此可透過內部培育和外部招募並行，並透過外部企業獲取專業服務等方式因應。在組織架構上，可採取集中與分散並行的「輻射式網路(Hub-and-Spoke)」模式，有專精於資料分析處理之專門團隊，同時也將相關人才分散在各部門，使各部門內部均有瞭解如何利用有效率應用資料。未來在人力資源政策上，需提高薪酬競爭力，為員工創造誘因。

六、「全球背景下，亞太區在金融業AI監理的多元方法」座談會

(一)臺灣在 AI 領域之監管政策

本會銀行局之代表童副局長政彰擔任本座談會之與談人，就我國金融業 AI 發展現況及監理政策進行分享。

我國在 AI 之監理政策採取開放且謹慎的態度，臺灣金融業已積極採用 AI 技術，透過公私部門合作，使用 AI 協助防制詐騙且有顯著之成效。為金融機構妥善利用 AI 技術，金管會於 2023 年 10 月發布「金融業運用人工智慧(AI)之核心原則」，強調以負責任創新為核心，鼓勵金融機構善用 AI 科技投入創新，該原則可用 SAFEST（最安全的）六個英文字母總結：

- 保護(**S**afeguarding)隱私和客戶權利。
- 問責(**A**ccountability)和治理機制
- 公平性(**F**airness)和以人為本的價值，
- 確保(**E**nsure)系統穩健性和安全性，
- 可持續(**S**ustainable)發展，
- 透明度(**T**ransparency)和可解釋性。

隨著全球各地出現各種監管方法，監理制度互操作性(interoperability)是確

保經商便利度和促進創新的一個重要面向，如聯合國大會即於 2024 年 3 月通過首個 AI 決議，其意旨在拉近各國人工智慧發展鴻溝，平衡創新與監管。在促進 AI 監理互操作性方面，本會政策框架可總結為"S-T-A-R"四個重點：

- **引導(S**teering**)**：監理機關在金融機構導入 AI 運用時仍應保持主導地位，確保政策和規範能夠有效執行，並且引導金融機構在法令遵循的基礎上創新。
- **透明度(T**ransparency**)**：金融機構在使用 AI 技術時，在 AI 模型之設計、資料使用及決策過程均應保持透明，這有助於落實監理，並且增強客戶信任。
- **聯盟(A**lliance**)**：金管會持續與國際組織和人工智慧服務提供者進行溝通和合作。目的是分享經驗、瞭解最佳實踐，追蹤國際監管和技術發展趨勢，確保政策與國際接軌，同時兼顧實務操作。
- **風險導向(R**isk-based**)**：金管會要求金融機構在導入和運行 AI 技術時，採取風險導向的方法，確保風險識別、評估和管理的流程完善，並且將風險控制在可接受的範圍內。

(二)AI 與促進女性普惠金融

男性與女性在獲得貸款等金融服務有巨大的性別差距，因此已有金融機構透過 AI 分析數據，在低收入婦女中尋找合適之客戶，提升女性獲得金融服務的機會，不僅促進性別平等，也能促進整體經濟發展。AI 也可以改善金融服務和監管決策，促進多元化和包容性，例如在金融業員工聘僱上採取更多元包容的做法。

AI 可能產生偏見問題，特別是無意識偏見(unconscious bias)，因為過去基於先入為主觀念而產生之資料若用於 AI 訓練，AI 將複製既有之偏見，雖偏見不必然導致歧視，也不一定產生不良之結果。因此與會者建議在產品設計和政策制定時，應考慮性別觀點多樣性，將金融普惠視為重點。

(三)金融業 AI 風險控管之實務

AI 帶來的風險包括模型風險、公平性、敏感性和準確性問題。現有的風險類別可能無法完全涵蓋 AI 之潛在影響範圍，因此需要保持開放心態。

目前各國 AI 監管政策仍有不一致的情形，短期內會出現多種監管方法並存的情況，但長期可能會趨向融合。因此建議各國監理機關應促進對於風險理解及相關用字的一致，並制定風險緩解之國際標準，同時關注服務提供者集中度帶來的潛在風險。

AI 正在為金融業注入新的活力，但風險挑戰也無時無刻不在。採取以風險為本的審慎監管，鼓勵創新但同時堅持審慎，並在公私營部門間建立廣泛合作，將是有效管控人工智慧風險的關鍵所在。

七、「欺詐和新的風險向量：利用AI實現快速因應」座談會

(一)不斷變化的支付威脅

隨著科技的進步，支付領域的威脅也在不斷演變。現在網路攻擊不再是尋找最嚴重系統漏洞，而是尋找最薄弱的環節。犯罪即服務(crime as a service)的商業模式，使得幾乎任何人都可以購買相關工具發動攻擊。在亞太地區，常見的詐騙類型包括求職詐騙、電子商務詐騙、愛情詐騙等。值得注意的是，電子商務、貸款和投資詐騙的數量有所下降，這可能與企業加強防禦措施相關。然而，愛情詐騙、冒充詐騙和社交詐騙卻在增加，這代表攻擊變得越來越複雜。

(二)應對新興威脅的策略

為應對不斷變化的威脅，業者的因應策略正從偵測轉向事前預防。產業界正在投資分層防禦策略，並加強系統韌性計劃。政府、監理機關和董事會也越來越重視網路安全和營運風險，這有助於企業進行相關必要的投資。跨部門合作以及與監理機關的合作也在加強，特別是在生成式 AI 出現帶來新的挑戰和機遇。AI 被用於預測詐騙，改善和個性化用戶體驗。然而，生成式 AI 也被使用於詐騙活動，這使得詐騙防制變得更具挑戰。

(三)生成式 AI 的監管與企業應用

生成式 AI 的出現對監理機關和企業都帶來了新的挑戰。監理機關正在與私部門合作，制定政策，確保 AI 的透明度、責任和公平性。企業則需考慮 AI 設計的安全性和隱私性，並建立機器學習開發生命週期。對於企業資訊安全主管來說，其角色也在不斷改變，需要與監理機關及服務提供商等合作夥伴密切合作，瞭解 AI 的潛力和風險，並確保在採用 AI 時有適當的查核、記錄、監控和保護措施。

八、「金融業的集中風險探討」報告

該研究對 11 家金融機構[9]、2 家雲端服務業者及 2 監理機關進行訪談並蒐集相關資料進行分析，探討金融業使用雲端服務之集中風險現況及提出其觀察。重點內容如下：

(一)第一段：雲端集中風險的現況與擔憂

全球的雲端服務採用率正逐年增加，但同時引起相關疑慮，特別是對於受監管之產業，主要顧慮包括雲端服務之可用性[10]、網路安全威脅、供應商鎖定、法令遵循等問題。該研究發現，大多數受訪單位對於主要雲端服務提供者在

[9]以產業別區分，有 7 家保險業者，2 家國際性銀行，1 家投資銀行，1 家零售銀行(consumer bank)；以經營地區性區分，3 家為國際性機構，3 家主要經營在東南亞地區，2 家主要在亞洲地區，1 家經營含括澳洲及亞太地區，1 家僅在一個國家內經營，另一家則是在其他地區跨區經營。

[10]可用性 (Availability)：意即當使用者需操作資訊系統時，資料與服務須保持可用狀況(能用)，並能滿足使用需求(夠用)。

處理網路安全的能力抱有信心。

根據最新統計資料顯示，三大雲端服務提供商在系統穩定之表現雖有差異，整體每年平均故障時間約為 5.6 小時，至今未發現對單一機構或整體系統造成重大影響。從系統韌性的角度分析，即使使用單一雲端服務供應商，亦可透過該雲端服務不同地區之機房相互備援，降低單一機房故障造成之風險。儘管雲端服務提供商聲稱其設計就是為了提高系統韌性，但許多受訪者仍對集中性風險存有疑慮。

(二)多雲策略與法令遵循議題

面對集中風險，許多受訪者採取多雲策略，這有兩種作法。一種是讓同一應用功能在不同雲端服務平台上運作，但這種方式較為複雜，只能用於即時性要求較低的功能。另一種較為實用的作法是針對不同應用功能選擇最適合的雲端服務平台。該研究建議採取後者作為主要策略，輔以妥善之應變計劃應對可能的系統遷移需求。

在法令遵循方面，歐盟數位營運韌性法案(Digital Operational Resilience Act，簡稱 DORA)為應對集中性風險，制定了「直接監理模式」，由監理機關直接對提供金融機構服務之大型第三方服務提供商(如雲端服務業者)進行監理。但大部分受訪者認為由金融機構依法規落實對雲端服務業者管理之「間接監理模式」更有利，因為金融機構更能掌握其雲端服務使用狀況，並決定與雲端服務業者的互動方式，受訪者擔心直接監理模式會增加法令遵循之複雜度，影響靈活性與適用性。該研究建議監理機構不應過度關注集中風險，而是與業界進行更多對話，瞭解不同利害關係人之觀點。

(三)利害關係人之責任與合作

研究的結論是，所有利害關係人都應在所謂的共同責任模型下扮演特定角色和承擔責任，以從雲端服務價值鏈中受益。雲端服務提供商應致力提供更有系統韌性之服務，金融機構應專注於如何利用這些服務為客戶創新並提供更佳體驗，而監理機關則需協調所有活動，以實現整體價值創造。

整體而言，雖集中性風險是一個新的挑戰，但並非無法克服的障礙。關鍵在於不同利害關係人之間需要加強溝通與合作，以充分利用雲端帶來的好處，同時妥善規避風險。監理機關角色應作為促進者，避免過度管制影響創新與系統韌性。

九、「透過雲端實現營運韌性、網路安全和風險緩解」座談會

(一)雲端服務帶來的風險與挑戰

雲端服務的採用為金融機構帶來了應用程序的靈活性和彈性，並有助於系統漏洞管理的標準化及降低成本。然而，雲端服務也帶來了諸多風險和挑戰，包括熟悉雲端技術之人才短缺、系統遷移的能力不足、配置錯誤

(Misconfiguration)風險、監管期望與雲端產業之落差等。金融機構面臨來自各方面的壓力，包括加速採用 AI、營運環境日益複雜等。

AI 等新興技術也為風險管理帶來新的挑戰。監理機關更加關注資料安全性和合規使用新技術。大型金融機構在獲取訓練 AI 模型所需資料方面具有優勢，將進一步擴大與小型金融機構間競爭差距。此外，量子計算和區塊鏈技術的發展也將為金融業風險管理帶來新的變革。

(二)第三方風險與監管期望

金融機構與第三方服務提供商間的關係日益緊密，但雲端服務業者相較金融機構規模更大且有更大的議價能力，雙方關係不對等增加風險管理的複雜度。監理機關對於金融機構使用第三方雲端服務保持開放態度，但同時對風險管理提出更高的期望。

金融穩定委員會(Financial Stability Board，簡稱 FSB)所發布之監理文件及歐盟數位營運韌性法案(DORA)等規範，提供金融機構管控第三方風險之指引。金融機構需與法令遵循及法務團隊建立良好合作關係，瞭解相關義務，並積極參與公私對話，提供產業意見。

監理機關之主要監管對象仍為金融機構，但也需與雲端服務提供商保持溝通，以瞭解行業發展和新興風險。監理機關需要適時調整監理政策以應對新技術之發展，確保相關政策與潛在風險相符。

(三)公私協作與未來展望

展望未來，風險管理將面臨新的挑戰和機遇，隨著 AI、機器學習和量子計算等新技術不斷發展，將對金融市場產生深遠影響。在雲端環境中，安全性和法令遵循的基本原則將保持不變，但資料之規模和複雜性將不斷增加。資料安全仍將是各方關注議題，同時需要新方法來整合和理解非結構化資料。量子計算將加速金融市場發展，但也可能產生既有加密標準強度不足和資料保護方面的挑戰。預期區塊鏈和分散式帳簿技術將在量子計算的推動下，得到更廣泛應用，可能引發金融市場結構的重大改變。為應對這些挑戰，公私合作夥伴關係的重要性日益重要。需要縮短新技術與政策制定之間的時間落差，並保持足夠的靈活性以適應技術的快速發展。

十、「亞太區以外的政策實踐與見解」爐邊會談

(一)美國政府的 AI 行政命令

美國政府發布於 2023 年 10 月 30 日發布第 14110 號行政命令(Presidential Executive Order 14110)，要求財政部從網路安全的角度，對 AI 進行評估。財政部網路安全和關鍵基礎設施保護辦公室 (Office of Cybersecurity and Critical Infrastructure Protection，簡稱 OCCIP) 於 2024 年 3 月 27 日發布「管理金融服務領域人工智慧特定的網路安全風險 (Managing Artificial

Intelligence-Specific Cybersecurity Risks in the Financial Services Sector)報告[11]，探討 AI 在金融領域的應用以及其帶來的網路安全風險以及防制詐騙之挑戰。該報告強調與私營部門和其他監理機關的密切合作，透過深入訪談了解各方對 AI 的擔憂、使用情況以及對現行監管的看法。

(二)美國財政部 AI 報告之重點

該報告的調查結果發現，AI 應用可協助金融機構提升資訊安全及防制詐騙，但大型公司和小公司在取得資料及處理資料之能力存在顯著差異，特別是在防制詐騙領域。大型公司往往將原始資料視為競爭優勢，不願與小公司分享，使小公司難以獲得足夠的資料來訓練其 AI 模型，進而影響了整個金融業的防制詐騙之能力。為解決此一問題，財政部及美國銀行協會等單位刻正著手於強化產業間資訊共享機制，讓所有公司都能夠公平地利用這些資料，提升整體行業的防制詐騙能力，以彌平資訊差距造成之潛在風險。

此外，為促進資料透明度，產業正在推動 AI 之資訊揭露機制，用於標示那些資料被用於訓練模型、資料的來源及使用方式的資訊。為實現生成式 AI 等尖端 AI 之治理，可解釋性仍為許多金融機構所面臨之挑戰，目前產業正在推動相關研究以提供解決方案，金融機構可參酌較為成熟之實踐用例以導入 AI 應用。

(三)美國財政部對 AI 的未來規劃與展望

財政部計劃在未來更多關於 AI 的研究成果，此外，美國政府將積極參與 G7 網路專家組關於新興技術的工作，並在集中風險、欺騙防制等關鍵領域與業界展開深入合作。財政部充分認識到 AI 技術的複雜性，強調應對這些挑戰需要耐心和嚴謹的態度。未來，他們將繼續與其他政府部門和監理機關緊密合作，共同制定全面的國家戰略，以應對 AI 帶來的機遇和風險，確保 AI 技術在金融領域的穩健發展。

[11]U.S. Department of the Treasury Releases Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Sector. Available at: https://home.treasury.gov/news/press-releases/jy2212

參、心得與建議

一、持續瞭解創新技術的優勢、限制、產業實務及政策動態

IIF 於會議中分享之「人工智慧、資料和雲端—金融服務中的連結、創新和價值創造」報告，整理國際 AI 相關監管宣言及政策文件，並歸納國際 AI 發展之共同項目，包括打擊歧視和偏見、加強安全、促進問責、創造 AI 發展機會、產出可解釋和可理解的結果等原則及相關子項目(見本出國報告第 7 頁，表格 2)。經比對本會「金融業運用人工智慧之核心原則」及銀行公會「金融機構運用人工智慧技術作業規範」，我國整體政策規劃與國際發展趨勢相符，並可就國際政策值得參考之子項目納為未來推動措施。

我國金融機構在使用雲端服務及生成式 AI 等創新應用，目前尚在發展階段，而此類技術產業鏈之跨境特性，突顯跨國合作及法規國際互操作性之重要性。建議持續透過參與國際會議、建立與金融業者及科技業者之溝通管道、與各國金融監理機關及國際組織進行交流等方式，瞭解相關創新技術之優勢、限制、產業實務及政策動態等資訊，作為相關政策制定或執行之參考。

二、推動人才培訓及鼓勵創新

本次會議與會之金融業者與監理機關均指出，AI 與雲端服務已然成為金融創新的關鍵驅動力。然而，在這波科技浪潮下，金融監理機關與金融業者都面臨了 AI 人才短缺的困境。AI 人才的缺乏不僅限制了創新應用的擴大，更對風險的有效控管構成了挑戰。

在延攬 AI 人才方面，金融機構及監管部門面臨著與大型科技公司在薪酬福利上競爭劣勢。此外，金融業所需資訊人才除了須具備資訊、統計等專業，還需在開發、部署及維護過程中，將金融監管與相關法規要求納入考量，才能合規將 AI 技術應用於金融服務，額外的限制與挑戰，都增加人才招募之困難。

為解決此問題，可參酌與會單位之建議，透過內部培育和外部招募並行。在內部培育方面，建立完善的內部培訓制度，透過教育訓練、工作輪調、專案參與等方式，培養員工的 AI 技術能力，並鼓勵員工進修相關課程。相關技術之應用可考量從風險較低之專案開始導入，累積內部人員對創新技術之應用經驗，再逐步提高應用之複雜性。在外部招募部份，除提高薪酬條件和工作環境外，亦可考量透過外部專業服務公司之協助，取得專業之技術服務或補充人力。

三、完善金融機構透過雲端服務使用人工智慧之配套作法

AI 與雲端服務已成為金融創新的關鍵驅動力，其中近期新興之生成式 AI 技術，多涉及使用外部之雲端服務，此類 AI 技術提高金融機構對雲端服務之依賴程度。此外，雲端及 AI 產業之高集中度，又為金融產業帶來服務供應商高度集中之風險。

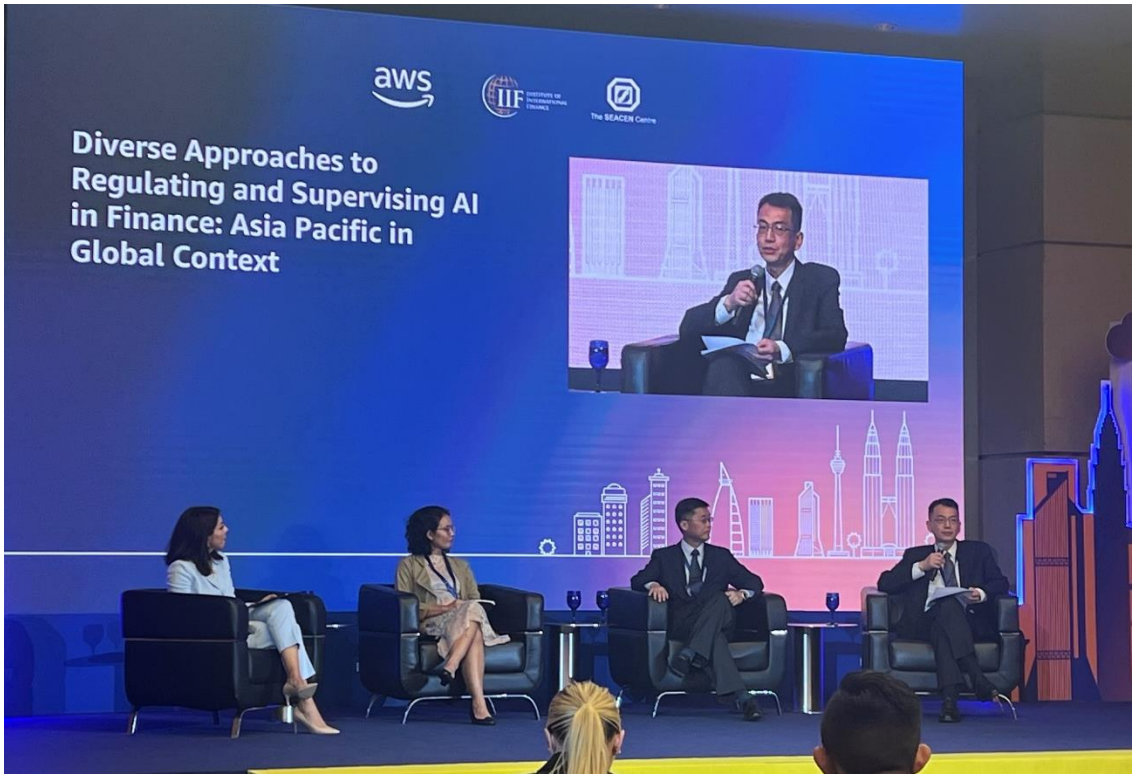
為利金融機構對雲端作業建構完整風險管理及控管程序，本會前於 2023 年 8 月修正「金融機構作業委託他人處理內部作業制度及程序辦法」，並請銀行公會研議訂定「金融機構作業委外使用雲端服務自律規範」(下稱自律規範)，組成工作小

組，作為我國金融機構採用雲端服務的溝通平台，辦理研議自律規範及最佳實務作業守則、蒐集國際雲端實務及規範、舉辦論壇及研討會等事項，分享雲端服務之使用經驗並推動人才培訓，以強化金融機構對於雲端服務管理之專業能力及人才培訓。

銀行公會在自律規範研議期間已邀集金融機構及國內外雲端服務業者共同參與，就法遵實務及契約應載事項等進行討論，均有助金融機構落實雲端風險控管及法令遵循。銀行公會另擬具「金融機構使用雲端服務實務手冊」(下稱實務手冊)提務實務做法供業者參考利用，未來銀行公會將持續滾動檢討該手冊，以符合實務所需。

考量生成式 AI 多涉及雲端服務之應用，且為金融機構所重視之發展項目，將請銀行公會後續研修自律規範及實務手冊時，將生成式 AI 之應用情境納入考量，適時邀請相關業者參與討論及辦理相關教育訓練，俾利業者在落實風險控管及法令遵循之前提下，應用新興技術提升金融服務之品質與效率。

附件：會議照片



本會銀行局代表童副局長政彰擔任座談會與談人分享我國 AI 監管政策

來自 11 個國家約 100 位金融服務業及科技業代表參加本次峰會