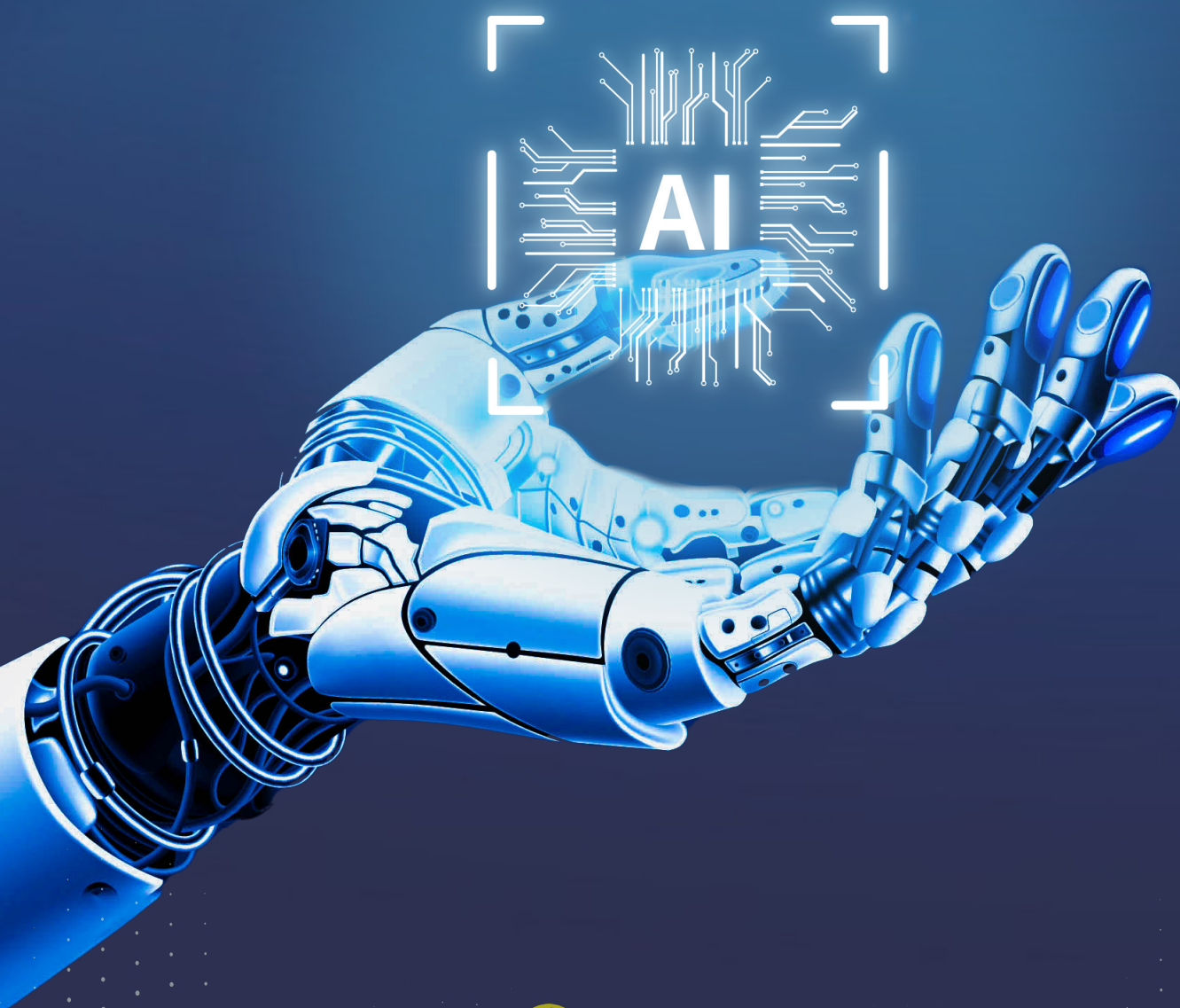


我國銀行業 面對生成式人工智慧的 影響與因應

2024年7月



台灣金融研訓院
TAIWAN ACADEMY OF BANKING AND FINANCE

目錄

- 03 | 前言
- 04 | 時代的里程碑：從分析型 AI 到生成式 AI
- 07 | 當生成式 AI 遇到銀行業

現況篇

- 11 | 現況一：五成銀行業者已經投入專責人力在 AI 技術創新及應用相關職務
- 14 | 現況二：五成銀行業者至少與一家 AI 技術廠商展開合作
- 17 | 現況三：如何使用 ChatGPT？七成銀行已經制定明確規範及指導原則
- 20 | 現況四：導入大型語言模型：國內銀行業者先行與觀望各占一半
- 22 | 現況五：銀行業 LLM 首戰場：客戶服務與支援

洞察篇

- 26 | 洞察一：AI 會取代銀行目前的工作？行員在擔心什麼？
- 30 | 洞察二：簡單重複性的工作被 AI 自動化後，應該把時間投入到哪裡？
- 36 | 洞察三：銀行業未來三年的重點人才需求與新興職務的崛起
- 40 | 洞察四：軟實力：AI 時代下的競爭利器

策略篇

- 44 | 策略一：生成式 AI 布局應該先行還是跟隨？
- 48 | 策略二：建構安全的 AI 使用環境
- 54 | 策略三：提前布局規劃各職務行員再培訓 (Reskill) 與技能提升 (Upskill)
- 58 | 附錄：26 類銀行職務資訊圖表 --AI 時代下的現況與未來



計畫主持人
台灣金融研訓院
副院長
Tel: +886 2 3365 3699
Email: dennis@tabf.org.tw

林仲威
Dennis Lin



計畫負責人
台灣金融研訓院 金融研究所
資料科學家 | 助理研究員
Tel: +886 2 3365 3767
Email: nww@tabf.org.tw

吳文蔚
William Ngo



計畫主持人
台灣金融研訓院 金融研究所
所長
Tel: +886 2 3365 3760
Email: kjchang@tabf.org.tw

張凱君
Kai-Jiun Chang



計畫負責人
台灣金融研訓院 職涯服務處
專案經理
Tel: +886 2 3365 3706
Email: ting764@tabf.org.tw

王亭亭
Christine Wang



計畫主持人
台灣金融研訓院 金融科技創新處
處長
Tel: +886 2 2393 2530
Email: corry@tabf.org.tw

柯榮哲
Jung-Che Ko

專案成員：李宛蓁
吳書瑜
楊絲宇
排版設計：胡惠俐

CONTACT US

聯絡我們

致謝

在此衷心感謝所有參與問卷調查的各家銀行管理層、金融從業人員及消費者。同時，我們特別感謝為本研究提供專業建議的金融領域學者及業界專家，希望未來的調查可以繼續獲得各界的支持。

免責聲明

本研究報告的分析皆根據客觀調查結果陳述，即使我們致力於提供精確之資訊，但無法確保問卷回饋內容百分之百正確無誤。建議事項僅供參考用途，具體執行策略仍需結合各行實際狀況及預期目標，請務必進行綜合評估。

© 2024 台灣金融研訓院。版權所有，保留所有權利。

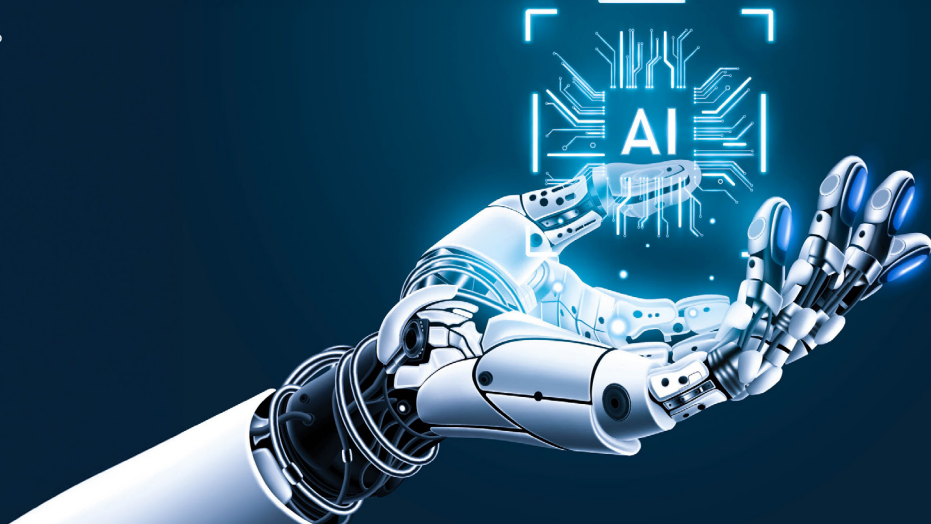
引言

在當今迅速變遷的新時代，生成式人工智慧（Generative AI，GAI）已成為各行各業推動業務轉型與創新的核心動力，自 OpenAI 發布 ChatGPT 以來，各家銀行均開始探索及評估可行的應用場景。根據 Accenture 2024 年發布的調查，將近 59% 的美國銀行行員已在日常工作中接觸到 AI 技術，未來約 73% 的行員其工作時間極有可能受到生成式 AI 的影響，其中 39% 的工作時間透過自動化技術被轉變，而 34% 的時間則透過增強方式得到效率提升。

傳統銀行業在價值創造的過程中，對於服務條款、產品說明、往來公文信件和評估報告等文字內容的高度依賴，凸顯出生成式 AI 極大的應用潛力。這類 AI 技術不僅能提升中後台的作業效率，如風險評估、法遵審查和交易報告處理等，也能增強前台服務，例如客服人員和櫃員在即時客戶服務與個性化產品推薦等方面的工作效能。

生成式 AI 的興起雖然帶來了前所未有的機會，但這股變革浪潮也伴隨著顯著的風險和不確定性。首先，生成式 AI 有時可能會“一本正經胡說八道”，即生成的訊息或建議雖然聽起來合理卻可能完全不符合事實，這對依賴精確數據驅動決策的銀行業來說可能導致嚴重的後果。此外，個資安全也是一大挑戰，如何保護客戶資料不被非法取得或濫用，是各家銀行導入生成式 AI 必須重視的問題。

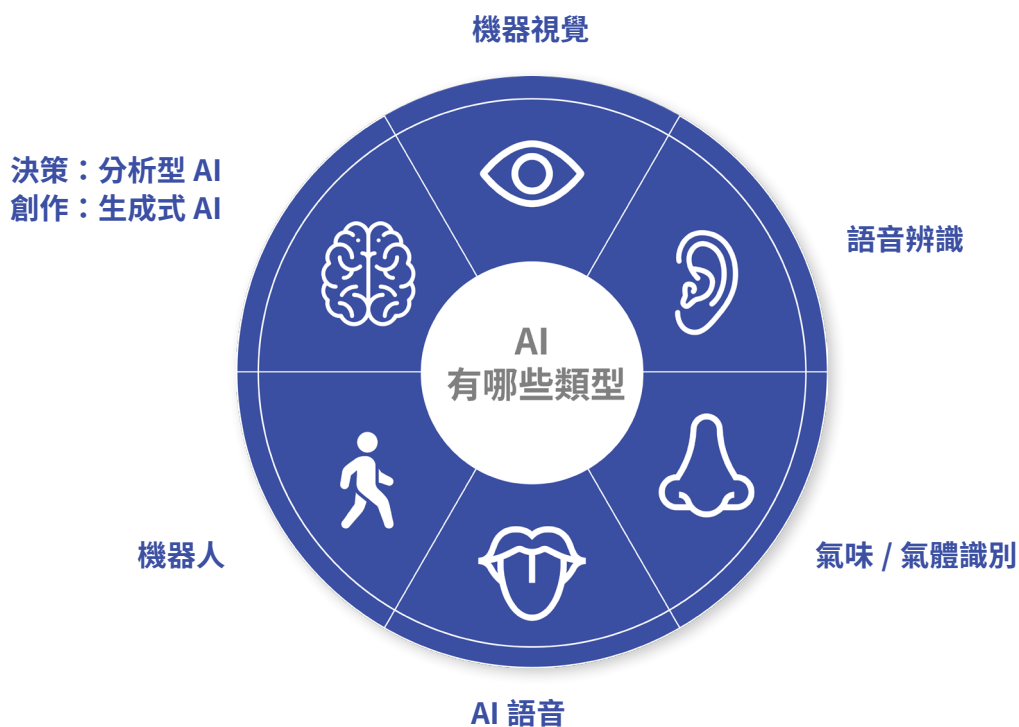
考量到當前生成式 AI 的影響性，台灣金融研訓院於 2023 年 9 月展開了一項針對國內銀行業者及銀行從業人員的全面性調查，深入探索目前 AI 技術在銀行業中的應用廣度、從業人員對此技術的接納程度以及生成式 AI 可能帶來的潛在影響。本次調查機構問卷涵蓋國內七成銀行以及 2,803 份銀行從業人員的有效問卷，同時也透過與多位各領域的專家學者深入訪談，共同探討銀行業應如何策略性地應對這波科技變革。本調查報告歸納出銀行業在 AI 技術投入的五大產業現況及四大趨勢洞察，並提出三項策略建議，旨在幫助銀行業策略性地應對科技變革。



時代的里程碑： 從分析型 AI 到 生成式 AI

人工智慧（AI）是一種使電腦和機器能夠模擬人類智慧和解決問題能力的技術，我們訓練 AI，希望它在未來能代替人類執行一些重複性且繁雜的工作，甚至超越人類的極限。提到模擬人類行為，我們可以用「眼耳鼻舌身意」來描述，透過不同的裝置和技術讓電腦及機器進行學習，包括機器視覺（眼）、語音辨識（耳）、氣味 / 氣體識別（鼻）、AI 語音（舌）、機器人（身），其中難度最大的是模仿人類大腦的思維（意），我們可以將大腦的工作簡單分為決策和創作，即對應分析型 AI 與生成式 AI。

圖一：AI 有哪些類型





讓 ChatGPT 告訴你生成式 AI 與分析型 AI 的差異



ChatGPT

在人工智慧的廣闊天地裡，分析型 AI 與生成式 AI 猶如兩位性格迥異的兄弟，共同推動著這場智能革命。首先，分析型 AI 是那位始終按部就班、數據梳理能力一流的大哥。它專精於處理和分析大量資料，用以預測市場趨勢或客戶行為，例如當銀行想要知道哪種信用卡產品最受歡迎時，分析型 AI 便會出馬，透過複雜的數據分析，告訴你“按照目前趨勢，消費者偏好帶有旅遊獎勵的信用卡”。

轉到生成式 AI，這位則是科技家族中的創意潮人，不僅分析數據，它還能創造出全新的內容，如文章、圖片乃至音樂作品。假如你問它：“我需要一篇銀行業科技發展趨勢的預測分析”，生成式 AI 不僅能提供文字，還能生成投影片，內容豐富得讓你眼花撩亂。

這場“智慧的盛宴”中，分析型 AI 的嚴謹與生成式 AI 的創新正好形成了一種互補，分析型 AI 堅守數據的客觀真理，而生成式 AI 則追求創意的極限。就像在繁忙的交易日中，分析型 AI 是那位穩重的分析師，深入挖掘數據洞見；而生成式 AI 則是策劃部的“創意怪咖”，隨時準備著讓你的廣告煥發新意。

在實務應用上，這兩種 AI 的結合可以帶來前所未有的效益。想像一下，當分析型 AI 告訴你哪些客戶最可能流失時，生成式 AI 便能立刻炮製一套量身定做的行銷策略來挽留這些客戶。這就是技術的力量，不僅分析過去，還能創造未來！



生成式 AI 讓人工智慧走進每個人的生活

如果說科技發展有其關鍵性的里程碑，那麼生成式 AI 正經歷著其「iPhone 時刻」，象徵著技術從專業領域向一般大眾市場的轉變，這種技術的親民化和易用性正在徹底改變人們的工作和生活方式，例如過去遇到不會的內容，大家都是透過 google 進行搜尋，而今透過詢問 ChatGPT 可以獲得更精確、更個性化的回答。

ChatGPT 的出現是生成式 AI 走向大眾的一大關鍵，不同於過去我們所習慣的聊天機器人，它能更好的理解和回應我們的提問，甚至協助我們完成工作任務。這種技術的進步使得無論是學生、教師、作家或是程式設計師等，都可以透過自然且直接的方式與 AI 進行交流，例如學生可以使用 ChatGPT 完成作業、教師可以利用它來設計教案、而作家可以透過 AI 來獲得靈感、程式設計師則可以與 AI 協作來撰寫程式碼。



勤業眾信
溫紹群副總

正如我們在網際網路時代和 iPhone 時代所經歷的一樣，新一代年輕人已經習慣人機協作的模式，透過提示工程使用 ChatGPT 來完成任務。這種方式雖然目前正處於初期階段，並且面臨著法律規範的限制，但我們必須意識到，當代社會已經在很多傳統方式上進行了改變，特別是在金融業，我們應該思考的不僅僅是如何使用這些技術，而更重要的是如何適應它們。在透過 POC 來探索生成式 AI 的應用場景時，建議在這一過程中避免碰觸那些容易引起爭議或目前法規不允許的領域。雖然 Gen AI 短期內不太可能對金融從業人員的工作產生太大影響，但我相信這種變化會自然而然地發生。

當生成式 AI 遇到銀行業

在科技驅動的浪潮下，不同時期的銀行業都面臨著轉型的挑戰與壓力，如數位轉型、永續轉型，以及時至今日最為熱門的 AI 轉型。其中，生成式 AI 以其能夠生成文本、圖片、音樂、語音、影像及程式碼等多元能力，成為目前 AI 轉型的焦點。

對銀行而言，投資研發某項生成式 AI 技術的決策，主要取決於該技術所能創造的商業價值，例如雖然圖片生成技術在設計與電商行業已造成重大影響，但對銀行業的主要業務影響有限。相較之下，文本生成技術則在整合海量金融資訊、處理繁瑣文件資料以及提升客戶互動效率等方面極具應用價值，使其成為銀行業導入應用的首要目標。國外銀行業者在導入生成式 AI 方面非常積極，下面列舉出實際應用案例供國內銀行業者參考：



內部聊天機器人

由於生成式 AI 仍有穩定性與資訊安全疑慮，目前大多數金融業者會優先選擇將生成式 AI 應用於內部的聊天機器人，以支援員工查詢操作流程、內部管理規範以及法規等相關內容。美國的南州銀行（South State Bank）透過導入企業版 Google Bard（現 Gemini），於銀行內部建立一個提供員工使用的 Chatbot，它不僅是一個資訊查詢的工具，更是一個能夠協助他們整理長篇文本、彙總討論、查看錯過的會議中是否有被分配工作項目的智慧型助手。

同時，這項技術也可以用於撰寫電子郵件、產出可疑活動報告或定期查核報告等日常作業，使得日常工作流程得以簡化及高效化。該行指出，自從推出該系統以來，過去尋找答

案可能需要 12 至 15 分鐘的時間，而現在只需幾秒鐘，顯著提升了工作效率，也因此使得員工生產力提升了 5 ~ 8 倍。

知識數位化

金融機構儲存著龐大的知識資本，其中包括各類研究報告、市場趨勢分析等，若要有效利用這些資訊，通常需要投入大量時間進行研讀與整合。摩根士丹利銀行（Morgan Stanley）與 OpenAI 展開了一項合作計畫，目的是利用 OpenAI 的技術讓行內理財顧問及其團隊能透過與生成式 AI 協作，快速對行內龐大的知識資本進行內容訪問、處理及摘要。

該計畫建立了適當的控制機制，確保其內容完全由內部分析資料生成，並附帶參考資料的連結，以保證訊息的準確性與可追溯性。透



玉山金控
張智星科技長

生成式 AI 應用於聊天機器人是一個非常合適的選擇，雖然目前仍存在一定的風險，但過去金融業已經廣泛使用的分析型 AI 同樣有出錯的問題，關鍵在於如何有效控制最終的輸出結果。我們可以使用 RAG 的方式來處理客戶的提問，首先提取問題相關訊息和段落，然後一起送入我們的大型語言模型進行處理，要求模型在回答時指明依據的是哪一段訊息，同時建立後期的 Post Processing 機制以確保回答的準確性。儘管如此，無論是傳統的決策型 AI 還是分析型 AI 都無法保證完全正確，如果信心水平不夠高，最好的做法是直接回應「抱歉，我不知道答案」。此外，生成式 AI 的應用範圍非常廣泛，不僅限於文本生成，從語音識別後的細節調整到使文本更加流暢，再到最後的摘要等，新的應用場景會不斷被發現，關鍵在於保持風險可控。



過這種知識數位化的實施，成功釋放了理財顧問的寶貴時間，讓他們能更專注於為客戶提供高品質的服務。

客戶通話摘要

金融業作為一個以服務為本的行業，對於客戶服務的重視程度自不待言，因此透過分析客服中心的通話記錄來了解客戶需求，已成為提升服務品質的重要環節。美國艾利銀行（Ally Bank）選擇優先於客服中心導入生成式 AI，以解決客服人員在交談時需做筆記與總結通話內容的多任務處理壓力。他們將通話內容即時轉錄至內部平臺，並自動生成通話摘要，不僅減輕客服人員的負擔，亦保證通話記錄的準確性和完整性，同時滿足法規要求與提供良好的客戶服務。

另一方面，澳洲的西太平洋銀行（Westpac）透過 KAI-GPT 技術，將客戶通話內容進一步提取，並應用於協助客戶自動填寫貸款申請表格。這個創新的應用不僅大幅簡化前臺人員的工作流程，也提升客戶在申請貸

款時的體驗，使得申請過程更為順暢、高效。

輔助程式開發

生成式 AI 能夠很好地理解並學習程式碼的結構和邏輯，因此可以為程式開發人員提供強大的輔助。高盛集團（Goldman Sachs）將生成式 AI 應用於提升程式開發人員的生產力，並取得了顯著的效果。據統計，搭配生成式 AI 工具後，開發人員的整體產出效率提高了 30%~40%，其中一個重要的應用是為開發人員提供可審查及微調的程式碼建議。

他們強調這是一種「副駕駛（Copilot）」而非「主駕駛」的概念，生成式 AI 並未真正創建可以直接投入生產的程式碼，程式人員仍需依照步驟對其進行檢查、驗證，並確保它是安全的。

詐欺偵測

金融業所面臨的詐欺風險日益嚴重，在網路安全威脅持續上升的當下更是如此，大型語言模型作為一種新興的技術，逐漸成為銀行與

其他金融機構對抗詐欺及金融犯罪的有力工具。

摩根大通 (JPMorgan Chase) 是此領域的先行者之一，針對業務電子郵件詐欺等常見的詐欺行為，開始採用生成式 AI 進行詐欺偵測。透過大型語言模型的技術，可以有效處理大量文字資料，分析電子郵件中的模式與上下文關聯，以識別可能的詐欺行為。此外，環球銀行金融電信協會 (SWIFT) 也積極與 Google 及 Microsoft 等科技巨擘共同開發新的生成式 AI 模型，用於提高詐欺檢測的成功率。

客製化行銷內容

在金融業的市場推廣活動中，客製化的行銷內容是提升客戶參與度與滿意度的重要

策略。隨著生成式 AI 技術的出現，金融機構現在能夠針對不同客群，更有效地創建客製化內容，從而提高市場推廣的效率與成效。Accenture 指出，他們近期與一家大型國際零售銀行合作，透過利用生成式 AI 技術使該銀行能夠創建更加個性化的行銷文案，大幅提升客戶的參與度，甚至在同樣的時間內產出了超過 30 倍的創意內容。

然而，國內金融機構的行銷文案一般需要通過法遵審查，以確保內容的正確性與合規性，如果利用生成式 AI 大量產生客製化的行銷內容，可能會對法遵審查作業造成困擾。不過，未來可以嘗試透過結合其他分析型 AI 模型，對生成式 AI 產出的內容進行自動化的審查與檢測，實現真正的個人化行銷內容生成與審查自動化流程。



Boise State University
生成式 AI 學程召集人
洪瑞隆教授

生成式 AI 未來對金融業的影響主要可以從三個面向切入，首先是「客戶服務」，LLM 基礎的聊天機器人可以透過檢視文字內容抽取如客戶的姓名、年齡、居住地等關鍵資訊協助預填申請表單，還可以檢視資料的完整性並提醒客戶補全缺失資料。同時，聊天機器人可以根據客戶數據完成試算，即時進行產品推薦或提供個人化貸款條件，這種應用也可以延伸到信用卡申請和財務管理業務的推薦。第二是「內部流程輔助」，LLM 與 RPA 結合後可以讓內部流程進一步自動化，包含文字翻譯、校對和除錯，自動總結會議記錄並列出各單位需完成的事項，以及自動更新專案管理和發送落後事項的提醒郵件等。第三則是「內部資料應用」，使用 RAG 技術將內部資料轉成向量化資料庫後，LLM 針對超出內部資料範圍的訊息不會編造虛假答案，只會回答「不知道」，可以大幅減少提供不正確訊息的風險，因此未來透過 API 串接可以把 LLM 跟現行的很多 web service 進行自動化整合。

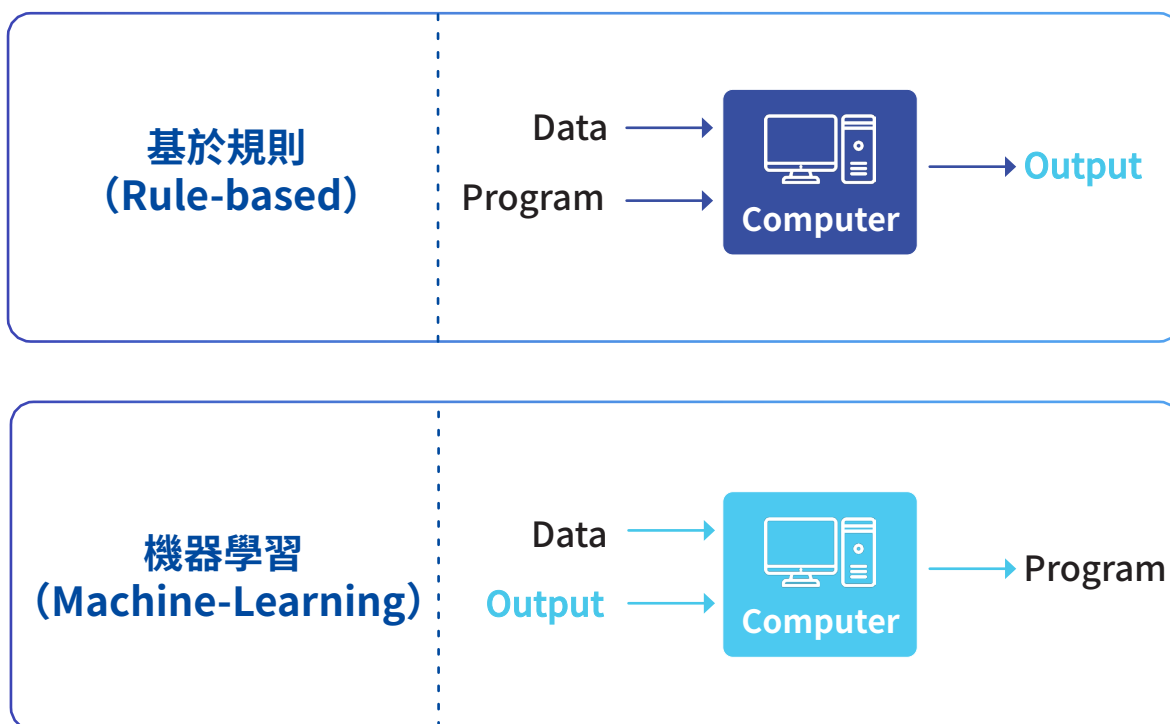
現況一：

五成銀行業者已經 投入專責人力在 AI 技術創新及 應用相關職務

在金融業，AI 技術已從早期的基於規則（Rule-based）的系統演變至今日的機器學習和深度學習模型，並且逐漸成為推動業務創新和效率提升的關鍵力量。這種轉變可以追溯到二十年前，當時金融機構開始嘗試利用客戶數據來優化銷售策略和客戶服務，從簡單的數據分析到複雜的客戶行為預測，這些早期的應用奠定了今日金融業 AI 應用的基礎。



圖二：傳統程式與機器學習的差異



隨著 AI 技術的成熟，一些銀行開始建立專責的 AI 技術團隊，透過建置機器學習模型及深度學習模型在資產管理、信貸評估、防詐應用以及產品推廣等方面展開多元的創新應用。本次調查發現，國內高達五成銀行已經設立專門團隊來負責 AI 技術的創新和應用，這不僅反映了 AI 技術在現代金融業務中的核心地位，更凸顯出銀行業對這一技術迫切的需求與依賴。然而，我們透過進一步的了解後發現部分銀行在定義「專責於 AI 技術創新的職務」上存在差異，其中可能納入了僅負責傳統資料工程和資料庫管理相關工作人員，而非直接參與 AI 研發或 ML/DL 建模人員。

有鑑於此，在排除定義不明確的資料後，我們發現實際投入 AI 技術創新的專責人力，平均而言占全行人員的 0.3%。對比國外銀行，

以 JPMorgan Chase 為例，他們聘雇了約 2,000 名 AI/ML 專家及資料科學家投入在 400 多個應用場景，人力占比約 0.6% (截止 2023 年約 309,926 名員工)。

對於國內銀行業者來說，如果以往沒有導入 AI 技術的經驗，各業務部門主管可能會懷疑新技術是否能超越現有模式，同時考量可能需要承擔額外的風險，因此在對新技術認知不足的情況下，較難提供一個適當的發展平台。此外，部分銀行在資源有限的環境下，組建一支 AI 團隊本身就是一大挑戰，組建後應如何評估該團隊創造的價值亦是重大挑戰之一。與國際銀行相比，國內銀行缺少足夠的市場規模來支持一個龐大 AI 團隊的成立，但初期可以考慮透過成立專案小組或與同業交流來逐步接軌未來 AI 趨勢。

國內同業技術交流的案例之一是由台北富邦銀行發起的鷹眼聯盟，無私將 AI 防詐經驗和技術分享給國內各家銀行業者，對於還未全面應用 AI 技術的銀行而言，透過加入這類型的聯盟不僅能夠獲得 AI 技術支持，還能在其

他機構成員的協助下加快行內的技術學習和應用。這種銀行機構間的合作模式，不僅增強了個別銀行的技術能力，更加强了國內整體金融生態系統的穩定性和安全性。



富邦金控暨台北富邦銀行
蔡佩玲副總經理

過去，我們的風控主要關注的是信用風險，即借款方是否有能力償還貸款，然而近年來詐騙案件急遽上升，成為一個不可忽視的風險因素。多數銀行由於擔心引發客戶投訴，並缺乏專門部門來負責此類問題，因而未能有效對抗詐騙活動。一些銀行將此任務交由 IT 部門、客服或是法務部門處理，但這種分散的做法往往難以有效對抗詐騙集團。防詐的關鍵要素在科技運用與公私合作，富邦與內政部刑事警察局合作開發「鷹眼模型」AI 偵測專利技術，並分享給國內 33 家銀行，希望攜手強化國內金融安全。未來，我們將導入聯合學習 (Federated Learning) 的概念，希望各家銀行在不交換資料的情況下提供各家鷹眼模型的樣態和權重，訓練出國家級鷹眼模型。

現況二：

五成銀行業者至少與一家 AI 技術廠商展開合作

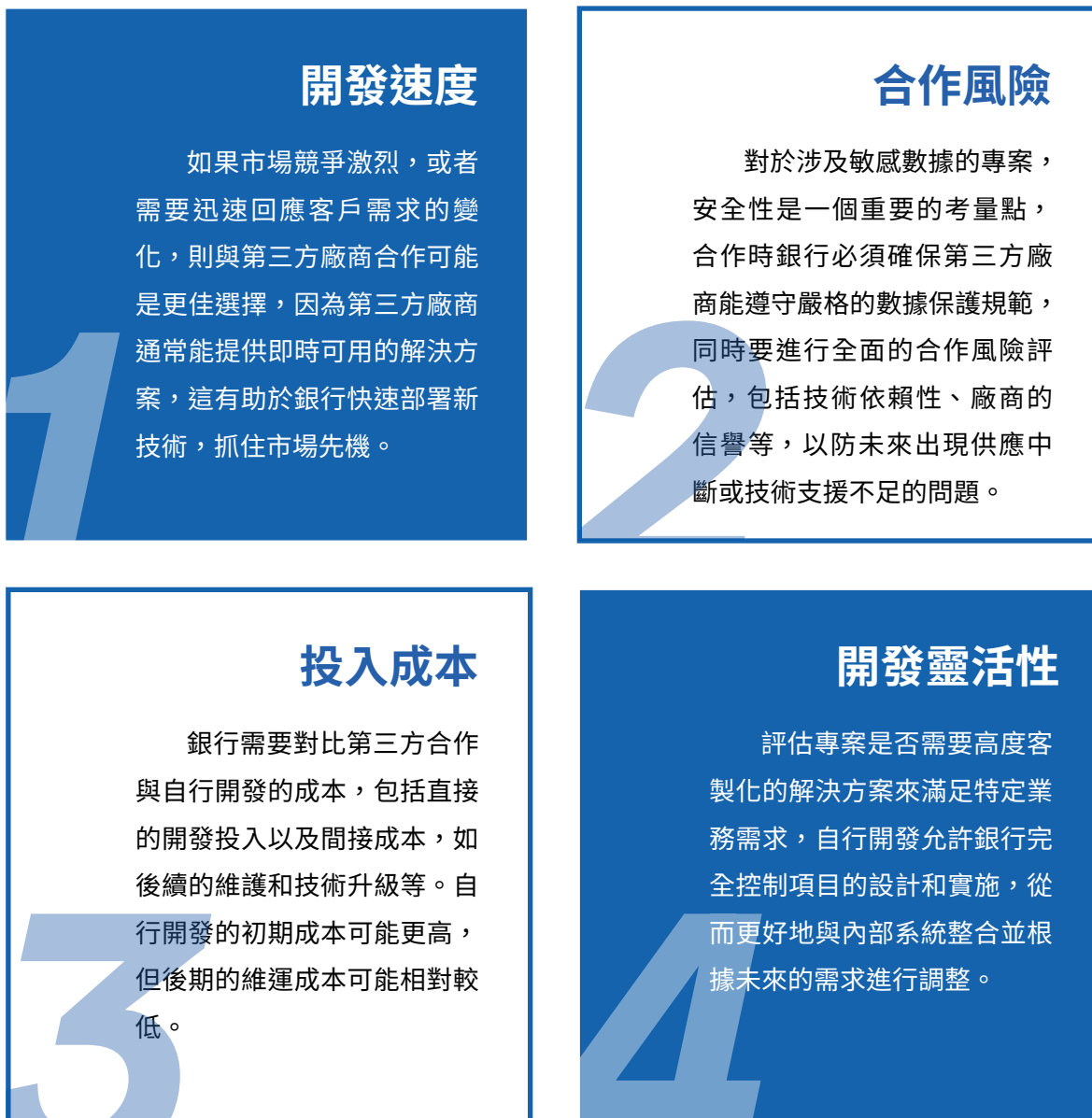
在選擇是否與第三方 AI 技術廠商合作或自行開發 AI 技術上，銀行業者需權衡多項因素。首先，與第三方業者合作可讓銀行快速導入最新的 AI 技術，利用第三方業者的現成解決方案來解決特定問題，節省開發時間與資源。然而，這種合作一般極其仰賴第三方廠商提供的關鍵技術和服務，甚至涉及對銀行核心系統大規模的技術改造，且第三方技術供應商的服務性能和安全性將直接影響到銀行的日常營運和聲譽，因此第三方風險管理已經成為一個不容忽視的關鍵領域。

相對地，自行開發 AI 技術賦予銀行更高的靈活性與控制權，能更好地整合內部系統並符合特定業務需求，但自行開發需要較長的研發時間和更高的初期投資，且需要建立或擴充相應的技術團隊。

本次調查發現，國內五成銀行業者至少與一家 AI 廠商合作，其中更有與高達 12 家第三方廠商合作的案例，展示出部分銀行正積極尋求外部專業技術來優化業務流程和客戶服務。另一方面，部分領先者銀行傾向與較少的 AI 廠商合作（平均合作家數較少），反映出這些銀行可能擁有較成熟的內部開發能力。



圖三：評估是否與第三方 AI 廠商合作開發的關鍵因素



AI 應用的重點領域

本次調查同時發現，目前最多國內銀行業者投入在 AI 智能客服的開發，智能客服系統能夠提供 24 小時不間斷的服務，能有效處理大量常見問題，提升客戶滿意度並降低人力成本。此外，AI 預測模型的開發以及機器人流程自動化 (RPA) 的投入銀行家數並列第二，其中分析型 AI 的預測與分類功能對於銀行的業務有極大的助力，可廣泛用於客群分類、防詐、貸款評分等。

RPA 主要應用於自動化簡單、重複性高的工作，可以記錄動作順序並與應用程式互動來建立工作流程，適合優化需要大量手動輸入或重複點選的電腦操作，嚴格來說並不屬於大家今天所定義的 AI。然而，智慧自動化 (Intelligent Automation, IA) 將會是 AI 技術與 RPA 技術的混合體，特別是結合生成式 AI 後其拓展性大幅提升，是未來各家銀行投入研發的重點領域。

圖四：與第三方廠商合作與自行開發 AI 的利與弊



利



弊



工研院
王邦傑經理

對於銀行業而言，投入 AI 研發的關鍵在於滿足業務需求，我們不會為了喝牛奶去養一頭牛，當外部已有優秀的解決方案時，引入這些方案無疑是迅速解決問題的最佳途徑。我們不期望 AI 完全替代人類，但期待一個人力加上 AI 能帶來比單獨執行或兩個人力更大的效益。在討論如何導入 AI 前，銀行必須有良好的資料治理，確保擁有高質量的數據，這不僅有助於我們精準評估外部方案的適用性，還能確保在導入 AI 到銀行業務過程中，我們能夠走在正確的道路上，避免可能的問題和風險。

源和正確性，導致被控違反律師倫理面臨紀律處分。另外，三星 (Samsung) 員工將公司機密資訊輸入 ChatGPT 而導致外流的事件也是一個廣為人知的案例，這不僅涉及到敏感資訊的洩露，而且對公司的資料安全構成了威脅。

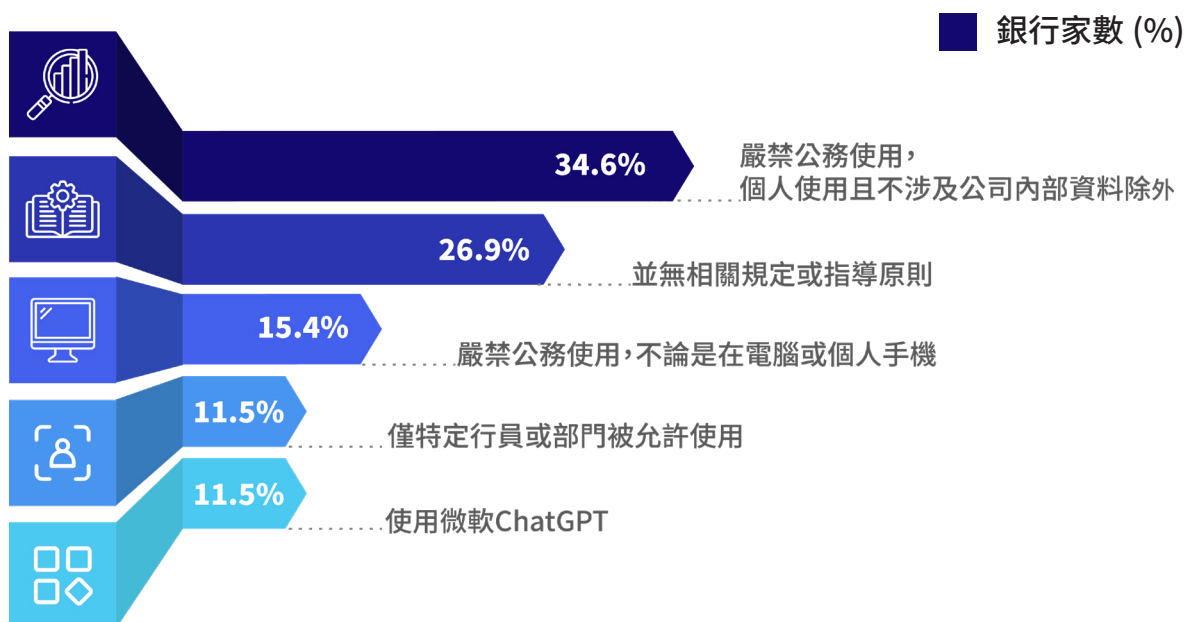
由於金融業涉及大量敏感數據且需嚴格遵守法令規範，因此對於新興技術如人工智慧的採納需格外謹慎。隨著 ChatGPT 在多個行業逐漸普及，金融機構必須嚴格規範員工使用這些工具，以確保客戶資料的安全與隱私。本次調查顯示，34.6% 的銀行業者嚴禁員工在工作中使用 ChatGPT，除非是在非工作環境中且不涉及公司敏感資料的個人使用；同時，有 15.4% 的銀行完全禁止在任何公司設備上使用 ChatGPT，無論是公司電腦還是員工個人手機，這反映出業界在保護敏感資訊和遵循資料保護法規方面的謹慎態度。

此外，有 11.5% 的銀行則採取更靈活的策略，只允許特定員工或部門在嚴格監管下使用 ChatGPT。這些銀行通常設有詳細的使用



規範和管理機制，確保 AI 工具的使用不違反任何內部政策或法律。另外，11.5% 的銀行選擇使用微軟企業版 ChatGPT，透過與大型科技公司合作不僅可以提高資安防護，也有利於系統整合與管理。

圖五：行員使用 ChatGPT 的管理方法





平衡風險與創新

在推動創新的過程中，銀行業必須在創新帶來的潛在效益和可能的風險之間找到平衡點，使用如 ChatGPT 等 AI 工具可以大幅提升工作效率，但同時也可能面臨資料洩露、誤用 AI 所產生的不當建議等風險，因此制定明確的管理辦法變得極其重要。

銀行可以制定明確的管理辦法，限定在哪些情況下可以使用這類工具，確保所有使用都在安全的網路環境中進行，並且所有的查詢和回應都要經過審查和記錄，同時對員工進行相關的培訓，增強其對於數據保護的意識和責任感。透過這些措施，可以最大限度地減少濫用和風險，同時發揮 ChatGPT 在提高工作效率和決策品質上的優勢。



台灣人工智慧學校
蔡明順校務長

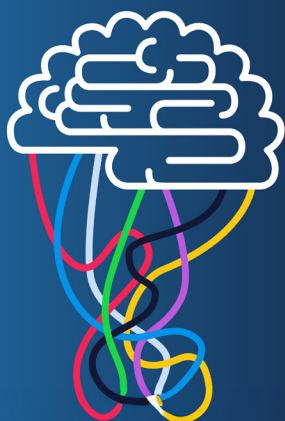
以銷售保險為例，過去我們認為購買保險是困難的，但現在已可直接在網上購買保單。保險業務員未來可能仍會存在，但這個行業的變革並非僅由於科技的進步，而是終端用戶已經被培訓得懂得如何利用科技。雖然現今 AI 的使用仍有一定門檻，但這種情況正逐步變得更加便利，技術發展的成熟將讓 AI 更加貼近我們的日常生活，成為我們不可或缺的助手。不是說未來 AI 將取代人類，而是終端使用者的行為模式已經改變，這些改變將驅使金融業不斷創新和改進。銀行業這樣競爭激烈的環境中，在科技創新上取得領先至關重要，尤其是在推動 AI 等技術創新方面，自上而下的推動力是成功轉型的關鍵因素。

現況四：

導入大型語言模型： 國內銀行業者先行 與觀望各占一半

隨著 ChatGPT 等大型語言模型（LLM）在銀行業的普及，這些技術已展現出對提升客戶服務品質、優化內部流程及降低營運成本等方面的顯著潛力。導入 LLM 不僅可以提高服務效率，還能透過自動化處理大量的數據與查詢，支援決策制定過程，並提供更個性化的客戶體驗。

目前國內銀行業者對於 LLM 的態度分為兩派，一半積極規劃中、一半則持觀望態度。其中，約 35% 的銀行正在進行 LLM 相關的策略規劃；11% 的銀行已經在實施實驗階段的 POC（Proof of Concept）專案；而 4% 的銀行則已經開始部分導入此技術於實際營運中。



LLM

Large Language Model

導入 LLM 的重要考量點

1. 技術和成本的考量

導入 LLM 技術有很多方式，例如與第三方業者（如輝達、微軟、谷歌等科技巨擘）合作，在他們所提供的平台上進行訓練及運行，按使用量計費，但缺點是必須將資料上雲。國內亦有個別廠商提供地端 LLM 服務，將預訓練好的「大腦」安置到企業內部，但效能必然無法媲美 GPT4 等級的大型語言模型，同時在模型微調和後續維運部分也相對較麻煩。另一種方式是自行使用開源 LLM 進行微調，訓練出一個企業專屬的「大腦」，但相對初期投入的資源是最為龐大的，同時也需要行內具備相關技術的開發人員。

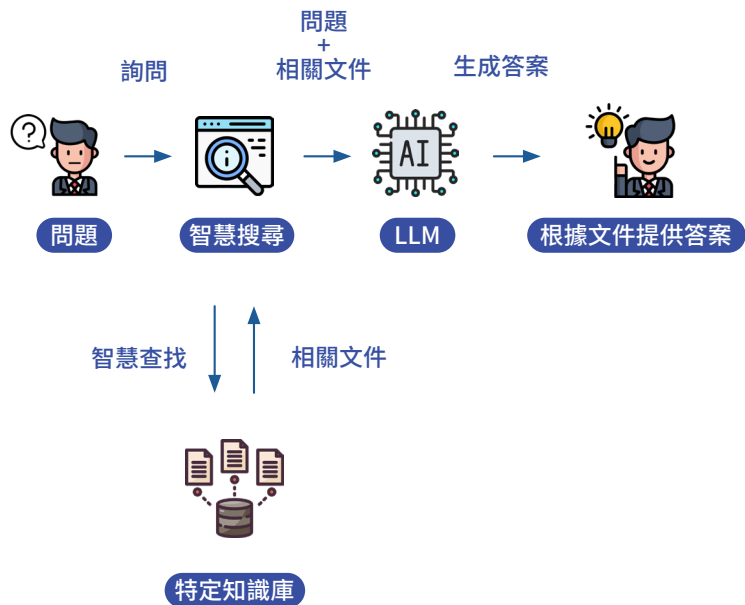
2. 數據品質和可用性

LLM 的訓練和導入仰賴於大量高品質的數據，銀行擁有大量各類型的文件報告書以及客戶資料，但這些數據的整合、清理與串連卻是一項龐大的工程，若用於訓練或分析的數據品質不佳，可能會導致 LLM 的輸出不準確，甚至產生誤導性的結果從而影響決策的品質。

3. 客戶個資保護與授權

目前國內非常重視客戶個人資料的保護，銀行必須確保所有利用 LLM 處理的數據遵守法律規範，要在獲得客戶的同意下進行模型的訓練和使用，不當的數據使用不僅可能導致法律風險，還可能損害銀行的聲譽，引發客戶對其個資安全的擔憂。

圖六：RAG 方法示意圖



中研院
蔡宗翰研究員

著手開發 TAIDE 模型的原因，主要是由於在諸如金融領域和政府公部門中，許多情況並不適宜直接使用 ChatGPT，可能會引發洩密事件及衍生後續問題。因此，關鍵在於是否有像 TAIDE 這樣的模型，可部署在機構的地端設備，才能更安全的使用。根據我們的經驗，經過適當的調教後，模型出錯的機率並不高，產生錯誤的可能性也相對較低，例如使用 RAG 的方法，透過檢索真實的資訊源，提供給模型做為回答的參考，這樣模型產生錯誤的機率就會大大降低。

現況五：

銀行業 LLM 首戰場： 客戶服務與支援

我們進一步調查了國內銀行業者在未來導入大型語言模型後，他們主要期望應用於哪些業務領域，同時探討了 LLM 技術如何賦能並提升銀行現有的技術。根據調查結果顯示，約 46% 的銀行會優先投入到客戶服務與支援、39% 會投入到內部操作流程的自動化、21% 會投入到詐欺偵測、18% 則選擇優先投入到風險評估與貸款審核中。

當 LLM 遇上智能客服

目前市面上常見的智能客服系統，一般依賴於預設的回答或較簡單的關鍵詞比對，LLM 則可以更深入地瞭解客戶的具體需求和語意，提供更加人性化和精準的回答，使其在處理複雜或非常規性問題時表現更佳，從而提升客戶的整體服務體驗。

本次調查結果顯示，大部分銀行會考慮投入到客戶服務與支援（46%），希望透過 LLM 技術理解並回應客戶查詢，從基本的帳戶訊息查詢到回應更複雜的交易問題，都能夠提供快速且準確的回應。由於 AI 能 24 小時不間斷地提供服務，不受假日或工作時間的限制以及情緒的影響，在整合 LLM 技術後有望可以大幅提升客戶滿意度及銀行業的競爭力，同時解決銀行客服人員長期不足的問題。

當 LLM 遇上 RPA

LLM 在自動化方面的應用與傳統的機器人流程自動化（RPA）有顯著不同，傳統 RPA 技術主要專注於自動執行結構化的、規則化的基礎任務，例如自動化數據輸入或者固定流程的文件處理。相比之下，LLM 的應用則



更加廣泛和靈活，能夠處理更加複雜和非結構化的數據，這是因為 LLM 利用自然語言處理的能力可以理解和生成人類語言，從而在處理如客戶服務對話、內容創建、複雜數據分析等更加多元和非標準化的任務上展現出優勢。

本次調查結果顯示，大約 39% 的銀行考慮將大型語言模型應用於內部操作流程的自動化，如會議摘要和文檔審核等重複性高且耗時的任務，不僅可以提升中後台運作的效率，還能減少人為的錯誤，同時能釋出行員處理大量繁雜且重複性工作的時間，使他們能夠專注於更具戰略性的工作。

當 LLM 遇上詐欺偵測

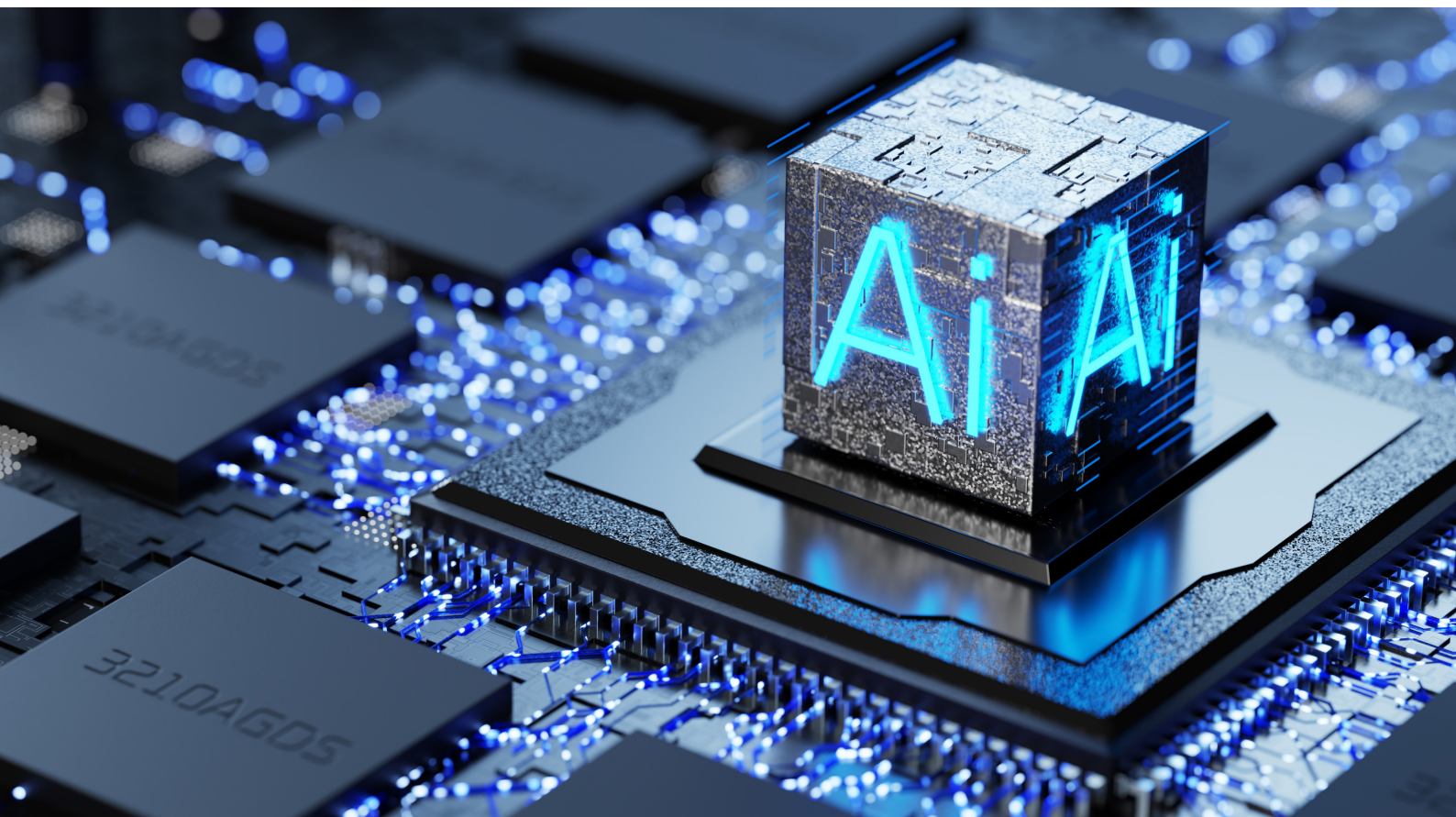
傳統的詐欺偵測技術往往依賴於固定的規則 (Rule-based) 識別詐欺行為，這種模式可能產生大量錯誤的警示通報。近期銀行業開始導入機器學習或深度學習，可以大幅提升模型精準度，但當遇到新興的或較少見的詐欺手段時則往往難以快速適應和識別。相對而言，

LLM 透過其先進的自然語言處理能力，能夠從大量的非結構化數據中學習和識別潛在的詐欺模式，包括但不限於文字內容、交易描述、用戶行為數據等。LLM 可以分析這些數據的深層語意和隱含的異常模式，從而更有效地預測和識別新出現的詐欺手段。

本次調查結果顯示，大約 21% 的銀行考慮將大型語言模型應用於詐欺偵測，以透過學習大量的交易模式和行為數據，有效識別出異常交易，提前預防可能的詐欺行為。這不僅保護了客戶的財產安全，也避免了銀行可能面臨的巨大損失。

當 LLM 遇上風險評估與貸款審核

過去風險評估與貸款審核的工作主要依賴於人工作業，首先客戶需要填寫繁瑣的申請表，並提供各類證明文件，審核人員根據標準化的流程對這些資料進行審查，評估客戶信用風險的主要方式則是使用傳統的信用評分機制。



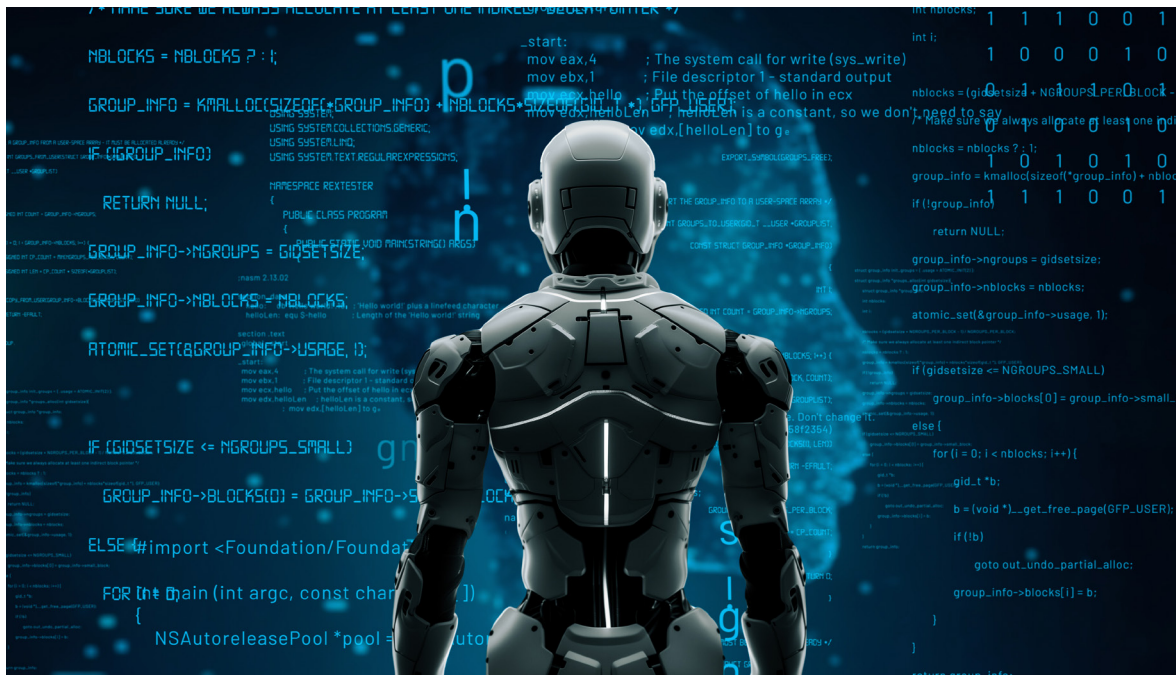
本次調查結果顯示，18% 的銀行考慮將大型語言模型應用於風險評估與貸款審核中。傳統信用評分模型通常依賴有限的數據來源，如信貸歷史和收入資訊，LLM 則可以處理大量非傳統數據，包括社交媒體活動、電子商務交易、公共服務支付記錄等。這些新型數據來源有助於更全面地評估個人的信用狀況，尤其對於那些傳統數據不足的消費者，例如沒有信用卡或銀行貸款歷史的年輕人或新住民。

當 LLM 遇上產品推廣及行銷

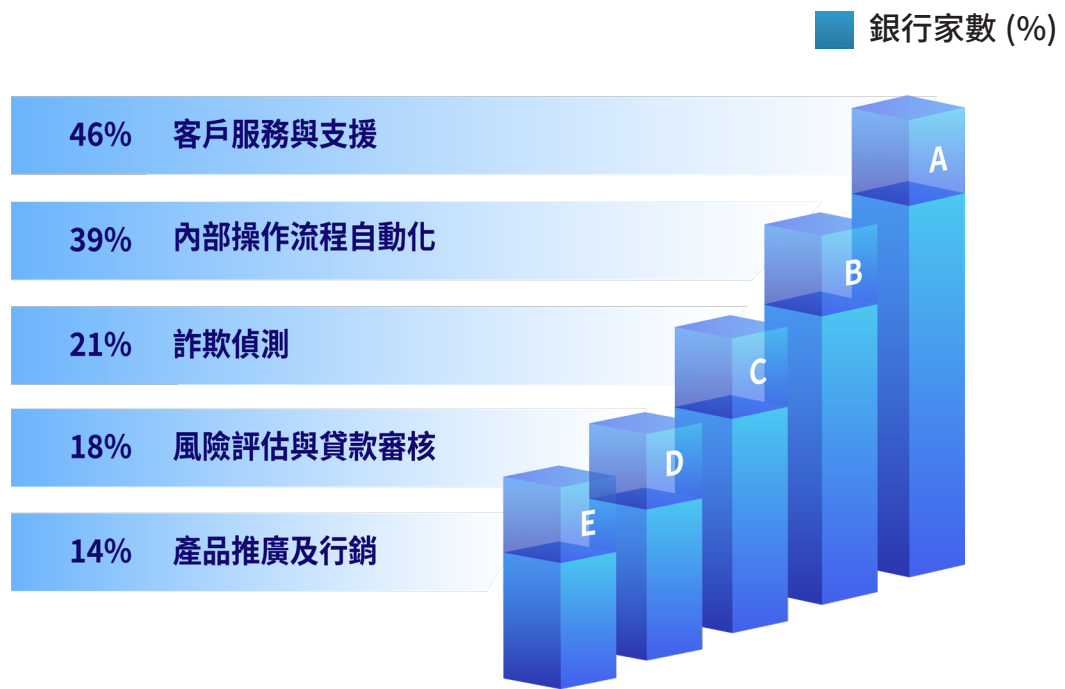
傳統上銀行的產品推廣主要依賴於標準化的廣告文案和相對固定的行銷策略，這種方法

缺乏針對客戶偏好和需求的個性化行銷。相對而言，LLM 可以分析客戶的交易歷史、瀏覽行為和回饋，從而創建高度個性化的推廣訊息和產品建議，這樣的策略比傳統的“一刀切”方法更有可能引起特定客戶群的興趣。

但調查發現，僅有 14% 的銀行考慮將 AI 應用在產品推廣及行銷，主要原因在於處理客戶數據時必須嚴格遵守數據保護和隱私法規，同時 LLM 在 AI 幻覺的不確定性也是一大障礙。這些幻覺可能導致生成的行銷內容存在誤導性或不準確性，從而影響顧客信任和品牌聲譽甚至導致大量客訴，因此國內銀行在這方面會特別謹慎。

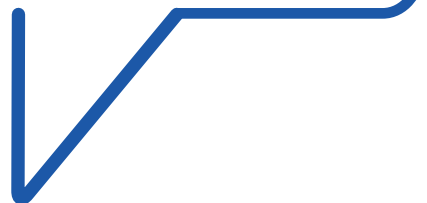


圖七：銀行導入 AI 大型語言模型（LLM）的應用領域



台新金控
王正男資深經理

對於運用生成式 AI 的觀點，我認為不應單一聚焦於技術本身，生成式 AI 為我們開啟了廣闊的想像空間，然而要有效利用它，需要多項配套措施。特別是訓練所使用的資料，無論是內部交易資料還是外部的產業資料，不能單純透過預先訓練整合進來。因此，我們必須考慮如何與分析型 AI 結合，以創造更佳的應用場景。從策略上，我們不僅要考量生成式 AI 對內部作業流程或對外服務的影響，還要將各種情境納入考量，從資料收集到資料治理等各方面。我們對於 AI 的全自動化應用採取謹慎的態度，雖然 AI 是一項先進技術，但伴隨的風險也不容忽視。在風險無法完全控制的情況下，我們認為員工的適當介入在報告生成或客戶服務過程中是必要的，在確保安全和可控的前提下，審慎地將 AI 技術融入我們的應用中。



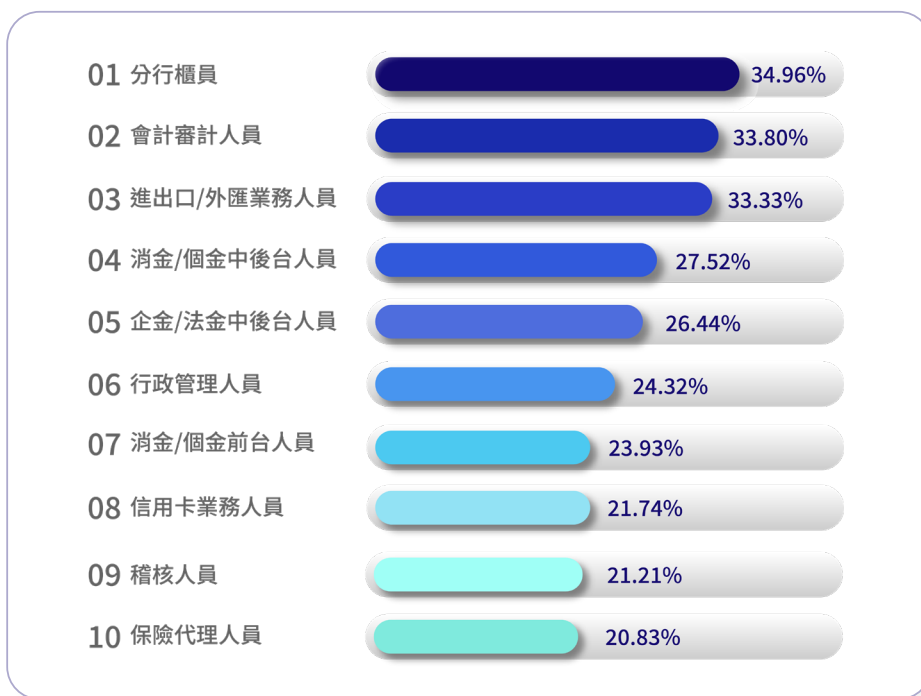
洞察一：

AI 會取代銀行 目前的工作？ 行員在擔心什麼？

隨著 AI 技術的飛速發展，台灣銀行業對於 AI 的運用越來越普遍，AI 技術展現出的能力讓行員不禁開始擔心未來自己的工作是否會被取代。根據本次調查結果，2,803 名受訪者中約 21% 的銀行行員對於 AI 取代人力的潛力感到憂慮。數據顯示，最擔心被 AI 取代的前三類銀行職務分別是分行櫃員（35%）、會計審計人員（34%）、以及進出口 / 外匯業務人員（33%）。



圖八：擔心被 AI 取代的前十類銀行職務



為甚麼行員擔心會被 AI 取代？

在進一步探討銀行員工對於被 AI 取代的擔憂後，我們發現了幾個核心原因。行員們主要擔心一旦銀行大規模引入 AI 技術後，他們現有的技能將變得過時，同時因缺乏適當的培訓使他們無法掌握新的技能，最終面臨被淘汰的風險。根據受訪行員的回饋，我們可以將這些擔憂歸納為以下三個主要方面：

1. 擔心銀行人力需求減少：

受訪行員指出，隨著網行銀服務和自助服務設備的快速發展，顧客越來越少親自前往銀行櫃檯辦理業務，導致對櫃檯人力的需求逐漸減少。他們認為這不僅影響到櫃員的工作穩定性，也使得櫃員的角色需要重新定義。同時，行員普遍認為銀行為了要降低營運成本和提高效率開始導入 AI 技術及自動化解決方案，這直接導致對於人力的依賴度降低，尤其會計和審計人員，認為由於其領域高度的標準化和規

則性，更容易被自動化技術取代。

2. 對未來工作職務的不確定：

受訪行員表示，金融業務流程具有高度的可程式化特性，使自動化成為可能，進出口及外匯業務人員認為這對該領域的服務造成巨大衝擊，因為這些業務中的大量重複性計算和交易可以由 AI 快速且無錯誤地完成。當 AI 技術可以自動化處理現有的工作後，行員會對自己的工作職務感到迷茫，不知道自己還可以做什麼。

3. 自己不具備新的技能：

行員普遍認為未來他們不僅需要掌握傳統的銀行業務知識，還需涉略數據分析、機器學習等新興技術領域的知識。隨著 AI 技術的不斷進步，如果他們無法及時提升自己的技能以適應新的工作環境，將容易被 AI 取代。

讓銀行的工作變得更有溫度

據《金融時報》統計，全球 20 家規模最大的銀行在 2023 年共裁減了 61,905 個工作崗位，其中包括瑞銀集團、富國銀行、花旗銀行等，成為自金融危機以來裁員最嚴重的年份之一。《彭博》2024 年 3 月的報導指出，英國巴克萊銀行計劃在未來數月內裁撤全球市場、研究和投資銀行等部門數百個職位，儘管官方聲明強調這是年度淘汰績效不佳員工的既定制度之一，但我們可以看出其中不乏因 AI 技術成熟導致銀行人力過剩的影子。

西方國家的銀行往往以追求利潤最大化為原則，因此在經濟不景氣或新技術應用導致人力需求減少的情況下，裁員往往成為一種快速降低成本的主要手段，經營者會毫不猶豫地縮減規模，以保持競爭優勢。雖然不會直接指出是 AI 取代人力所致，但業務大幅自動化已明顯成為這些機構重組的重要環節，這種結果導致了大量金融從業者失業或被迫轉型。

反觀東方國家的銀行，尤其是亞洲華人地區的銀行，經營方式更具人情味，通常會將穩定的雇用關係視為維持員工忠誠度和企業形象

的重要手段，鮮有出現大幅裁員的現象。因此在 AI 時代下，重新思考人力資源的配置和培訓策略變得至關重要，銀行不僅應強化員工在傳統業務方面的能力，還應幫助他們掌握新技能，尤其在數據分析、AI 技術、創新開發等，協助他們在數位轉型中找到自己嶄新的角色，進而在未來轉變成為銀行的核心競爭力。

銀行業者應時刻關注員工的心理狀態與感受，許多員工可能對新技術抱有抵觸心理，擔心自己的工作會被 AI 取代，或對學習全新技能感到焦慮。因此，管理層必須在推動技術創新的同時，打造出一個有支持性、有溫度的工作環境，透過開設培訓課程、工作坊和心理輔導，來幫助員工理解 AI 的優勢，減少對技術的恐懼，並鼓勵他們主動擁抱變化。

管理層應明確指出導入 AI 的目的是為了提升員工的工作品質，而非替代人力。當員工從繁瑣的重複性工作中解放出來，投入到對策略和創新有重大影響的領域，他們的參與感和成就感將顯著提升，不僅能促進個人的職涯發展，也使銀行整體的創新力和市場競爭力得到加強。



雖然 AI 可以承擔一些基本任務，例如接聽電話，但在處理客戶投訴等複雜的高階任務上，它是否能像人類一樣表現得這麼細膩和周到？當系統處理出現錯誤或不足以應對的情況時，是否仍需人工介入來解決問題？因此，我認為 AI 可能在某些領域替代人類工作，但並不能完全取代人類的職位。在金融業，儘管 AI 可以提高服務效率和質量，但人類員工仍然扮演著不可或缺的角色，例如在提高交易效率和客戶體驗的同時，金融機構也在增加提供更專業、更個人化服務的人員配置，證明技術進步並非僅僅意味著減少人力。因此，我相信，至少在未來五到十年內，台灣不太可能見到因 AI 而導致大規模的職位流失。但是，職位的職責、工作內容及工作方式勢必重組或改變。



永豐金控
廖家宏人資長



輔仁大學
黃淑芬副教授

在這個跨領域的時代，過去主修的科系和專業技能的界線變得越來越模糊，這個情況下如何找到自己的專業核心就變得特別重要。類似 ChatGPT 這類型工具，他能提供很多非常有用的資訊，但也可能是在一本正經胡說八道，這就要求我們有辨別的能力，建立起自己的核心競爭力。這個核心競爭力可以是很多方面的，法律、風險管理、創新思維，必須要找到知識的主軸才有辦法更妥善的使用 ChatGPT。根據我的觀察，金融從業人員可以分為兩種截然不同的態度：一部分人努力適應變化，而另一部分則選擇放棄、安於現狀，尤其對於三十至四十歲的職場人士而言，這種變化帶來了巨大壓力。這其實不僅僅是關於職業生涯的問題，更觸及到心理健康的層面。我們在關注專業技能更新的同時，也不能忽視這些心理壓力，需要為不同資歷、層級的從業人員提供必要的支持和引導。

洞察二：

簡單重複性的工作 被 AI 自動化後， 應該把時間投入到 哪裡？

在探討 AI 技術對銀行各職務的影響時，本研究將銀行的主要工作職務分為 26 項，並對 2,803 名銀行從業人員進行調查，以了解各職務的日常工作事項主要集中在哪些領域，以及各項工作平均需要花費多少時間。接著，我們進一步探討 AI 技術可能對哪些工作內容帶來改變，可以透過自動化技術減少行員投入在這些工作上的時間。

在問卷中，我們首先請受訪者從 26 項銀行工作職務分類中勾選出自己最符合的一項，接著對該職務的工作事項填寫工作時間分配（本研究透過前置問卷初步調查各類職務的日常工作



事項，在正式問卷中提供預設選項，同時也保留自填項）。蒐集資料後，我們對每項銀行職務使用 Kmeans 進行分群，並計算出各分群在每項工作中平均花費的時間比例。舉例而言，客服人員可以按各工作內容所投入的時間占比被明顯分為兩群人，其中一群主要在處理“信用卡及帳務相關問題”，另一群客服人員大部分時間則花在“行政與文書工作”及“各項會議及跨部門溝通”（圖九）。

如果我們想評估是否應該導入 AI 技術對各職務的工作進行自動化或人機協作，首先必須詳細檢視每個職務的日常工作事項以及每項工作所耗費的時間。由於各家銀行的職務工作內容及管理規範差異較大無法一概而論，本次調查將以概括的方式探討 AI 技術對國內銀行業各職務的影響，具體應由各家銀行在內部進行調查和檢視。

透過本次調查，我們發現許多銀行部門主管對於下屬的工作內容及時間分配缺乏清晰的概念，這可能會導致人力資源無法有效的利

用。同樣的，若想要在行內推動 AI 轉型並評估各職務與 AI 協作所能產生的價值，首先必須檢視行內各職務的工作內容及投入時間，以便更有效地評估 AI 技術帶來的影響並規劃對應的策略。AI 的應用不僅是技術上的轉變，更是對現有工作模式的一種挑戰和機遇，透過合理的工作職務重新規劃，銀行可以更好地適應這一變化，並從中獲益。

AI 將人們從重複性的工作中解脫

本研究對國內多位專家學者進行深入訪談後，大家達成一致共識：AI 技術並不會取代銀行業的職位，而是透過自動化將員工從重複性的工作中解放出來，使他們能夠專注於更具價值和挑戰性的工作。AI 技術展現出巨大的潛力，不僅能提升效率和降低成本，更重要的是它改變了傳統銀行職務的性質。綜合受訪專家學者的觀點，我們歸納出 AI 技術對現有工作模式帶來最大變化的銀行職務主要會集中在以下三個領域：

圖九：客服人員工作內容時間分配與職務分群（詳見附錄）



客服人員

AI 技術正在顛覆銀行客服人員的工作模式，它們減少了重複性、機械化的工作，釋放出大量時間讓客服人員集中於更具價值的活動，如複雜需求處理、客戶關係維護等。這不僅能解決國內銀行客服人員長期短缺的問題，還有助於提高銀行整體的服務品質。

客服人員應被鼓勵將更多時間投入到處理較為複雜的客戶問題、提供個性化服務給 VIP 客戶，以及參與訓練和優化 AI 客服模型。這不僅能提升客戶服務品質，也能增強員工的專業能力和職業滿足感。以下是導入 AI 技術後，銀行客服人員可能改變的工作模式：

1. 自動化客戶查詢解答

過去客服人員需要親自處理大量的常見問題，例如帳戶餘額查詢、轉帳操作指引和信用卡繳費查詢等。導入 AI 聊天機器人可以全天候處理這些查詢，減少了人員的重複性工作，多出的時間讓客服人員有機會轉向處理更複雜的客戶問題，提供更加個性化的服務。

2. 常見問題管理與客戶回饋作業

過去客服人員需要花費大量時間登記、分類和處理客戶投訴，導入 AI 技術後能對客戶投訴進行自動歸類及優先度排序，使得客服人員能更高效處理客戶投訴。在與客戶溝通的同時，後台可以即時對客戶情緒進行分析，並根據對談記錄給出溝通方式的建議，從而提高客戶滿意度。通話結束後，AI 會自動將對談內容記錄到系統，並用生成式 AI 進行重點摘要以及後續跟進建議。

3. 個性化客戶推薦

過去客服人員在推薦產品時（主要是 call-out，但部分 call-in 也會被要求進行產品推薦），一般會依據主管交辦的目標產品進行介紹，因此成功開發率偏低。導入 AI 技術後，可利用客戶數據生成精準的產品推薦，客服人員可以更專注於與客戶互動，解釋產品細節和增強客戶的信任感，從而提高成功轉化率。



會計審計人員

AI 技術減少了銀行會計審計人員處理重複性工作的時間，讓他們聚焦在更具價值的活動，如提供更深入的財務分析和策略建議、或是參與到財務風險評估和內部流程的改進工作等。以下是導入 AI 技術後，銀行會計審計人員可能改變的工作模式：

1. 自動化數據輸入和處理

生成式 AI 可以自動化許多重複性任務，例如數據輸入、發票處理和對帳等，同時也能快速分析和提取財務報表中的相關訊息，使得處理和檢索資訊的過程變得更加快捷和精確，減少了人力查找和整理資料的需求。

2. 改進審計流程

傳統審計通常依賴定期檢查，但 AI 的引入可以透過不斷分析交易和合規性實現持續性的審計。這意味著，審計能夠即時檢測並糾正異常和問題，從而提高了整體的合規性和準確性，不僅確保了數據的準確性，還可以大幅提高處理速度。



3. 強化數據分析與決策

過去會計和審計人員需要手動整理和分析大量財務數據，AI 技術具備強大的預測分析能力，能夠從大量的歷史數據中識別其中的模式和趨勢，提出傳統分析方法難以發現的細微趨勢和關聯。



風險管理人員

在風險管理領域，AI 的核心貢獻在於其預測能力和決策支援，透過大數據分析和機器學習演算法，AI 可以分析過去的交易數據和市場走向，預測未來的市場風險趨勢。信用風險的部分，AI 可以透過分析客戶的交易記錄和財務行為，精確評估其還款能力和信用風險。以下是導入 AI 技術後，銀行風險管理人員可能改變的工作模式：

1. 自動化風險評估與報告生成

過去風險管理人員需要花費大量時間進行資料搜集來分析和評估每位客戶或項目的風險，導入生成式 AI 技術後能夠自動化分析客戶信用記錄、交易行為及其他外部資料，快速生成風險評估和預測報告，多出的時間讓風險

管理人員可以深入分析風險預測結果，為高風險客戶或項目制定具體的風險緩解策略。

2. 強化數據分析和風險建模

過去風險管理模式中，數據分析和風險評估主要依賴於人工和基於規則的系統，其中的數據通常是結構化，且來自特定的資料庫和報告。然而生成式 AI 能夠處理大量的結構化和非結構化數據，提供更準確和全面的風險評估，這些非結構化數據可能來自社交媒體、新聞報導、客戶回饋等多種來源，進而提供更豐富的數據資源，幫助銀行全面了解風險狀況。

3. 潛在風險事件的即時識別與分析

傳統的風險辨識與分析依賴人工收集和 분석數據往往耗費大量時間，而生成式 AI 能夠實時監控國際政經情勢和金融市場趨勢，自動識別和分析潛在風險事件。此外，該技術可以自動整合子公司和跨國子公司的風險數據，提供綜合的風險評估報告提供即時的風險預警和應對建議，幫助決策者快速反應。



亞洲資採國際
尹相志創辦人

以 Copilot 為例，這樣的工具在不久的將來就能大幅縮短完成工作的時間。想像一下，大多數人花費超過一半的時間在製作 PPT 上，透過這樣的工具可以顯著減少這部分的時間消耗，從而提高工作效率。隨著日常瑣碎事務的高效率處理，人們將有更多時間思考如何實現以前認為不可能的事情。可能因為雇主認為不再需要那麼多人手，導致某些職位的減少，但也可能為個人提供了成就更好自我的機會。當不想做的事情被有效率地簡化後，人們便有機會從事更有意義的工作。隨著 API 成本的降低和 AI 智能的提升，未來的工作場景將包含由 AI 代理完成大部分工作的情形，同時也會出現全新的職業機會，正如過去技術的發展一直伴隨著新工作的創造和舊工作的消失。



我們的產品定位為「Copilot（副駕駛）」，意味著它可以作為一個輔助工具，協助處理那些通常覺得繁瑣的任務，進行預先的準備和處理，然而最終決策和判斷仍需由「主駕駛」來完成。從 low risk high impact 的視角出發，我們確實可以看到生成式 AI 在金融業多方面的應用潛力，包括但不限於電子郵件回覆、報告撰寫和會議記錄的快速生成，這些改進能夠瞬間提高工作效率。此外，考慮到金融業在全球範圍內的溝通和翻譯需求，生成式 AI 憑藉其卓越的語言能力，能夠快速協助跨國溝通。同樣，IT 領域也能從生成式 AI 中受益，特別是在程式開發支援方面，從而提高 IT 專業人員的工作能力。



台灣微軟
花凱龍首席技術長



人工智慧技術將逐步替代那些重覆性高且相對簡單的任務，例如，星展在推動 AI 人才招募系統時，雖然過程中部份同仁擔憂工作會被取代，但事實上 AI 主要替代的是那些耗時又低價值的工作。從實踐經驗來看，這不僅提高了工作效率和選才的公平性，更釋放了人資專員的時間讓他們從事更高價值的工作，如市場趨勢分析、競爭對手分析等。在這種背景下，人資部門面臨的挑戰不僅是如何保護工作崗位，更關鍵的是如何保障員工在不斷變化的勞動市場中，能夠持續提升技能、重新定位自己。對於如何與這波技術浪潮共存，星展已開始探索哪些職務的工作可能會被自動化技術取代，同時也著眼於員工的再培訓和技能提升。



星展集團人力資源
行政暨系統管理
盧方傑負責人

洞察三：

銀行業未來三年的 重點人才需求與 新興職務的崛起

AI 技術固然備受矚目，但要發揮其最大潛能，仍須仰賴人才的專業運籌與創新思維。擁有 AI 專業知識與創新思維的人才，不僅能夠熟練運用 AI 技術提升效率，更能透過獨到的見解，開拓嶄新的營運模式，突破銀行業原有的發展藩籬，為金融服務帶來革命性的變革。在 AI 浪潮的驅動下，吸納並培育 AI 人才將是銀行業未來發展的關鍵所在。

本研究廣泛蒐羅業界專家學者的意見，匯整出未來三年銀行業最為垂青的三大關鍵職務，分別是「資訊安全」、「數據分析」和「創新科技研發」。預期在與 AI 的協作下，這些職務將為銀行營運帶來巨大的創新動能與價值。

AI 時代下的資訊安全

在金融服務數位化的時代，金融交易和個人數據的保護變得尤為重要，AI 技術正協助銀行在資訊安全領域進行突破，運用機器學習模型來檢測並預防潛在的詐欺活動及網路攻擊。然而，與此同時，犯罪分子也正利用 AI 進行更為複雜的攻擊方式，這使得銀行在資訊安全方面面臨更高的風險。

在 AI 時代下，資訊安全人員需要具備全面的 AI 知識，深入了解機器學習、自然語言處理等技術，並能夠運用這些技術

對安全威脅進行實時監控和分析。「AI 安全分析師」將成為未來三年銀行業急需的人才，負責分析人工智慧模型的漏洞並增強人工智慧系統的安全措施，確保資料免於未經授權的存取、修改或破壞。

數據分析的無限潛力

數據已被譽為 21 世紀的新石油，而銀行業無疑坐擁著大量的數據資源。人工智慧技術，特別是機器學習和深度學習，使銀行得以從傳統的業務處理方式轉向更加智能和自動化的流程。數據分析的廣泛應用使銀行能夠更精確地識別和預測市場趨勢及客戶需求，例如透過分析客戶的持有產品和交易模式，銀行可以開發個性化的金融產品和服務，從而更有效地滿足客戶的個別需求。

未來三年，銀行將對「資料科學家」、「數據分析師」和「客戶體驗分析師」等相關職位產生巨大的需求，這些職位將成為各家銀行實現客群精準行銷和個性化服務的關鍵。其中，「客戶體驗分析師」在銀行業的重要性逐漸凸顯，他們透過收集和分析客戶互動的數據，例

如客戶服務的互動過程、線上平台的使用行為、以及客戶回饋，來識別潛在的痛點和改善機會。

創新科技研發

金融服務的創新隨著科技的進步而不斷演進，然而商業模式的創新不應僅依賴於技術進展，關鍵在於如何將新的業務模式與金融領域的具體應用場景結合，並有效整合科技資源。這不僅涉及技術的整合，還包括對市場動態的敏感度和創新思維的應用，以確保金融解決方案能夠在增加效率的同時，也滿足現代消費者的多元化需求。

創新科技研發人才需求，會因不同時代的熱門技術而出現差異，例如過去幾年的元宇宙技術人才、區塊鏈人才等，到時下最熱門的「生成式 AI 工程師」。此外，「AI 專案管理師」和「創新科技應用規劃師」也是未來三年的重點需求人才，一項創新商業模式是否能成功落地，除了技術因素外，最關鍵的是對業務和需求的理解，因此專案管理及應用規劃亦是不可或缺的重要人才。



台新金控
孫一仕資訊長

我相信隨著時間的推移，那些重覆性高的工作將逐漸被自動化技術所取代。然而，這並不意味著人類將被完全取代，相反，這將使人們有更多的精力去關注那些需要深度思考和創造力的領域。以編程為例，雖然簡單的程式碼可以透過工具生成，但深層次的邏輯理解、客戶溝通以及對需求的深刻把握，這些技能是無法透過人工智慧來實現的。因此，即使在金融業等領域，未來也許會看到人員的精簡和服務質量的提升，但核心的創造性工作和人際互動，將依然依賴於人類的智慧和創新能力。無論技術如何發展，人類對於工作本質的理解和創新能力，是不可被取代的。

銀行業未來可能的新興職務

未來三年，隨著金融科技的發展趨勢日益明朗，銀行業的人力資源需求也將發生變化。一方面，科技驅動將加速傳統金融崗位的更迭，許多職位面臨被取代或整合的風險；另一方面，新興職業將開始湧現並逐漸成為引領銀

行業創新發展的中流砥柱。具備數據分析、人工智慧、網路安全等尖端技能的複合型人才，將在未來金融行業中備受重視和青睞。本研究廣泛蒐羅業界專家學者的意見，匯總出銀行業未來將可能出現的新興職務：

1 AI 工程師 (AI Engineer)

隨著 AI 技術的快速發展，銀行在未來必然將 AI 納入戰略規劃，成為銀行業轉型創新的重要驅動力。然而 AI 複雜的理論基礎和工程實踐要求，與銀行過去的人才儲備大相逕庭，導致業內嚴重缺乏這類人才，因此培養和引進 AI 工程師將成為銀行的當務之急。過去推動數位轉型的過程中，部分銀行雖然已經開始招募資料科學家將行內的大數據價值充分發揮，但 AI 工程師與他們的工作性質有所區別。資料科學家主要從事數據分析、建模和發現洞見，而 AI 工程師則專注於設計、開發和部署 AI 系統的工作，雖然兩者需具備的技能有所重疊，部分資料科學家可以兼顧兩種職務，但從長遠規劃應專業分工互相搭配才能發揮出綜效。

2 AI 訓練師 / AI 標註師 (AI Data Annotator)

人工智慧模型的準確性和效能取決於訓練數據的品質和多樣性。銀行業務涉及大量複雜的金融數據，如交易記錄、客戶資訊、風險報告等，需要專業人員對這些原始數據進行清理、整理、標註，為 AI 模型提供高品質的訓練數據集。這一職務很可能源自銀行業內現有的專業人員，如風控人員、法遵人員、理財專員等，他們精通金融領域知識，能夠從專業視角對原始數據進行準確理解和標註，將他們的專業經驗 "教" 給 AI 模型。AI 標註師的主要職責包括：整理和標註大量複雜的金融數據，構建高品質的 AI 訓練數據集、從專業角度審視原始數據，確保數據標註的準確性和一致性、參與 AI 模型的設計和優化，為其注入金融領域知識、以及培訓其他員工 AI 數據標註技能，推動 AI 在銀行各業務層面的應用。

AI 倫理官 (AI Ethics Officer)

未來各家銀行將逐步採用人工智慧系統輔助貸款審批、交易監控、客戶行銷等業務，但若 AI 演算法存在偏見或缺乏透明度，可能導致決策不公、侵犯隱私等倫理道德問題。AI 技術雖高效但也充滿風險，需要有專業人員從倫理層面把控，避免 AI 系統歧視少數族裔或特定群體，以維護消費者權益。AI 倫理官的主要職責包括：審視銀行的 AI 系統是否符合道德標準和監理規範、評估 AI 演算法的公平性、透明度和問責制、協調制定 AI 技術的倫理規範和風險管控政策、以及培訓員工 AI 倫理意識，糾正違反道德的 AI 模型。

科技法遵人才 (Technology Compliance Professionals)

傳統的法遵人員通常擁有法律、會計或金融背景，但往往缺乏資訊科技、數據分析等專業技能，難以全面審視和管控科技風險。銀行迫切需要具備雙重背景的複合型人才，能夠理解最新科技並評估其適法性。科技法遵人員的主要職責包括：評估新技術的適法性、制定科技風險管理政策、規劃法令相關培訓、監控科技系統營運合規性等。他們需要具備資訊科技、數據分析、法律法規等綜合知識技能，幫助銀行提前識別和防範潛在風險，避免重大違規事件發生。



洞察四： 軟實力： AI 時代下的 競爭利器

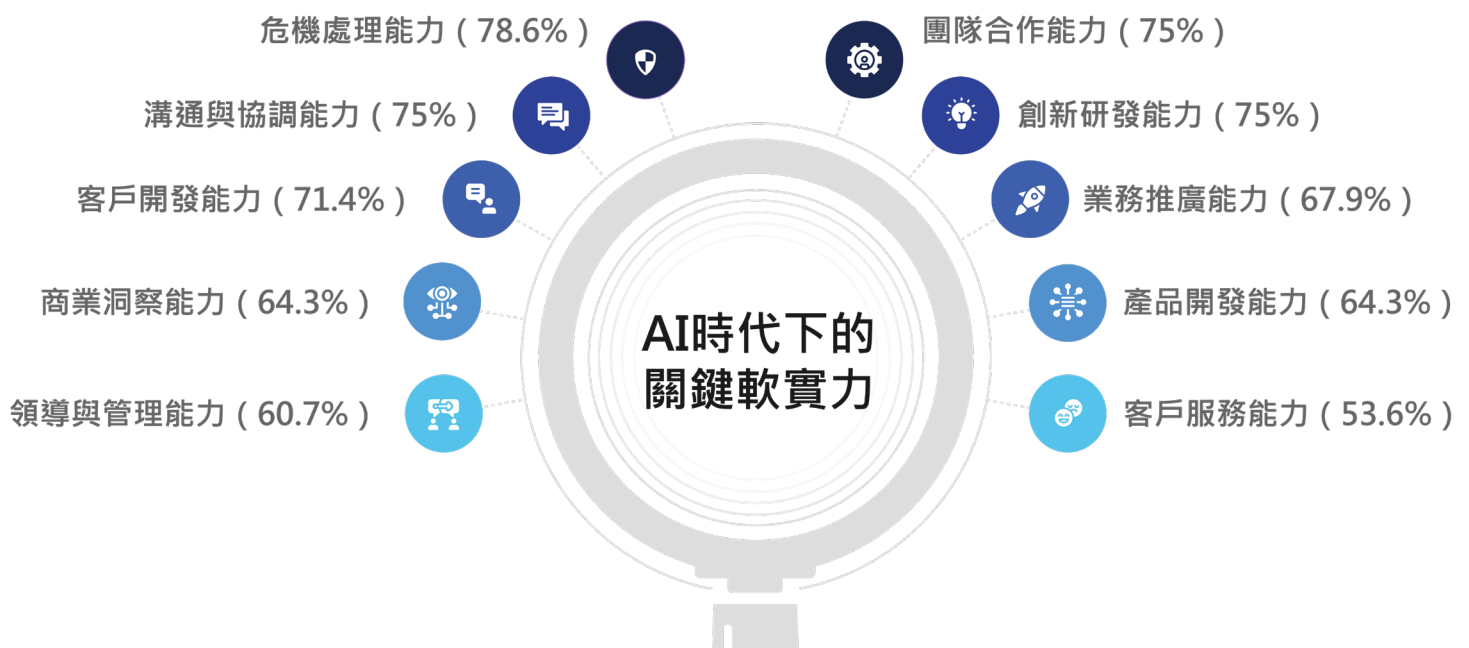
人工智慧的迅速崛起正逐步改變銀行的工作方式，如前述提到部分行員會擔心曾經的金飯碗是否會被這個新時代所拋棄，他們擔心現在的工作會被 AI 所取代，或是被會 AI 技術的人所取代。經本研究訪談多位專家學者以及國內各家領先者銀行的高管，得出的答案是：不一定。他們強調了在 AI 時代下，如果能夠善用一項關鍵武器——軟實力，將在這場變革中立於不敗之地。

AI 時代下更需重視培養行員的軟實力

客戶之所以願意與銀行建立長期關係，不僅是因為產品優勢，更是因為行員能提供值得信賴的服務和專業建議。銀行行員的貼心服務、對客戶需求的深入理解及靈活應變能力，可以提供客戶溫暖與信任，良好的溝通和同理心是 AI 無法完全替代的關鍵因素。

在 AI 時代，銀行業對行員的軟實力要求比以往任何時候都要高，尤其是在危機處理、

圖十：銀行管理層認為 AI 時代下最重要的軟實力





團隊合作、溝通協調和創新研發等方面，銀行應該積極投資於行員的軟實力培訓和發展，這不僅能提升行員的職業素質，也是推動銀行持續進步和應對未來挑戰的關鍵。

銀行業者最重視的軟實力

1. 危機處理能力

近年來「黑天鵝事件」出現的次數趨於頻密，金融業必須時刻準備迎接過去被認為不可能發生或前所未有的重大危機，這類事件要求銀行行員需具備高度的危機處理能力和適應能力，迅速評估情況並制定策略，以將風險降低。雖然 AI 技術能夠提供數據分析和預測，但在危機發生時，人類的直覺、實戰經驗以及戰略規劃能力仍是不可或缺的。

2. 團隊合作能力

面對日益複雜的金融市場和不斷變化的經濟環境，單打獨鬥已經遠遠不足以應對各種挑戰，透過建立一個多元化的工作團隊，將不同背景和專業知識的專才結合，更能夠產生出創新的解決方案。團隊合作特別重要的原因在於，它能夠促進團隊間知識和技能的共享，使

成員能夠彼此學習並更加多元互補，有助於建立一個向心力極強的企業文化。

3. 溝通與協調能力

良好的溝通與協調能力包括能夠清楚地表達自己的想法、同時聆聽他人觀點，以及如何在不同意見衝突的情況下尋求共識，這不僅涉及與客戶的溝通，更包括與同事、跨部門、甚至跨國界的合作。儘管 LLM 已經可以模擬人類語氣進行對話，但人際間的協調與溝通是建立在人類情感和認知基礎之上，這是目前 AI 所無法完全取代的。

4. 創新與研發能力

創新與研發能力是推動銀行業務成長和適應市場環境快速變化的關鍵因素，雖然生成式 AI 有時候可以產出讓人驚艷的創意組合，但本質而言是從 1 到 n 的創意。可以創造巨大價值的顛覆性創新往往是從 0 到 1 的創新，這種從無到有的能力涉及到對市場需求的獨到理解，以及在面對未知和不確定性時所展現的靈活性與應變能力，這是目前 AI 所無法取代的。

5. 客戶開發能力

客戶開發不僅僅是吸引新客戶，更重要的是能夠深化與現有客戶的關係，提供個性化的服務，並識別客戶的潛在需求，從而增加客戶的忠誠度和滿意度。在 AI 技術支持下，銀行行員可以利用大數據分析來更好地理解客戶的行為模式和偏好，但是人與人之間的信任和深層連接還需要透過人類的直接交流。

未來的 Skill-based 時代

在面對全球人才短缺和少子化的挑戰中，技能導向（Skill-based）的招聘策略日益成為企業尋找和培養人才的主流方式，過去強調的是企業培養頂尖人才以獲得組織於市場上的競爭優勢；現在不僅強調實際工作技能，還促

使企業更注重個人在職場上的即戰力。

依據 McLagan(1980) 提出職能的概念，一項工作的職能項目歸納為知識 (Knowledge)、技能 (Skills)、態度 (Attitude)，技能便是肢體與認知上的操作能力，亦即「會什麼」(Know-How)？在當今多變的勞動市場中，技能導向的招募模式已漸漸取代傳統的學歷導向模式，成為企業尋找合適人才的重要策略，組織不再僅是聚焦於應徵者的學術背景及學位，更強調他們實際「會什麼」？

此項招募轉變對於擁有多學科知識和技能的跨領域人才來說，頗為有利。跨領域的人才通常能有效解決複雜問題並推動創新，對於快速變化的市場環境而言，這類人的多樣性及適應能力尤其寶貴。若能以不同領域的觀點和方



法融合，推動創新並增強團隊的多樣性，不僅可增強組織的適應能力，還能開創新的合作機會，為企業帶來持續的競爭優勢，是企業的寶貴資源。

而隨著 AI 的普及和技術的迅速發展，市場對於技術技能的需求不斷增加，無論是數據分析、機器學習、程式設計等專業技能皆成為

基本要求。然而，除了這些硬技能之外，依據本研究的大調查所示，危機處理能力、團隊合作能力、溝通與協調能力及創新研發能力等軟技能將成為 AI 時代下的競爭利器，這些技能有助於在 AI 環境中提出新解決方案和進行有效的人際互動。



中信金控資訊最高主管
賈景光

要真正發揮生成式 AI 在銀行業的價值，關鍵在於培養我們的核心幕僚掌握應用 AI 技術的三大能力：首先，與 AI 溝通的能力，特別是在 prompt 能力方面；其次是能夠識別 AI 產出內容準確性的能力，因為即使是最先進的技術也可能會出錯或產生所謂的「AI 幻覺」；第三，我們必須培養創新思維，學會在不同情境下靈活運用 AI，特別是在可以將人類工作價值提升到更高層次的任務上。為實現這一目標，我們建立了種子團隊並對其進行 AI 應用的培訓，透過舉辦競賽鼓勵團隊成員分享他們的使用經驗，從而發現有效的應用場景並推廣至更廣泛的範圍。這個過程不僅有助於我們識別哪些場景適合 AI 應用，也讓更多的人認識到 AI 的潛力。最關鍵的是，創新始於對 AI 工具的深入了解。只有當我們的全體員工對這些工具有足夠的熟悉度，才能真正務實的推動與應用 AI。

策略一：

生成式 AI 布局 應該先行還是跟隨？

我國政府為掌握 AI 技術發展契機，宣示 2017 年為台灣 AI 元年後，部分大型金控及銀行開始陸續導入 AI 技術應用到各業務領域，根據本院 2022 年對國內銀行業數位轉型大調查的結果，綜合專家評分、同業互評及行員評分後列舉出七家「先行者銀行」，在本次調查中發現七家「先行者銀行」同樣在 2017 年前後就陸續開始導入並發展 AI 技術應用。

在過去尚未啟動數位轉型之時，銀行內部的資料並沒有得到充分的整理，各個系統之間無法串連導致資料無法被充分運用，而數據的品質會直接影響 AI 訓練及開發的效能。七家「先行者銀行」在資料治理方面投入了龐大的資源，為推動 AI 技術打下了堅實的基礎，因此今天可以看到他們正在採擷早期投入所帶來的豐收果實。

同樣的，2023 年被視為生成式 AI 的元年，該技術已經顯示出其顛覆傳統工作和業務模式的巨大潛力，我們再次迎來與 2017 年相似的關鍵抉擇時刻，各家銀行的決策領導階層必須審慎思考，究竟應該在生成式 AI 的布局上領先市場，抑或觀望現況後再跟隨同業的步伐。採取先行策略的優點在於，可藉由前期投資，掌握核心技術並累積實作經驗，奠定未來發展的基礎，搶占先機贏得市場優勢。

然而，先行者所面臨的風險亦不容小覷，由於生成式 AI 技術尚在發展之中，技術更替非常迅速，投入過多資源而未見成效，不啻是無謂的資源浪費。此外，生成式 AI 技術仍存在 AI 幻

覺等不確定因素，過於激進的創新亦可能引發消費者及行員的不信任與反彈，有可能危及銀行的聲譽，因此先行者須審慎評估研發成本、風險管控及法令規範等多重面向。

另一方面，採取跟隨策略看似有些保守，但卻可從先行者的布局中汲取經驗教訓，避免重蹈覆轍。等待技術和監管環境日趨成熟後再行部署，不僅可降低營運風險，更可觀察他人的實踐結果，作為自身規劃時的參考依據，不過這樣也可能錯失搶占市場先機的良機。

無論銀行業者選擇先行或跟隨，都必須秉持審慎的態度，先行者當權衡資源布局與風險控管，跟隨者則需保持對市場發展的敏銳度，做好隨時調整策略的準備。在生成式 AI 的浪潮下，唯有持續觀察、快速回應，才能在瞬息萬變的金融版圖中持續領先。

先行者執行策略

1. 強化研發和創新能力

先行者應投資於自身的研發部門，同時與大專院校和研究機構合作，吸引及培養 AI 頂尖人才，推動技術創新。此外，可建立專門的

創新實驗室或加速器，以種子成員的方式帶領各單位熟悉運用生成式 AI，並嘗試將該技術與現有業務整合。

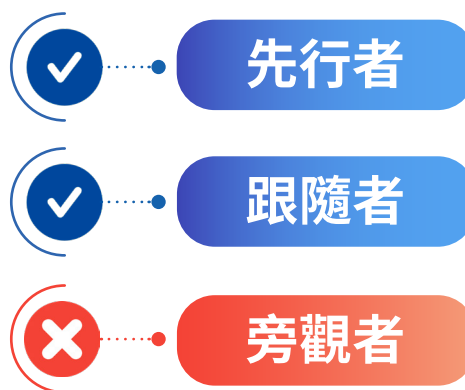
2. 建立戰略夥伴關係

先行者可與微軟、輝達等 AI 科技巨擘建立緊密的合作關係，這不僅能加速技術的集成和優化，同時也能獲得前沿技術的最新應用。透過這些戰略夥伴關係，銀行可以更快獲得創新技術的市場應用訊息，並應用在產品的制定以更好地滿足其特定需求。

3. 完善的管理框架

先行者必須建立好一套完善的生成式 AI 應用管理框架，確保全面評估和監控相關的風險，避免出現客戶個資外洩以及 AI 幻覺等問題。這包括建立嚴格的數據治理政策，包括數據收集、處理和儲存的規範，以符合相關的法律法規。此外，在 AI 模型部署前進行廣泛的測試，包括壓力測試和場景分析，以評估模型在各種極端條件下的表現和可靠性。

圖十一：生成式 AI 布局的選擇





跟隨者執行策略

1. 持續追蹤最新技術發展

跟隨者可建立一個專門的研究分析團隊，對行業最新動態進行深入研究，持續監控市場趨勢和技術發展，包括分析先行者的成功案例和挑戰等，待技術及市場成熟時，做出更加有利的決策。

2. 強化內部資料治理

跟隨者需要確保行內已建立一套全面的資料治理策略，包括資料收集、儲存、處理、保護和銷毀等方面的標準程序，透過完善的資料治理策略，銀行不僅為當下的營運提供了堅實的基礎，也為未來可能的技術升級和生成式 AI 技術導入做好充分的準備。

3. 基礎 AI 素養的普及

為了在現有業務基礎上進行創新，跟隨者應普及基礎 AI 素養，讓行內所有行員學習了解何為 AI，包括 AI 的基本概念、應用實例以

及 AI 如何助力金融業務創新和效率提升。透過提升全員的 AI 知識水平，不僅促進內部創新思維的激發，也加強團隊對於技術變革的接受度和靈活應對能力。

可以不當「先行者」，但千萬不要當「旁觀者」

在生成式 AI 技術的應用上，銀行可以選擇成為先行者或跟隨者，但絕不應選擇成為旁觀者，因為在未來這個數據驅動、以技術為核心的時代，旁觀者可能會迅速失去在激烈競爭的市場中立足的機會。

靜觀其變在今日的銀行業等同於自我放棄市場份額，當其他銀行透過生成式 AI 技術提供更個性化、更高效的服務時，那些選擇旁觀的銀行將面臨極大的客戶流失風險。我們建議每家銀行都應至少成為跟隨者，持續掌握最新的市場發展和技術進步，在學習同業實踐方法的同時，逐步將新技術整合入自家業務模型中。



目前對大多數的國內銀行來說，即便是 IT 部門，可能都還沒有專業人員能夠自建 LLM 模型或是進行 Fine-tuning，短期比較可行的是使用 RAG 的方式，這樣就可以把它轉化成從業務優化的角度來看，哪些東西可以先進行嘗試。生成式 AI 短期內可能會從如何幫助營業單位的員工或從總行事務開始嘗試，特別是一些比較偏向產品開發、風控或法遵的工作。距離可以落實運用生成式 AI，我認為可能需要二到三年的時間來確認生成式 AI 不會在客戶使用時產生任何誤導，例如在理財建議上運用生成式 AI 提供具規模的客製化和個人化能量。



第一金控
劉培文資安長



銀行應當注重培養行員的 AI 基礎知識，確保他們對 AI 技術有基本的了解，強化他們對 AI 技術的概念理解和實際應用能力。其次是提高與 AI 協作的的能力，建議銀行鼓勵同仁分享在工作中如何與 AI 進行協作的經驗，發展出自己專屬的 know-how。此外，基礎的程式能力也十分關鍵，Python 雖然是當前的主要工具，但未來可能會有更多新工具出現，因此理解程式語言背後的邏輯和思維方式比單一工具的操作更為重要。我認為不論是哪一個專業領域的人才都應掌握基礎的程式技能，這不僅有助於激發業務創新的潛力，還能豐富他們的領域知識，激發更多創新思維。

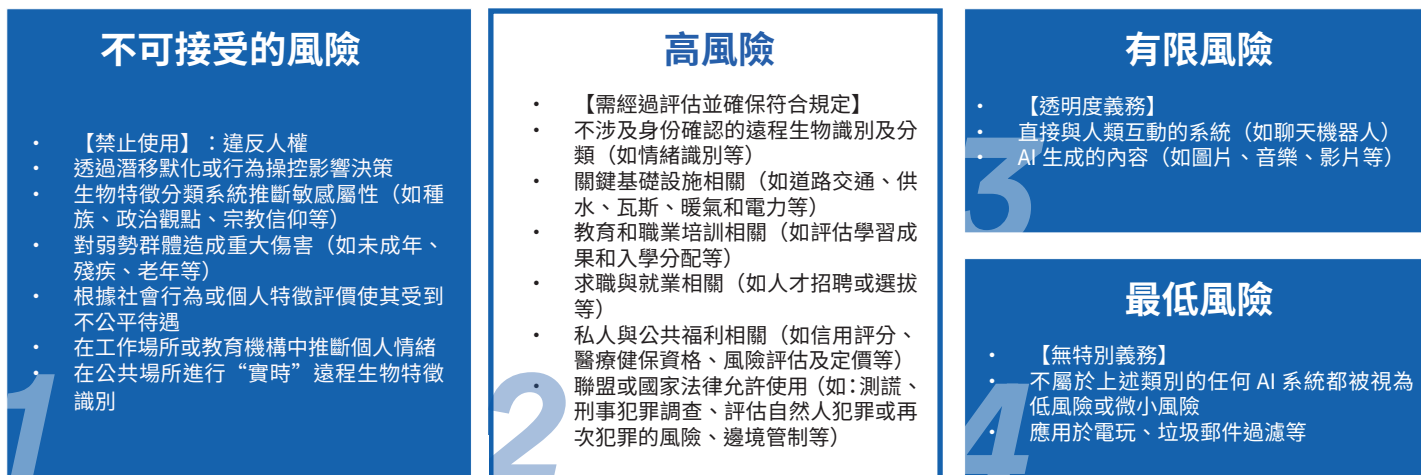


生成式 AI 創新學院
李啟龍院長

策略二： 建構安全的 AI 使用環境

生成式 AI 技術為銀行業所帶來的顛覆性潛力大家皆有目共睹，但導入該技術所伴隨的風險不容忽視，因此如何建構一個安全的 AI 使用環境是各家銀行推動 AI 轉型的關鍵問題。由於 AI 技術的導入對大部分產業而言都是全新的概念，因此對相關技術的監管仍沒有非常明確統一的規範，目前國際主流的大框架是歐盟在 2024 年 3 月通過的「人工智慧法案」，裡面將人工智慧系統劃分為四種風險等級，即「不可接受風險」、「高風險」、「有限風險」與「低風險」，並針對不同風險類別採取相應的監管策略。

圖十二：人工智慧系統風險等級劃分





如何建構可信任 AI 框架

根據美國國家標準暨技術研究院 (NIST) 對可信任人工智慧 (Trustworthy AI) 的研究，他們指出可信任 AI 應包含有效性與可靠性、安全性、防禦與韌性、透明度與問責制、可解釋性、隱私保護、以及公平性 (避免 AI 偏見)。銀行在建立行內 AI 系統時，應充分考量下面的關鍵要素，以建立一個可以被社會大眾信任的商業模式。

1. 有效性與可靠性：有效性是指 AI 系統是否能完成它被設定的既定事項，並在各種情況下都能表現得很好，例如 LLM 可能會生成一些會造成傷害的內容 (仇恨言論、錯誤訊息等)，需要不斷地測試和監控 AI 系統，確保它在實際使用中的表現符合預期，同時建立內容審查系統、部署檢測並阻止不當內容的過濾器以在發現有害輸出時迅速回應。可靠性則是強調 AI 系統的穩定性和耐用性，可以在規定的條件和時間內持續正常運作的能力。
2. 安全性：人工智慧的安全性是指在 AI 系統的設計、開發、部署及運作過程中，不會在任

何條件下危及人類生命、健康、財產或環境等重要領域。要實現這一目標必須從多個層面入手，首先開發者和部署者需要對 AI 系統的潛在影響有深入的理解，並在整個開發過程中充分考慮到安全相關議題。此外，風險管理策略需根據 AI 面臨的具體安全風險制定，例如那些可能導致嚴重傷害或死亡的風險需要被優先處理，並透過嚴謹的風險管理過程控制，促進更為全面和有效的 AI 安全策略。

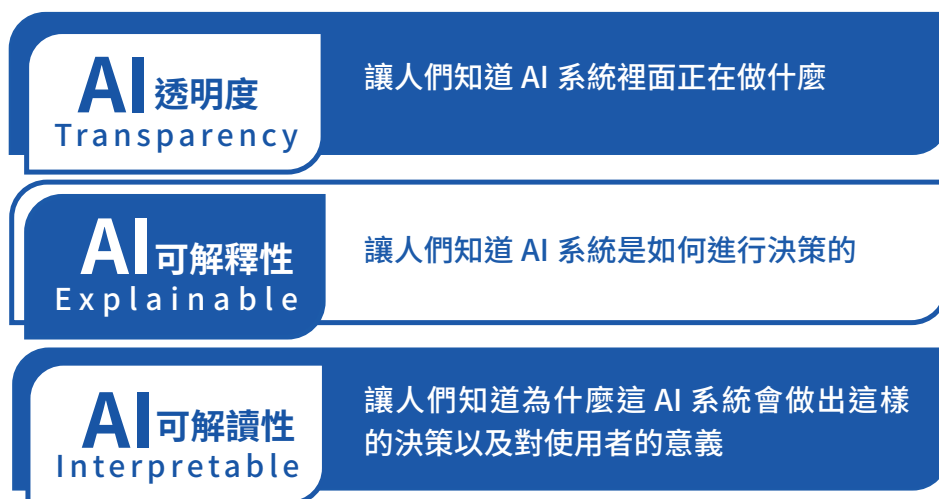
3. 防禦與韌性：AI 系統中的防禦主要指透過各種安全協定與措施，防止未授權的訪問和使用，保護系統免受攻擊，包括對抗數據污染、提示注入攻擊、訓練數據或其他智慧財產的非法盜取等。韌性則是指當 AI 系統遇到非預期的挑戰或變化時，例如面對外部攻擊或內部故障時，能夠迅速恢復至正常狀態、維持正常運作或在必要時安全降級的能力。
4. 透明度與問責制：透明度的建立是為了讓所有與 AI 系統互動的人，都可以獲得該系統的充分資訊，其中包括模型設計的理念和基本原則、訓練數據的來源及數據處理方式、模型

訓練使用的演算法及模型效能、系統的用途與使用限制等。問責制始於透明度，只有當決策過程、數據來源、演算法設計和操作結果都是公開和可檢查的，外界才能對 AI 系統進行有效的評估和監督。在 AI 系統的各階段，必須清楚地識別出誰是責任主體，例如模型的開發者、部署者、維護者或使用者等，確定這些角色有助於在出現問題時，誰可以負責解決問題，同時應制定清晰的指導原則來確保不同的

角色都清楚自己的責任所在。

5. 可解釋性：開發可解釋的 AI 模型是讓使用者不僅能看到結果，還能理解 AI 如何得出這些結果，這是提升使用者對 AI 系統的信任並有效確保負責任地使用 AI 的重要因素。雖然有部分機器學習演算法先天具有較好的可解釋性，例如決策樹、線型迴歸、邏輯迴歸等，其決策過程清晰且易於解讀，但若要追求更好的

圖十三：AI 透明度、可解釋性、可解讀性



模型預測成效，無可避免會需要使用到更進階複雜且難以直接解釋的模型如深度學習模型等。因此，必須透過一些模型解釋工具如 LIME、SHAP 等，可以向使用者提供較好的模型可解釋性。

更重要的是與客戶建立起信任的基礎。另外，透過 AI 隱私強化技術 (PET) 或其他去識別化技術，可以強化對客戶隱私的保護，但這類技術可能會導致準確性降低，從而影響某些領域中有關公平性和關鍵決策效能。

6. 隱私保護：尊重客戶隱私是 AI 應用中至關重要的，其中包含建立個資同意使用機制，並確保在訓練過程中嚴格保護客戶個資。模型建立和訓練的過程中，必須清楚闡述客戶數據蒐集、使用與保存的方式，並賦予客戶對其數據的控制權，這不僅為了確保遵守個資保護法，

7. 公平性：AI 模型或 LLM 可能會產生各種形式的偏見，主要體現在過往的刻板印象或是對特定群體的歧視，例如在美國的信用風險模型判斷黑人違約風險較高等。因此，人工智慧的公平性著重於透過解決有害的偏見和歧視問題，來促進平等和公正，然而公平的標準可能

相當複雜且難以明確定義，因為公平的理解會因文化差異而不同，並且可能會根據其應用場景有所差異。NIST 提出了需要關注和管理的三種主要偏見：系統偏見、計算及統計偏見和人類認知偏見，並指出緩解 AI 偏見需要從多方面著手，包括多樣化的訓練數據集、嚴格篩選訓練數據集的特徵變量、以及透過演算法持續監控輸出結果以識別並糾正其中的偏見。

如何降低 AI 幻覺

導入 LLM 的一個重大挑戰是，它們有可能會生成一些看似合理但實際上並不正確的資訊（一般稱為 AI 幻覺），這是因為這些模型基於從訓練數據學習的模式來生成回應，而不是透過實時訪問並進行事實驗證，在特定領域如醫療、法律或金融投資等，誤導性資訊的傳播可能帶來廣泛的負面後果。實務中若要減少 LLM 輸出中的誤導資訊和幻覺風險，可以參考以下幾種策略：

1. 採用檢索增強生成技術（RAG）

RAG 同時結合了檢索（Retrieval）和生成（Generation）兩種方法，當 AI 需要生成回答時，它會先從一個龐大的文檔數據庫中檢

索相關訊息，這些文檔可能來自網路、專業書籍或已經被專家驗證的資料。透過這個檢索過程，AI 能夠獲取真實且相關的訊息，利用這些文本作為參考進行整合和重組，生成更精確和可靠的文本。這種方法可以顯著減少 AI 生成虛假或不正確訊息的風險，因為生成過程是基於已檢索到的可靠資料。

2. 信心評分系統

信心評分系統的核心在於為 AI 生成的每一段文本或每一個答案提供一個信心分數，這個分數基於模型對自身生成答案的信心程度，同時考慮背後支持該答案的數據或來源的強度和相關性。在此系統中，AI 在提供答案時也會展示其信心分數，可以是 0 到 100 之間的數字，分數越高表示對答案的信心越大，若針對特定問題的信心程度過低，則可以回傳類似“對不起，我不確定”的訊息。

3. 建立回饋機制並持續監控

如同我們在使用 ChatGPT 的介面中，可以對它產出的內容進行回饋或提交建議，因此銀行在導入 LLM 後，同樣應建立回饋管道並鼓勵使用者直接提供使用體驗和回饋，用於



確定未來模型調校或改進的方向。開發 AI 或 LLM 模型不會是一次性任務，而是一個需要持續監控和微調的循環過程，透過用戶回饋搭配持續進行的監控與測試，盡可能將 AI 幻覺出現的機率降到最低。

生成式 AI 時代下的新型態資安風險

LLM 技術在文本生成、自然語言理解和聊天方面展現出驚人的潛力，這些模型能夠自動撰寫程式碼、撰寫專業文件、甚至協助進行複雜的數據分析。然而，這些能力也給惡意使用者提供了工具，例如 LLM 可以被用來自動生成釣魚郵件、社交工程攻擊的腳本，或者模擬特定人物的語言風格以進行身份冒充。AI 與 LLM 等技術的進步無疑為我們帶來了便利和機會，但同時也帶來了新型態的資安風險挑戰：

1. 提示注入 (Prompt Injection)

攻擊者透過巧妙設計的提示輸入來操控模型的輸出，以實現不正當的目的，例如一個提示注入攻擊可能會利用模型的回應功能來透露敏感資訊、引導客戶進行危險操作，或者在不知情的情況下散播錯誤訊息。

2. 訓練數據污染 (Training Data Poisoning)

是一種針對機器學習模型的攻擊方式，其核心目的是在模型的訓練過程中故意加入惡意數據，從而影響模型的學習結果和行為。當這些被污染的數據與正常數據一起被用來訓練機器學習模型時，它們會逐漸扭曲模型的學習過程，導致模型學到錯誤或偏差的行為模式。這種攻擊手法對於任何依賴大量數據訓練的系統都可能造成嚴重的安全隱患，尤其是在開放訓練環境中，攻擊者有可能輕易地植入惡意數據。



3. 模型阻斷服務攻擊 (Model Denial-of-Service)

這類攻擊目的是使 AI 系統或模型因過度負荷而無法正常提供服務，對於依賴 AI 模型進行日常營運的系統尤為嚴重，因為它可能導致服務中斷，影響客戶體驗，並可能帶來經濟損失。

4. 自動化的社交工程攻擊 (Automated Social Engineering Attacks)

LLM 可以分析大量的公開訊息，如社交媒體帳號、部落格和論壇貼文，從而學習特定目標的寫作風格和溝通習慣。接著，攻擊者可

以利用這些模型來自動生成看似來自可信朋友、同事或家人的郵件或訊息，這些郵件或訊息會誘使受害者點擊惡意連結或透露敏感訊息。

5. 深度偽造 (Deep Fake)

深度偽造可以創造出極其逼真的假影像或聲音，尤其是在身份認證方面，這類技術可以被用於製造假新聞、模仿公眾人物的語音或面孔，甚至在社交媒體上散播虛假訊息，對社會造成混亂和不信任。此外，它還可能被用於偽裝成熟人透過電話或視訊進行詐騙，因此未來需要更高級的偵測技術來對抗其風險。



安永管理顧問
萬幼筠總經理

金融業在導入與使用人工智慧時，應納入兩項關鍵原則：一是 "put human on the loop"，意即引入外部 stakeholder 的意見來進行評估和審查，需留意勞基法、平權等問題及補償等事項，並嚴格遵循相關法律與倫理規範。二是 "put human in the loop"，這意味著回到企業內部，進行 AI 系統發展與佈建 end to end Life Cycle 中，內部的風險評估，控制與監督，涉及設定模型規格、確認數據來源，確保數據使用不偏離原始目的等。同時，訓練與測試過程的數據應被保留，因為人工智慧的操作本質是一個「黑箱」過程，我們只能透過周邊數據的使用來理解其正確性。對於 AI 應用的風險等級，可參考歐洲框架分為四大類：高風險項目須進行專業機構驗證；中等風險可請求第三方專業審查；低風險或無風險則可進行內部自我評估，以確保所有過程遵循 AI 倫理和個資保護等標準。

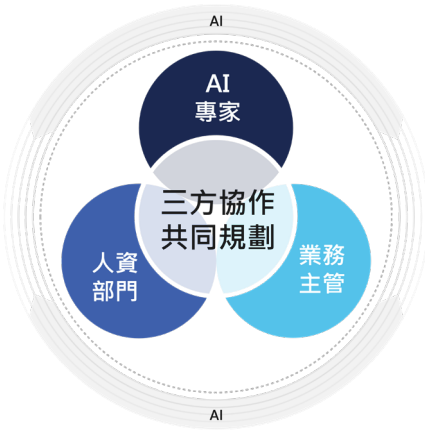
策略三：

提前布局規劃 各職務行員 再培訓 (Reskill) 與 技能提升 (Upskill)

生成式 AI 技術不僅能理解人類語言，還能透過深度學習和自然語言處理技術，自動生成符合人類語言習慣的文字。這對於需要大量文書處理和客戶服務的銀行業來說，意味著必須重新考慮員工的職業路徑和技能發展。對於銀行業而言，這是一個重新評估和規劃人資策略的絕佳機會，銀行應當針對可能受 AI 影響的職務進行全面檢視，思考當他們的工作可以被 AI 自動化後，應該安排哪些新的工作內容，或是要學習哪些新的技能。

為了有效因應這些變化，銀行業需要制定全面的再培訓 (Reskill) 和技能提升 (Upskill) 計劃，要使員工可以適應新的技術要求，如數據標註、AI 模型訓練及 AI 系統監控與偵錯等，同時還要增強他們的戰略思維和創新能力，從而在 AI 時代中找到新的價值和位置。透過系統性的再培訓計畫，這些原本可能被取代的傳統職務人員，不僅能轉任 AI 時代所需的新興工作，更能成為 AI 系統的後勤支援，提升銀行業的整體 AI 實力。

圖十四：三方協作布局行員再培訓與技能提升



AI 時代下各職務的技能缺口

AI 技術能透過自動化流程來提高工作效率，但同時也帶來了人力資源運用的重大考驗，因此銀行需主動評估哪些工作可以交由 AI 自動化處理，哪些職務需要進行重新設計和技能提升。

首先，自動化和機器學習技術將顯著減少對於傳統人工處理和重複性任務的需求，這將直接影響到銀行的前中後台人員，例如交易處

理、帳戶管理和客戶服務等職位將面臨重大的技能重塑。這些職位的員工需要被重新培訓，以掌握數據分析、客戶體驗設計和 AI 協作等技能。

其次，風險管理和財務分析領域的技能缺口將更為顯著，AI 能提供更深入的見解和預測模型，但這要求員工不僅要熟悉金融知識，還要能夠理解和應用機器學習演算法，缺乏這種跨領域技能的員工將難以適應新的工作需求。再者，隨著 AI 技術的整合，新的監管和倫理規範知識、法令遵循和個資安全的重要性日增，員工必須具備相應的法律和技術知識，以確保 AI 應用的合規性和道德性。

銀行各部門有必要成立專案小組，深入評估 AI 將如何影響當前的工作流程和職務設計，全面檢視可自動化環節的同時，並對職能定位和所需技能進行重新審視。接下來，管理層應制定詳細的人力資源轉型計劃，針對這些技能缺口設計專業的培訓計劃，包括提供在職培訓和持續教育機會，幫助行員學習新的關鍵技能，協助他們擺脫簡單重複性工作的掣肘，提升戰略規劃、創新思維、數據分析等綜合能



凱基銀行
周旺墩資安長

隨著 AI 技術的進步，其能力將不斷增強，當 AI 的能力達到相當於五年工作經驗人員的能力時，我們應如何調整人員的配置？以程式開發為例，在 AI 的輔助下即便是非專業人士也能編寫簡單的程式碼，並可能超越大多數初級工程師的水平。當考慮到銀行及其合作夥伴中約 80% 的開發人員屬於初級水平時，這些人員很可能成為 AI 替代的對象。但是，我們的目標不僅是減少對初入職場人員的依賴，而且更希望培育他們成為公司未來的中堅力量。因此，新進員工必須學會利用 AI，將其能力基於 AI 這一平台來提升，在 AI 技術之上創造額外的價值，否則未來將難以與 AI 競爭。



力，以因應 AI 時代的新挑戰。

培養行員 AI 基礎與應用能力

技術本身並不會是銀行推動 AI 轉型的唯一挑戰，行員對 AI 技術的認知與熟悉程度，更是推動創新的關鍵因素。傳統銀行業務依賴於人工處理大量的交易與客戶互動，而 AI 技術的導入意味著這些過程將逐步自動化，其應用範圍涵蓋基本的文書處理、到複雜的數據分析、決策支持等。行員需要意識到 AI 不僅是一個工具，更是一種全新的工作模式，但這需要行員具備對 AI 技術的基本理解和適應能力。

為了克服這些認知挑戰充分發揮 AI 的潛力，首先需要普及基礎 AI 知識，對所有行員進行培訓，其中包括對 AI 的基本概念、技術原理、以及應用場景的了解，同時讓行員知道使用 AI 工具會有哪些潛在的風險。這不僅有助於員工在工作中更有效地與 AI 系統協同作業，同時也能建立員工對 AI 技術的信任感，減少對 AI 的抗拒心理。

考慮到不同職務對 AI 技術的需求差異，銀行應設計並實施客製化的 AI 培訓計劃。例如，對於客服人員，培訓重點可能在於如何使用 AI 工具提升客戶互動的品質與效率；對於

徵授信人員，則需要深入了解 AI 如何協助進行更精確的信用風險評估。銀行業者應該不僅提供工具，更要在培訓的過程中進行實際操作，使行員能在實際操作中快速熟悉這些技術，同時定期舉辦教育訓練，以確保行員不斷更新其技術技能，適應快速變化的 AI 環境。

行員的 AI 能力提升不僅是一個技術問題，更是一個戰略發展問題。成功的 AI 轉型不僅依賴於技術和培訓到位，更需要一個鼓勵創新、支持學習的組織文化，只有當行員能夠熟練運用 AI 技術時，銀行業務才能真正創新。銀行應制定清晰的策略與行動計劃，短期目標可聚焦於提高所有員工的 AI 素養和實施基礎 AI 技能培訓；長期則應著眼於將 AI 技術無縫整合到銀行業務，鼓勵跨部門間的協作、交流與經驗分享，並透過設立技術創新獎勵機制，激勵員工在 AI 應用上的創新和嘗試。

關注 human factor，促進 AI 轉型

儘管 AI 在處理計算和數據分析方面的能力非常強大，但它仍然無法取代許多情感判斷和倫理道德方面的能力，面對複雜和非結構化的問題時，人類的適應性和創新能力仍展現出無可比擬的優勢。

1. 以客戶為中心

銀行在導入 AI 技術的過程中，應當以客戶為中心，以確保這些技術的應用真正符合客戶的需求。例如導入 AI 聊天機器人和語音助理等工具來提供基礎服務，從而增強客戶體驗和服務效率。與此同時，銀行仍應保持真人諮詢服務，以滿足其更專業或個別化的需求。這種策略不僅可以提升客戶滿意度，也有助於銀行在競爭激烈的市場中保持競爭力。

2. 人機協作的轉型策略

銀行應該積極擁抱 AI，卻也不能忽視人類員工的價值，行員應被重新定位為“人機協作”的角色，除了運用 AI 工具完成重複性任務，同時也利用自身的專業知識和人際交往能力，為客戶提供高層次的服務，例如理專可以利用 AI 生成的數據洞察，向客戶提供更加精

準的理財建議。

3. 技能提升與轉型培訓

銀行應為員工提供全面的技能提升和轉型培訓計劃，使其能夠適應數位時代的需求，包括資料分析、程式設計、創新思維等內容，幫助員工掌握新的工作技能。此外，銀行應該鼓勵員工探索新的職業道路，例如資料科學、數位行銷和新產品開發等。

4. 加強文化與心理支持

銀行需要培育一種能夠包容 AI 轉型的企業文化，並提供心理支持，同時管理層應該公開承諾重視員工的價值，並制定政策保證員工的職位安全，建立開放的溝通渠道來降低其對未來的不確定感。



KPMG 安侯建業
賴偉晏數位長

對於面對客戶的前台工作，我認為仍需保留一定的人工溫度，特別是服務於高端客群的業務，這些仍需要人來協助完成。即使在數據分析和自動化盛行的今日，針對特定客戶群的客製化服務依然十分關鍵，這是 AI 無法完全替代的。另外，在程式設計、數據分析等技術性工作中，雖然 AI 能夠執行這些任務，但仍需要人類負責指揮 AI 執行指令和解讀數據以供決策參考。科技應作為一個 enabler，讓每項職務重新思考轉型的背後如何提升自身價值，例如，財務與人力資源等部門不應僅限於執行傳統職責，而應更積極投入數據分析和價值創造，透過 AI 優化工作流程，開拓新的工作方式。



台灣金融研訓院

TAIWAN ACADEMY OF BANKING AND FINANCE

院本部

10088 台北市中正區羅斯福路三段 62 號
NO.62, Sec. 3, Roosevelt Rd.,
Zhongzheng Dist.,
Taipei 10088, Taiwan
TEL. (02)3365-3666
FAX. (02)2363-8968

芬恩特創新聚落

10066 台北市中正區南海路 3 號 4 樓
4F, No. 3, Nanhai Rd.,
Zhongzheng Dist.,
Taipei 10066, Taiwan
TEL. (02)2393-2810
FAX. (02)2393-2866

中部服務中心

40446 台中市北區錦平街
40 號 3 樓 H316 室
3F.-H316, NO. 40, Jinping St., North Dist.,
Taichung City 40446, Taiwan
TEL. (04)2225-6171
FAX. (04)2225-6191

南部服務中心

80147 高雄市前金區中正四路
230 號 3、5 樓
3F., No.230, Zhongzheng 4th Rd.,
Qianjin Dist., Kaohsiung City 80147, Taiwan
TEL. (07)211-2928
FAX. (07)215-8580