

高峰對談 #人才轉型 #數位勞動力

當 AI 成為企業新同事：數位勞動力與治理新秩序

主持人 施君蘭 Lana Shih／陳冠學 Quincy Chen・劉浩翔 Jeremy Liu・李倩 Maggie Lee・王儷玲 Jennifer Wang

11:35-12:15 有效內容 50.2 分鐘 逐字稿 16,623 字

/ 一、Quincy：不做漸進式，直接建一個與 AI 合作的團隊

面對「如何讓 AI 能力真正滲透進龐大的金融組織」，國泰世華選擇的不是漸進調整：

- 直接 build 一個與 AI 一起合作的 Team，規模約原 Scrum Team 的 **三分之一**
- **不做實驗室專案**——接的是其他 Scrum Team 同樣會接的真實需求
- 用「拓荒者」快速撞到能力天花板，再從成功經驗做快速輸出

「與其讓大家漸進式地調整，我們要直接去 Build 一個跟 AI 一起合作的 Team。」

目前已有成功範例並進入**擴大輸出期**，最近上線的部分 Cube App 功能已是由這個 AI Scrum Team 產出。

撞到天花板之後的真正瓶頸

「我有一段高速公路可以開到 200、300 都沒問題的時候，你馬上就知道哪個地方會塞車。」

塞車點依序是：1. **數位化根本不完整**——很多人說要 AI 做這些事，「你連數位化都沒做到，你連 API 都沒有」
2. **知識 Silo**——即便企業體內有知識，仍散落各處，必須全部打通 3. **80 分等於零**——「很多東西你做 80 分就會 Zero Adoption，你要做到 100 分 Adoption 才會起來。因為他會說，如果這東西只能幫我完成 50% 的工作，那我不如全部自己來。」 4. **組織與角色的重新定義**——工具都有了但人不願跨出去，「主力可能是在心態，還不見得是在 skill」

引用 Oliver Jay 的關鍵提問

「大部分人用 AI 的時候只想到前半句 *Is AI completing work?*，但真正的重點在 **matters**。我不是要 create 一大堆 Agent 去做那些 work that doesn't matter。」

/ 二、Maggie（微軟）：從 AI 助手到 Workflow，再到 Enterprise IQ

導入路徑

金融業起手多半是先給員工 AI 助手（Copilot）——撰寫文件、整理 email、RM 出門前快速備妥資料。看似簡單，但這是建立「員工該怎麼使用 AI」的最佳起點。

下一步是把 AI 放進 **workflow**：「在金融業通常不會有一個工作是由單一個人完成的，它要跨組織、跨系統、跨角色。」

兩個國際案例

- **AD Financial (美國)**：客服接線後的大量手打整理工作交給 AI，人類專注處理客戶敏感問題與同理回應
- **Rabobank (荷蘭)**：用 Copilot Studio 建 Customer Self Service Agent，**同時支援文字與語音**；能辨識客戶來電意圖，**能回答就回答，不能回答也不會胡思亂想**，而是導引到正確單位；信用卡掛失、重發等較複雜工作也能完成

企業的兩個能力缺口

1. **人的缺口**——不是不會用 AI 工具，而是「不知道**什麼流程**該用 AI、什麼叫 matterful、什麼產出必須 double verify」
2. **Intelligence Layer 缺口**——AI 模型負責推理，但它不知道你公司的核保規則、從屬關係、客戶過去 claim 過什麼。要在 Microsoft IQ 之上建立你自己的 **Enterprise IQ**

最鮮明的一句話

「大家不是在 **deploy** 一個 agent，你是在 **onboarding** 一個 agent。」員工走進公司你會給他識別證，你的數位員工也要有。你給他什麼 access control、什麼 data protection、怎麼 monitor 他看過哪些資料——**要像管理真實員工一樣管理數位員工**。而且要在 build 之前就想，不是 build 完才想。

對 PM 與主管的提醒

- PM 過去擅長設計系統與 workflow，未來要跨 Business User／IT／法遵去判斷：哪些題目交給 AI、哪些要人來 escalation、哪些要人做最後判讀
- 主管更辛苦——過去只管真實員工，未來要管數位員工，成為 **Hybrid Workplace**；對真實員工訂 KPI，對數位員工也要訂
- 治理建議：**中央設定標準，但由部門設計場景**

/ 三、王儷玲（政大）：金融大語言模型與評測標準

為什麼需要金融專屬模型

金融業大量知識庫跨公司甚至跨產業不能分享，又有法規限制，因此由產業聯盟主導**金融代言模型**，目前正在為 **20 家銀行** 打造銀行大語言模型。

訓練與評測方法

- **不是 RAG 的 open book 往外找答案**，而是先讓模型讀完該讀的知識庫，再測驗是否真的讀懂
- 重視**邏輯思考能力**：「我們讓 AI 去上大學讀理論基礎、讀 paper，最後考的**不是是非題選擇題，而是申論題**」
- 在訓練前先把每一題的解題思維鏈寫出來，讀完豐富知識庫後再考

- 規模：4,500 題的評測
- 四大 Domain：金融知識、法規合規、授信、財富管理（未來延伸至保險、投資）
- 必須是繁體中文版——外商已開發的 AI 能不能在台灣用，涉及台灣法規與消費者情境的差異，評測是關鍵門檻

三重安全部署的評分設計

- 總分之下再分項（法遵、消費者權益、金額大小等）並給予不同權重
- zero tolerance 項目：只要錯一題就必須重新回去訓練

AI 治理框架

呼應上午 Demo 提出的五要素：身份、職權、權限、主管、工作紀錄——這些在真人世界本來就有，AI 治理只是 attach 到數位員工身上。

關鍵設計判斷：

「Human in the loop 不是每一個點都要，而是放在一個不可逆的點，或是那個點本身會對消費者保護、風險產生重大影響的地方。」

法遵風控不能最後才出現，必須在設計 end-to-end domain 的邏輯思考階段就放進工作流程。

數位員工的 KPI 三個 Domain

1. 風險（守門員）——在 human in the loop 的斷點擋掉風險
2. 價值創造——金融業需要有溫度的加值
3. 優化——end-to-end 流程與效率的整體提升

引述 McKinsey：用 AI Agent 時 use case 不是最重要的，重要的是怎麼創造那個例外的管理機制。

工作底稿與紀錄「就像飛機的黑盒子」，用來回饋成正向循環；把人的經驗用思維鏈的方式寫清楚，放回 Agent 的工作流程，才是經驗傳承。

/ 四、Jeremy：實作踩過的坑

設計階段一定要先想好的三件事

1. 獨立身份——要能識別這個行動是人做的還是 Agent 做的。（特別強調：數位同事的責任最後還是人類負責，不能什麼事都推給 Agent）
2. 能力邊界——依職責與任務明確畫出可操作範圍，並用統一的 Gateway 管理可存取權限
3. 可視化軌跡——「總不可能 Vanessa 昨天晚上默默在後台做了什麼你不知道，這其實是蠻危險的一件事情。」

運行階段最常踩的兩個雷

雷一：記憶汙染（Memory Pollution）

記憶儲存必須有非常精密的設計——什麼時候該記、該記什麼、記下來怎麼分門別類儲存。否則「他記了太多事情之後，反而把自己所有的記憶全部汙染了，到最後產出不好的效果」。

雷二：Over-skill

公司 skill 越來越多時會有重複。「有些時候他身上背了太多 skill，他會不知道自己到底要做什麼，**他會做一大堆你感覺起來很忙、但事實上是在繞圈圈的事情。**」

/ 五、一句話結語

與談人 結語

Maggie 不要等到所有事情都有完美答案才開始；但也不要再在流程邊界還不清楚時貿然冒進。找**高價值、低風險**且能讓 Agent work 的部分，並重視 continued learning loop

Jeremy 先畫好安全邊界，然後**選一條垂直應用的賽道直接實操實作**，在實作中自然學會如何在企業環境做好 Agent Adoption

Quincy AI 要上車，但不要為了 AI 而 AI。**問價值至少要問五層**——對你的 Team、對股東、對客戶各有什麼價值？「你如果只能說做了 AI 以後茶水間可以多聊天、看盤時間可以多一點，那只是第一層價值。」

王儷玲 勇敢嘗試，但**評測控管標準要先做好**，再逐步擴大許可權與最佳化流程。已進入**雙重 Agent (teamwork)** 階段，AI 員工之間可互相 call each other，希望五年內實現

/ 可行動要點

- 「**onboarding 而非 deploy**」應作為所有 Agent 專案的預設心智模型，且治理要在 build 之前設計
- **Human in the loop 放在不可逆的點**——這是可直接寫進設計規範的判準，避免每步都卡人工審核
- 記憶汙染與 over-skill 是兩個已被驗證的失敗模式，設計 Agent 時應列入檢查項
- Quincy 的「價值問五層」可作為 AI 專案立案時的過濾器

2026 國泰金控技術年會，會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。