

專題演講 #IT現代化 #集團布局

AI in IT：驅動國泰集團 IT 全面升級的策略與布局

國泰金控數發中心雲端策略發展部協理 | 顏勝豪 Otto Yen

13:50-14:10 有效內容 24.0 分鐘 逐字稿 6,707 字

/ 開場：一支「失控的 Agent」悔過書影片

Otto 以同仁 Terry 製作的影片開場——Terry 在使用 Agent 時創造出一個失控的 Agent，主管要他寫悔過書，他很有創意地做成影片。事件發生在雲端 LAB 環境，雲端本來就適合建立隔離環境，所以雖然失控但未造成重大危害。

「Terry 這個影片做得很好，可是下次不要再這樣做了。」

影片中的關鍵論述（也是全場的治理基調）：

- AI knows common answers. **It does not know your company.**
- It learned recurring patterns, the average cases it had seen. **Your private context is not part of that average.**
- **So the control point must come before the action.**
- Give it only the permission this task needs. Test somewhere that cannot hurt the real project. Review exactly what it plans to change. For an irreversible action, a human presses the button.
- **Never let a reasonable guess become an irreversible action.**

/ 一、技術路線的三個取捨

1. **算力用雲端**——不在第一天就蓋 GPU 機房，因為當時對自己的需求還不確定
2. **模型以三大開源模型為主**——底層算力層與模型不是 focus 重點
3. **專注應用層與交互層**——Agent 的使用與互動介面

交互層的觀察：IT 人員習慣對話框、CLI、IDE；但一般使用者不太可能透過 CLI 或 IDE 與 AI 互動——這正是強調安全與安全應用重要性的原因。

/ 二、Agent 的定義：Model + Harness

引用軟工大師 Martin Fowler（提出重構、Code Smell 的那位）網站上的定義：

AI Agent = Model + Harness

- **Model 是 stateless**——本身不記錄任何狀態
- **所有狀態操作都在 Harness**——harness 負責 handle state
- **所有控制手段、讓它更聰明的機制、護欄，講的其實都是 harness**

Otto 以今年初爆紅的 Agent 工具為例：**大家覺得它好用，其實是它的 Harness 做得很好**——像真人、能記錄東西、能使用工具、甚至能操控電腦。

個人級 Harness（Codex、Claude Code）vs **企業級 Harness**（Google／AWS／Azure 平台）：架構同樣是 Model + Harness，**差別在控制機制、治理能力與處理規模，完全是不同量級。**

企業級 Agent 依賴的既有 IT 核心能力

驗證授權、知識庫、API Gateway、工作流、CI/CD、觀測性、Security、Audit、SDLC 設計。

「這些東西其實你本來就應該做好。**如果沒有做好，即便有這樣的平台還是沒有用。**」

/ 三、上雲的意外紅利

- **2021 年啟動集團上雲計畫**
- **今年 4 月成果展達成「5 年 100 套系統上雲」，現已超過 150 套**
- 最終階段是 **Cloud First**：未來所有新系統開發建置以上雲為優先

關鍵觀察：

「發展上雲的時候並沒有想到今天 AI 發展的狀況。可是走到今年我們覺得，**我們本來以為整個上雲是為了系統現代化做準備，實際上它同時也是在為 AI 的發展做準備。**」

因為 AI 需要大量數據作為燃料，而雲端是很好的承載環境。

/ 四、AI & IT 藍圖

兩大核心

- **開發**：軟體工程、IT 知識管理
- **運維**：IT 的 AI 應用、治理維運（今年看到很多雲端資安事件，AI 在這塊可做不少貢獻）

下含 17 個子領域。

三階段，且總期間控制在兩年以內

「因為 AI 的發展速度太快，**你的計畫如果拉太長期它沒有意義。**」

階段	內容
一	100 天 pilot——模型都在雲端上，啟動實驗專案很快
二	找到好案例做 scale；同時設計 AI Budget 概念
三	AI Scale，把好案例擴散到全集團

AI Budget 的設計動機：AI 工具太多，很難約束同仁「只能用 A 不能用 B」。因此改為**給每位 IT 人員一個可使用的 AI 額度，在符合預算控制的前提下自己組合工具。**

/ 五、AI SDLC：用工程的確定性消弭 AI 的不確定性

這是全場最核心的一句話。Otto 對「幻覺」的定義極為犀利：

「AI 給我們的答案我們覺得很酷，我們會說它是**湧現**；如果它回的答案我們覺得怪怪的，我們會覺得它是**幻覺**。**所以湧現跟幻覺其實是在做一樣的事情**，只是我們最後得到的那個答案是不是符合我們的需求。可是**IT 在用 AI 的時候不應該出現這麼多幻覺，因為我們還是以工程的手段在做整個流程。**」

三個發展重點：測試流程並形成工具與方法論 → 培養懂這些工程手段的人才與團隊 → 最終建一個 **IDP 平台**，讓開發與工具使用統一在單一平台操作。

/ 六、AI Squad Team：6 + 1

項目	設計
團隊規模	原本 12 人 → 壓縮到 6 人
配備	足夠的 AI 工具、一台獨立電腦、獨立帳號、個人化 agent
「+1」	就是 AI Agent
組成彈性	PM/UI/UX/RD/QA 各要幾人由團隊自己決定
佈署	銀行 4 個團隊（數銀 2、資訊板塊 2）

Otto 的一段自嘲：

「我一直提到我要設計一個 **6+1** 的團隊。可是我在跟 AI 的對話過程中，**他一直問我為什麼加 1 不是 1+6**——他覺得應該是由 AI 去帶領 6 個人去開發。然後我就覺得還蠻不錯的思考，我以後可以想一下。」

四個驗證目標（前兩項已達成不錯效果）

1. 交付量放大——「都已經給 AI 工具了，你不可能說開發速度跟以前一樣」 ✓
2. 協作路徑縮短 ✓
3. 每個角色做的事情可 Agent 化

4. 測試出的流程能變成企業可複製的能力

AI member 實際承擔的工作

會議記錄、程式碼監控、產生日報週報、需求整理、ticket 阻塞分析。

/ 七、SDLC 流程本身的重構

傳統 SDLC 的問題：一關一關走（BU 提需求 → UI/UX → SA/DE → Coding → QA → 上線），只要有一關卡住，下一關就進入 Waiting 狀態，也沒辦法提前做。

新的分類方式：把團隊角色重新分成兩種人——

- **Design Owner**：決定要做什麼、做功能設計
- **Deliver Owner**：負責交付與最終品質

最關鍵的變化：BU 團隊寫出 PRD/BRD 之後，就能直接產出會動的 HTML Prototype。有了會動的網頁，後續需求確認與開發的需求確定性大幅提高。

人機投入的微笑曲線：整個 SDLC 中，前段與後段人的投入較高，中段（開發、測試）AI 可承擔較多——這與過去整條線都要人力投入差異極大。

/ 八、明年的規劃

- **集團 SDD Hackathon**：因為集團內用 SDD 開發方法的團隊太多（有用 BMAD、有用 SpecKit、也有不走框架的），希望透過活動交流。三種場景：既有系統重構、開發新系統、既有系統新需求。會找三位外部評審
- **AI Apps（運維）是明年重點**：先建立 **AI Ready Data**（呼應 Harry 的論述），再讓運維達到更智能的境界。基礎是 INFRA 事實、可觀測性、Log，以及運維同仁累積的 SOP、Runbook、故障文件

/ 九、結語：AI 是放大器

引自 AI Con 的一句話，Otto 認為說得極好：

「AI 是一個放大器，它放大的是已經存在的東西。如果你的團隊本來就很混亂很散漫，加 AI 只是增加了這些混亂跟焦慮。你本來的開發工程體系、流程就沒做好的話，加入 AI 只會讓 AI 產生更多的技術債。所以最終還是要把底層的工具、方法、工程事件的方法做好，在這樣的情況下導入 AI 才能發揮更大的效果。」

/ 可行動要點

- **Model + Harness** 是理解 Agent 產品差異的最佳框架——評估工具時該問的是 harness 的治理能力，而非模型
- **AI 計畫期間控制在兩年以內**，是應對技術變化速度的具體管理決策
- **AI Budget**（給額度而非指定工具）解決了「工具太多無法約束」的實務問題

- **Design Owner / Deliver Owner** 的角色重分類，是把 AI 導入 SDLC 的關鍵前置動作，比導入工具本身更重要
- 「AI 是放大器」可作為評估任何團隊是否該導入 AI 的第一道檢查

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。