

Digital Transformation & AI Advisory · 事務所數位轉型與實務應用

AI × 事務所工作應用

從文件理解、知識管理到 Workflow / Agent

From Document Intelligence & Knowledge Management to Enterprise Workflows & Autonomous Agents

Crowe × Force Cheng · 2026 / 09

◆ 核心戰略：人 × AI × 系統之企業級工作分工重新設計



AI 在事務所工作的真正定位

超越日常對話問答 · 深度融入事務所全流程作業鏈
Strategic Positioning: Integrating AI into Core Firm Operations

核心戰略與操作要點

- 文件解析：讀取非結構化文稿與合約憑證
- 資料整理：跨來源資訊擷取、清洗與結構化
- 勾稽比對：跨文件一致性核對與異常提示
- 知識查詢：封閉來源問答與法規判例檢索
- 文件撰寫：商務信函、SOP、管理摘要草擬
- 數據分析：資料字典建立、變動原因解釋
- 任務協作：會議共識提煉與待辦追蹤
- 工作流與 Agent：自主調用工具執行任務
- 管理決策：BI 深度診斷與前瞻決策支援

✕ 傳統迷思盲點

- 試圖將所有複雜工作全部交給 AI 自動化
- 忽略法律責任與法規底線
- 遇到幻覺即全盤否決技術

✓ 現代典範分工

- 系統：計算、留痕、防呆
- AI：多模態理解、草擬初稿
- 人：價值裁量、法定義務承擔
三方各司其職構建無瑕防線

事務所全流程 9 大深度落地維度

01 文件解析

OCR

合約、掃描傳票
非結構化資訊萃取

02 資料整理

ETL

跨來源資訊清理
自動結構化入庫

03 勾稽比對

CHK

跨文件一致性核對
自動揭露異常提示

04 知識查詢

RAG

封閉底稿即時問答
精確法規判例檢索

05 文件撰寫

DOC

商務信函、SOP
管理摘要高仿草擬

06 數據分析

DAT

資料字典建立
重大變動原因解釋

07 任務協作

COP

會議共識智慧提煉
跨組待辦自動追蹤

08 工作流 Agent

AGT

自主調用多工具
跨系統多步自動化

09 管理決策

DEC

BI 深度前瞻診斷
決策情境模擬推演

✦ 核心思維：不是全部交給 AI，而是重新定義「人 × AI × 系統」的分工邊界

三方分工：AI、程式與人的能力邊界

精準辨析擅長特質 · 構建無可替代的黃金協同三角

Division of Capabilities: Semantic AI, Deterministic Systems, and Humans

✦ 核心戰略與操作要點



✦ 責任防線：AI 賦能流程，系統確保精確留痕，專業人員承擔法定簽核責任

事務所 AI 落地應用的十大核心面向

由底層文件解析至頂層管理決策的全景矩陣藍圖

Ten Strategic Application Dimensions for Professional Practice

核心戰略與操作要點

一、核心查核與專業作業層 (01 - 05)

- 01

文件理解與資料整理
發票、報單、水單非結構化欄位萃取與對齊
- 02

比對、抽憑與盤點
帳載與憑證勾稽、清冊與現場影像多模態比對
- 03

知識管理與資料問答
封閉來源問答、歷史案例沉澱、準則法規即時檢索
- 04

文件生成與翻譯
單一事實源衍生通知函、英文報告、SOP、會議摘要
- 05

Workflow / Agent 串接
結合外部 API 與資料庫，自主調用工具執行多步流程

二、行政協作與決策治理層 (06 - 10)

- 06

一般行政流程自動化
Email 智慧分流、差旅報支初審、會議排程與催辦
- 07

文件撰寫與修訂檢核
跨章節數據勾稽、術語一致性、雙語對照排版防呆
- 08

結構化數據分析
自動建立資料字典、缺失值探勘、變動趨勢圖表敘事
- 09

簡報與溝通視覺化
長篇查核底稿濃縮轉化為合規 16:9 商業母片簡報
- 10

BI 與管理決策支援
從靜態指標儀表板躍升為前瞻決策智慧 (Decision Intel)

循序推進：涵蓋作業層、協作層與治理層，全方位釋故事務所智力資本

文件理解：從「看文件」到「結構化資料」

發票、報單、水單與薪資名冊之自動化擷取鏈

Document Understanding: From Raw Scans to Structured Schemas

✦ 核心戰略與操作要點

- 階段 1 · 多模態 OCR：高解析光學字元與版面定位
- 階段 2 · 關鍵欄位擷取：抽取金額、日期、統編、品項
- 階段 3 · Schema 嚴格對齊：映射至企業標準資料庫欄位
- 階段 4 · 缺漏與邏輯提示：標記欄位不全或稅額不符項
- 階段 5 · 人工作業覆核：關鍵異常確認，完成入庫



✦ 專業準則：AI 可以高效率整理資料，但不應直接取代專業處理判斷

跨文件比對：AI 與程式的最佳工程組合

以程式確保確定性比對 · 以 AI 洞悉語意差異與異常

Cross-Document Reconciliation: Best Practice Architecture

✦ 核心戰略與操作要點

- 程式層 (確定性) : 負責絕對精確的數值計算、主鍵核對與規則篩選
- AI 層 (語意層) : 負責跨版型欄位對齊、縮寫品名模糊匹配與差異原因摘要
- 專業層 (責任層) : 依重大性原則進行專業裁量，決定是否進行查核調整



✦ 最佳分工：程式做確定性比對 · AI 做語意解釋與差異整理 · 人做專業判斷

審計確信：抽憑、盤點與查核輔助

劃清 AI 輔助與會計師法定職責邊界 · 確保底稿確信力

Audit Sampling & Verification: Boundaries of AI and Professional Duty

核心戰略與操作要點

- 查核母體完整性確認 (Completeness Testing)
- 選樣方法論與重大性門檻設定 (Materiality)
- 查核程序妥適性之規劃與執行 (Procedures)
- 審計例外項目之風險裁量與評估 (Exceptions)
- 正式查核報告意見簽署與法定確信 (Audit Opinion)



◆ 確信鐵律：母體完整性、選樣依據、例外判斷與結論，必須由會計師親簽承擔

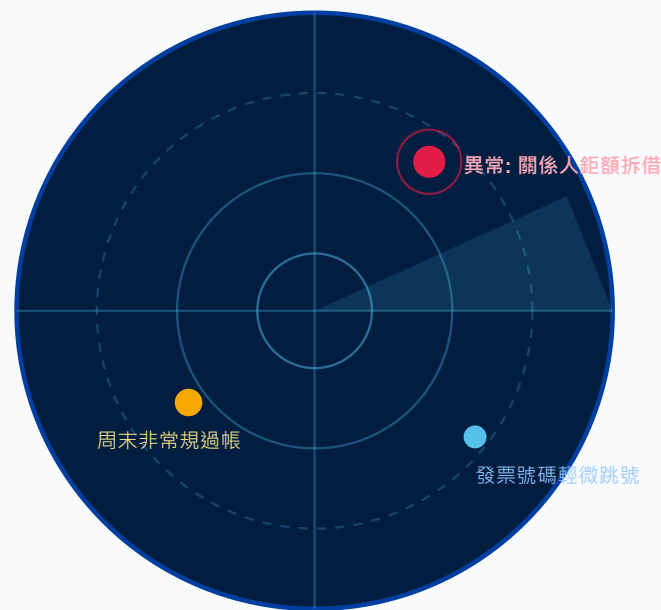
知識管理 (KM)：從沉睡文件庫到可用知識

擺脫單純檔案存儲 · 打造可搜尋、可問答與沉澱之知識中樞

AI Knowledge Management: Transforming Static Files into Dynamic Assets

✦ 核心戰略與操作要點

- Metadata 元數據：標記產業、稅目、生效年份
- Role-based 權限：嚴格區隔一般案件與高機敏案件
- Version 版本溯源：避免引用舊法或過期範本
- Source 來源驗證：僅收錄主管機關與所內核准文件
- 動態更新機制：自動追蹤法規修訂並警示變更
- 人工專業驗證：資深同仁定期驗收知識問答品質



即時異常偵測雷達掃描

1 第一道防禦：硬性規則引擎過濾

- 金額臨界值跳躍 (Benford's Law 班佛法則檢驗)
- 交易對手黑名單與高風險國別比對
- 重複請款、發票重複報支系統級攔截

特徵：100% 確定性 · 零假陰性 · 運算速度極快

2 第二道防禦：AI 語意多模態異常識別

- 模糊會計科目挪移與跨期費用隱匿判斷
- 合約免責附款背後隱藏之重大風險識別
- 跨郵件通訊語調急迫性與舞弊風險關聯分析

特徵：洞察隱蔽風險 · 動態自適應 · 輔助深度抽核

✦ KM 真諦：企業知識管理不只是存文件，而是讓歷史經驗隨時可被問答與複用

來源導向知識工作：RAG 與封閉來源問答

鎖定指定權威出處 · 杜絕模型無邊界幻覺與誤導

Source-Grounded AI: Retrieval-Augmented Generation & NotebookLM

核心戰略與操作要點

- 核心價值：讓 AI 的所有回答嚴格回到指定資料來源
- 杜絕胡說：不在來源文件內的內容，模型必須主動回答「文件中未提及」
- 關鍵認知：有引用出處 ≠ 推論邏輯一定百分之百正確
- 防呆機制：模型可能引用正確句子，但誤解該句在特定法規脈絡下的除外條款
- 同仁角色：專業同仁必須親自點擊引文連結，核實上下文定義



◆ 關鍵風控：讓 AI 的回答回到指定資料來源 · 謹記「有引用 ≠ 推論一定正確」

超越公開法規 · 將實務例外與覆核經驗轉化為組織資產

Capturing Tacit Know-How: From Exceptions to Firm Assets

核心戰略與操作要點

- 1. 錯誤暴露：在實際查核或申報作業中發現疏漏
- 2. 人工修正：資深主管介入指導並完成正確調整
- 3. 案例沉澱：將該筆錯誤與修正過程記錄為案例卡
- 4. 規則提煉：萃取通用性檢核規則 (If-Then 邏輯)
- 5. 存入 KM：將規則與案例納入組織核心知識庫
- 6. AI 參考引用：下一次同仁撰寫文案時由 AI 主動提示防範



核心護城河：真正的 Know-how 不是公開法規 · 而是實務例外與覆核經驗

多向度文件生成：單一事實源的多樣態轉化

以核心事實資料為基準 · 彈性轉化為對內對外專業成果

Multi-Modal Generation: Diverse Deliverables from a Single Source of Truth

✦ 核心戰略與操作要點

- 6. 執行檢核清單：拆解為一線同仁可逐項打勾之 Checklist
- 7. 標準作業程序 (SOP)：將專案流程規範化為教學步驟
- 8. 常見問題集 (FAQ)：預判客戶疑慮並預先準備應對口徑
- 9. 簡報視覺架構：提煉標題與次標，直接套入官方 16:9 母片
- 【不可逾越之鐵律】：可以根據受眾變換風格與措辭，但嚴禁補造或推導不存在的事實



高階簡報 (Executive Slides · 16:9)

提煉標題與精華、自動套入官方母片、字數 < 40 字



標準作業程序 (SOP & Checklist)

拆解為一線同仁逐項打勾之執行清單與檢驗標準



工作底稿與正式報告 (Audit Working Papers)

詳盡長文敘述、附註完整試算平衡與法規條號



客戶常見問答集 (Client FAQ & Guidance)

平易近人白話口吻、預判客戶疑慮並預先提供應對路徑

✦ 生成鐵律：可以重組改寫與變換受眾風格，嚴禁無中生有補造不存在之事實

文件修訂與品質檢核：第一道智慧防線

跨章節日期、數據、術語與雙語語意之一致性排查

Document Review & QA: First-Pass Intelligent Consistency Auditing

核心戰略與操作要點

- 第一道防線 · AI 品質初篩：
 - 毫秒級通讀上百頁長篇文稿
 - 標註所有前後矛盾、錯別字與格式違規
 - 產出結構化之「待核實差異疑義清單」
- 第二道防線 · 專業人員最終核准：
 - 研判差異是否具備實質商業合理性
 - 做出合規修正並簽署專業意見
 - 確保交付成果完美符合事務所聲譽



定位清晰：AI 做高敏感度品質初篩，專業人員做權限內最終簽核確認

Prompt 工程：從臨時指令升級為工作方法

將合夥人專業思考維度沉澱為組織級 Prompt CMS

Prompt Engineering as Methodology: Institutionalizing Best Practices

核心戰略與操作要點

- 階梯 1 · 個人臨時指令：個別同仁在聊天框隨機提問
- 階梯 2 · 標準範本庫 (Templates)：整理常見提問與格式標準
- 階梯 3 · 技能專案包 (Skills)：封裝業務邏輯與參考材料
- 階梯 4 · 組織級 Prompt CMS：統一版本受控、API 分發與審計
- 【核心成果】：將個人的優秀直覺，轉變為整所同仁均能複製使用的組織資產



```
SYSTEM PROMPT TEMPLATE

# ROLE
資深國際審計與稅務執業合夥人

# HARD CONSTRAINTS
1. 僅基於隨附封閉底稿，嚴禁聯網臆測
2. 每項推論必須標註 [Doc_ID$頁碼]
3. 遇到未記載事實，直接回傳 UNKNOWN

# OUTPUT STRUCTURE (Strict JSON)
{ "conclusion": "...", "confidence": 0.95,
  "evidence": ["Doc#1", "Doc#2"],
  "cpa_review_required": true }
```

⚡ Output Validation: Passed

◆ 成熟定義：成熟的 Prompt 即是可複用、可稽核的組織智慧資本 (Prompt CMS)

團隊協作 (CoWork)：結構化會議與跨人工作流

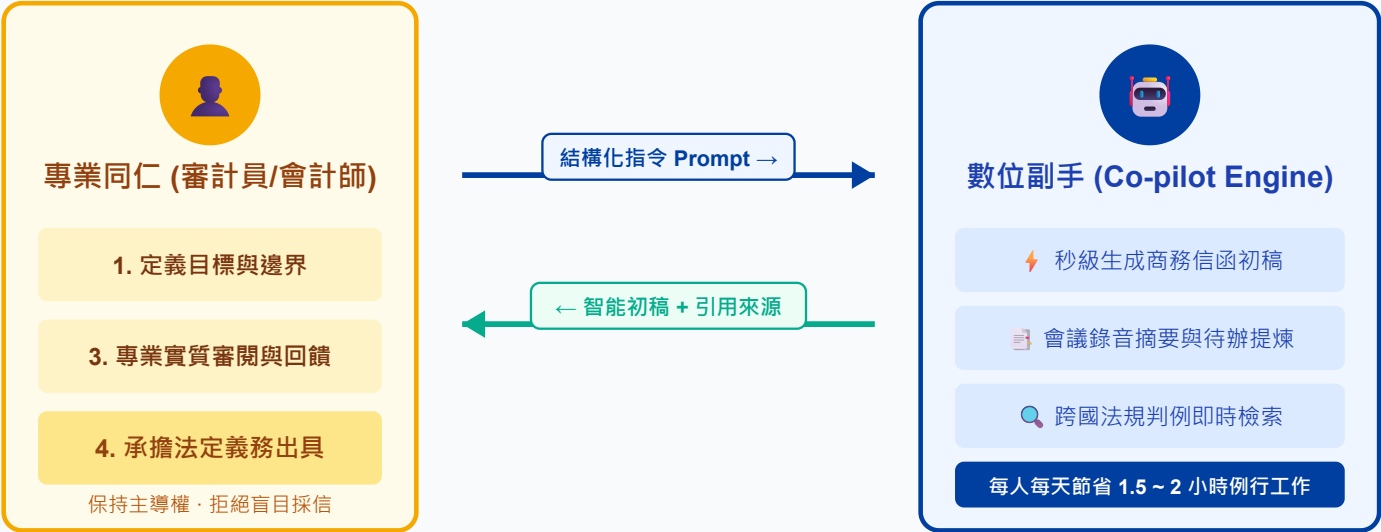
將混亂討論萃取為共識、分歧、待辦與責任分工

Collaborative AI: Transforming Discussions into Sustainable Work Structures

核心戰略與操作要點

- 價值本質：不是讓 AI 替團隊做決定或取代跨部門協商
- 核心賦能：把發散甚至混亂的口頭討論，沉澱為可持續推進的工作結構
- 消除盲區：避免「會而不議、議而不決、決而無人執行」的組織耗損
- 經驗積累：每一次專案討論的精華都成為後續專案的參考底稿

專業同仁 × 數位副手 (Co-pilot) 協同閉環工作流



核心心態：AI 產出永遠只是「第 0.8 版草稿」，最後 0.2 版由同仁專業判斷定稿

◆ 協作真諦：價值不是由 AI 幫團隊決定，而是把討論變成可持續工作的結構

Agent 典範轉移：從回答問題到執行任務

賦予語言模型調用外部工具之手腳與行動能力

Autonomous Agents: Bridging Language Intelligence with Tool Invocation

✦ 核心戰略與操作要點

- 1. 讀取與寫入文件：自動開啟目錄、讀取 PDF、產製報表
- 2. 查詢專有資料：透過 SQL 查詢 ERP、或向量搜尋 KM
- 3. 呼叫系統 API：向銀行系統、稅局入口或 CRM 發送請求
- 4. 建立排程與待辦：將決議直接寫入行事曆與專案看板
- 5. 結構化資料整合：自動完成跨系統資料清洗與同步
- 6. 觸發自動化流程：依條件自主啟動下游簽核與通知

ReAct 自主循環思考行動引擎

1. Plan (目標拆解)

將大任務分解為子步驟

2. Act (工具調用)

呼叫 API / 查詢資料庫

4. Reflect (自我修正)

未達目標則重整計畫

3. Observe (環境觀察)

評估回傳結果與錯誤碼

達成收斂標準 (Stop Condition)

出具完整查核報告底稿並提交會計師簽核

Agent 自主調用工具箱 (Tools)



精確算術求解器 (Calculator)

交由 Python 直譯器計算 · 杜絕 LLM 算術錯誤



ERP / SQL 只讀查詢器

透過自然語言轉 SQL · 安全查詢歷史總帳



法規與判例檢索器 (RAG)

查詢主管機關最新函令與解釋文



簡報 / 報告產生器 (PPTX Engine)

自動將結論填入官方母片完成出具

✦ 質變躍升：Agent 與一般聊天最大的差異，在於 Agent 具備主動調用工具的能力

Agent 治理：自然語言不等於無限制授權

企業級身分識別、最小權限、審計留痕與阻擋機制

Agent Governance: Natural Language Does Not Equal Unlimited Authority

✦ 核心戰略與操作要點

- 【不可妥協之原則】：AI 技術上能做到，不代表在法律與風控上應被授權做到
- 自然語言的模糊性不能成為權限漏洞的藉口
- 外部 LLM 絕不能直接持有高權限資料庫密碼或管理員金鑰
- 所有涉及客戶商業機密之不可逆操作，必須設計斷路器 (Circuit Breaker)

🔒 ENTERPRISE AGENT SANDBOX

1 只讀存取限制 (Read-Only DB)

- 嚴格禁止 Agent 具備資料庫寫入 (DROP/UPDATE) 權限
 - 僅能讀取指定查核年度之沙盒副本
- 防止意外覆寫正式總帳記錄

2 工具白名單 (API Whitelist)

- 僅允許調用經資安小組預先簽核之本機 API
 - 阻斷任何任意代碼執行 (Arbitrary Code Execution)
- 阻絕聯網外洩或惡意腳本注入

3 個資與機密脫敏 (PII Masking)

- 身分證字號、銀行帳號、薪資在進入模型前遮罩
 - 本機正規表達式自動取代為 Token (e.g. [PERSON_1])
- 確保模型零接觸原始機密個資

4 不可篡改留痕 (Audit Log)

- 記錄 Agent 每一步 Thought, Action, Output
 - 包含完整的調用參數與時間戳印 (Timestamp)
- 主管機關抽查隨時可完整重現軌跡

✦ 資安警語：AI 技術上能做到，絕不代表在治理上應被授權做到

雙軌共生：Personal Agent 與 Enterprise APP

無需推倒重來 · 在既有核心系統上層疊加敏捷智慧層

Dual-Track Architecture: Personal Agents over Robust Enterprise Applications

✦ 核心戰略與操作要點

- 權威基準：穩定運行的正式資料庫與財務 ERP 系統
- 權限守門：嚴格執行組織職位劃分與職權分離 (SoD)
- 法定核准：正式簽核流、電子簽章與法律生效節點
- 交易一致：保證資料庫 ACID 一致性，絕不遺失或重複入帳
- Audit Trail：完整留存操作歷史，滿足監管機關外部查核
- 【架構精髓】：無需推翻重造，AI 成為企業系統前面最貼心的智慧界面



✦ 架構思維：無需推翻核心系統，AI 成為既有企業系統前面靈活的智慧層

Multi-Agent 架構：聚焦任務邊界而非盲目堆疊

清晰定義職能、交接協議與人工覆核點 · 嚴防錯誤級聯放大

Multi-Agent Orchestration: Clear Boundaries Over Model Count

核心戰略與操作要點

- 任務邊界明確：每個 Agent 僅專精單一職能，切忌全能包辦
- 資料隔離邊界：各 Agent 僅接觸其職權所需之最小資料塊
- 交接標準契約：Agent 之間的輸出與輸入必須為嚴格 JSON Schema
- 關鍵節點插入：高危判斷節點強制插入人工專業覆核
- 運算成本防範：避免 Agent 陷入無效死循環導致 API 費用暴增
- 【核心警語】：多個 AI 互相背書同意，不等於結論具備法律或審計正確性



◆ 風控警語：多個 AI 互相背書同意，不等於結論具備法律或審計正確性

行政賦能：高重複度與文件密集場景的速效落地

以規則明確之流程為起點 · 快速獲取生產力躍升勝果

Administrative Automation: High-Yield, Low-Risk Productivity Wins

✦ 核心戰略與操作要點

- 文件數量極大：佔據行政同仁大量打字與排版時間
- 高度重複循環：每週、每月均需常態反覆執行相同程序
- 業務規則明確：具有清晰的內部制度或審批作業標準
- 需跨人大量溝通：涉及頻繁催促、確認與格式校正
- 【戰略價值】：行政場景風險低、效果立竿見影，是所建立 AI 信心的最佳突破口



✦ 導入良機：文件多、重複高、規則明確之行政場景，是 AI 落地首選試驗田

數據分析基本功：先理解資料結構，再談 AI

落實資料清洗與結構盤點 · 數值計算一律回歸確定性工具

Data Analytics: Master Data Hygiene Before Applying AI Intelligence

核心戰略與操作要點

- 【絕對鐵律】：LLM 本質是語言預測模型，不是專業計算機
- 算術校驗回歸公式：Excel SUM/VLOOKUP 永遠比 AI 算術精確
- 大數據萃取回歸 SQL：億級資料比對應撰寫標準 SQL 語句
- 複雜演算法回歸程式：Python / R 腳本保證每次執行結果 100% 相同
- 管理視覺化回歸 BI：PowerBI / Tableau 保證指標定義權威統一
- 【整合架構】：AI 負責提供分析思考方向，由確定性工具產出精準數值



底層磐石：沒有資料字典的 AI 分析，只是在流沙上建高樓；有結構定義方能釋放分析價值

✦ 算術原則：數值精確計算一律回歸公式、SQL 與程式，避免 LLM 數值幻覺

管理分析：從冰冷數字穿透至關鍵營運問題

透視工時成本、應收帳齡與 What-if 敏感度分析

Management Insights: Translating Raw Figures into Probing Inquiries

✦ 核心戰略與操作要點

- 1. 看懂深層變化：不只看數字高低，看透結構性轉變趨勢
- 2. 快速揪出異常：在數千個專案中秒級圈出指標偏離常態者
- 3. 提出前瞻追問：引導主管在管理會議中切中要害提問
- 4. 整理可能歸因：從跨部門資料中提取多重潛在關聯因素
- 【統計學重大警示】：相關性不等於因果關係！
- AI 找到數據關聯，不代表 A 必然導致 B，管理決策仍需實務驗證



✦ 統計警語：AI 協助主管看懂變化並提出追問，但相關性絕不等於因果關係

決策智慧：傳統 BI 結合 AI 的深度演進

由被動回顧「發生何事」躍升為主動提示「原因與下一步」

BI + AI: Evolution from Static Dashboards to Decision Intelligence

核心戰略與操作要點

- 深度剖析「為什麼可能發生此類異常」(Diagnostic)
- 主動標記「全所目前哪些專案最值得合夥人優先關注」
- 明確指出「哪些潛在財務或法律風控問題需要深入追查」
- 前瞻預警「下一步管理階層應該提出什麼問題與應對決策」
- 【演進目標】：從 Dashboard 走向 Decision Intelligence · 讓數據真正指導管理



演進方向：從 Dashboard 走向 Decision Intelligence · 賦予管理層前瞻決策力

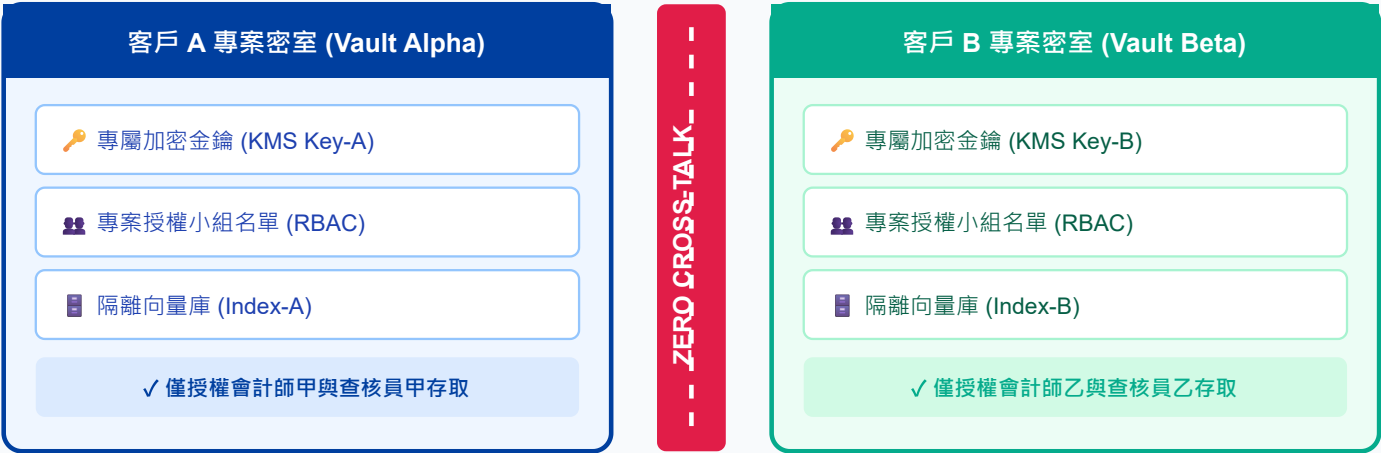
合規安全底線 · 依職責動態隔離敏感數據與商業機密

Data Access Governance: Multi-Tenant Role-Based Data Isolation

核心戰略與操作要點

- 【資安第一鐵律】：權限隔離必須由後端與資料庫底層強制執行
- 絕不能在 Prompt 裡面叮嚀模型「請不要告訴他別人的薪資」
- 在資料進入 AI 之前，檢索層 (RAG) 必須先依據 User Token 過濾權限
- 只有當前使用者具備讀取權限的資料區塊，才被允許納入 Context
- 建立全生命週期身分審計日誌，防止任何 Prompt 注入 (Injection) 竊密

多租戶與專案級別密室資料隔離 (Project Vault Isolation)



企業級合約承諾：Zero Data Retention (零資料留存訓練)

所有 API 呼叫均簽署 BAA/Enterprise 協議，客戶資料絕不用於 Google/OpenAI 公共模型二次訓練

資安鐵律：資料權限必須由後端與底層資料庫硬性執行，絕不能只靠 Prompt 保密

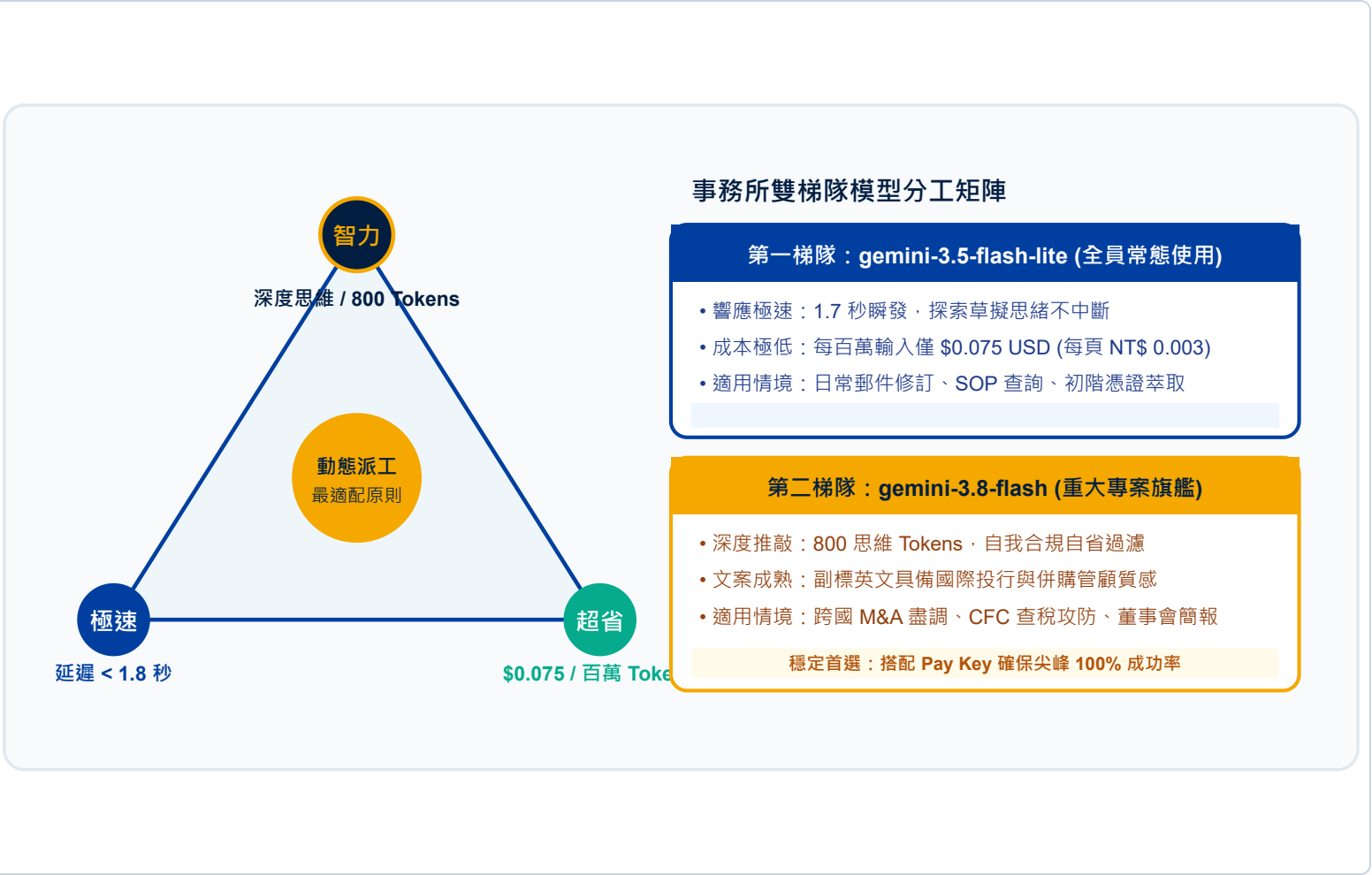
模型選型迷思：不能只看基準排行榜 (Leaderboard)

全面權衡準確率、人工修正量、總持有成本與資安政策

Model Selection: Beyond Leaderboard Hype to Total Cost of Ownership

核心戰略與操作要點

- 排行榜上的第一名，往往也是價格最高、延遲最長、伺服器最容易 503 當機的模式
- 企業導入不能被公關宣傳牽著走，必須回歸總體擁有成本 (TCO)
- 【核心計算公式】：
- 可用成果總成本 = API 成本 + (人工修正工時 × 同仁時薪) + 延遲等待機會成本
- 若 3.5 Flash 加上 2 分鐘人工微調就能達到合夥人標準，它在商業上就遠勝昂貴的旗艦模型



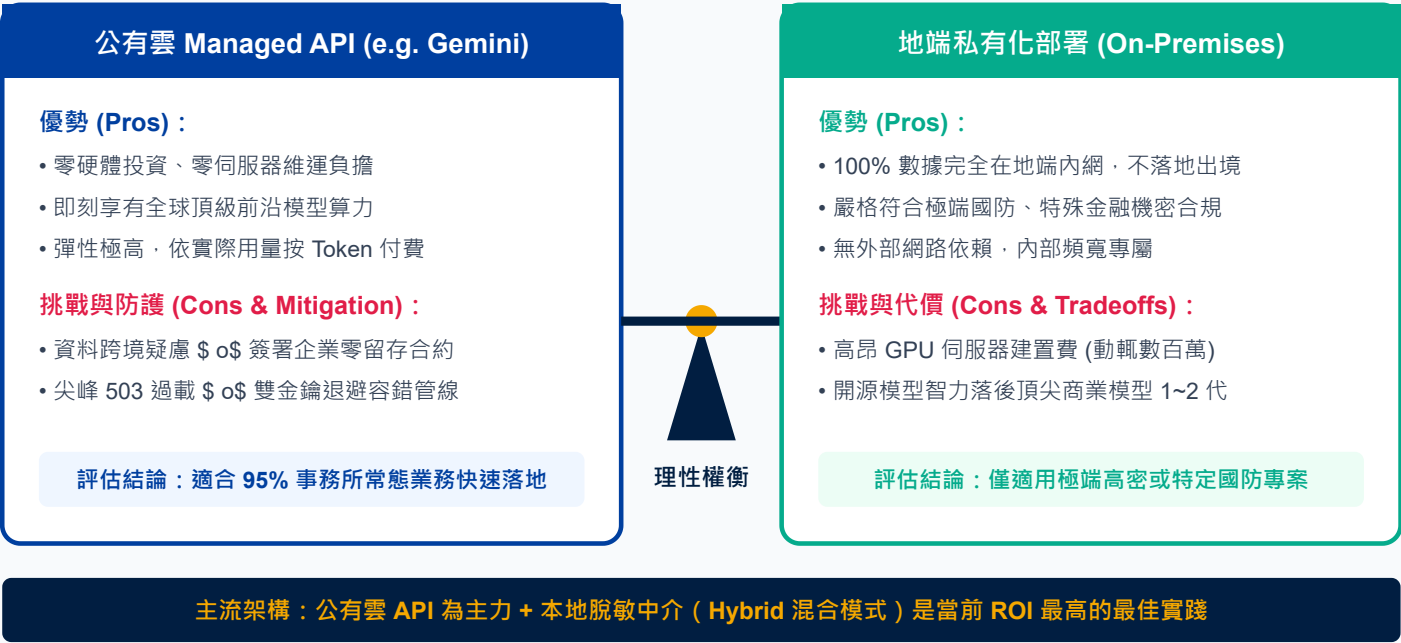
◆ 衡量標準：真正要比較的是每一個可用合格成果的綜合總持有成本 (TCO)

架構部署抉擇：Cloud、Local 與 API 之權衡模型

依據機敏要求、任務頻率與整合深度量體裁衣

Deployment Topology: Balancing Cloud, Local, and Dedicated APIs

✦ 核心戰略與操作要點



✦ 架構決策：沒有單一完美答案，選擇應回歸「風險 × 成本 × 業務情境」最佳解

韌性架構：AI 服務中斷與異常容錯機制

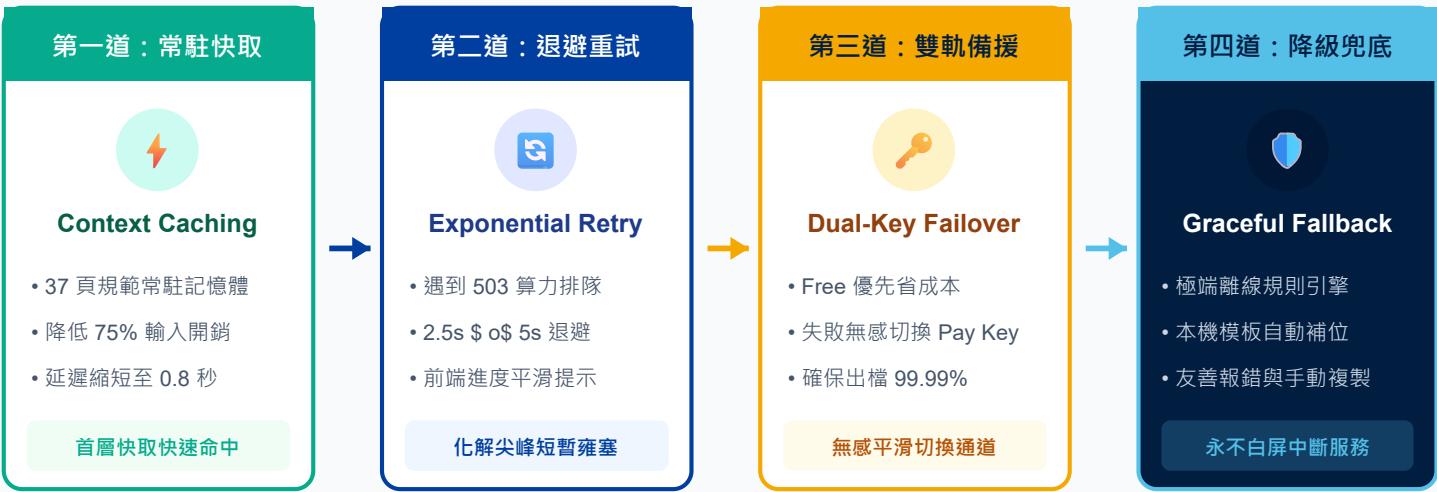
預先設計 API 故障、超額限流、排隊重試與人工備援

System Resilience: Graceful Degradation & Failover Engineering

核心戰略與操作要點

- 1. 指數退避重試 (Exponential Backoff)：2.5 秒自動重發
- 2. 金鑰與模型平滑容錯 (Failover Pool)：Free 斷網自動切換 Pay，3.8 壅塞自動降級至 3.5 Flash
- 3. 非同步作業排隊機制 (Async Message Queue)：將耗時任務放入背景佇列，避免瀏覽器卡死
- 4. 人工無縫接手 (Manual Fallback)：當 AI 完全不可用時，提供標準傳統表單供同仁手動完成作業
- 【不變信條】：AI 服務中斷時，事務所的核心業務絕不能跟著停擺！

四道防禦縱深管線 (Resilience Pipeline Architecture)



工程心法：把 AI 的不可預測性包覆在防禦性軟體管線中，賦予系統企業級的高可靠度

◆ 業務連續性：當 AI 服務不可靠或中斷時，事務所的核心業務絕不能停擺

人機迴路 (HITL)：專業把關的工程化落實

超越「最後放確認按鈕」· 建立阻擋條件、校正反饋與閉環

Human-in-the-Loop (HITL): Systematic Engineering of Human Oversight

核心戰略與操作要點

- 1. 哪一步人一定要看？(確信重要性門檻節點)
- 2. 人具體看什麼？(關鍵數據勾稽與實質商業合理性)
- 3. 什麼情況必須阻擋？(借貸不平、未經核准之關係人交易)
- 4. 誰擁有核准權限？(經理級、合夥人級之法定權限)
- 5. AI 判斷錯了怎麼修？(直覺的單元格修訂介面)
- 6. 修正是否回到 KM？(錯誤案例自動反哺入庫)
- 7. 是否留下完整軌跡？(記錄誰在何時確認了何項數據)



◆ HITL 真諦：不是形式按鈕，而是清晰定義阻擋條件、責任人與修正回流閉環

多維價值主張：AI 的深層效益超越單純工時節省

效率、品質、知識傳承、跨界協作與合規治理之五維躍升

Multi-Dimensional Value: Efficiency, Quality, Knowledge, Teamwork & Governance

✦ 核心戰略與操作要點

- 4. 協作賦能 (Collaboration) :
 - 讓不同專業背景同仁能快速理解彼此工作語境
 - 讓剛入職之新進同仁迅速共享事務所頂級智力能力
- 5. 合規與治理 (Governance) :
 - 保持嚴密的資料權限劃分與法律責任追溯性
 - 建立符合主管機關與國際網絡標準的審計軌跡
- 【結論】：只追求省時間是狹隘的，AI 是事務所全面升級的催化劑

1 效率倍增與工時節流 (Cost & T 節省工時

- 枯燥例行作業工時降低 60% ~ 80%
- 忙季審計底稿產出速度提升 3 倍以上
- 大幅減緩初階審計員超時加班與人員離職率

2 開拓高階諮詢新開源 (New Rev 開源獲利

- 從傳統記帳查核，升級為企業 AI 稅務諮詢
- 跨國併購 FDD / QoE 報告深度與收費顯著提升
- 開發專屬企業內部轉型輔導高附加價值業務

3 查核品質與一致性保證 (Quality 品質磐石

- 排除疲勞帶來之低級加總與登打錯誤
- 全所數百位同仁輸出之簡報與報告規格統一
- 專業術語、色票與字型 100% 官方標準合規

4 法規遵從與風險規避 (Risk Co 風險防線

- 100% 全母體交易過濾，大幅降低漏查重大不實
- 完整留痕系統，面對主管機關評鑑從容應對
- 杜絕同仁私用未授權工具導致客戶機密外洩

✦ 價值格局：導入 AI 追求效率，更要追求降低疏漏、傳承經驗與守護合規

智財防護：數位時代真正值得保護的專業核心

一般流程極易被重構 · 裁量邏輯、風險參數與案例庫才是核心資產

Defensible Know-How: Protecting What Truly Matters in the AI Era

核心戰略與操作要點

- 1. 涉及商業機密的客戶私密營運與財務資料
- 2. 面對法規灰色地帶之特有專業裁量與平衡邏輯
- 3. 歷經數十年審查實戰驗證之量化風險控制參數
- 4. 事務所專屬、經過監管考驗之高品質工作手冊
- 5. 歷年遭遇重大查稅或訴訟案件之完整應對底稿
- 6. 資深 Reviewer 合夥人的直覺經驗與批閱紀錄
- 7. 與稅捐稽徵機關溝通之實務例外處理默契規則
- 8. 事務所獨門之企業併購與評價諮詢方法論

事務所無形數位資產護城河架構

外層護城河：私有底稿與專案經驗池 (Private Project Vault)

客戶不可替代之專屬底稿庫與長期合作累積數據

中層城牆：專業 Prompt 工程與業務邏輯規則庫 (Proprietary Prompts & Logic)

經資深合夥人覆核反覆調校之 System Prompts 與查核防呆檢核規範



核心城堡：Crowe 官方品牌聲譽與客戶信賴 (Brand & Trust)

合約防護 · 數位資產不可搬移 · 形成對競業之巨大護城河

同仁流動帶不走的機構智慧資產 (Institutional Capital)

結論：模型會商品化 (Commoditized) · 但沉澱在事務所內的私有資料與 Prompt 規則永不貶值

✦ 思維升級：保密思維應從「流程不能講」，升級為「深耕真正的競爭優勢知識」

漸進導入路徑：從低風險場景啟動快速驗證 (POC)

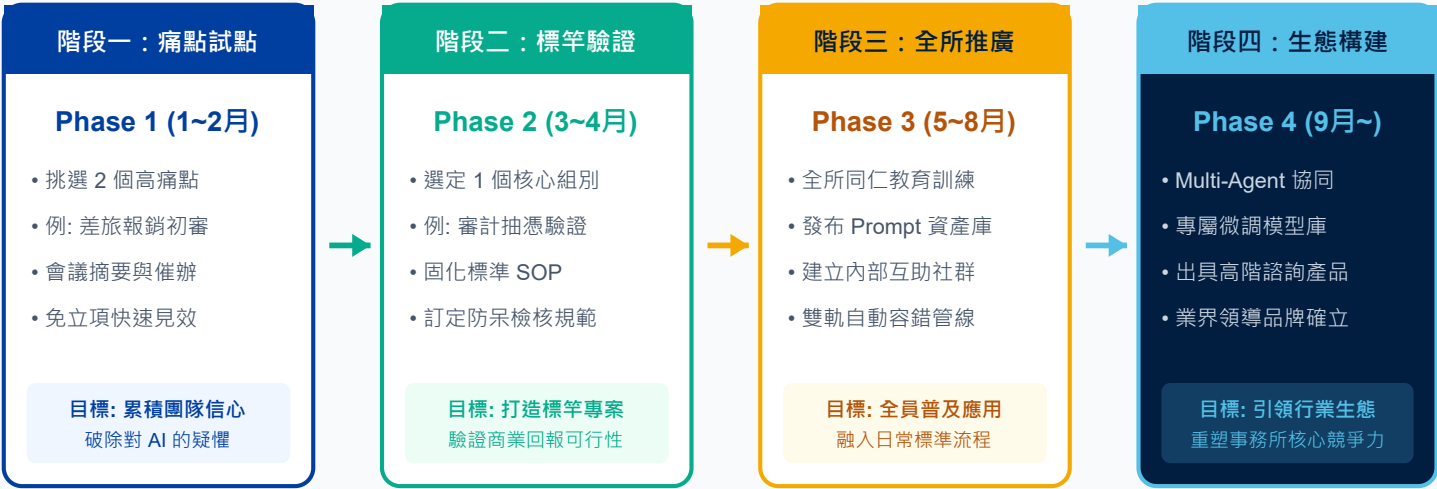
去識別化資料、內部教材與草稿生成先發 · 穩健進階至全流程自動化

Phased Adoption: Starting with Low-Risk, High-Confidence POCs

核心戰略與操作要點

- 第二階段 · 流程協作：串接審計抽憑與底稿整理 Workflow
- 第三階段 · 工具調用：打造具備 ERP/API 讀寫能力之專屬 Agent
- 第四階段 · 系統整合：與事務所核心 CMS / 差勤完成全面對接
- 第五階段 · 自主受控執行：在嚴格人機迴路下實現批量自動化處理
- 【成功金律】：低風險場景打出勝仗建立信心，高機敏場景自然水到渠成

事務所漸進導入四階段路線圖 (Four-Phase Phased Roadmap)



導入鐵律：切忌大而無當、一口氣全面重構；務必「小步快跑、以戰養戰、沿途沉澱資產」

落地心法：先在低風險場景累積成功經驗，再逐步推展至核心業務系統

演進階梯：從零散個人工具走向企業級工作系統

Tool → Copilot → Workflow → Agent → Multi-Agent → Governance

Systemic Evolution: From Point Tools to Trusted Enterprise Systems

✦ 核心戰略與操作要點

- 工具隨時在換：從 GPT 到 Claude 到 Gemini · 底層模型日新月異
- 系統才是資產：將業務邏輯、審批權限與風控結合成的工作系統
- 信任無法複製：合規、可追溯且經過外部驗證的系統才能獲得信賴
- 【戰略結論】：
- 事務所最終的競爭壁壘，不是買了哪一家 AI 軟體授權，而是能否構建出「能被合夥人、客戶與監管機構完全信任的 AI 工作體系」

事務所組織演進 5 階成熟度階梯 (Organizational Maturity Staircase)



✦ 終極目標：最終競爭力不是工具多寡，而是整套系統能否獲得客戶完全信任

人機協作本質：重新配置專業同仁的精力與時間

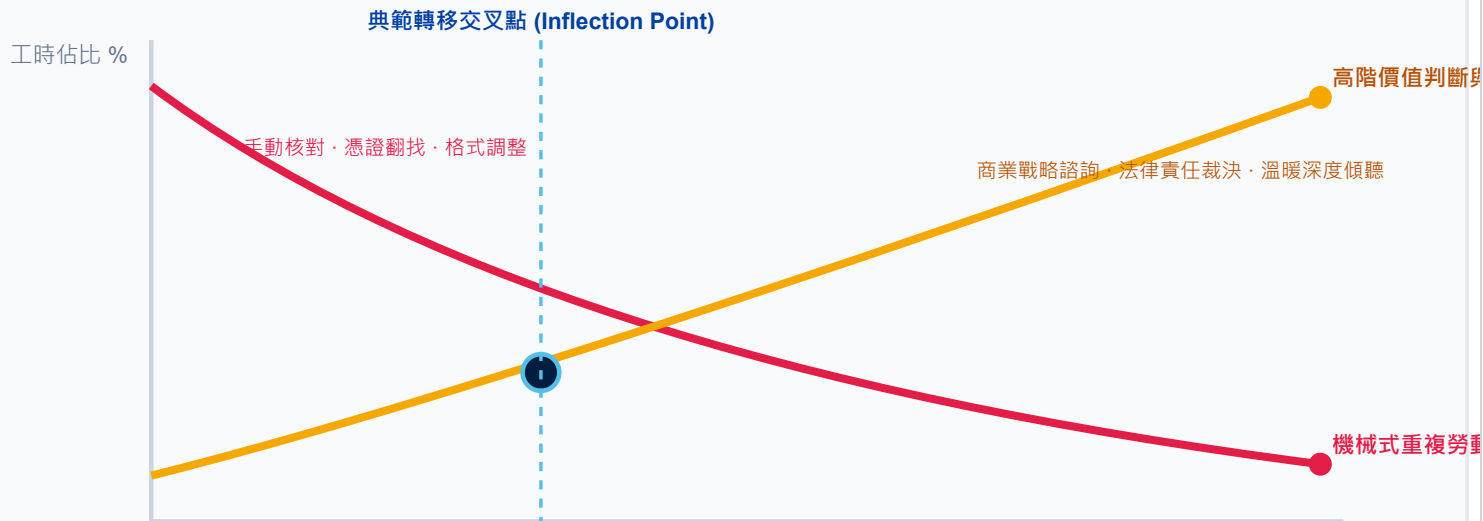
擺脫低階重複性搬運 · 聚焦價值創造、專業判斷與客戶信任

Human-AI Synergy: Elevating Professional Practice Above Tedium

✦ 核心戰略與操作要點

- 深入客戶商業模式，提供高洞察力之財務與稅務建議
- 面對複雜爭議交易之重大審計例外裁量與風險把關
- 與客戶決策層進行深度的策略性溝通與信任建立
- 針對未知變數做出具備專業前瞻性的商業決策
- 以會計師專業聲譽承擔法定的簽證責任與確信報告
- 【協作本質】：不是人與 AI 的淘汰競賽，而是專業人員如何善用 AI 重塑自我價值

專業人員價值演進雙曲線 (Value Trajectory Curves)



核心真理：AI 不會取代會計師，但懂得使用 AI 重塑自我價值的會計師，將取代不使用的同行

✦ 協作真諦：不是人 vs AI 的競爭，而是專業人員如何善用 AI 重塑自我價值

七大起手式：事務所導入 AI 的落地實戰守則

盤點重複痛點、選定小場景驗證、確立覆核點後再行推廣規模化

Seven Actionable Steps for Pragmatic AI Implementation

✦ 核心戰略與操作要點

- 5. 設定明確的人員覆核點 (HITL)：在關鍵節點焊接專業品質防線
- 6. 客觀衡量效益指標：以節省工時、錯誤率下降與同仁滿意度驗收
- 7. 獲取成功勝果後再行擴大：以具體成果說服其他部門主動跟進
- 【實戰精髓】：先打贏局部小戰役，用事實建立信心，勝過十場空談論壇

事務所立即能啟動的七大低門檻高回報任務 (Quick-Start Playbook)

1 長篇複雜合約摘要

- 快速萃取免責條款、罰則與期限
- 門檻：極低 · 見效：當天

2 跨表清冊勾稽比對

- 發票與銀行水單差異自動標記
- 門檻：低 · 見效：1 週內

3 查核工作底稿初稿

- 依事實數據標準化輸出敘述文案
- 門檻：中 · 見效：2 週內

4 客戶郵件與公文初擬

- 嚴謹商務語氣、雙語流暢轉化
- 門檻：極低 · 見效：當天

5 會議錄音重點提煉

- 萃取決策共識與各組待辦期限
- 門檻：極低 · 見效：當天

6 法規與準則問答 (RAG)

- 內部知識庫即時精準檢索條號
- 門檻：中 · 見效：1 個月

7 官方規範 16:9 簡報一鍵生成 (Presentation Automation)

將長篇查核底稿或專案筆記，一秒自動套入 Crowe 官方母片，完成字數控制與版型組裝出頁

啟動心法：挑選同仁最討厭做、最浪費時間的前 3 項任務，作為第一週試點切入點！

✦ 落地守則：先盤點高頻痛點，選定小場景打贏第一仗，再穩健擴大戰果

專案立項檢核：啟動前必須釐清的六大關鍵提問

痛點、分工邊界、資料來源、人工檢核與審計軌跡自查表

Six Mandatory Checkpoints Before Automating Any AI Project

核心戰略與操作要點

- 4. 流程中哪些地方一定要由人做最後判斷？ (Human Gate)
- 明確指定哪位同仁或主管對該節點的錯誤承擔法律責任
- 5. 我們到底該怎麼客觀驗證 AI 的產出結果？ (Verification)
- 建立客觀驗收評量集 (Gold Standard Dataset)
- 6. 系統該怎麼為全流程留下審計紀錄？ (Audit Trail)
- 確保每一步操作皆可供內部查核與外部主管機關檢驗
- 【自查心法】：只要這六題中有一題答不清楚，就還不適合直接上線自動化！

專案立項 6 道檢核關卡 (Feasibility Gates Checklist)

Q1 痛點是否真實且高頻？

- 每年/每季重複發生多次？
- 解決後能省下可度量的工時？

✗ 拒絕為技術而技術的偽需求

Q2 資料來源是否充足安全？

- 底稿格式是否能數位化讀取？
- 機密個資是否具備脫敏機制？

✗ 資料混沌不清嚴禁硬上

Q3 容錯界限與防呆為何？

- 該任務能容忍多大的錯誤率？
- 是否有剛性規則進行二次檢核？

✗ 零容錯任務不得全委託 AI

Q4 人機責任如何切分？

- 誰負責提供 Prompt 指令？
- 最終由哪位會計師簽章認可？

✓ 權責劃分清晰方能啟動

Q5 ROI 與投入產出比？

- 算力 API 成本 (NT\$ 0.003/頁)
- 預期省下的高級同仁時薪？

✓ ROI 通常應大於 50 倍

Q6 團隊接受度與變更管理？

- 一線同仁是否願意日常使用？
- 是否備妥完整的內部操作手冊？

✓ 解決人的抗拒是成功的關鍵

六大問題全數獲得肯定答案，專案才予以正式立項編列預算

✦ 防踩坑箴言：只要這六題答不清楚，就代表該專案還不適合直接自動化

AI 成熟度模型 (CMM)：六大演進層級定位

評估組織現狀 · 尋找最適發展階段而非盲目追求頂峰

AI Capability Maturity Model (CMM): From Personal Use to Governance

核心戰略與操作要點

- Level 4 · 工作流串接 (Integrated Workflow) :
 - AI 嵌入業務軟體，跨步驟資料流實現半自動化銜接
- Level 5 · 任務型代理 (Autonomous Agent) :
 - 具備主動調用 API 與工具能力，在授權範圍內執行目標
- Level 6 · 企業級治理 (AI Governance) :
 - 權限、成本、資安、審計與倫理全面受控，贏得網絡完全信任
 - 【發展真諦】：目標不是盲目追求 Level 6，而是找到當下最適合事務所的甜蜜點

事務所 AI 成熟度模型 (Five-Level Maturity Matrix)

Level 1: 探索	Level 2: 試點	Level 3: 普及	Level 4: 賦能	Level 5: 引領
 - 同仁私下嘗試 - 零星聊天對話 - 缺乏統一規範 - 資安外洩隱患 特徵: 散兵游勇	 - 成立專案小組 - 試點審計/稅務 - 訂立金鑰使用守則 - 初步 Prompt 沉澱 特徵: 局部突破	 - 全員標準化 SOP - ETL 管線常態運作 - 雙軌自動容錯備援 - 工時顯著節流 特徵: 流程固化	 - 專案密室沙盒隔離 - Agent 自主調用工具 - 決策智慧前瞻模擬 - 諮詢開源新業務 特徵: 業務創新	 - 智慧驅動型生態 - 專屬微調垂直模型 - 參與法規標準制定 - 難以超越的護城河 特徵: 行業標竿

自我診斷：多數事務所目前處於 L1 ~ L2，2026 年的戰略目標是全員跨入 L3 並打造 L4 核心能力

成熟度心法：層級並非越高越好，關鍵在於找到與事務所最匹配的成熟度

行動指南：跨出第一步，從解決一個痛點開始

尋找最重複、最易遺漏或最耗時的任務作為切入突破口

Immediate Action Plan: Selecting Your First High-Yield Task

✦ 核心戰略與操作要點

- 【核心行動原則】：
- 先做出一個具體可見、有量化數據的小成果，再決定下一步格局！
- 不要等待完美的政策或龐大的專案小組成立
- 從身邊最痛苦的一個痛點出發，用兩週時間打通人機協同閉環
- 用實質省下的工時與品質提升說話，變革的種子就會在事務所生根發芽



✦ 行動金句：先做出一個具體有感的小成果，用事實說話，再決定下一步

結語：工作方式的重新設計

AI 不只是工具升級 · 而是事務所工作方式的深層重塑

Conclusion: Redesigning How We Work in the Age of Intelligence



◆ Smart decisions. Lasting value. · 攜手邁向人機協同的卓越事務所