AI AGENT 需求探索工作簿

你需要哪一類 AI Agent？

把服務對象、工作流程、資料工具、行動界線及試點驗收整理成可交給方案設計／開發團隊的需求摘要。

52 題 • 約 20–30 分鐘　不計分 • 不預設自動授權　可留白／可補充

公司／團隊（可選）：_____　日期：_____

填寫提示：單選題勾一項，多選題可勾多項；不確定時可勾「視情況／待確認」，或留白後與方案團隊討論。選擇某種 Agent 不代表授權其對外發送訊息、修改正式資料、付款／承諾或持續監控。請勿在紙本記錄不必要的敏感個人資料。

一、目標與服務對象

從要改善的結果和實際使用者開始，先定義 Agent 的服務對象與主責範圍。

第 01 題　你的公司／團隊屬於哪個行業或服務領域？

可填行業、主要產品／服務、營運地區；可略過不便透露的資料。

補充／條件：

第 02 題　這次最希望 AI Agent 帶來甚麼主要改善？

- ☐ 減少重複人手工作時間，讓團隊處理更高價值工作
- ☐ 降低錯漏、延遲或流程中斷，提升作業一致性
- ☐ 增加營收、轉換率或客戶跟進覆蓋率
- ☐ 縮短客戶／員工等候時間，改善服務體驗
- ☐ 把分散的資訊整理成可採取行動的判斷或建議
- ☐ 視情況／尚未確定主要目標

補充／條件：

第 03 題　你初步想建立哪一類 Agent？

- ☐ 內部知識助理：從核准文件或系統查找答案並附來源
- ☐ 流程自動化 Agent：依規則推進多步驟內部工作並更新狀態
- ☐ 文件／資料處理 Agent：擷取、分類、核對或轉換文件與紀錄
- ☐ 混合型／視情況／不確定，想先盤點再決定
- ☐ 客戶服務／銷售支援：分類查詢、整理客戶脈絡、草擬回覆或跟進
- ☐ 研究／分析 Agent：彙整資料、比較選項、產生分析或報告
- ☐ 專案協作 Agent：追蹤任務、彙總進度、提示阻礙與整理交付

補充／條件：

第 04 題　誰會直接使用或受益於這個 Agent？

- [ ] 公司內部前線／營運同事
- [ ] 銷售／客戶服務團隊
- [ ] 公司客戶或合作夥伴
- [ ] 視情況／尚未確定
- [ ] 管理層／決策者
- [ ] 財務／人力資源／法務等專業部門
- [ ] 單一負責人或小型專案團隊

補充／條件：

第 05 題　目前最困擾的工作問題是甚麼？

- [ ] 資料散落多處，搜尋或核實答案很慢
- [ ] 查詢量大，回覆／跟進容易延誤
- [ ] 需要跨系統比對資訊才能完成工作
- [ ] 尚未量化／仍待確認
- [ ] 重複輸入、複製貼上或手動整理太多
- [ ] 流程依賴個別員工記憶，交接容易遺漏
- [ ] 內容、文件或數據需要大量初步檢查

補充／條件：

第 06 題　目前每週大約有多少相關工作量？

例如：每週約 300 宗查詢、每天 2 小時對帳、每月 500 份文件；不確定可寫「待量度」。

補充／條件：

二、工作流程與交付

描繪目前流程、輸入輸出與例外情況，讓第一版範圍可被估算及驗收。

第 07 題　希望 Agent 優先負責哪些工作？

- ☐ 回答內部常見問題並附文件／資料來源
- ☐ 整理、比對或更新內部業務紀錄
- ☐ 提醒期限、分派任務或追蹤未完成事項
- ☐ 執行固定規則的步驟式內部流程
- ☐ 分類、摘要或草擬客戶回覆
- ☐ 產生報價、報告、表格或其他文件草稿
- ☐ 從多個來源蒐集資料並提出比較／建議
- ☐ 視情況／尚未確定

補充／條件：

第 08 題　第一版最重要的工作流程應由甚麼事件開始？

- ☐ 員工主動提問或提交工作要求
- ☐ 系統出現一筆新紀錄或狀態改變
- ☐ 客戶在指定網站／聊天渠道提出查詢
- ☐ 視情況／未有決定
- ☐ 收到一封指定信箱的郵件或表單
- ☐ 固定時間的批次作業（例如每日／每週）
- ☐ 先由人工挑選資料，再啟動 Agent

補充／條件：

第 09 題　一項工作完成後，期望交付甚麼結果？

- ☐ 附引用來源的文字答案或建議
- ☐ 已填妥的表格、紀錄或欄位草稿
- ☐ 待審核的任務／工單及處理原因
- ☐ 視情況／尚未確定
- ☐ 可供人工審核的郵件／訊息草稿
- ☐ 摘要、報表、清單或例外項目
- ☐ 在核准後完成的內部系統更新

補充／條件：

第 10 題　Agent 會在哪些渠道供使用者操作？

- ☐ 公司網站／客戶入口
- ☐ 電子郵件
- ☐ 獨立網頁或內部工作台
- ☐ 尚未選定，希望先比較渠道
- ☐ WhatsApp、WeChat、Teams、Slack 等訊息渠道
- ☐ CRM／ERP／工單或內部業務系統
- ☐ 手機／桌面應用程式

補充／條件：

第 11 題　需要支援哪些語言或地區習慣？

- ☐ 繁體中文（香港用語）
- ☐ 簡體中文
- ☐ 日文／韓文／其他語言
- ☐ 視情況／尚未確定
- ☐ 繁體中文（台灣用語）
- ☐ 英文
- ☐ 須按客戶或地區自動切換

補充／條件：

第 12 題　相關工作通常多久發生一次、是否有尖峰？

- ☐ 全天候即時處理，工作量波動大
- ☐ 每日多次，有明顯繁忙時段
- ☐ 每週固定批次或例行工作
- ☐ 每月／季度等低頻流程
- ☐ 只在有人提出要求時處理
- ☐ 尚未量度／視情況

補充／條件：

第 13 題　有哪些例外、禁做事項或必須轉交人員的情況？

例如：資料互相矛盾、客戶投訴、涉及退款、缺少必填欄位、超過金額門檻；沒有把握時可寫「待訪談」。

補充／條件：

三、能力、系統與資料

列出 Agent 要使用的工具與可信資料來源，避免只寫「接入所有系統」。

第 14 題　要串接哪些工具或系統？

- ☐ Microsoft 365／Outlook／Teams／SharePoint
- ☐ Google Workspace／Gmail／Drive／Calendar
- ☐ CRM（如 Salesforce、HubSpot 或自建系統）
- ☐ ERP／會計／庫存／訂單系統
- ☐ 客服工單／知識庫／網站內容管理系統
- ☐ WhatsApp／WeChat／其他訊息渠道
- ☐ API、資料庫或內部自建應用程式
- ☐ 第一版不需串接／尚未確定

補充／條件：

第 15 題　請列出現有系統名稱、版本或供應商（如知道）。

可補充系統管理者、是否已有 API、資料匯出方式；不確定可留白。

補充／條件：

第 16 題　Agent 可以依據哪些資料來源回答或做判斷？

- ☐ 已核准的政策、SOP、產品手冊或 FAQ
- ☐ 內部文件、知識庫、雲端硬碟
- ☐ CRM／ERP／訂單／庫存等即時紀錄
- ☐ 電郵、聊天記錄或客服工單
- ☐ 公開網站或指定外部資料來源
- ☐ 試算表、CSV 或人工上傳文件
- ☐ 只用使用者當次提供的資料
- ☐ 視情況／尚未確定

補充／條件：

第 17 題　目前的資料品質與負責人情況如何？

- ☐ 有明確資料負責人，內容定期更新且版本清楚
- ☐ 資料可用，但分散或有少量重複／過期內容
- ☐ 資料品質不一，需要先清理或訂立權威來源
- ☐ 不同部門答案可能不一致，需建立優先次序
- ☐ 尚未盤點，需在試點前做資料盤點
- ☐ 視情況／不確定

補充／條件：

第 18 題　遇到缺資料、過期資料或來源互相矛盾時，Agent 應怎樣處理？

- ☐ 停止作答，列出缺口並交給指定人員
- ☐ 同時呈現不同來源與日期，不自行選邊
- ☐ 只採用預先指定的權威來源並附註未採用資料
- ☐ 可按一套已確認的優先規則判斷，低信心時轉交
- ☐ 只提供一般資訊，清楚標記不可視為已核實
- ☐ 視情況／待確認

補充／條件：

第 19 題　第一版對接系統時，最合適的資料權限是甚麼？

- ☐ 只讀取核准資料，不寫回任何系統
- ☐ 可建立草稿／待審紀錄，人工批准後才正式寫入
- ☐ 可修改限定欄位，但需保留修改前內容及稽核記錄
- ☐ 限定流程內可執行明確可逆的更新
- ☐ 按系統及任務逐一決定，暫不給預設寫入權
- ☐ 尚未決定／視情況

補充／條件：

四、自主程度與批准

逐項界定可建議、可草擬、可修改及可對外執行的範圍；未回答不等於授權。

第 20 題　整體而言，第一階段希望 Agent 有多少自主程度？

- ☐ 只查找、整理、分析和提出建議
- ☐ 可自動完成低風險、可撤回的內部步驟
- ☐ 按不同工作分級，先建立批准矩陣再決定
- ☐ 可產生草稿／預覽，所有執行由人員批准
- ☐ 在每項任務明確授權的範圍內執行並回報
- ☐ 尚未決定；不應由 Agent 自行推定

補充／條件：

第 21 題　Agent 草擬的電郵或訊息，甚麼時候可以送出？

- ☐ 每次都只可存草稿，必須由人員檢查及按送出
- ☐ 某些低風險例行通知可按明確規則送出，其他要批准
- ☐ 第一版不接訊息傳送功能
- ☐ 僅可發給事先核准對象，並使用核准模板／範圍
- ☐ 每個專案逐次授權；完成後回報收件人及內容
- ☐ 視情況／待確認

補充／條件：

第 22 題　Agent 對 CRM、ERP、工單或其他系統紀錄可做甚麼？

- ☐ 只讀取並提出修改建議，不寫入
- ☐ 只可更新預先指定欄位，且可追溯及回復
- ☐ 所有新增、修改、合併及刪除都須個別批准
- ☐ 建立草稿／待審變更，由人員確認後正式更新
- ☐ 可在一個已核准的固定流程內更新狀態
- ☐ 尚未決定／視情況

補充／條件：

第 23 題　涉及付款、下單、退款、預約或合約承諾時，Agent 可以做甚麼？

- ☐ 只整理資料或準備建議，不可提交／承諾
- ☐ 只有低於已確認門檻且可取消的項目，才可依書面規則處理
- ☐ 第一版完全不處理這類任務
- ☐ 準備表單或草稿，必須由授權人逐次確認
- ☐ 必須由不同於提出需求的人員核准
- ☐ 視情況／尚未決定

補充／條件：

第 24 題　對外公開發布內容、代表公司承諾或改變客戶權益時，批准方式為何？

- ☐ 任何內容都先交人工審閱，Agent 不自行發布／承諾
- ☐ 明確授權後可在限定渠道、對象與內容範圍執行
- ☐ 第一版不提供對外發布或承諾能力
- ☐ 只可發布已預先核准的固定模板或資訊
- ☐ 涉及例外、價格、法律、退款或爭議一律升級
- ☐ 尚未決定／視情況

補充／條件：

第 25 題　是否需要定時、自動觸發或持續監控？

- ☐ 不需要，只在使用者要求時執行
- ☐ 有新事件時執行內部分析，結果交人工確認
- ☐ 需先定義監控對象、頻率、停止條件及負責人
- ☐ 需要定時整理／提醒，但不自動採取外部行動
- ☐ 可在明確限制與停用機制下自動跑固定流程
- ☐ 尚未決定／視情況

補充／條件：

五、私隱、安全與部署

說明資料敏感度、所在區域、權限與記錄要求，供技術方案與風險評估使用。

第 26 題　工作可能接觸哪些敏感資料？

- [ ] 一般公開或非敏感業務資訊
- [ ] 員工資料、薪酬或人事紀錄
- [ ] 健康、生物特徵、兒童或其他高度敏感資料
- [ ] 尚未盤點；不要先輸入真實資料
- [ ] 客戶聯絡資料或一般個人資料
- [ ] 身份、財務、付款或交易資料
- [ ] 商業機密、未公開價格／合約／設計資料

補充／條件：

第 27 題　需遵守哪些地區規則、合約或認證要求？

- [ ] 香港《個人資料（私隱）條例》或客戶合約要求
- [ ] 中國內地資料本地化或行業規則
- [ ] ISO 27001、SOC 2 或客戶供應商審查
- [ ] 尚未評估；需法務／私隱負責人確認
- [ ] GDPR／歐盟資料保護要求
- [ ] 金融、醫療、法律或政府等行業規範
- [ ] 資料處理協議、保留／刪除或跨境限制

補充／條件：

第 28 題　對資料保存、模型訓練及刪除有甚麼要求？

- [ ] 不保留對話；僅在當次處理後清除
- [ ] 保留稽核紀錄，但避免記錄敏感內容
- [ ] 不得用本公司資料訓練供應商的通用模型
- [ ] 尚未確認
- [ ] 短期保留以支援除錯，設定明確期限後刪除
- [ ] 可保存工作紀錄，須有存取控制與刪除流程
- [ ] 需按資料類別／地區分開訂定

補充／條件：

第 29 題　偏好的部署或資料處理方式是甚麼？

- [ ] 商用雲端服務；資料可按核准條款處理
- [ ] 公司自有伺服器／本地部署
- [ ] 先提供架構與資料流圖，再由 IT／法務選擇
- [ ] 指定雲端區域／私有雲，資料不得跨指定地區
- [ ] 混合式：敏感資料留內部，其他功能用雲端
- [ ] 尚未決定／需要比較成本及限制

補充／條件：

第 30 題　誰可以使用 Agent、看見哪些資料或批准哪些操作？

- [ ] 所有使用者權限相同，先做小規模封閉試點
- [ ] 依部門／角色分權，禁止跨部門讀取未授權資料
- [ ] 需有管理員、使用者及稽核者等不同角色
- [ ] 按公司既有系統的使用者權限繼承
- [ ] 敏感操作需指定批准人或雙人覆核
- [ ] 尚未盤點，需和 IT／流程負責人確認

補充／條件：

第 31 題　你期望有哪些安全監察與緊急停止安排？

- ☐ 記錄使用者、時間、來源與結果，供稽核
- ☐ 錯誤率或異常觸發告警，暫停自動流程
- ☐ 有回復／復原方案與事故通報窗口
- ☐ 尚未決定
- ☐ 對高風險動作保留批准人及變更前後內容
- ☐ 管理員可立即停用整個 Agent 或單一整合
- ☐ 先以只讀／人工批准模式運作，累積證據再擴權

補充／條件：

六、使用體驗與營運

決定人員如何與 Agent 協作、如何交接，以及誰負責監察和維護。

第 32 題　你希望 Agent 與使用者如何互動？

- ☐ 簡潔直接：先給結論，再列重點與來源
- ☐ 以表單／按鈕引導，減少自由輸入及錯誤
- ☐ 需按不同使用者／工作選擇不同介面
- ☐ 像同事一樣對話，先釐清問題再逐步協助
- ☐ 提供工作清單或佇列，讓員工批次檢查與批准
- ☐ 視情況／尚未確定

補充／條件：

第 33 題　答案或建議需要如何展示依據？

- ☐ 每個重要結論都附資料來源、連結及更新日期
- ☐ 一般答案可簡短回覆，只在使用者追問時提供來源
- ☐ 依任務風險分級：高風險必須引用，低風險可摘要
- ☐ 列出引用資料；無法找到依據時明確說明
- ☐ 提供信心／不確定提示與缺少資料清單
- ☐ 尚未決定

補充／條件：

第 34 題　遇到超出能力、低信心或情緒敏感的個案，如何交接？

- ☐ 立即停止推斷，交由指定人員接手
- ☐ 讓使用者選擇聯絡真人或繼續補資料
- ☐ 需設定服務時段、回覆時限及緊急升級方式
- ☐ 先整理已知資料、已做步驟與待辦，再交接
- ☐ 依任務類別轉交不同部門／值班人員
- ☐ 視情況／尚未定義

補充／條件：

第 35 題　你希望怎樣檢視 Agent 的工作紀錄或成效？

- ☐ 每次處理完成後即時摘要與待辦
- ☐ 管理儀表板檢視使用量、成本及錯誤類型
- ☐ 只在例外或需要批准時通知，不發例行報告
- ☐ 每日／每週彙總成功、失敗、轉交及節省時間
- ☐ 抽樣檢查答案、引用來源及人工修改情況
- ☐ 尚未決定

補充／條件：

第 36 題　對可用時間、無障礙或使用者培訓有甚麼要求？

- ☐ 支援手機優先及不同螢幕尺寸
- ☐ 須涵蓋香港／台灣／內地等地區用語差異
- ☐ 需支援不同時區、營業時間或輪班安排
- ☐ 需符合螢幕閱讀器／鍵盤操作等無障礙需要
- ☐ 需提供新手指引、FAQ 或短時間培訓
- ☐ 暫無特別要求／尚未盤點

補充／條件：

第 37 題 **試點期間由誰負責產品決策、資料及日常營運？**

可填角色或部門即可，例如：業務負責人決定流程、IT 管理權限、客服主管審核樣本；無需填個人姓名。

補充／條件：

七、試點、成本與限制

把第一階段縮到可驗證的範圍，並記錄預算、時程與內部準備。

第 38 題　第一階段試點應包含多大的範圍？

- [ ] 單一團隊、單一流程、少量測試使用者
- [ ] 多部門共用，但先以只讀／草稿方式驗證
- [ ] 先做可點選原型／離線測試，不接真實系統
- [ ] 尚未決定／視情況
- [ ] 一個部門的數個相近流程
- [ ] 面向客戶的有限渠道與限定服務內容
- [ ] 希望直接覆蓋多種流程（需先拆分風險與階段）

補充／條件：

第 39 題　哪些事情明確不應納入第一版？

- [ ] 付款、下單、退款、預約或合約承諾
- [ ] 自動刪除、覆寫或合併正式紀錄
- [ ] 未經核准的外部網站／系統整合
- [ ] 目前沒有排除清單，需一起定義
- [ ] 自動向客戶／公眾發送訊息或發布內容
- [ ] 處理高度敏感資料或跨境資料
- [ ] 多語言、全渠道或全天候承諾

補充／條件：

第 40 題　你希望用哪些主要指標判斷 Agent 是否有價值？

- [ ] 每宗工作所需時間／人手工時下降
- [ ] 正確率、引用可信度或人工接受率
- [ ] 員工採用率／每週活躍使用者
- [ ] 每月總成本、單位處理成本或投資回收
- [ ] 首次回覆時間或案件完成時間改善
- [ ] 錯誤、重工、漏跟進或升級次數減少
- [ ] 客戶滿意度、轉換率或服務量提升
- [ ] 視情況／尚未定義

補充／條件：

第 41 題　是否已有目前基準值或可量度的目標？

例如：平均每宗要 12 分鐘，希望降至 5 分鐘；回覆時間由 4 小時縮至 30 分鐘；如未量度可寫待建立基準。

補充／條件：

第 42 題　最不能接受的失誤或風險是甚麼？

- [ ] 錯誤答案被當成正式政策／事實
- [ ] 個人資料或商業機密外洩
- [ ] 偏頗、歧視或不一致的服務
- [ ] 可接受少量低風險錯誤，但必須易於發現與修正
- [ ] 錯誤外發訊息、價格或承諾
- [ ] 誤改／刪除正式資料
- [ ] 成本失控、服務中斷或無法追溯
- [ ] 尚未完成風險排序

補充／條件：

第 43 題　目前可接受的預算或採購模式是甚麼？

- [ ] 先以低成本原型／短期試點驗證，再決定投資
- [ ] 可接受按月／按年訂閱，需估算使用量及維護費
- [ ] 尚未設定預算，希望先比較可行方案及成本範圍
- [ ] 按一次性建置費及整合範圍評估
- [ ] 需要分階段報價，列明平台、模型、整合與營運成本
- [ ] 暫不提供／待內部討論

補充／條件：

第 44 題　預期何時需要原型、試點及正式上線？

- [ ] 2–4 週內先看可操作原型
- [ ] 3–6 個月內完成內部試點
- [ ] 目前只在探索階段，沒有固定日期
- [ ] 1–3 個月內啟動小型試點
- [ ] 需配合採購、法務或系統改造時程
- [ ] 視情況／尚未決定

補充／條件：

第 45 題　目前有哪些技術、採購或內部限制？

- [ ] 只能使用已批准的雲端／模型供應商
- [ ] 內部沒有 API／IT 人手有限
- [ ] 有指定系統、模型、開發語言或供應商
- [ ] 尚未盤點，需做可行性評估
- [ ] 需配合既有 SSO、MFA、網絡或裝置管理
- [ ] 需經法務、私隱、資安或採購審批
- [ ] 須支援離線／低連線環境或特定裝置

補充／條件：

第 46 題　上線後誰會維護知識、流程、權限及供應商？

- [ ] 內部 IT／數據團隊可全權維護
- [ ] 需要供應商提供持續維護與服務支援
- [ ] 需先估算更新、監察及支援的月度成本
- [ ] 業務部門管理內容，IT 管理整合與安全
- [ ] 希望先外包建置，再逐步培訓內部接手
- [ ] 尚未安排／待確認

補充／條件：

八、成功指標與驗收

用具體情境和可量度標準判斷試點是否成功，而不是只看「感覺好用」。

第 47 題　請寫下 1–3 個試點必須通過的實際情境。

建議描述：輸入／觸發 → Agent 應做甚麼 → 必須避免甚麼 → 如何判斷通過。可用真實資料的匿名或合成案例。

補充／條件：

第 48 題　你認為甚麼條件代表可以進入下一階段？

- ☐ 達到已確認的時間／成本改善目標
- ☐ 所有高風險動作都有批准、記錄及復原測試
- ☐ 試點期間沒有重大私隱／安全事件
- ☐ 還沒有驗收門檻，需要共同制定
- ☐ 抽樣正確率或人工接受率達到門檻
- ☐ 員工能完成上手訓練並按流程使用
- ☐ 業務、IT、資安及法務等指定負責人共同簽核

補充／條件：

第 49 題　哪些資料或測試案例可用於驗收？

- ☐ 去識別化的歷史案例
- ☐ 由內部專家提供標準問題與正確答案
- ☐ 少量經批准的真實案例並採取遮罩／存取限制
- ☐ 視情況／待確認
- ☐ 合成／虛構資料，不用真實客戶資料
- ☐ 已核准公開文件或測試環境資料
- ☐ 目前沒有測試集，需要先整理

補充／條件：

第 50 題　對試點的錯誤率、回退方式或服務中斷，有甚麼要求？

- ☐ 錯誤容忍度極低，先以人工審核及影子模式測試
- ☐ 遇到異常即停用自動流程，回到現有人工流程
- ☐ 依不同工作風險分級，尚需共同定義
- ☐ 可以容許低風險錯誤，但需快速轉人工與記錄
- ☐ 需明定可接受錯誤類型、上限、通報及修復時限
- ☐ 尚未決定

補充／條件：

第 51 題　正式驗收需要哪些人員或部門簽核？

- ☐ 提出需求的業務負責人
- ☐ IT／系統管理人員
- ☐ 採購／財務／管理層
- ☐ 尚未確認簽核流程
- ☐ 實際使用的前線／營運代表
- ☐ 資訊安全／私隱／法務負責人
- ☐ 客戶代表或外部合作方（如適用）

補充／條件：

第 52 題　還有哪些必須知道的背景、疑問或成功條件？

可補充重要例子、既有方案、公司內部決策條件，或列出你希望方案團隊先回答的問題。

補充／條件：

試點需求摘要與驗收紀錄

以下由需求方與方案團隊共同填寫；尚未確認的自主權、資料處理、成功門檻及簽核方式，應明確標記待確認。

初步 Agent 角色／第一版範圍

待確認事項及責任人

試點通過條件（指標、門檻及簽核人）

風險／批准界線及停止／回復安排