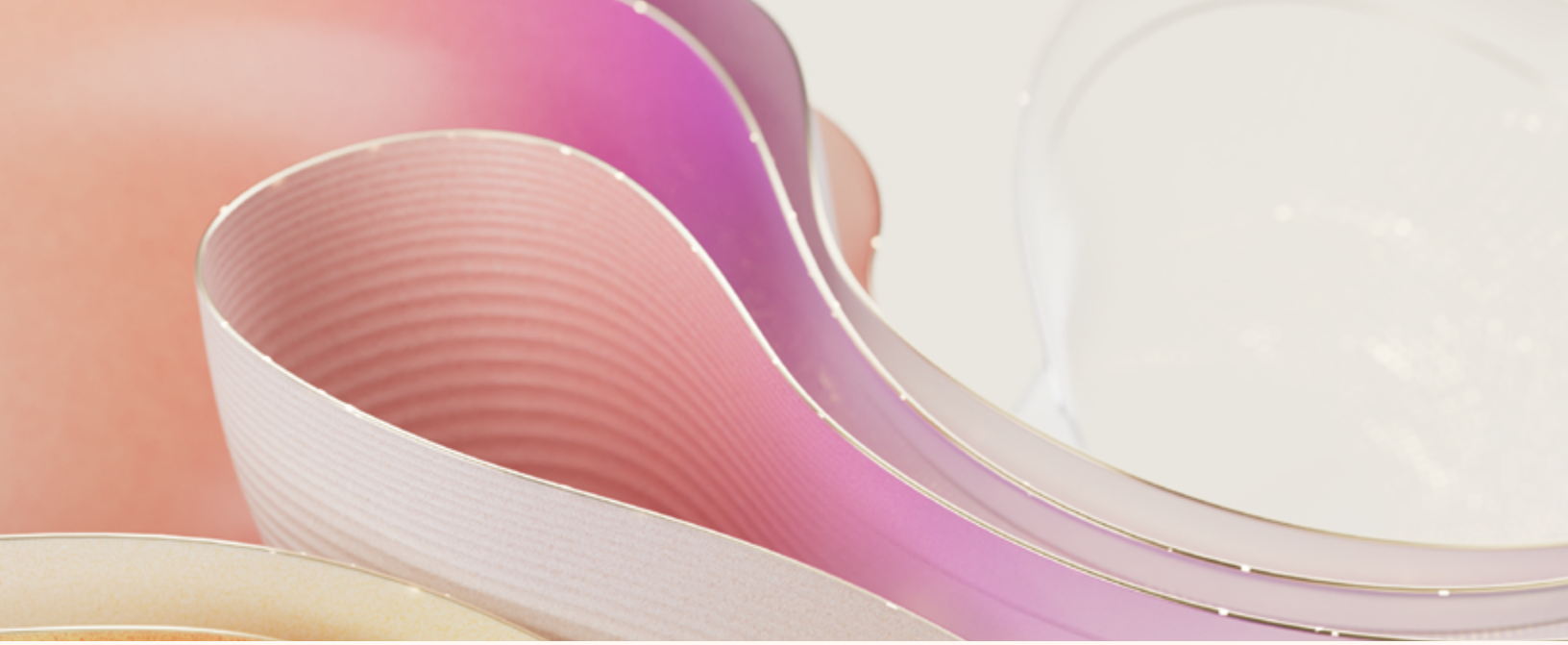
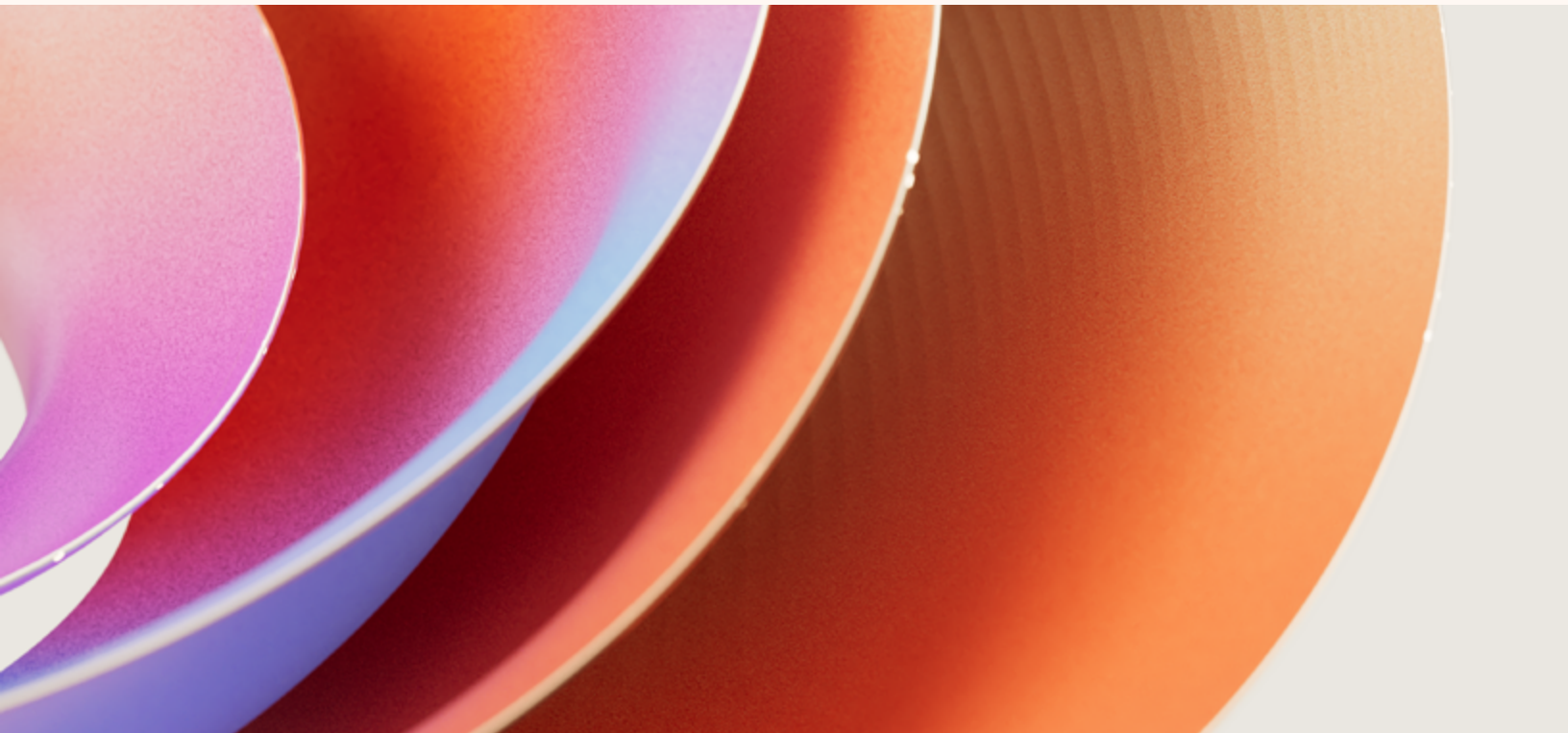


Microsoft

AI 策略藍圖

組織如何實現前沿轉型



執行摘要

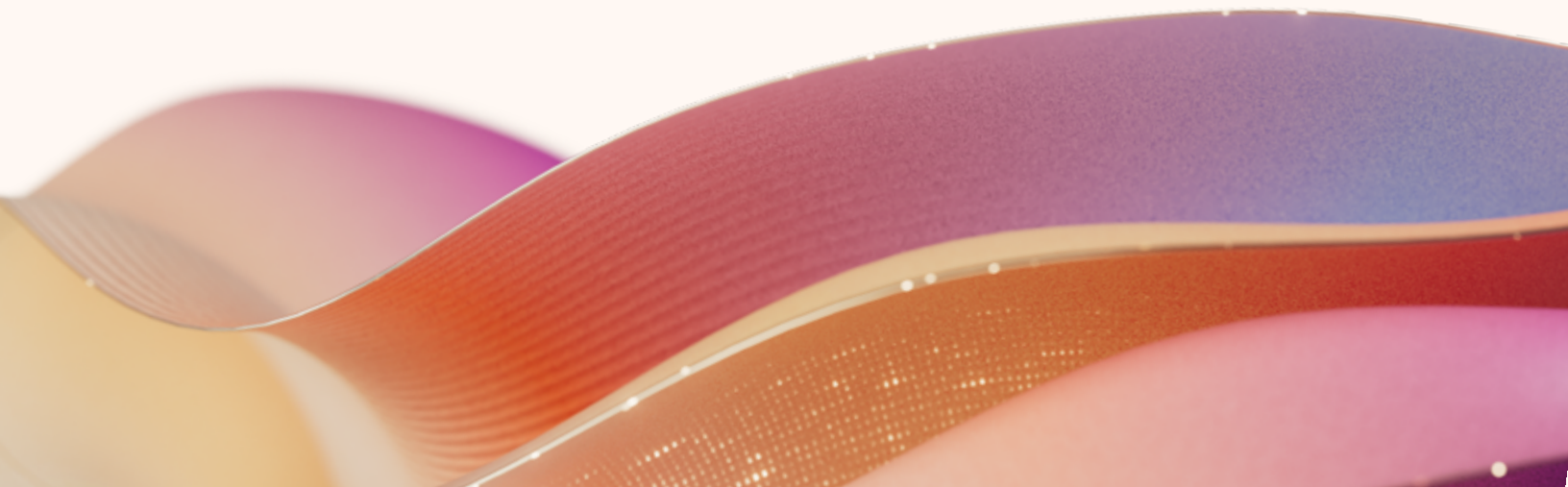
AI 正在重塑完成工作的方式，協助組織最佳化營運、獲得競爭優勢，並更快實現更多價值。獲取這些權益的前提是一個能支持負責任、可擴展且成果驅動式採用的基礎。這同時也取決於員工素質，讓員工具備與 AI 系統有效協作所需的 AI 與人類技能。

組織正透過前沿轉型作業以建立基礎，並加速組織內的創新與成長。他們正將 AI 系統納入業務流程的核心：改變組織的運作方式，並賦能員工聚焦於需要人類判斷、知識與創意的任務。

什麼是前沿轉型？

前沿轉型是數位與 AI 轉型的下一階段演進：全面重新改造能結合 AI 與人類抱負的商業模式，並實現組織最高的願景與成長潛力。期間需要不受限於生產力和效率為主導的獨立 AI 使用案例，以便 AI 全面整合併入關鍵業務流程。

這份藍圖將成功前沿企業的經研究驗證模式與經驗，轉化為實用策略與行動，讓您的企業成為 AI 支援營業。



成功經驗啟示

此處提供的建議與指引源於 70 位來自領先組織的商業與資訊科技決策者進行的詳細訪談，這些決策者皆積極參與其轉型旅程。[1]他們也受到 Microsoft 內部 AI 轉型以及我們支援許多客戶轉型工作所做工作的啟發。

這些經驗反映出了一系列共通的瓶頸。

致力於 AI 轉型的組織缺乏的通常不是願景與善意，而是在落實時陷入四大困境：範圍失控、信任缺乏、複雜度劇增，以及員工轉型能力不足。

相較之下，成功的前沿企業會及早行動，規劃迭代，並以清醒且現實的態度看待 AI 的能力、需求與範圍，從而應對挑戰。他們的轉型會以解決實際問題為基礎，並藉由一系列小型勝利，逐步建立信心。

借鑑前沿企業的成功心法，借鏡其應對策略，將大幅加速您的前沿轉型步伐。

問題	潛在挑戰	前沿企業採取方法
想法層出不窮，卻無明確起點。	排山倒海的機會使優先排序成為重大挑戰。	率先鎖定一個可衡量的使用案例，再進行擴展。
由於投資報酬率 (ROI) 難以具體量化，管理階層往往對注資進行規模化擴展感到猶豫。	要讓領導階層接受「具體的 ROI 資料並非最終目標」，往往是轉型過程中最大的溝通挑戰。	企業與其關起門來做不透明的黑盒子試驗，不如建立高透明度的機制，用看得見的 KPI 資料來證明轉型的實質進展。
資料不完整或未就緒，輸出結果不可靠。	系統孤立且資料管理不善，導致輸出不準確或產生虛構資料。	視資料準備作業為關鍵路徑。先從建立標準流程或範例開始，再接著擴大應用。
合規性評估與資訊安全審查，往往成為延遲業務規模化擴展的瓶頸。	法規與審查流程橫跨眾多利益關係人，且測試需求缺乏一致性。	透過「人機協同」與「分層簽核」來實證系統安全性。
試點成效顯著，但規模化擴展顯得風險重重且方向模糊。	治理、營運與成本架構漏洞百出，解決權責卻含糊不清。	逐步擴展規模，先驗證一個使用案例，再推進下一個。
使用者/客戶不信任 Agent，導致使用陷入停滯。	初期遭遇效能不穩、不良資料、治理不彰與文化排斥，將重挫團隊對 AI 的信任。	提供選擇加入、安全測試，並向使用者證明成果。
團隊缺乏廣泛推行 AI 的能力與信心	AI 素養不足、對如何負責任地使用 AI 存在不確定性，以及過度依賴少數專家，可能會減緩採用步伐並使規模化變得困難。	投資於依角色訓練、實務學習及變更協助，協助員工建立信心，負責任地採用 AI，並將其應用於實際工作流程中。

[1] Emerald Research Group：由 Microsoft 贊助，AI 轉型策略定性研究報告，2026 年 5 月。

內容

02
執行摘要

05
如何著手
前沿轉型

09
AI 價值驅動因素 #1
商業策略

20
AI 價值驅動因素 #2
技術和資料策略

30
AI 價值驅動因素 #3
AI 策略和經驗

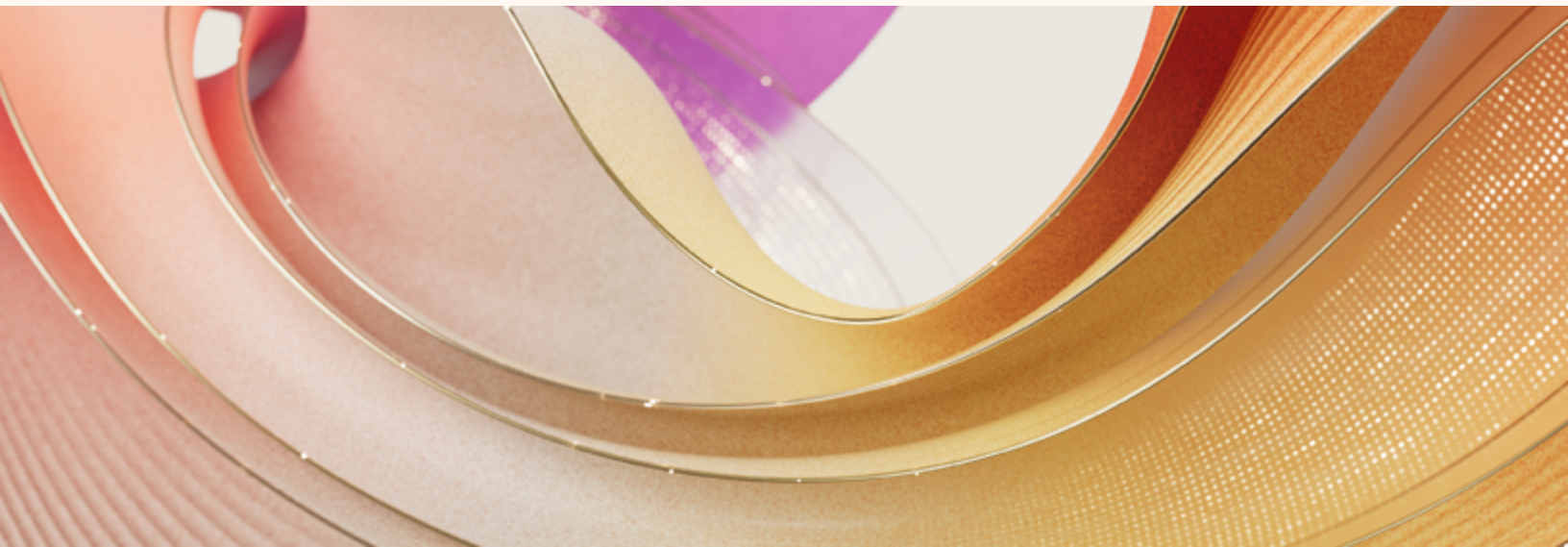
38
AI 價值驅動因素 #4
組織和文化

47
AI 價值驅動因素 #5
AI 治理和安全性

58
Microsoft
身為零號客戶

63
Microsoft
如何協助？

65
結論



如何著手前沿轉型

大多數組織都看到了前沿轉型的優勢及其帶來的好處：在組織內擴展 AI，並善用它來改善業務流程。

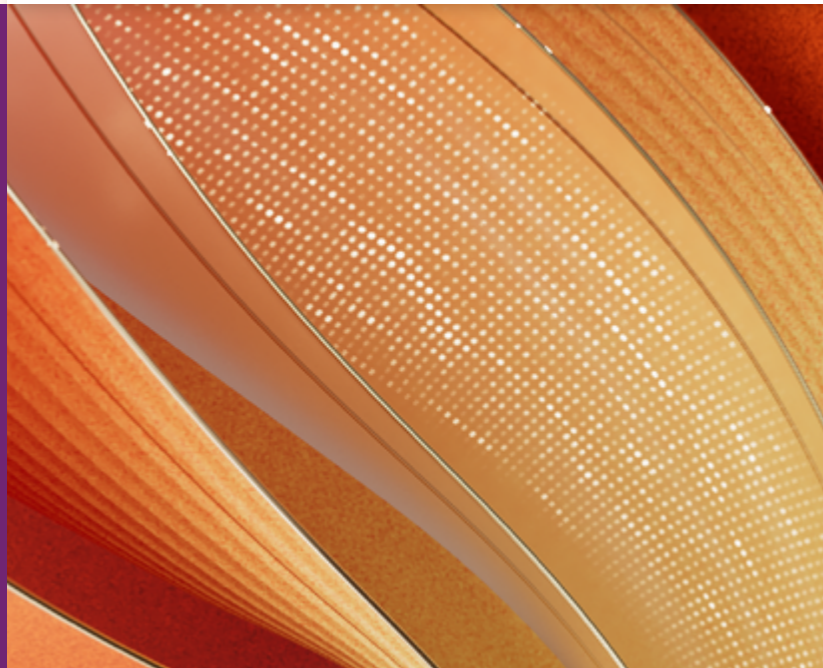
為了充分發揮轉型的效益，您需要採用深思熟慮且反覆的 AI 方法，能提前解決潛在挑戰，並將您的 AI 抱負與技術及組織現實對齊。

前沿轉型帶來了哪些改變

- **AI 成為基礎架構**，並嵌入於所有業務職能之中。
- **人機協同**，員工與 Agent 直接協作成為常態。
- **流程重塑**，將 AI 深度整合至工作流程中。
- **AI 整合至持續性的商業智慧之中**，使決策更快速且更廣泛地去中心化。
- **試驗被全企業規模的執行所取代**，其成功減少對試點專案的依賴，轉而更側重於在全公司範圍內擴展治理完善的 AI 系統。
- **技能與 AI 同步演進**，因為員工在培養 AI 素養的同時，也提升了與 AI 系統高效協同工作所需的人類技能(判斷力、批判性思考、協作)。

歸根結底，轉型意味著 AI 的作用絕不只是單純提高員工生產力或自動化工作流程。它為您的組織導入了全新的能力，讓您可以達成過去無法實現的成果。

> 這一切其實始於一個提問：「我們工作流程中最大的低效率之處在哪裡？」我們當時正審視那些需要耗費大量人工心力的事務，並思考是否有更好的方式來處理它們。
>
> —科技解決方案副總裁，金融服務



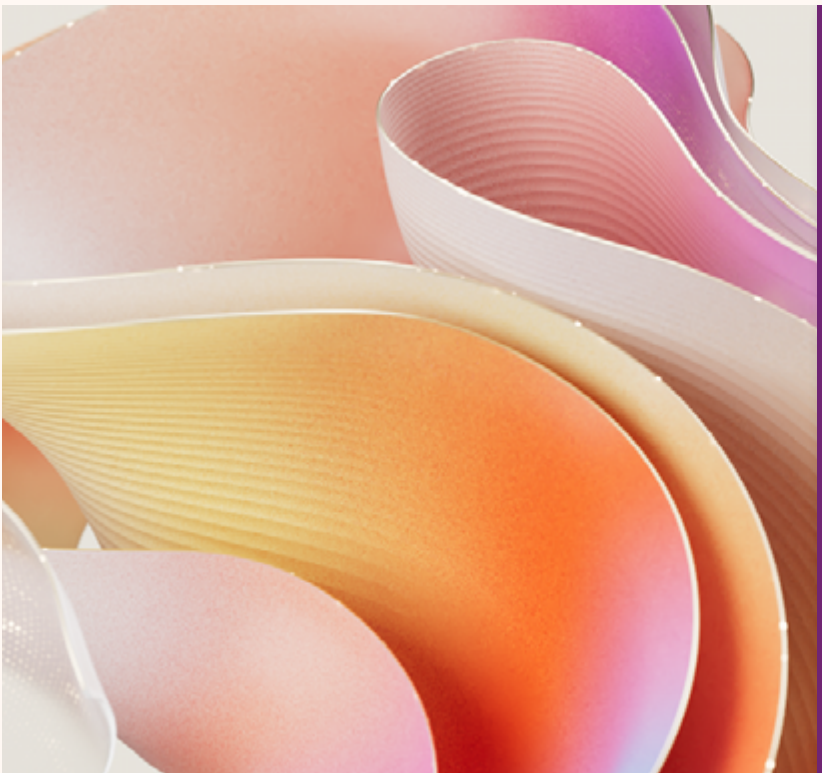
將前沿轉型視為一場旅程，而非終點

前沿轉型不僅局限於科技領域。這是企業創造價值與完成工作方式的根本改變。

從明確的業務目標開始：

- **建立早期動能**，專注於易於追蹤的 AI 成果。這通常意味著從低風險、高量的工作流程開始。
- **透過反覆疊代追求進展，而非追求完美。**面對員工不同程度的 AI 採用率與知識背景，持續且親自參與的實務經驗能建立對 AI 系統的信任，並強化員工有效運用 AI 工具所需的技能與信心。
- **選擇能早期展現 ROI 的使用案例。**高價值的使用案例雖能帶來巨大效益，但往往需要投入大量的時間與資源來應對。
- **將每個專案視為學習平台**，並在執行過程中記錄工作內容與經驗教訓。隨著系統逐步擴展與演進，持續在共享知識庫中更新相關文件。

隨著轉型成熟，試點與驗證週期縮短，治理更加整合，AI 素養提升，信心增強。透過整合明確防護的工具，更多員工成為創作者，能夠安全地打造自己的 AI 工具與 Agent。隨著時間推移，您在 AI 領域的投入將從零散的專案集合，轉變為可複製的系統化運作，進而為整個組織創造持續成長的商業價值。



> 我們長期以來反覆嘗試以傳統方式解決此問題，卻始終未能取得突破。這正是促使我們轉而尋求全新解方的關鍵契機。
>
> —客戶服務副總裁，專業服務

評估 AI 就緒度

組織的 AI 就緒度，亦即擺脫孤立的 AI 試驗，並將 AI 作為基礎商業能力進行可靠部署、擴展與治理的能力，就是前沿轉型成功的關鍵。

建議依據這五個階段來評估您的 AI 就緒度。

探索

在此早期階段，您將探索 AI 的潛力、激發創意構想，並進行低風險的測試。孤立的試點與概念驗證可能展現潛力，但若沒有集中努力，且未在員工間建立早期理解與信心，這些努力無法為整個組織帶來價值。

規劃

在此時，您正努力將重心從純粹的試驗，轉向探索 AI 能為核心業務創造價值的具體路徑。這包括評估並排定使用案例的優先順序、明定成功指標、促進業務與技術關係人的協調一致、建構初步的治理防護，並著手檢視擴大採用所需的職能強化與變更支援。

實施

在此階段，您開始將 AI 解決方案視為「推進中的系統」來進行建構與部署：為其配置成效衡量機制、明確界定權責歸屬，並為決策者明定清晰的成功指標。少數排定優先順序的使用案例將邁入生產環境，讓您得以驗證系統的可靠性、安全性與實用性，進而幫助員工建立在實際工作流程中運用 AI 的信心。

擴展

在建立對 AI 的信心與信任後，您將擴展至可複製、具備治理且全企業範疇的 AI 解決方案交付。這包括採用共享平台、可重複使用的資產、一致的生命週期管理以及更廣泛的技能提升，以便讓新的使用案例能更快速交付、更廣泛採用並更有效地擴展。

實現

AI 已完全嵌入並轉化為核心商業能力，其價值也持續獲得衡量與最佳化。由 AI 賦能的工作流程已成為標準常態、領導階層充分信任其產出結果、治理機制成熟且具備可審計性，而全體員工亦具備相關技能、信心與營運節奏，能持續進行反覆疊代並創造複合價值。

擁抱推動 AI 就緒的五大驅動因素

我們已明確界定出五大核心驅動因素，這些因素能持續協助企業組織運用 AI 在其整體業務中創造價值：

商業策略	AI 的投入與可衡量的商業策略及清晰願景緊密連結，這有助於領導階層針對 AI 倡議進行排序、資助並安排工作先後順序。
技術和資料策略	健全的技術與資料基礎有助於將試驗系統轉化為可擴展的核心能力。
AI 策略和經驗	有計畫且循序漸進的導入能建立使用者與領導層的信任，促進持續採用，並帶來持續的商業成效。
組織和文化	有計畫的變更管理、領導願景，以及新營運模式的開發，有助於推動 AI 的採用並創造價值。
AI 治理和安全性	強健的治理與安全規範能建立信任、促進採用，並提升利用 AI 系統進行擴展與自動化的信心。

這些驅動因素共同構成了實用且相互關聯的框架，可用於評估您目前的現況，以及您需要採取哪些行動才能繼續邁進。當並行開發時，您的團隊能更快行動、管理和緩解風險，以及實現 AI 的全部價值。

"

我們目前正處於實施階段，但內部技能、資料安全，尤其是投資報酬率不明的挑戰，正在拖慢進展。我們需要更清晰且貼合業務的使用案例，來推動跨單位的擴展。

—銷售部門全球副總裁，
製造

AI 價值驅動因素 #1

商業策略

前沿企業從一開始就將 AI 使用案例與商業策略、IT 及治理團隊保持一致。他們從明確的業務問題出發，設計 AI 工具與 Agent 來加以解決，並衡量投資報酬率。

初期的 AI 專案通常是負責自動化處理低風險、高產量任務的 Agent，其投資報酬率極易衡量。透過反覆取得小規模的成功、建立治理機制並進行團隊訓練，這些專案將逐步演進為整合式的工作流程。這並非一個「全面汰換」的過程，而是點滴重構，並在推進中不斷累積信心。

與您的 AI 投資策略保持一致，使用案例將透過不斷提升的成功經驗進行疊代，最終演進為與您商業策略融為一體的關鍵系統。

當 AI 投資與策略性商業成果及可衡量的影響保持一致時，便能實質釋放商業價值。



"

我們一開始並沒有一個龐大且完整的 AI 策略。這更關乎於找出一個我們能務實做出改變的單一領域，並在該處率先進行測試。一旦我們有了初步成果並能展現具體的效益，這就成為協助我們進一步擴充規模、並帶動他人共同加入的關鍵。

—成長行銷資深副總裁，
金融科技



評估 AI 商業策略

您是否具備端對端的 AI 營運模式，並對高價值使用案例排定清晰的優先順序？深入瞭解您目前的就緒程度，並檢視下一階段的成熟度，以明確界定您應該在哪裡投入時間與資源。

無明確方向的試驗	企業級 AI 策略的基礎	AI 於商務規劃中的應用	由領導階層引領的大規模 AI 策略	AI投資與產品組合管理
• 領導階層參與度有限 • 商業集團中的試驗性 AI 專案 • 最少投資 • 不明的商業價值	• 明確的 AI 目標 • 優先考慮使用案例 • 可衡量的成果	• 由商業計畫驅動的 AI 專案 • 組織層級追蹤的 ROI 與 KPI	• AI 倡議擴展至整個組織 • 領導階層定期檢討績效	• AI 完全整合至商業模式與決策 • 可衡量的全企業 ROI • AI 做為商業能力

決定後續步驟

根據您目前的現況，下一步該如何採取行動，以建構出具備優先順序及高價值使用案例的端對端 AI 營運模式？

建立您的 AI 願景並識別使用案例

缺乏這些要素，AI 的投入往往會走向碎片化。在我們訪談過且面臨 AI 執行複雜度困境的組織中，有 15% 指出缺乏高階主管支持與策略一致性是推動 AI 的阻礙。

您不需要一份完整的 AI 宣言來啟動，但即使在前沿轉型旅程的早期階段，擁有一個能提供清晰、一致性與持續執行力的願景，以及具備可衡量 ROI 的 AI 使用案例，仍然會帶來益處。

> 我們理解 AI 具備核心價值，然目前仍處於導入初期，正積極探索其綜效的衡量機制。現階段各項推進工作分散於各團隊，因缺乏統一的策略指引，導致資源重疊與協同效應不足。
>
> —資訊科技副總裁，零售

探討 AI 願景的核心要素

您的 AI 策略願景應包含這些要素。

高階主管的支持。在取得實質進展的組織中，高階領導者所做的絕不僅止於批准 AI 倡議。他們持續參與其中，積極捍衛各項倡議、強化優先事項，並要求團隊對成效負責。這種支持不僅賦予了創新的權限，也讓最關鍵的核心事務變得清晰明確。

AI 與企業優先事項之間的明確連結。超過 70% 擁有先進策略與執行就緒度的組織表示，領導層傳達的 AI 願景與商業策略明確一致。[2]他們清楚為何投資 AI 及其支持的商業成果，並且在短期投資報酬率計畫與長期、高風險的投資間取得平衡，這些投資能改變組織的運作與競爭方式。

企業核心關鍵指標。
前沿企業在著手實施前會明確成果，聚焦於清晰且可衡量的指標，並持續聚焦於目標。期望的成果可能相當簡單，例如降低通話量或提升內部流程效率。只要 AI 價值能轉化為看得見、可追蹤的業務成果，就會持續列入決策層的議程。

員工能力與技能培養。組織定義如何建立 AI 素養、角色導向技能及持續學習計畫，以支持大規模採用。

審慎的資金決策。成熟的組織不會將 AI 投資分散在無關聯的計畫中，而是優先為與關鍵業務流程相符、且能帶來明確成效的使用案例編列預算。為了在短期內展現成果並持續推動 AI 策略，他們在「已驗證、能快速帶來回報」的投資，與「高風險、需長期發展但能徹底顛覆組織運作與競爭方式」的投資之間取得平衡。

主動風險管理。有效的 AI 願景，必須明確應對其技術帶來的潛在風險。這些風險涵蓋了資料隱私與安全、模型偏見、合規性，以及營運可靠性。前沿企業將風險管理責任內部化，及早預見這些挑戰，並制定明確的風險管理框架、權責歸屬與因應策略。他們將討論焦點從*「我們該做嗎？」*轉向*「我們該如何安全地執行？」*

對負責任 AI (RAI) 的承諾。領先組織從一開始就將 RAI 原則直接融入策略，確保公平、透明、隱私、安全與問責貫穿每個 AI 專案。透過將 AI 計畫與明確的倫理標準及風險管理實踐相結合，他們建立了廣泛採用所需的信任、降低了法規與聲譽風險，並樹立了大推進規模創新的信心。

具備這些元素後，您的 AI 願景將指引您優先推動能實現商業效益的 AI 計畫。

[2] Microsoft Agent 就緒度調查，2025 年 9 月。

從小規模開始，選擇具體且容易評估的使用案例

儘管起點各異，所有前沿企業最終都會聚焦於單一、可成且可衡量的使用案例，從試驗走向實際執行。他們不會立刻建立大規模的 AI 開發計畫。相反地，他們從一個易於衡量的單一使用案例開始，藉此幫助團隊建立實務技能與信心，並為更廣泛的採用奠定基礎。

評估內部流程以優先排序使用案例

若要選擇首個使用案例並設定其他案例的優先順序，請先從識別與評估內部流程開始。那些產生最多摩擦、成本或風險的流程（例如耗時或低效的工作流程），正是 AI 使用案例的理想選擇，能在短時間內帶來顯著的投資報酬率。

您可以確信，這些使用案例在實務上完全可行。考量資料與系統互動的複雜度、安全與合規要求，以及具體成果如何與投資報酬率、效率、品質或合規性與企業優先事項相呼應。

在您的第一個使用案例中，您希望能快速取得有意義的成果，並能以此為基礎持續推進。

隨著 AI 相關計劃的擴展，利用這些標準評估 AI 使用案例，將協助您實現工作流程現代化，並釋放代理部署的價值。



> 讓我們選擇一個非常具體的使用案例，明確知道什麼是良好的成果，並以此為目標推進。
>
> —科技解決方案副總裁，金融服務

將 AI 嵌入商業計畫並追蹤成果

您的第一個使用案例會帶來小小的勝利和明顯的投資報酬率。在執行的同時，同步規劃全企業 AI 業務計畫：建立流程以持續推動高優先級使用案例，並制定指引以協助安全擴展。

建立一套基於商業標準的使用案例優先排序框架

建立一套涵蓋可行性、風險與商業價值的使用案例優先排序流程，並將其全面應用於全公司。在全公司範圍內一致評估各項使用案例，有助於促進廣泛參與並提升產品組合層級的能見度，從而幫助您管理與擴展 AI 策略。

每個選定的使用案例都應符合以下標準：

- 它解決了一個商業難題。
- 風險已完全釐清且在可管理範圍內。
- 使用案例與策略優先事項相符。
- 它非常適合 AI。
- 您可以在進行擴展前，先驗證其成效。
- 您可以在保持全面掌控的前提下，建立可複製的擴展循環。
- 資金與人力充足。
- 您可以贏得高階主管的支持與關注。

如果您想採用現有的優先排序框架，Microsoft AI 決策框架 (有時也稱為商業、體驗、技術，簡稱 BXT 決策框架) 將協助您從三個面向評估代理的使用案例：商業影響、體驗與技術可行性。綜合這些因素評分後，您可以挑選出能創造價值、被使用者接受且能安全實施的使用案例。



建立 AI 的商業案例

- 針對高價值的使用案例，可以考慮那些具重複性、以規則為基礎，但仍需要人工判斷的工作。
- 評估現有的工具與流程，找出 AI 能帶來整合資料與簡化工作流程機會之處，實現目前無法達成的目標。
- 將使用案例整合至現有工作流程。
- 探索可以逐步重新改造的現有流程。

隨著使用案例獲得批准且確保高層支持，請將已批准的使用案例整合到您的業務策略中，並納入組織的 AI 產品組合。

代理型 AI 使用案例及跨業務功能的衡量指標

AI 的價值集中於重複性高、耗時且以規則為基礎但需具備判斷力的工作，當 AI 應用於業務關鍵的工作流程並有計劃地擴展時，能夠發揮最大的價值。代理型 AI 使用案例能在核心業務功能中帶來顯著的投資報酬率。

	Agent	ROI
客戶服務	• 自助式 AI 助理 (支援任務) • 全天候 AI 助理 (問題解決)	• 減少來電量 • 縮短處理所需時間
銷售	• 銷售 AI 助理 (潛在客戶開發) • 提案請求 (RFP) 回應自動化 (客戶參與度) • 全天候銷售 AI 助理 (客戶參與度)	• 提高交叉銷售和追加銷售 • 提高平均銷售 ROI
人力資源	• 問 HR (員工參與度) • AI 支援的候選人搜尋 (招聘) • 招聘 AI 助理 (人才管理)	• 降低每人招聘成本 • 縮短上線時間 • 降低每位新招聘同仁所耗費的 HR 工時
法律	• 自動化合規管理 (合規性) • AI 最佳化的合約管理 (合約) • 諮詢法律專家 (諮詢服務)	• 每份合約所需的律師工時減少 • 縮短記錄審閱時間
IT	• AI 賦能的應用程式現代化 (IT 營運) • AI 資訊服務台 Agent (IT 營運) • AI 驅動的評估與調解 (安全性與合規)	• 減少 IT 作業負擔 • 減少未計劃停機時間 • 縮短解決問題的時間

定義可衡量的結果

您會發現 AI 能夠承擔各種任務，帶來可衡量的效益。

提高生產力：自主完成多步驟任務，減少對人工監督的需求，並讓團隊成員能專注於更具策略性的工作。

成本節約：接管固定的工作流程，以減少營運負擔、手動例外處理及額外負擔，推動顯著且持續的成本效率。

提高正確性：在可變或模糊情境下，根據詮釋、情境評估與動態驗證做出決策，減少傳統規則自動化無法偵測或處理的錯誤。

進階合規性：持續監控行動，根據背景關聯應用原則，並即時上報異常事件。解讀法規要求，以減少人工或靜態自動化流程中產生的合規缺口。

更好地協作：做為能夠理解人類意圖、跨系統協調並與其他 Agent 協同運作的智慧隊友，進而最佳化溝通流程，並減少跨團隊與跨部門之間的摩擦。

更穩固的安全性：主動評估模式、偵測偏差並自主執行安全規則，強化安全性態勢，超越靜態存取控制或預設規則集。

更快的處理速度：Agent 能夠自我策劃端對端的流程，在無需等待人類輸入的情況下解決模糊之處並處理邊緣個案 (Edge Cases)，加速複雜流程的完成時間。

精簡決策流程：Agent 能夠自動執行研究、分析回饋並產出競爭洞察，為您的團隊摘要所需細節，以利更快速地做出明智決策。

可擴展性：Agent 能擴展認知工作的規模，而不僅僅是處理可重複的任務。他們協調任務、分配工作負載，並因應需求調整，且無需相應增加人力或自動化工程資源。





在領導階層的積極參與下擴展 AI 倡議

成功的組織將 AI 計畫視為受管理的產品組合。他們持續評估績效、資金與目標的一致性。透過反覆取得小規模的成功，他們逐步建立對 AI 的信任，並發展出健全的治理與營運實務。

評估您的 AI 產品組合

在不同團隊和專案之間，組織通常同時處於多個階段。成功擴展 AI 的企業不會將倡議視為單一專案。他們將這些倡議作為產品組合來管理，並進行明確的監督、績效追蹤，以及根據條件變化進行再平衡。

確認建立擴展信心是一個漸進的過程。資料就緒度是組織投資於使用案例的基準。成功的使用案例會帶來更多業務量。變更管理能提升採用率，進而促進更進一步的擴展。在此過程中維持能見度，則能建立信任。

請準備好評估您目前的 AI 產品組合現狀

- **是否有監督與重新平衡的策略？**為了策略性地分配資源，您應定期考量績效、與組織策略的一致性，以及時間框架，以確保最大化投資報酬率。
- **您是否有整體的 AI 投資計畫？**為確保關鍵 AI 專案獲得所需資金與綜效支持，您應制定明確的資源配置計畫，以利於各專案間進行精準的預算與資源調配。投資計畫可以加速專案交付、彰顯高階管理階層之決心，並有效降低資源過度分散之潛在風險。
- **您是否定期檢視產品組合？**定期檢視能提升您的產品組合管理的敏捷性，讓您有機會因應業務需求變化、技術開發及專案里程碑，進行改進、調整方向、注入新活力，甚至暫停。
- **您是否有記錄並分享經驗教訓？**這在 AI 旅程初期尤其重要，儘管每個階段都應該利用成功與挫折，讓未來走勢發揮最大效益。善用經驗教訓，有助於組織減少錯誤、有效投資，並加速業務轉型。



整合整個企業的 AI

隨著 AI 採用的擴展，您將可望在各項 AI 使用案例與成熟專案中，洞察出具備共通性的核心主題。成功擴展規模，仰賴持續的高階主管支持、積極且全盤掌握的推進、潔淨且具公信力的資料、可靠的治理機制、具備策略性的持續資金投入，以及建立於具體成果之上的信任。

深化 AI 信任機制，以加速推動規模化採用

隨著 AI 採用率的提升，深化信任機制已成為擴大組織影響力的核心根基。

在組織內部，隨著 AI 系統展現精準度並接管更多日常工作負載，信任機制將逐步深化，進而加速推動規模化採用。員工有更多時間專注於策略性與創意工作。

隨著信任機制獲得實證，各項應用程式與 Agent 將陸續推向客戶，此舉能有效提升客戶滿意度、減輕客戶服務同仁之工作負載，並為解決更具複雜性的客戶議題爭取充裕時間。

在整個企業內部，各項 AI 倡議已開始跨團隊與跨業務功能落實規模化擴展。

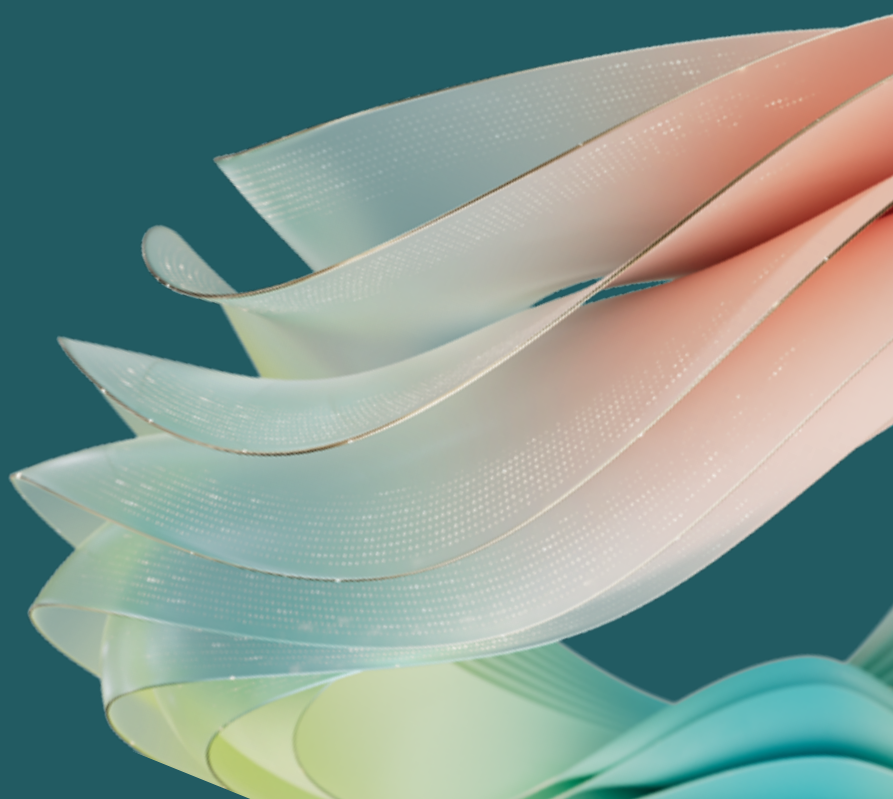
AI 已完全嵌入組織策略與價值創造之中。做為關鍵的競爭鑑別因素，AI 已成為公司願景的核心。AI 倡議均能交付可衡量且具備可複製性的價值。

隨著 AI 應用逐漸擴展，積極宣傳您的成效

此時正是定義如何衡量全公司 AI 倡議價值的最佳時機。建議於高階管理階層導入計分卡或儀表板，以落實監控 AI 計畫之關鍵績效指標，其範疇涵蓋風險降低與治理機制。

隨著規模化擴展，已建置的 AI 流程已成為組織營運之核心脈動。

- 高階主管持續提供支援，定期檢視 AI 專案組合與成果。
- AI 策略獲得資金、監控與重新平衡，隨著進展及商業與競爭需求變化。
- 使用案例均定期透過一致性架構進行優先順序評估。
- 既有經驗會整合至產品組合與流程中。



安全且有效地擴展

為了在擴展過程中保持控制，前沿企業採用以下策略：

一次聚焦擴展一項商業挑戰。
從狹窄且明確的使用案例開始。避免大規模推展，以免增加風險與複雜度。

先驗證成功後，再著手擴展。
及早衡量效能與成果，使用明確指標建立信心，再轉向下一個使用案例。

運用透明度以維繫信任。
明確的防護、人工監督以及可見度的效能表現，有助於在 Agent 規模化擴展時建立關係人的一致性並減少阻礙。及早將法律與合規納入討論，利於消除障礙。

建立可複製的擴展循環。
每個成功的 Agent 均為資料、治理與工作流程確立了標準範式，進而促使後續部署更臻高效與便捷。隨著文件逐漸完備，重複利用的效益將顯著提升。

預見障礙

管理創意流程。太多想法若沒有明確的起點，會讓人感到壓力過大，導致停滯不前。

保持衡量機制與進度的透明度。當投 ROI 未被察覺或顯得抽象時，領導階層將對大規模的資助黑箱試驗感到遲疑。

協調 IT、治理與業務團隊以確保核准與部署。越早讓所有關鍵人員達成一致，效果越佳。

識別可能抗拒的關係人，並及早回應其疑慮。風險規避型關係人可能涵蓋法務、資訊安全、財務，以及其他可能對 AI 安全、職涯衝擊與 ROI 感到憂慮的同仁。



> 您必須在初期即全面審查架構、安全與風險，以確保各項要件達成一致性。一旦該根基建置完備，後續推動解決方案並取得業務單位的共識與支持將更臻高效。
>
> —資訊科技副總裁，零售



達成目標：AI 已嵌入策略與價值創造

您已達到 AI 蔚為企業核心能力之成熟階段，並已全面嵌入至企業願景、商業模式與決策架構之中。

- AI 做為驅動投資報酬率之核心要素，透過企業級範疇之綜效衡量，不僅能交付具備可複製性的價值，更可望締造關鍵的競爭鑑別因素。
- 做為企業策略的一環，AI 投資與目標已納入組織各項規劃流程，並向高階主管層級報告 AI 相關計畫。
- AI 投資計畫會定期檢視，根據優先順序及預期回報來定義預算與資源配置。
- AI 計畫透過投資組合方法進行管理、審查與再平衡。(組織通常會加倍投注資源於具備實質成效之 AI 倡議，並針對成效不彰之項目採取暫停或最佳化調整之措施。)
- 所有 AI 導入皆已納入治理、符合合規要求且具備安全防護。相應的流程與防護機制均已建置完備，以利您持續擴展 AI 能力，進而支援全新業務領域、市場拓展、團隊編制、產品開發等多元維度。
- 您的規模成長將不再受限於員工人數。相反地，您可透過軟體擴充營運產能，以利在調適市場需求之際，具備處理更高工作業務量與彈性調配工作負載之能力。

以自信的行動取代猶豫

- **不要等到完美才開始行動。**前沿企業運用現有技能與基礎結構推動發展，並在過程中不斷學習與成長。
- **儘管存在不確定性，仍要採取行動。**前沿企業透過推動用例，揭示並解決風險、治理及整合問題，而非預先消除這些問題。
- **以行動代替言語。**早期部署應聚焦於對 AI 最具開放態度的用戶和團隊。當員工看到 Agent 減少繁瑣的人工工作並協助他們的工作職責時，抵觸情緒會降低。
- **將早期的 AI 努力轉化為可重複的系統。**充分利用早期成果、間接 ROI、高層支持，以及 AI 擁護者，持續維持成長動能並加速擴展。接著推進新的、更複雜的應用場景，並加快擴展速度。

AI 價值驅動因素 #2

技術和資料策略

當資料值得信賴，且技術基礎結構專為規模化擴展而設計時，AI 即轉化為具備可複製性的核心能力，而非流於一系列孤立的試驗項目。憑藉這個基礎，您能交付穩定的成果，將 AI 融入組織，並產生可衡量的商業影響。

在著手擬定技術與資料策略時，請務必謹記以下核心要點：

將資料就緒度視為先決條件。在擴展 AI 能力之前，必須先解決資料品質、身份與存取控制，以及治理問題。

逐步建立並連結基礎結構。早期的 AI 使用案例可能需要極少的資源與系統間的整合。只有在 AI 工具和 Agent 的可靠性被證明後，才將它們整合進更廣泛的基礎結構中。



先打穩基礎，再著手擴展 AI 能力。一旦建立完成資料管線、治理模式和監控系統，就能以更快、更安全的方式擴展 Agent 和系統。



"

從一開始就建立完善的資料、基礎結構和資安架構非常重要。您必須考慮想要外掛的目的地，這些資料來源將會如何。

—科技與網路安全副總裁，零售

評估您目前的技術與資料就緒度

您的資料基礎、基礎結構與 IT 團隊是否已準備好負責任地擴展 AI？深入瞭解您目前的就緒程度，並檢視下一階段的成熟度，以明確界定您應該在哪裡投入時間與資源。

新興資料基礎	基礎建構	可投入正式環境的平台	全企業基礎結構	持續最佳化
• 資料分散孤立或品質受限 • 除了個別試驗，沒有專屬的 AI 基礎結構 • 開始評估資料，並建立代理型 AI 所需的平台	• 推進資料就緒，建置初步 AI 基礎結構 • 著手建置雲端、混合式及內部佈署資源、資料湖、沙箱環境，以支援代理型 AI 使用案例。	• 備有穩健且可擴展的資料與 AI 平台，可大規模部署 AI 解決方案 • 資料管線摘要正式環境 AI 模型 • 工具與環境，可靠支援模型開發、部署與監控	• 資料平台整合統一，服務多個團隊 • 代理型 AI 解決方案與企業級系統整合，並嵌入業務流程中 • 基礎結構能安全且高效地處理大規模即時 AI 工作負載	• 資料架構與 AI 基礎結構持續最佳化 • 新興 AI 技術能夠快速採用，並享有資料平台及工具支援 • 資料視為策略資產，推動持續的 AI 創新

決定後續步驟

根據您目前的狀態，您可以採取哪些步驟來建構可擴展且治理完善的資料與技術基礎結構，以支持日益增長的 AI 採用工作？

評估您的資料品質與 AI 就緒度

在探索階段，常常會發現資料是碎片化的，或需要大量人工整理，才能讓 AI 系統使用。若無法系統性地依賴資料品質、一致性或治理，AI 成果將可能不可靠、難以擴展，且難以信任。

有了可信、統一且治理完善的資料基礎，您的 AI 工具與 Agent 便能超越孤立的試點，可靠地擴展至安全、可重複的企業級能力。

若要為 AI 準備好資料與系統：

執行正式的資料成熟度評估。

- 審查您目前擁有的資料、其存取方式以及使用方式。
- 制定結構化且全盤的評估機制，以便在對您的 AI 使用案例造成問題之前，即先識別出資料品質、可用性與治理機制上的差距。

識別並解決支援您的使用案例所需的資料缺口。

- 記錄您所需的資料，其範疇涵蓋系統、記錄與屬性，以落實確保輸出結果之可靠性。
- 評估這些資料並找出缺口，例如缺失欄位、孤立的來源、有限的存取權限或不一致的標準。
- 識別輸入、輸出，及支援系統所涉及的資料與技術接觸點及其依賴關係。
- 制定計畫以彌補這些缺口，包括資料清理、整合、治理及持續維護。

合理化並現代化處理舊版資料。

- 辨識舊版資料來源與技術債。這類情況可能包括存在於過時平台、分散架構及不一致資料結構中的資料，這些都讓 AI 系統難以處理。
- 考慮現代化選項，例如再平台化、重構、歸檔或淘汰舊版資料集與系統。
- 將您的資料整合到具可擴展性且統一的現代平台中，這些平台支援標準化架構、完善治理，以及支援 AI 的雲原生能力。

建立統一的企業語意模型以應用於資料。

- 為核心業務實體定義一致的語意模型；例如，確保系統與團隊中對*客戶*、*訂單*和*區域*等概念有共同定義。
- 識別並解決資料在不同來源間定義與使用上的不一致，消除可能導致 AI 輸出不可靠的衝突。
- 標準化處理，並集中管理資料定義，使 AI 系統能正確解讀資料、跨使用案例擴展，並持續提供準確的輸出。

> 理論上，我們擁有所有需要的資料，但資料分散在不同系統，且品質不一定一致。我們必須建立一個結構，決定何時使用哪些資料，否則輸出就不可靠。
>
> —成長行銷資深副總裁，金融科技



著手開發 AI 就緒的基礎結構

如果已經進入規劃階段，則表示您已經開始建立資料就緒度的工作。您的下一個優先事項應該是為 AI 就緒的基礎架構奠定基礎，以支援持續的 AI 開發、部署與大規模營運。這個基礎結構應具備下列能力：

可擴展性，讓 AI 工作負載能隨著需求增加而擴展。

預設應有的安全性與身分，以便持續保護資料與行為。

可靠的資料存取，明確的邊界與受治理的整合。

營運可見度，可透明檢視效能、使用與成本。

彈性，支援混搭低程式碼、專業程式碼與套件解決方案。

成功的組織會逐步建立能力，在每個階段證明可靠性與治理，然後再擴展。轉型初期必須規劃能支援廣泛採用 AI 的基礎結構。

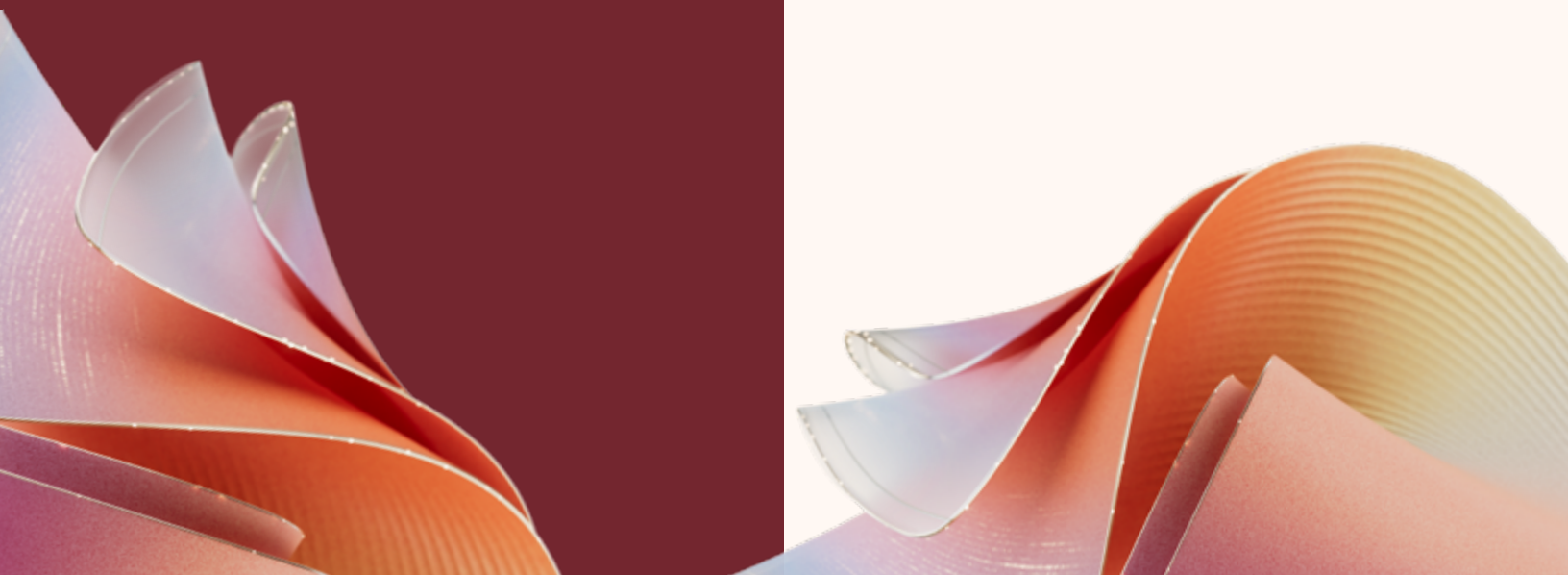
當您開始建立自己的 AI 基礎結構時：

及早著手資料治理。

- 為了能夠安全、可靠且放心地擴展 AI，建立涵蓋整個資料生命週期的治理，包括擷取、模型訓練、推論與營運。
- 將資料治理視為推動安全創新的途徑，而非限制或阻礙您的團隊運用新技術的框架。
- 於組織層級建立明確的權責歸屬、標準與資料管控機制，以利在確保安全性的同時，促使 AI 工具與 Agent 的開發與部署更臻高效與便捷。

採用受控的平台。

- 共享的受控 AI 平台提供一個共同的基礎結構，用於在組織中建置、部署及管理 AI 模型、應用程式與 Agent。
- 平台能減少重複建置，並可對所有 Agent、工具及資料連線進行集中管理與治理。
- 這同時有助於規模化擴展：模型、資料與見解可在多個使用案例中重複使用，同時落實一致的企業級治理與生命週期管理。



開發適用於 AI 的最佳化「雲端登陸區域」。

- 使用標準模式與配置，建立具備內建網路、身份、安全與政策控制的部署環境。
- 標準為具備可擴展性的 AI 提供結構化起點，以利為 AI 解決方案建立安全且可擴展的基礎結構。
- 於登陸區域設計中納入 AI 需求考量，有助於降低延遲問題、成本激增、模型行為不一致及安全缺口之風險。

標準化處理一致的 AI 整合框架。

- 採用可重複使用的整合框架 (例如：模型背景關聯協定 (MCP)、OpenAPI 或類似的企業連接器) ，能大幅縮減將全新 AI 工具整合至系統中所需的時間與心力。

更新您的成本管理實務。

- 由於 AI 採用率可能迅速擴展，且計價方式依模型與工作負載類型而異，因此微小的設計抉擇皆可能產生巨大的財務影響。請於初期針對成本效益進行設計、持續評估採用模式，並隨著系統演進不斷精煉設計決策。請持續且有意識地對營運進行最佳化處理，而非待預算超支後才著手應對。

共享 AI 平台功能

應優先採用共通功能，而非自訂功能。不要為每個試點專案重新發明輪子。相反地，盡量減少重複與營運負擔，讓團隊能專注於資料與功能。

標準化的安全與身份模式透過提供一致的保護與存取控制，建立信任，並能隨使用量擴展。

共通的整合框架使 Agent 與應用程式能一致且安全地連接資料及其他系統。

可重複使用的營運實務，包括監控、成本管理和生命週期管理，幫助您更安全且可靠地擴展 AI 系統。

有了這些共享基礎，團隊能隨著時間加快進展，因為每一項新的 AI 計畫都是建立在既有基礎之上，而非從零開始。隨著 AI 的採用規模逐步擴大，這些基礎結構亦將相應成長。



獲取並擴展 AI 能力

當您推進將 AI 整合至組織時，請決定如何以最佳方式建置與擴展 AI 能力：這需要透過培養團隊採用與交付 AI 解決方案所需的專業知識，以及針對何時該採取採購、延伸或自行開發做出審慎的決策。

規劃所需的 AI 專業知識

您可以透過多種方式獲取並培養成功轉型所需的 AI 專業知識。

策略性合作

外部合作夥伴如果能帶來經實證之範式、深厚技術專業以及從其他轉型中汲取實務經驗，可協助您加速自身轉型的推進。合作夥伴於初始平台設計、治理架構建置，以及內部團隊尚無能力應對的複雜整合與部署項目中，尤能發揮關鍵綜效。

外部廠商雖能加速專案推進，但決策權責、治理優先順序、風險評估以及問責機制仍必須保留於組織內部。目標在於迅速啟動推進動能並奠定堅實根基，同時隨著時間推移，持續培養內部團隊的專業技能、信心與領導能力。

考慮在以下情況下引入外部合作夥伴：

- 您已識別出具備發展潛力的 AI 使用案例，但內部團隊仍無法確定切入點，亦不知如何將既有構想轉化為實質的商業價值。
- 您正面臨固定的時程壓力，或者轉型進度已顯著落後於競爭對手，且缺乏能迅速趕上進度所需的專業知識或技能。
- 您的業務流程讓供應商能透過現成即用的方式迅速推進。
- 為了部署或規模化擴展 AI 解決方案，您需要只有經驗豐富的合作夥伴才能提供的專屬支援與龐大資源。

內部訓練

邁向長期 AI 成功的最穩固途徑，涵蓋在設計、部署與維運 AI 系統方面建立深厚的技術專業。在理想狀態下，技能提升應跨越技術職能與商業領導階層。此外，其範疇不僅需涵蓋 AI 工具的運作原理，更需包括何時及為何使用這些工具、如何解讀輸出結果，以及何處仍必須仰賴人工判斷。

若符合以下條件，請考慮在現有同仁中建立 AI 專業知識：

- 您的企業文化積極聚焦於 AI，且您希望現有同仁在組織內部廣泛擁抱試驗精神。
- 您正處於具備競爭優勢的市場地位，擁有充裕時間提升同仁技能以支援更廣泛的採用。
- 您的業務具備複雜性或獨特性，因此訓練內部同仁掌握 AI，相較於向外部人員傳授您的業務知識更為容易。
- 預算限制了額外人員名額的增加，或限制了對外部顧問的龐大投資。



聘請專家

專家可協助您引導初期的設計決策、規避常見誤區，並建置強固的技術與治理根基。新進員工唯有在融入既有內部團隊時始能發揮最大效益，以此落實知識的傳遞與建構，而非僅是孤立地運作。

請在下列情況下考慮聘請專家：

- 您的企業文化樂於整合新專業知識，並能更廣泛地分享專家知識。
- 您需要迅速獲得所需技能，才能讓組織從競爭對手中脫穎而出。
- 您能讓新進人員在短時間內熟悉業務，並開始做出實質貢獻。
- 您負擔得起聘顧額外人員。

最終，當專業知識融入整個組織時，前沿轉型才能成功。藉由適當的人才配置與外部支援，您將能創造出充分受惠於 AI 的卓越條件。

這些抉擇絕非全面性、排他性或永久不變。需求會持續演進。各項使用案例、Agent 或 AI 系統，皆可能需要不同的人才配置、訓練機制與合作夥伴支援。



明確掌握何時應採購、延伸或建置自訂 AI 解決方案

自訂開發雖具備強大潛能，但其成本高昂且難以在規模化擴展時維持。同理，完全仰賴現成工具則可能受限於自訂彈性，導致 AI 無法實質最佳化組織營運。成功組織的策略是採購無需具備獨特性的部分、在已有信任與整合基礎的受控平台上進行延伸，並僅在預期回報足以證明投資合理性時，才開始建置自訂解決方案。

AI 服務通常涵蓋一系列的努力、控制與責任範圍：

自備模型。基礎架構即服務 (IaaS) 方法實際上是完全自訂組建。組織選擇模型、管理資料管線、設計架構、實施安全與治理，並全面負責端對端的運作。此方法提供最大彈性與自訂，但同時承擔最高的成本、複雜度與營運負擔。

受控 AI 開發平台。
平台即服務 (PaaS) 解決方案提供管理模型、資料基礎建設、協調與營運工具，同時允許團隊打造自訂 AI 應用程式。這藉由簡化模型、基礎結構與治理管理來平衡彈性與速度，同時仍支援應用程式邏輯、整合及使用者體驗的自訂。

套裝商用 AI 解決方案。
軟體即服務 (SaaS) 解決方案提供現成即用的 AI 能力，其多數功能、基礎結構、安全性及更新皆由平台供應商進行管理。此類方案通常具備最快的部署速度與最容易規模化擴展的特性，使其成為無需獨特自訂標準化工作負載的理想選擇。

在轉型初期，採購或延伸經實證的工具可能是最佳的推進路徑。隨著 AI 嵌入組織業務越深，某些能力可能更值得進行更深度的自訂或完全自主開發。

指導購買、擴展或建置決策的關鍵問題

為了協助決定是否購買、擴展或建置 AI 解決方案，應制定一個包含以下問題的明確決策框架：

- 客製化開發在何處對競爭優勢或策略差異化具備關鍵效益？
- 現有服務與平台是否提供可擴展的整合及自訂功能，讓您無需從頭打造解決方案？
- 解決方案加速器、範本及參考架構是否能幫助您更快、更安全地推進？
- 您是否擁有打造並可持續運作客製化解決方案所需的專業人員、營運模式與治理機制？
- 是否值得引進低程式碼或無程式碼的 AI 工具，讓領域專家能夠打造簡單的 AI 解決方案，以提升或最佳化他們的日常工作？

打造 AI 基礎結構的最佳化與彈性

隨著 AI 工具與 Agent 從開發及測試階段邁向正式上線，其效能表現可能變得難以預測。若未進行積極管理，成本可能會出現偏差。當 AI 系統從試驗性或開發性用途移轉至實質業務流程時，可用性是其中關鍵要素。

專為大規模效能所設計。與傳統應用程式不同，AI 工作負載會產生突發性的密集活動，進而導致延遲激增並提高資源需求。請從初期即著手應對最佳化處理，以便在採用量增加時，各項使用案例能以可預測且具備可複製性的效能表現進行擴展。採用標準化處理的部署模式、於貼近現實的工作負載下進行效能測試，並落實持續監控，以便在影響使用者或業務營運之前偵測出問題。

強化 AI 系統的韌性。韌性的 AI 基礎結構透過容錯回復行為、關鍵與非關鍵組件間的隔離，以及明確定義的復原路徑來因應故障。其核心目標並非提前消除所有可能發生的問題，而是在服務中斷期間仍維持安全且可預測的營運運作。設計您的 AI 工具與 Agent，使其在正式上線規模下交付一致的效能表現；設計您的架構，使其可靠地處理 Agent 運作與多模態工作負載；並設計您的基礎結構，使其在斷線或模型失效期間仍能維持可用性。

建立安全與治理的基礎。隨著 AI 系統的規模化擴展，安全性與治理機制也需相應擴展。請建立一項基準，在您的 AI 環境中提供一致的身份識別管控、存取原則、監控機制以及合規防護。隨著 AI 採用量的增長，請確保此基準獲得持續強化，以落實保護資料、管理風險，並讓系統安全且可預測地營運運作。

歸根結底，最佳化處理與韌性皆攸關信任。組織能信任展現一致效能的 AI 系統。員工能信任維持可用且可預測的平台。而商業領導階層則能信任成本可預測且效益可見的解決方案。



預見障礙

高品質的資料與可擴展的基礎結構決定了 AI 系統發揮實效並獲得認同。當從初期即聚焦於這些常見問題時，全組織內部的廣泛 AI 採用將會加速推進。

高品質資料的存取權決定了 AI 系統可靠性。若缺乏精準且符合使用案例需求的資料，AI 系統恐將產生不準確、具備偏見或不可靠的輸出結果。建置任何 AI 系統不可或缺的首要步驟，就是確保擁有符合特定目的之高品質資料。

您對 AI 的信任度，完全取決於您對資料的信任度。當資料缺乏潔淨度、一致性或完整性時，便無法依賴 AI 系統產出準確且具背景關聯的輸出結果。一旦使用者獲得不一致或低品質的成效，對新 AI 系統的信任感將迅速瓦解，進而導致採用率低迷，並使商業效益停滯不前。

缺乏明確定義的資料階層架構，將使您在推進過程中面臨阻礙。資料散落於多個不同處所是企業常見的現象，但當這些資料出現不一致時，您的 AI 系統究竟該採用哪一個版本？您又該對哪一組數據寄予更高的信任？建立一套清晰、完整的資料集優先順序階層架構，才能引導 AI 系統輸出更具一致性的回覆成效。

基礎結構必須滿足 AI 工作負載不斷變化的需求。若新的 AI 解決方案無法確保可用性、高效能與安全性，AI 的採用進程便可能陷入停滯。隨著您部署更多 AI 系統，基礎結構必須具備擴充能力以滿足需求，並能優雅地處理錯誤或中斷事件。

謹慎評估您如何擴大 AI 存取權限並連結資料集。當 Agent 能夠存取的資料集愈多，其所能執行的任務就愈廣泛。然而，您必須在其中取得平衡，以降低因過度授權而無意間暴露敏感或受保護資訊的風險。

達成目標：AI 技術與資料成熟度

在精心擬定的 AI 技術與資料策略支持下：

- 您的資料已視為策略資產並加以管理，持續為創新注入動能。
- 強大的治理、品質與存取控管已到位，並在各個 AI 使用案例中發揮卓越成效。
- 您的可擴展、具彈性的平台能適應全新工作負載、隨時間推移持續最佳化效能，並在 AI 更深層地嵌入營運流程時依舊維持可靠性。
- 這些基礎結構並非一成不變，而是透過回饋、監控與疊代強化，持續達到最佳化。

在此成熟階段，由於您的資料平台、管線與工具已準備好整合全新模型與功能，您將能以極低的摩擦力快速採用新興 AI 技術。這使您能夠支援更快速的試驗與部署，並在新技術與新流程湧現時持續保持競爭優勢。

AI 價值驅動因素 #3

AI 策略和經驗

隨著時間推移，您的做法將演進為 AI 工廠模式，支援組織所依賴的可靠 AI 系統進行具備可重複性、可擴展的建置與部署。信任感將從單一工具擴展至系統、治理以及其背後的團隊，為持續採用與使用 AI 創造有利條件。

隨著您在組織中擴展 AI 的應用，採取一系列審慎的步驟，將有助於您的員工與高階主管在全新系統和工作模式中累積經驗並建立信任：

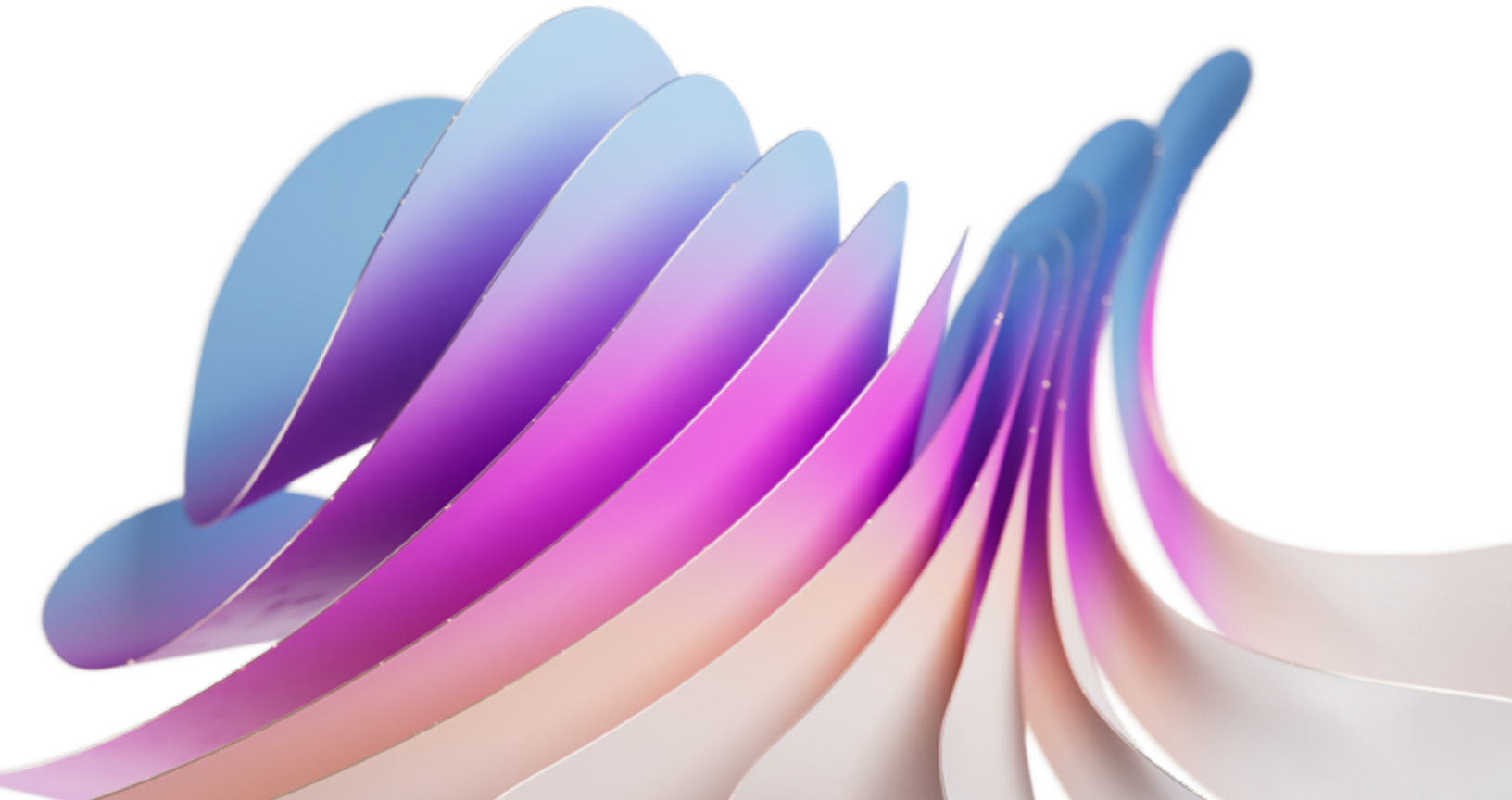
確保高階主管支持。透過讓高階主管全程參與從試驗到大規模採用的每個階段，您將能建立信任感並實證投資的合理性。

在擴大範疇之前，先確立防護機制與合規性。在每個專案啟動之初，即讓合適的團隊共同參與。確保初期的學習成果與基礎結構能夠進行大規模的重複使用。

透過顯著的 AI 成功案例建立信心。首先透過實證您的 AI 系統能有效處理簡單、低風險的任務來展開第一步。

透過誠實透明的溝通， 在全面推出時建立終端使用者的變更論述，將 Agent 定位為提升工作成效與促進成長的工具。

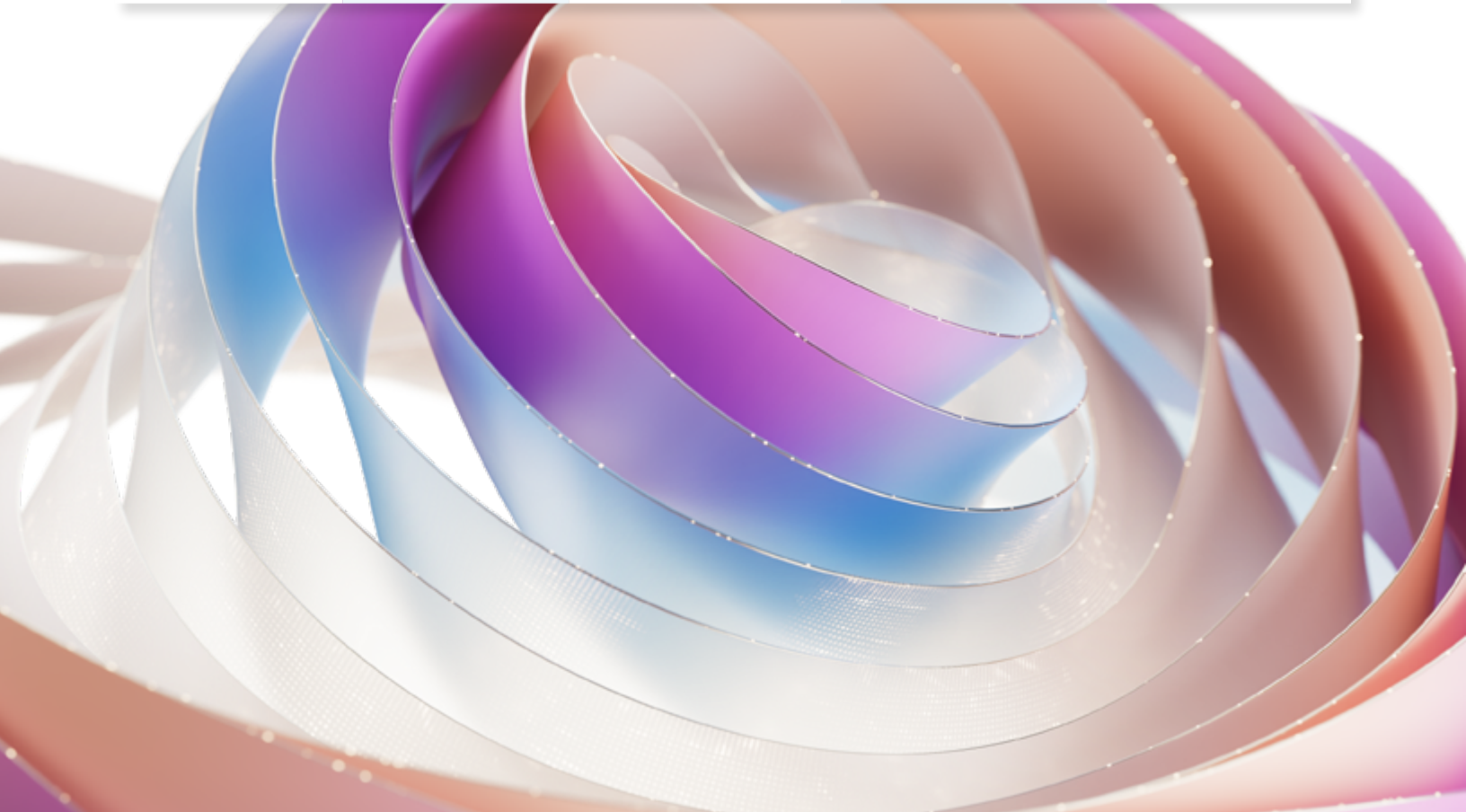
立足於既有基礎推動。在建立信任感並擴大採用範圍之後，將 Agent 應用於改善業務流程的其他步驟，直至實現全面的轉型。



評估您的 AI 體驗就緒度

您的組織是否正在透過部署與使用 AI 系統來累積經驗，以提升高階主管對 AI 系統的信任與信心，同時促進全組織內部的採用？了解您目前所處的就緒度階段，將有助於明確辨識您的下一個策略目標。

有計畫的試驗	結構化試點	營運型 AI 實務	可重複使用且可重用的 AI	創新與進階
• 少數個人或團隊正在執行試點計畫 (概念驗證) • AI 專長知識僅限於特定團隊或個人 • 零散或不協調的開發 • 零星成功	• 團隊積極開發多個 AI 使用案例 • 初步的 AI 藍圖或具優先順序的使用案例 • 從初期專案中逐步發展出具備可重複性的流程	• 組織從實驗性試點進展到營運型 AI • 正式環境中的 AI 系統，團隊遵循明確的工作流程 • AI 操作實務引入了模型的版本控制、測試與監控 • AI 專業知識包括專職的資料科學家、機器學習工程師	• AI 開發標準化且高效 • 最佳做法和範本已獲廣泛使用 • IT 角色從守護者轉變為賦能者 • 許多團隊具備 AI 經驗，知識分享也很常見 • 組織以工廠化模式推動代理型 AI	• 組織內具備深厚的 AI 專業知識與創新能力 • 過去的專案用來應對新的、更複雜的 AI 挑戰 • AI 以敏捷方式交付，並能在企業內可靠地擴展



決定後續步驟

根據您目前的現況，接下來該如何採取行動，以建立對 AI 體驗的信任，並促進全組織更廣泛的 AI 採用？

建立跨部門的 AI 團隊

有效的 AI 解決方案不僅取決於正確的技術選擇。成功的 AI 專案同時需要組織內部各個團隊的參與和支持。這些團隊在任何 AI 專案啟動之初，即共同匯聚了業務、技術與風險管理領域的專業知識。他們協助建立起單一的對齊機制，以便能夠全面性、而非分階段地處理各項優先順序、權衡取捨與限制條件。這種共同所有權與協調一致的決策模式，將有助於技術實驗轉化為具備商業價值的生產系統。

為了有效，AI 團隊應該包含多元觀點的平衡；例如：

企業或產品負責人負責價值、成果與優先順序。

資料與機器學習工程師負責設計、建置及評估 AI 元件。

軟體或整合工程師，將 AI 嵌入真實工作流程和系統中。

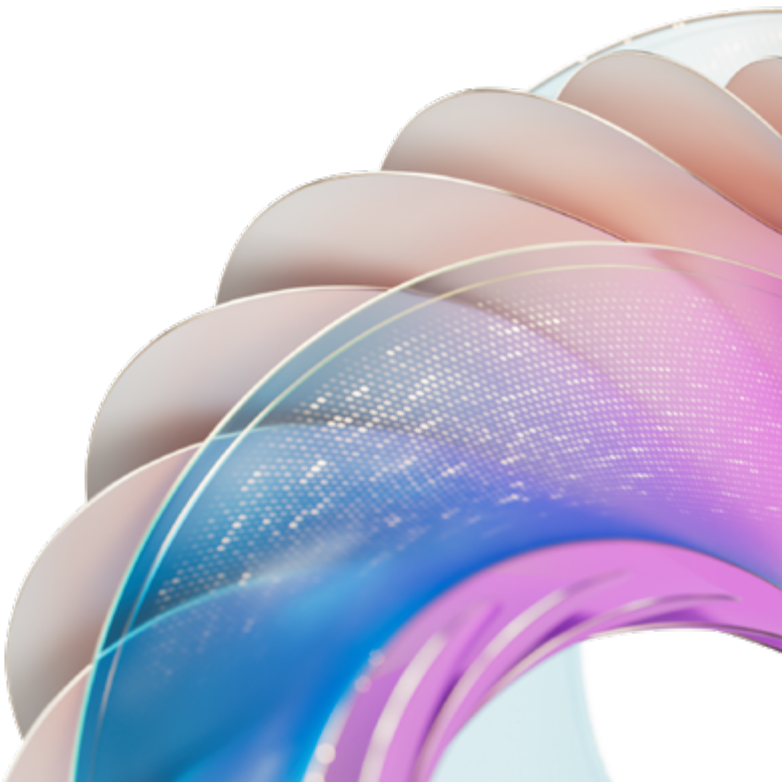
安全性、合規性、隱私權與 RAI 領導，幫助 AI 系統與您的信任、安全及法規要求保持一致。

支持有計劃的試驗

經驗是最好的老師，而團隊透過進行小型、安全的試點與概念驗證 (PoC) 實驗能獲得最豐富的學習。這些初期的實驗有助於團隊建立技能、信心與實務理解，從而能更廣泛地採用 AI。

試驗的方式很重要。若您缺乏明確定義的目標，或不知道如何衡量成功，亦不清楚該從試點與概念驗證 (PoC) 中汲取哪些經驗教訓，您將面臨徒勞無功並延誤進展的風險。

*有計畫的試驗*是其中關鍵。在啟動之初即明確界定成功的樣貌、運用實驗性試點來創造學習契機，並建立防護機制以確保此項實驗的安全性。在受控環境中進行人工驗證的成效，有助於降低疑慮，並與關係人及使用者建立信任感。其核心目標在於建立快速的回饋循環，將創意轉化為組織的學習資產，並打造出能傳遞真實商業價值的工具。



若要讓試驗產生最大效益，請留意以下重點：

設計實驗試點以最大化學習效果，
具備明確的假設、成功標準，以及捕捉與分享經驗教訓的機制。

在速度與責任感之間取得平衡，
確保快速迭代不會繞過安全、保全或資訊安全防護 (RAI) 規範。

及早建立治理，讓試驗者了解界限，並能自信地在其中創新。

提供解決方案加速器，如範本、設計模式，以可信架構打造 AI 解決方案。

在安全環境中評估試驗是關鍵步驟。為了降低風險，在進行更廣泛的部署之前，請先透過值得信賴的內部使用者來驗證 AI 工具與 Agent。規模較小的內部部署能為團隊留出空間，去辨識如幻覺、提示詞漏洞和整合落差等常見問題，同時將對聲譽、合規性及客戶信任的風險控制在一定範圍內。

在維持控制與治理的前提下支援試驗

當非技術員工能夠使用治理完善的低程式碼與無程式碼平台，建置出對內部有益的 AI 工具與 Agent 時，採用率與創新成效將會大幅提升。若能在維持強大控制力的同時，賦予使用者建置解決方案的彈性與能力，將能使推動廣泛的使用者實驗發揮最佳成效。

當資訊部門 (IT) 製造了瓶頸，導致安全且經核准的途徑變得緩慢或困難時，問題便會隨之而來，這將促使您的員工去尋找更快速的替代方案。這種挫敗感可能會導致員工去嘗試使用未經授權的公開工具，或在盲目追求進展的錯誤嘗試下，將資料移轉至受控環境之外，從而無意間增加了風險。

藉由將「安全途徑」*轉化為「便捷途徑」*來*避免此陷阱*。將資訊部門 (IT) 的角色，從擁有每項解決方案，轉變為治理使用者進行實驗的系統與資料。若您能將安全控制與負責任 AI 原則整合至可簡化 AI 試驗的工具中，您最終將能強化治理，而非削弱治理。



> 在內部引入摩擦的風險，遠低於直接從客戶端開始；因為在客戶端我們設有服務層級協定 (SLA)，且可能對營運表現造成影響。
>
> —副總裁，金融服務

鼓勵重複使用

與其讓每個使用案例都從零開始，不如在既有學習成果上持續推動。隨著您的 AI 能力隨時間推移產生複利效應，您將能把個別的孤立成功轉化為全組織的共同勝利。

為了促進 AI 專案的重複使用與經驗共享：

- **建立並維護可重複使用的 AI 資產庫。**一個包含模式、提示詞、元件、經驗證模型與治理工作流的精選資產庫，有助於將 AI 知識推廣至全組織。
- **以結構化且具備版本控制的格式記錄最佳做法，並將其列為建置或部署 AI 解決方案前的必讀規範。**高品質的說明文件是落實可擴展且負責任 AI 開發與營運的關鍵。
- **建立直接導入可重複使用資產庫的強制回饋意見迴圈。**包括事後檢討、回顧與模式報告等回饋意見機制，將特定專案的實務經驗教訓轉化為組織的制度化知識。
- **在所有可重複使用的範本與模式庫中，嵌入經標準化處理的治理、安全、資料處理與評估要求。**將防護機制與最佳做法直接嵌入可重複使用的資產中，有助於防止無意間發生的違規行為。
- **實作可擴展的生成式 AI 營運 (GenAIOps) 與代理型開發與營運 (DevOps) 實務。**請參閱第 35 頁的 GenAIOps 與代理型 DevOps 實作一節，了解詳細資訊。

隨著模型更迭、資料移轉、工具更新以及您的商業目標演進，請持續更新您的說明文件與資產。確保這些資源與最新的學習成果和經驗保持一致，將能提升新專案的基準品質，最終使 AI 能力持續穩定改進。



> 每次成功的實作都提供了可重複使用的藍圖。隨著時間推移，這發展出了一套教戰手冊，讓擴展至全新使用案例的過程變得更加簡單直接。
>
> —採購長，醫療保健

實作 GenAIOps 與代理型 DevOps

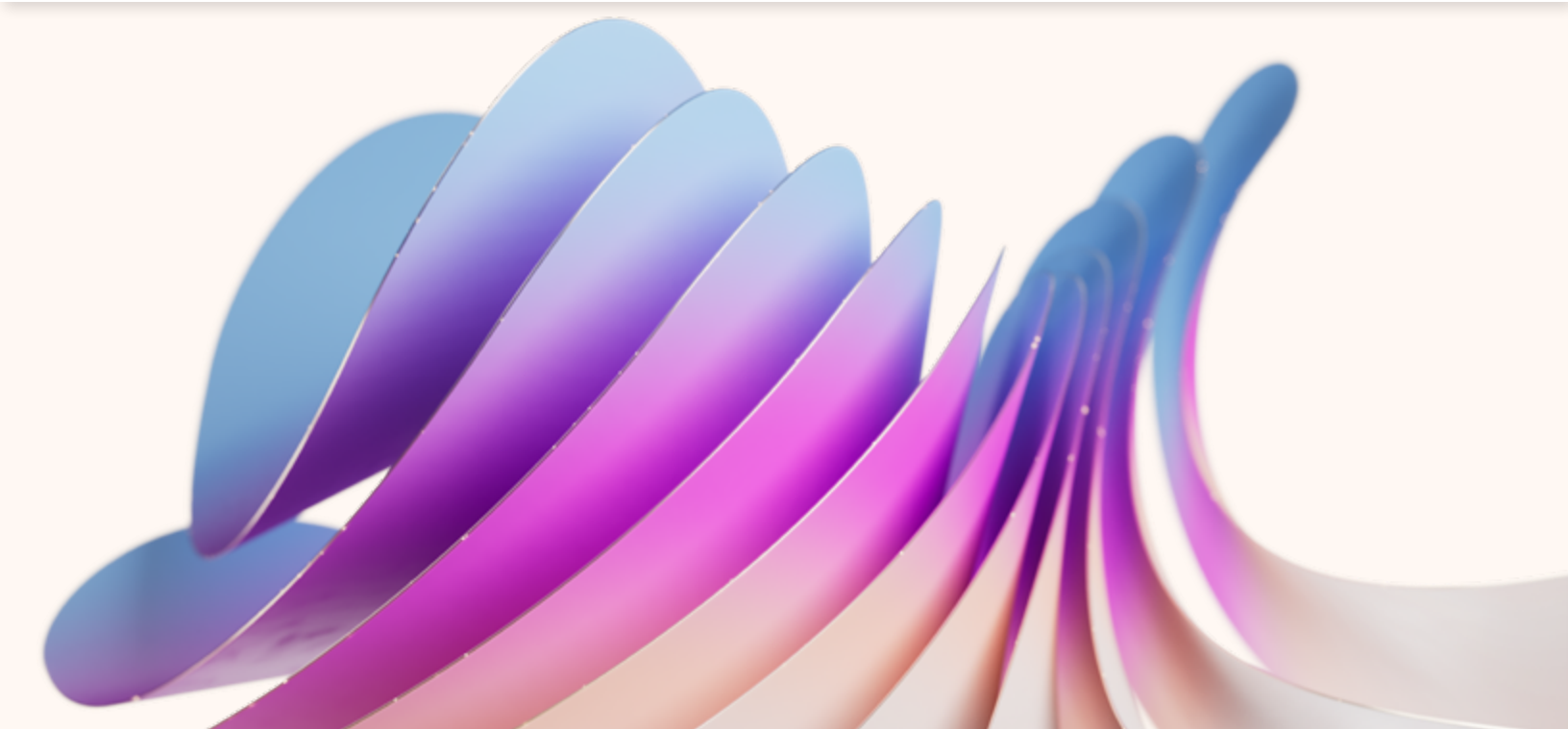
生成式 AI 營運 (GenAIOps) 實務、工具與作業流程，有助於可靠地部署、管理、監控並演進生成式 AI 系統。這些實務延伸了傳統的機器學習營運 (MLOps) 做法，以因應生成式與代理型 AI 的獨特特性，範疇涵蓋提示詞管理、模型更新、資料漂移以及非確定性輸出的評估等主題。

代理型 DevOps 在此基礎上更進一步，將 AI 整合為執行與最佳化技術營運的核心元件。它利用 Agent 來加速軟體交付、提升營運效率、減少停機時間，並使複雜的 IT 工作流實現自動化。

納入 AI 考量的營運實務可強制執行具備版本控制的資料、模型、提示詞與管線。這些實務能實現諸如持續測試與模型漂移監控等功能。

代理型 DevOps 將此延伸至 Agent 邏輯、工作流與整合，為變更帶來更高的可預測性。兩者結合可實現可重複使用的範本、模式與協調流程，使團隊在開發上搶占先機，並加速各個使用案例的交付。





衡量重要的指標

在 AI 專案中，衡量成效的核心在於實證商業效益、建立對新系統的信心，並指引未來發展的方向。在實務層面，這不僅僅是關注投資報酬率，還要納入採用率、信任度、系統品質、風險暴露，以及營運效率等指標。

將指標與真實成效對齊，而非憑空假設。與其追蹤所有項目，不如定義少數評估準則，其精確度須足以讓隨時間推移的進展清晰可見。透過聚焦且精選的指標與 KPI，關係人能清楚看到成效改進，支持明智的投資決策，並建立共同信心，確信 AI 倡議正持續傳遞價值。

將 AI 試點視為持續演進的系統來進行評估，而非一次性試驗。從啟動之初便為其配置遙測技術、使用者回饋機制與效能監控，以反映實際使用中的系統行為。

決策導向的指標與 KPI 能協助評估系統效益與潛力。這些指標通常聚焦於商業成效 (例如節省的時間、品質提升或採用率)、系統效能 (如延遲、可靠性與正確性)、風險與安全訊號，以及成本或效率衡量。正確的組合取決於使用案例，但核心目的皆在於實證價值、辨識問題並指引未來發展。

這些見解將使下一階段的疊代受益，指引您微調模型、調整工作流程、改善提示詞並修改防護機制。這個回饋意見循環讓您能獲得高階主管的持續支持，同時將初期的微型試點發展為支援核心商業功能的實質系統。



"

真正推動進程的關鍵在於能夠及早展現成效，並讓高階主管持續參與進展。同時，必須確保資料基礎穩固，以維持輸出結果的可靠性。一旦眾人看到一致的效能表現以及對日常工作的真實效益，信任感便隨之建立，我們也就能開始更廣泛地進行擴展。

—客戶互動副總裁，醫療保健

預見障礙

缺乏明確目標、未滿足使用者需求或未經妥善測試的 AI 系統，會增加懷疑並延緩採用。

透過階段性成果建立信任。隨著時間推移逐步提升 AI 能力，每次的漸進式成功皆能累積經驗。刻意縮小範疇並交付清晰成效，能向關係人與使用者展現 AI 的價值，並促進更進一步的採用。

設定可達成的目標，以確保成功建立信任。啟動專案以解決單一且定義明確的使用案例，並確信此專案將在生產環境中帶來效益。

只有在證明系統穩定且有價值之後，才應加入新功能。縮小範疇並採取嚴謹的做法能讓效益清晰呈現，使高階主管得以充分認同新系統的價值。

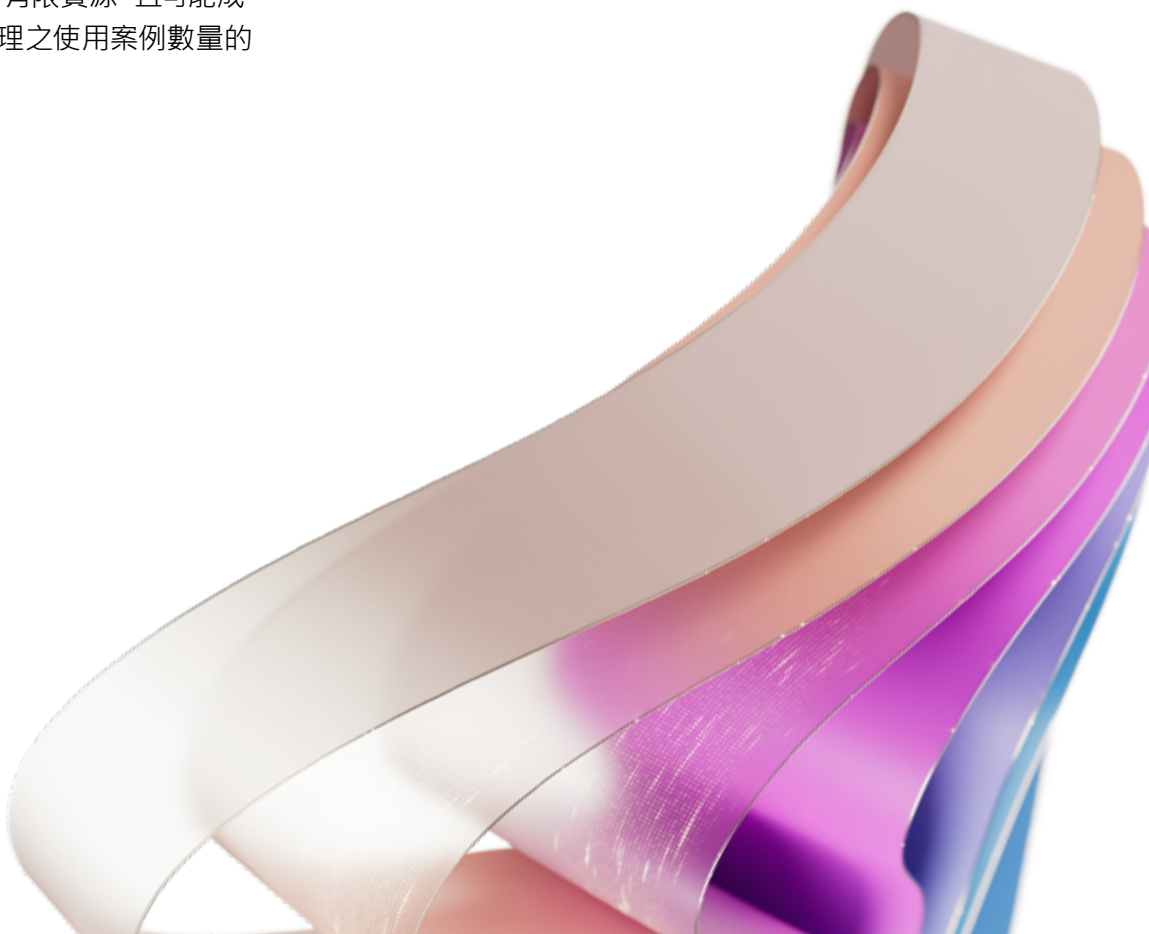
在每個步驟中維持可見性與控制力。監督機制、明確的所有權、透明的效能指標以及一致的成效，能降低疑慮，並將關係人的觀感從不確定轉化為信任。

尋找能讓非技術員工建立 AI 驅動解決方案的途徑。開發人員與 AI 專家屬於有限資源，且可能成為在任一特定時間內所能處理之使用案例數量的瓶頸。

達成目標：先進且具創新力的 AI 生態系統

隨著經驗產生複利效應，組織將在建置 AI 解決方案方面發展出深厚的專業知識，並建立經實證的部署與營運模式。過去專案所汲取的經驗教訓，伴隨與業務主管及關係人逐步建立的信任感，使您隨時間推移能以更高的信心與更低的摩擦，迎接更具挑戰性的複雜任務。

藉由上述流程，您能在全組織內以更高的速度、紀律與一致性交付全新 AI 解決方案。團隊能重複使用有效的方法、將其調整並符合全新的背景關聯，並透過可信賴的流程進行擴展，使您在維持可靠性、敏捷性與控制力的同時，能持續不斷地創新。



AI 價值驅動因素 #4

組織和文化

根據 Microsoft 2026 年工作趨勢指數年度報告，組織因素對 AI 所實現之價值的影響力是個人行為的兩倍，驅動了 67% 的實際價值。對許多組織而言，相較於技術能力，組織與文化因素才是擴大 AI 採用規模時更為重大的阻礙。

成功的轉型取決於重建營運模式，將團隊的重心從逐步執行任務，轉向設定方向、定義標準，並運用人類判斷來評估成果。若缺乏此轉變，即使是最具技能的員工，也可能無法充分發揮 AI 的效益，或將新技術轉化為組織的制度化優勢。

將全新的工作模式導入組織，對高階主管而言是一項關鍵挑戰，而如何讓這些變更深植組織內部同樣困難。若團隊缺乏與 AI 系統有效協同工作所需的技能、信心、支持與明確方向，即使是最宏大的高階主管願景也將陷入停滯。轉型成功與否，取決於是否已確立相應的指標、激勵措施與期望值，以獎勵員工採用全新方式履行職責。

這項轉型旅程並非線性發展，且組織內部的就緒度往往不盡相同。各個團隊、部門與工作負載可能處於截然不同的 AI 採用與接受階段；當某些團隊已在建置先進的 Agent 與自動化機制時，其他小組或許才剛開始理解 AI 如何融入日常工作。認清並包容這些差異，進而導入能促進組織內部持續變更的流程，將是成功的關鍵。

> 一切的關鍵皆在於文化。若缺乏全組織的廣泛採用，將難以推進 AI 倡議。擴大 AI 應用規模，完全取決於廣泛的共識與支持。
>
> —人資主管，科技



評估組織與文化就緒度

您是否正在建立團隊所需的技能、信心與支援架構，以使其能充滿信心且高效地與 AI 協同工作？了解目前的現況，能協助明確辨識未來需要推動哪些組織與文化變更。

未協調的努力	建立 AI 治理	有組織且獲得支持	AI 賦能文化	AI 優先文化
• AI 由愛好者在各自孤島中推動 • 沒有正式的 AI 角色或治理結構 • 文化上，對 AI 的認知處於初步階段 • 少數員工具備 AI 技能 • 領導層態度保守，尚未形成一致願景	• 領導層闡述 AI 願景並贊助初期專案 • 成立 AI 工作小組或 AI 卓越中心 (CoE)，協調 AI 推動工作並分享經驗 • 隨著人們看到初期使用案例的實際成果，文化從懷疑轉向好奇。	• 成立正式的前沿卓越中心，並在各部門制定清晰的運作模式 • 領導層溝通與變革管理推動用戶採用 • AI 倡導者促進採用 • 制定訓練方案，提升全組織的 AI 技能	• 組織在各部門全面擁抱 AI，由高階主管或決策委員會引領 AI 策略 • 大多數員工都具備一定的 AI 素養 • 許多職務已重新定義以協同 AI 工作，並將新職務 (AI 領導、資料科學家、機器學習工程師) 整合至組織內。 • 員工積極尋求 AI 驅動的工作改進	• AI 已深植於公司運作中 • 員工運用 AI 來支持決策，並以強大的變革管理與領導願景為基礎 • 健全的 AI 卓越中心負責管理 AI 解決方案組合，並建立回饋機制。 • 每個部門在其策略中都會考量 AI • 員工具備敏捷性並持續提升技能

決定後續步驟

根據組織目前的現況，接下來該採取哪些步驟，以打造出準備就緒的 AI 文化？此類文化能擁抱變更、持續培養技能，並對發揮 AI 系統所賦予的強大動能充滿熱忱。



建立集中式的指引、標準與支援

當高階主管清晰闡述 AI 如何與商業成效相互連結、投資推動員工能力建置，並積極鼓勵實驗時，便能創造變更動能。然而，若缺乏一致的架構加以引導，這些努力也極易失去動能。指引、標準與訓練支持能賦予團隊方向、工具與信心，以負責任且具規模地採用 AI。

前沿卓越中心 (Frontier Center of Excellence，簡稱 CoE) 團隊是滿足這些需求的強大工具。前沿卓越中心為 AI 的設計、部署與擴充建立中央指引與說明文件。團隊的任務並非擁有解決方案，而是為成功創造條件，並支援全組織負責任 AI 使用。

集中前沿 CoE 團隊可以協助您的組織：

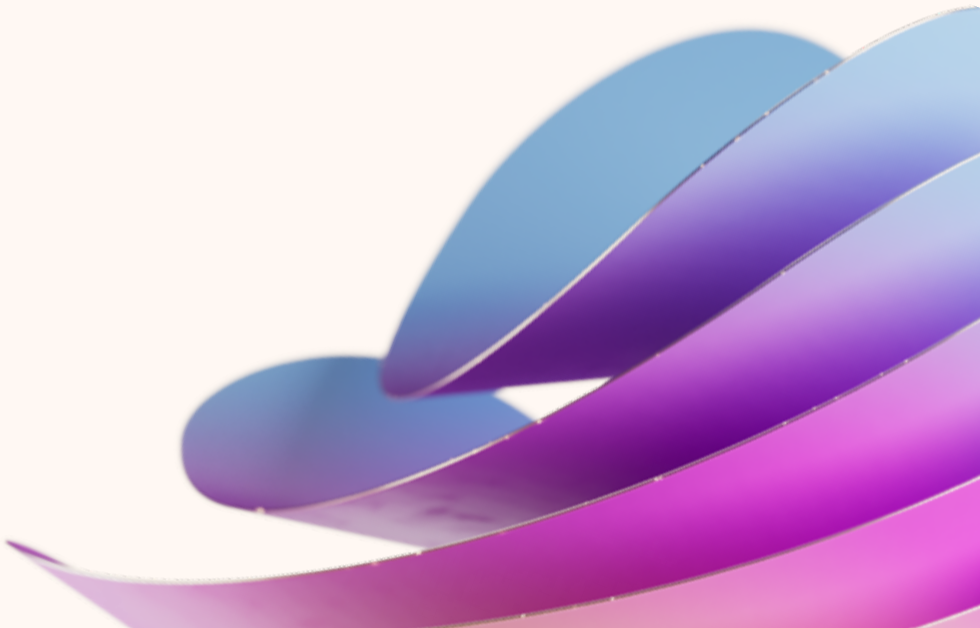
- 定義標準、治理與最佳做法。
- 建立共享的模式、規範和平台。
- 建立並鼓勵技能培養的活動。
- 辨識並記錄可重複使用的模式，避免每個專案都從頭開始。
- 建立相關流程，以鼓勵從一開始就將負責任且受治理的 AI 整合至所有 AI 解決方案中。
- 透過讓關係人參與整個流程，以促進更快速的採用與文化變更。
- 確保每個專案都與整體 AI 策略保持一致。

前沿 CoE 無法在第一天就掌握所有解答，而是隨著 AI 採用規模擴大而進行疊代擴展。為了及早辨識挑戰並加以解決，應持續整合員工與終端使用者的回饋，並隨著 AI 使用量增加，與時俱進地更新指引、標準及支援資源。

憑藉高階主管的強力支持、專屬的跨部門團隊以及充足資源配置，前沿 CoE 能在監督與授權之間取得完美平衡。在前沿 CoE 的協助下，團隊能更輕鬆地打造解決方案，同時維持信任度、安全性並與組織目標保持一致。

提供有組織的變更管理支持

當您跨越初期的實驗階段後，成功的關鍵便取決於建立正確的基礎。您需要與員工溝通有關 AI 的願景、賦予他們 AI 技能並鼓勵推動進展。藉由管理 AI 在跨團隊間如何被引入、理解與採用，您將能減少阻力、使員工與您的標準保持一致，並促進廣泛的採用。



建立變更管理團隊

高階主管定義並傳達組織的 AI 願景，這有助於員工理解自己將如何適應新技術與新的工作模式。變更管理團隊與高階主管緊密合作來傳遞該願景，並建立起用以化解疑慮與阻力的關鍵論述。

這個流程有助於員工理解 AI 倡議背後的目的，並能緩解他們對 AI 的疑慮或恐懼。先前持懷疑態度的員工將開始看見 AI 如何改善工作並傳遞商業價值。

變更管理能透過以下幾個重要方式，協助您促進 AI 採用並建立對持續變更的接受度：

確保眾人理解 Agent 是助力而非替代品。清晰的訊息傳遞能將 Agent 定位為生產力工具而非工作威脅，從而減少恐懼。

用經驗改變觀念。在員工透過親身使用與經驗看見自身的生產力與能力提升後，懷疑與阻力便會消退。

著重於人員，而非技術。接受度與採用率更取決於溝通、重新訓練與鼓勵，而非 AI 技術。

開始培養 AI 技能

缺乏 AI 技能與知識，會對新系統與新流程產生不確定性與懷疑。導入訓練與技能提升計畫，能協助團隊更深入理解 AI 的本質、如何應用於自身，以及它將如何影響日常工作。

具備運用 AI 所需技能的人，更有可能積極參與新工具與流程，進而促進採用與使用新 AI 系統。

除了基礎的 AI 素養認知與特定技術技能，訓練計畫也能讓員工與 CoE 團隊所定義的標準及最佳做法保持一致。這些計畫有助於建立 AI 知識與實務能力的共同基準、提升採用率，並引導團隊在負責任且高效使用 AI 方面，做出更好、更明智的決策。

為了幫助員工建立這些能力，請探索學習平台，例如 **AI Skills Navigator**。這些資源可協助探索角色型學習路徑、追蹤進度，並在整個組織中擴展 AI 技能。

> 團隊初期對於這對自身職責帶來的影響，無疑存在一些疑慮。我們必須非常明確地指出，這並非為了取代人力，而是協助他們卸下重複性的工作，好讓他們能專注於更有意義的任務。這種訊息傳遞上的轉變，對採用率產生了極大的正面影響。
>
> —策略副總裁，金融服務

利用 AI 倡導者來支持變更

AI 倡導者社群能回應領導層與員工的關切，並激發對您 AI 願景的熱情。選擇對 AI 專案具備充足實務經驗、足以理解技術細節與潛在效益的倡導者。他們同時也應理解高階主管的商業目標，以便能透過以下幾種方式支持 AI 的推展：

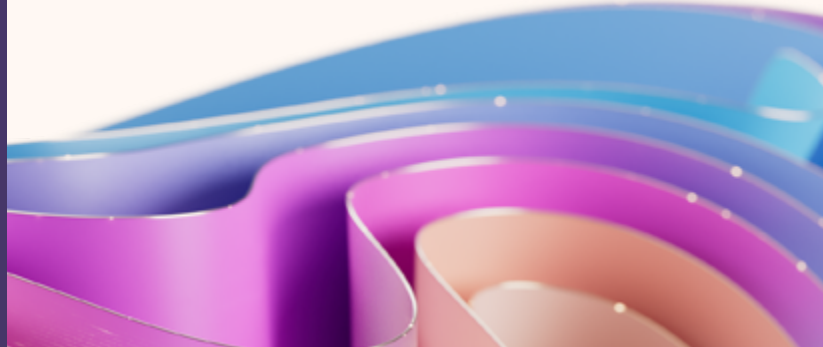
- **將進展轉化為高階主管所關切的成效。**他們將日常開發與聚焦於成效的高階主管期望相互連結。
- **在專案與高階主管之間維持動能。**他們追蹤成功案例、浮現阻礙因素並推動決策進程。
- **防範試點漂移。**透過掌握可見性與論述主導權，倡導者有助於讓 AI 專案持續聚焦於真正的商業目標。

將 AI 學習成果推廣至全組織

隨著 AI 承接更多常規任務，批判性思考、溝通、創造力以及適應能力變得更為重要。

- **隨著 AI 使用量增加，擴大訓練與技能提升的力道。**在培養全新 AI 技能熟練度的同時，著重於互補員工的既有優勢。
- **持續投資於員工技能與 AI 熟練度。**接受過新 AI 系統訓練的員工，往往更傾向去信任這些系統、理解它們如何減輕常規工作量，並辨識出改善或重新設計工作流的全新契機。
- **發展 AI 學習策略。**請勿依賴一體適用的做法。評估每個團隊的 AI 準備度，範疇涵蓋認知、思維模式、技能與信心。採用角色導向的訓練，讓學習與不同的角色和組別保持對齊。納入實作專案，將學習轉化為實務能力，進而促進採用並交付商業成效。
- **建立學習社群。**建立內部社群，讓員工能夠交流最佳做法、記錄運作良好的方法，並透過黑客松、構想討論會及資源共享等活動共同學習。邀請領導層、業務負責人、開發人員，以及值得信賴的 AI 倡導者，共同持續推動、提升可信度，並在組織內擴散最佳做法。

> 這不是推出後就結束的事情。您必須持續投資於訓練，並持續協助員工建立使用信心。這才是真正導致永續採用的關鍵。
>
> —客戶服務副總裁，專業服務



培養 AI 驅動文化

在 AI 優先的文化中，領導者會明顯鼓勵並參與 AI 驅動的工作流程，而非將其視為孤立的試驗。AI 優先的文化認可並鼓勵透過 AI 帶來真實且可衡量成果的團隊，並鼓勵廣泛嘗試。

以創新為導向的組織不會假設 AI 是完美的。相反地，他們明白反覆的過程會帶來學習，經驗能持續促進改進。最重要的心態轉變是從 *證明它有效*，轉變為*幫助我變得更好*。當團隊感覺安全，能夠隨時間試驗、精煉並改進 AI 驅動的工作流程時，AI 採用與創新將迅速加速。

當眾人看見 AI 在實際工作中取得成功，並獲得高階主管的支持，且透過激勵措施、表彰與共享成果加以強化時，文化轉變的速度最快。前沿企業具備以下特質：

- **他們以就緒度為準，而非技術。**這包括以可控的波次逐步擴充 Agent 與工具，同時讓部署進度與員工的就緒度及技能完美契合。
- **他們維持高階主管與其他領導者的持續支持。**當高階主管在專案啟動後仍保持參與，便能釋出將 Agent 部署視為優先要務的訊號。指派的 Agent 推動者則能協助進一步搭起員工與高階主管之間的溝通橋樑。



> 一旦他們看見這能消除重複性的工作，接受度便大幅提升。顯而易見地，這關乎於生產力的提升，而非人力的取代。
>
> —科技解決方案副總裁，金融服務



預見障礙

轉型速度常因領導力、文化與技能相關的多種障礙而減緩：

若缺乏共同願景或高階主管的持續支持，組織往往難以將其各項努力與整體 AI 策略保持對齊。

風險迴避的文化、抗拒改變，以及對 AI 技術的普遍恐懼，都可能阻礙試驗與採用新工具。

教育或技能培養不足，會進一步拖慢進展，因為員工缺乏對於有效運用 AI 工具的信心或真的缺乏能力。

識別、理解並克服這些障礙，能讓您的組織利用 AI 進行適應、學習與創新。當領導層協調一致、風險被理解與管理，以及員工具備正確技能時，試驗就能成為可用的生產工具，帶來真正的商業價值。

邁向自己組織的轉型時，請考慮下列這些可能需要克服的障礙：

組織內部是否認為 AI 採用值得承擔成本與風險？

關係人與領導層需要看到 AI 的明確價值，才能從好奇心轉為堅定信念。高階主管必須了解 AI 的好處，並說明投資的合理性。

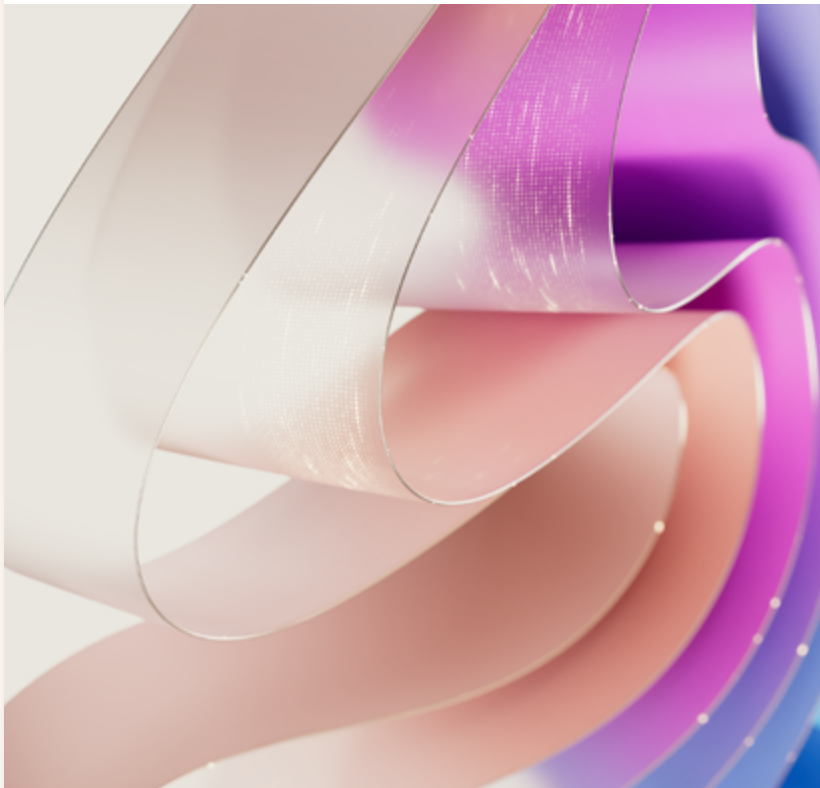
風險預防並非不可能的挑戰。教育關係人，使其了解 AI 風險管理是一個可管理的過程，而非巨大障礙。

建立支持轉型的文化

員工對於改變核心業務系統或流程通常會持情有可原的謹慎態度。然而，隨著 AI 成為生產力與日常工作的基礎，採用不均或抗拒變更可能造成摩擦、拖慢進展，並稀釋 AI 投資的價值。

讓員工和團隊接受新的工作方式，不僅僅是技能訓練和工具的問題。這需要一種支持轉型的文化。清晰的領導訊息、有效的變更管理、可見的成功案例，以及可取得的訓練課程，有助於員工了解 AI 如何支持他們的工作。建立實作學習、同儕支持和安全實驗的機會，能讓持懷疑態度的團隊以自己的步調參與，而不會感到被落下。

在 AI 系統被企業證明可靠且不可或缺之後，新的工作方式就不再是可有可無的存在。當組織積極協助員工渡過這個轉型階段之後，採用流程會順利許多。



組織當中是否存在隱藏或未明言的文化障礙？

- 若缺乏高階主管的持續支持，變更動能可能會陷入停滯。這時應爭取領導者積極支持各項努力，而非僅僅給予核准。
- 競爭對手和客戶可以是推動變更的力量。高階主管需要意識到代理型系統如何協助強化競爭優勢，並改善客戶參與度。
- 邀請外部合作夥伴與顧問協助您識別瓶頸，使各項計畫與業務目標保持一致，並讓關係人感到安心。
- 將公司的文化視為推動力，而非阻力。當領導層看到成效時，應給予 AI 創新獎勵，即使變更有挑戰。

您的組織是否認為自身擁有合適的技能與能力？

- 您的領導者與員工需要有信心，相信自己能成功運用 AI 技術。然而，同樣重要的是，他們必須理解「完美的就緒度」並非推動進展的必要前提。即使面對技術或能力差距，也要鼓勵前進，因為這些問題會隨著團隊累積經驗而得到改善。
- 風險管理固然重要，但若堅持要百分之百的風險都在事前解決，將會阻礙進展。在高階主管審查並改善原則、治理與風險緩解策略的同時，需要賦予團隊採取行動的權限。
- 確保已建立內部審查、測試與支援機制，使實驗性試點能安全地成長為核心商業能力。

達成目標：前沿轉型

當組織發展出成熟的前沿文化時，AI 將從根本上嵌入日常工作的執行方式中。員工依賴 AI 來提供決策、增強判斷力並加速成果。變更管理支持高階主管的願景，有助於確保 AI 採用具備明確目的、維持一致性，並直接與商業目標銜接。

在此階段，架構與文化兩者皆是維持成功的基石。強健的 AI CoE 為 AI 產品組合提供監督、指引與持續回饋，確保創新始終符合治理、商業優先事項與使用者需求。AI 成為一項共享能力，連結策略、執行與成果，跨越整個企業。

持續的技能提升能讓您的組織隨著科技與機會一同演進。員工具備嘗試、學習並改進工作方式的技能與支持，領導層則強化成長心態與對 AI 的信心。



AI 價值驅動因素 #5

AI 治理和安全性

治理不僅僅是追求更快、更安全的創新，也不是可有可無的。監管機構要求必須將控制和合規機制直接內建於 AI 系統中。從一開始就為 AI 工具和 Agent 設計完善的治理機制。

AI 治理聚焦於制定推動信任的規則、標準、系統及控制措施。這就是您在業務、技術和風險團隊中建立明確所有權、一致的防護措施，以及高度透明度的方法。在這個基礎上，您能夠與關係人及最終使用者建立信任，並明確規範允許事項、期望事項及界限所在。



> 我們正積極制定治理的規範、原則和控制機制，以規範 AI 的使用規則及可接受的使用案例，但這仍在持續進行中。這些框架與標準正與實務使用案例一同發展，並持續演進。
>
> —資訊科技總監，零售

代理型 AI 治理有何不同之處？

AI 系統及其生成的內容，必須如同其他企業系統般受到治理、審查與稽核。代理型 AI 導入了某些額外的獨特治理挑戰：

- **Agent 蔓延與資源存取。**隨著 Agent 數增加，維持明確的所有權、一致的身份控制及明確的存取邊界非常重要。未受管理的蔓延可能導致權限過大的 Agent、擴大攻擊面並增加合規風險。
- **資料過度共用。**Agent 與多個系統和使用者互動，如果系統未妥善管理和控制，將提高敏感資料外洩的風險。
- **新出現的 AI 特有威脅與弱點。**間接提示詞注入等攻擊以及相關弱點，可能不會出現在傳統的安全模型中。主動防範惡意行為者需要專門的關注。
- **日益增加的監管壓力。**政府與組織仍試圖釐清如何應對日益由 Agent 驅動的世界，且法律頻繁變更。掌握合規現況比以往任何時候都更加重要。

評估 AI 治理與安全性就緒度

了解您目前的治理現況，是明確辨識落實可信賴 AI 核心需求的第一步。您是否正在導入 RAI 規範、AI 安全性，以及標準化的開發與測試實務？了解您在治理成熟度旅程中所處的位置，能讓您明白接下來應前進的方向。

無正式治理	基本指引	新興控管	整合式控管	可信賴且可稽核的 AI
• AI 試驗在沒有官方指導方針的情況下進行 • 對倫理、安全性或法規曝露的管理很少 • 員工採用未經核准的 AI 工具 (影子 AI) • 缺乏營運可見性 (有限的遙測、監測、記錄)	• 初步擬定的 AI 原則或指引，以確保專案遵循道德準則 • 已識別每項試點的關鍵風險 (例如隱私權與合規問題) • 開始進行資料與模型的安全性審查	• 為所有新部署的代理型 AI 建立完善的治理流程 • 治理團隊審查所有主要 AI 專案 • 安全性與隱私權控制已整合於代理型 AI 解決方案 • RAI 已併入	• 將治理嵌入代理型 AI 的開發生命週期中 • 已制定針對 AI 系統的專屬事件應變計畫 • 針對安全態勢實施自動化監控，而非僅限於模型效能 • 專責團隊 (AI 倫理委員會、風險官員) 監督企業 AI 的應用	• 組織擁有業界領先的 AI 治理 • 讓 RAI 成為核心 DNA • AI 系統透明、可審計，並符合高標準的倫理規範。 • 治理能在信任、風險與業務成果方面帶來可衡量的商業影響

決定後續步驟

根據您目前的現況，下一步該如何實施並改善治理與安全實務，以協助您大規模部署安全且備受信任的 AI？

定義 RAI 框架

健全的 **RAI** 架構為 AI 建立「運作規則」，明確規範公平、透明、隱私權、安全性、問責及系統中人類監督的期望。它制定了一套結構化的原則、實務與治理流程，協助建立兼具倫理性與可信賴性，並契合組織價值觀、法律義務及社會期望的 AI 系統。

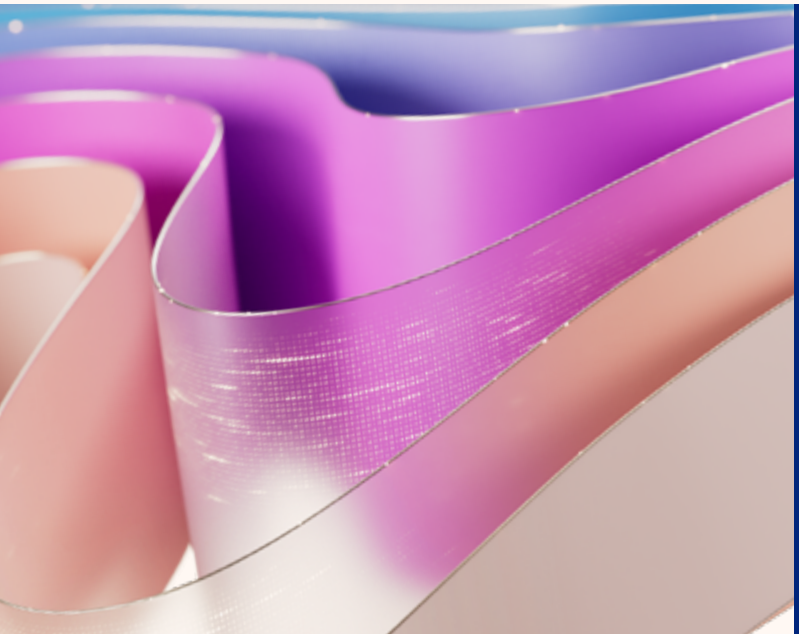
定義自己的 RAI 框架，意味著超越簡單的技術問題，比如*您是否能建置 AI 系統？*考慮貴組織的價值觀如何影響 AI 的開發，以及 AI 的應用如何影響貴組織的法律與倫理責任。

您的 AI 卓越中心團隊和 RAI 框架相輔相成。RAI 框架定義了*負責任 AI*對組織的意義，而前沿卓越中心將此理解嵌入原則、技術控管、審查流程、工具及日常執行中。隨著時間推移，它根據新法規、部署經驗教訓及組織風險容忍度的變化，協助框架演進。

為了讓此框架發揮成效，您的領導階層與 AI 倡導者必須公開且明確地給予支持，並向所有人表明：負責任 AI (RAI) 是全體共同的責任，而非合規上的事後補救措施。

建立 AI 治理

AI 治理可以涵蓋從非正式、結構鬆散的 IT 和安全審查，到能引導整個 AI 生命週期的完善基礎結構等不同層面。當您從試驗性的 AI 邁向組織層面的廣泛採用時，請將治理基礎結構升級為可信、可觀察且可稽核的 AI 系統。



> 如果您打算使用這些工具，您依然需要承擔與親自執行時相同程度的責任。您不能指望系統或外部解決方案來承擔這個責任。
>
> —IT 副總裁，金融服務

了解 AI 治理的核心要素

AI 治理是建立在一套協調一致的實務做法之上。隨著 AI 採用的普及，您將需要應對倫理期待、安全與風險管理、資料保護，以及跨團隊與跨環境的一致性問題。

RAI 框架與原則定義您對 AI 的倫理、法律及運作期望。透過共享的價值觀，您可以定義將要建構的防護，並形塑相關的原則、角色、審查流程與技術控制措施。這有助於確保您的 AI 系統安全運行、契合組織價值觀與法規，並與員工、客戶及監管機構建立信任。

AI 安全與風險管理是治理的關鍵要素，能提供支持符合原則、安全且合規運作所需的控制措施、可觀察性與問責制度。建立一個集中的風險控制平面，並配備持續監控與威脅偵測系統，以支持大規模且一致的身分識別、存取與原則執行。

資料安全與合規機制有助於確保您的 AI 系統負責任地處理資訊、保護敏感資料，並符合法規與組織的要求。隨著 AI 工具與 Agent 邁入生產環境，資料流動的管控難度也隨之大幅提升。因此，實施一致的資料隱私權控管措施才能防止受管制資料遭到非預期外洩。資料評估與監控必須持續進行，且隨著使用案例的演變與法規的更迭，法務與合規部門需全程保持緊密參與。

一致且全組織性的治理執行會在所有系統與團隊間實施控制。這有助於避免分散或不均衡的控管造成盲點、行為不一致，以及無法追蹤或稽核的情況。自動化有助於實現規模化治理，透過持續進行掃描與監控，及早發現潛在問題。

對於所有這些元素，目標並非從第一天起就達到完美。相反地，應逐步建立一套可隨 AI 應用擴大而持續最佳化的治理模式，並協助您在過程中避開潛在的隱蔽風險。

> 歸根結底，人們對系統的信任程度，完全取決於他們對背後資料的信任度。一旦對資料的正確性或完整性產生任何懷疑，採用率就會迅速下滑。
>
> —商業與行銷全球負責人，金融服務



將良好治理整合至整個組織

AI 治理需要在人員、平台與 Agent 生命週期中落實一致且具可擴展性的控制措施。透過您的 RAI 架構，您可以制定出決定您的組織應如何開發、部署與使用 AI 解決方案的指引。下一步則是確定您將如何以務實的方式，來應用並管理這些決策。

成立一個跨職能的 AI 治理委員會。為了切合貴組織的 RAI 架構並遵循前沿卓越中心團隊的指引，此特別小組全力投入各項 AI 專案的評估、監測與核准工作。他們憑藉卓越的領導思維與技術專家素養，嚴格根據倫理道德、風險管控、資料隱私、資訊安全及技術可行性等維度，為核心決策提供專業依據。

在您的組織中強制執行一致的治理、安全控管與可觀察性。AI 系統層層疊加，包含模型、提示、資料、API、Agent 與整合，這些都可能帶來風險或合規挑戰。務必確保組織具備跨系統與跨環境的能力，以統一的標準評估風險並落實管控機制。將防護機制與規範直接內建於 AI 系統。

在所有 AI 系統、提示與 Agent 中執行自動化的安全性、合規性與安全檢測。隨著 AI 規模擴大且資安與合規人員日益分身乏術，自動化掃描解決方案能識別出各項問題，例如不安全輸出、偏見、資料外洩、不安全配置以及不符合原則的組件。

建立整合的 AI 生命週期治理流程。治理 AI 系統，需要了解現有的 AI 工具與 Agent，以及它們的功能。註冊與生命週期管理系統可以追蹤您所有的 AI 系統，涵蓋從批准、部署到淘汰的完整階段。請將此系統整合至您的 Agent 建立流程與工具中，好讓團隊能更輕鬆地建構符合原則的系統。

> 他們最大的顧慮之一是：這是否會違反我們與供應商既有的任何合約協議？Agent 是否會做出打破這些規範的行為？答案是：不會，因為我只要寫好程式讓它不這麼做就行了。
>
> —見解部門資深副總裁，技術



識別並緩解 AI 安全性風險

AI 與 Agent 系統面臨著獨特的威脅情勢。傳統上，您的核心焦點在於透過控制存取權限與驗證輸入內容，來保護您的系統。儘管這些考量依然適用，但 AI 系統還必須防範對模型推論與內容生成能力的惡意操縱、潛在的學習行為風險，以及未經批准的 AI 系統 (影子 AI) 的整合。

Agent 還會帶來與其自主性及獨立行動能力相關的風險。它們連結到各種工具、API 與資料來源，這些管道一旦遭到濫用，可能會導致未經授權的行動或資料外洩。與傳統的 AI 聊天系統不同，Agent 通常會加入持久性記憶或背景關聯，惡意行為者潛在可能利用這些元素來入侵系統並存取敏感資訊。

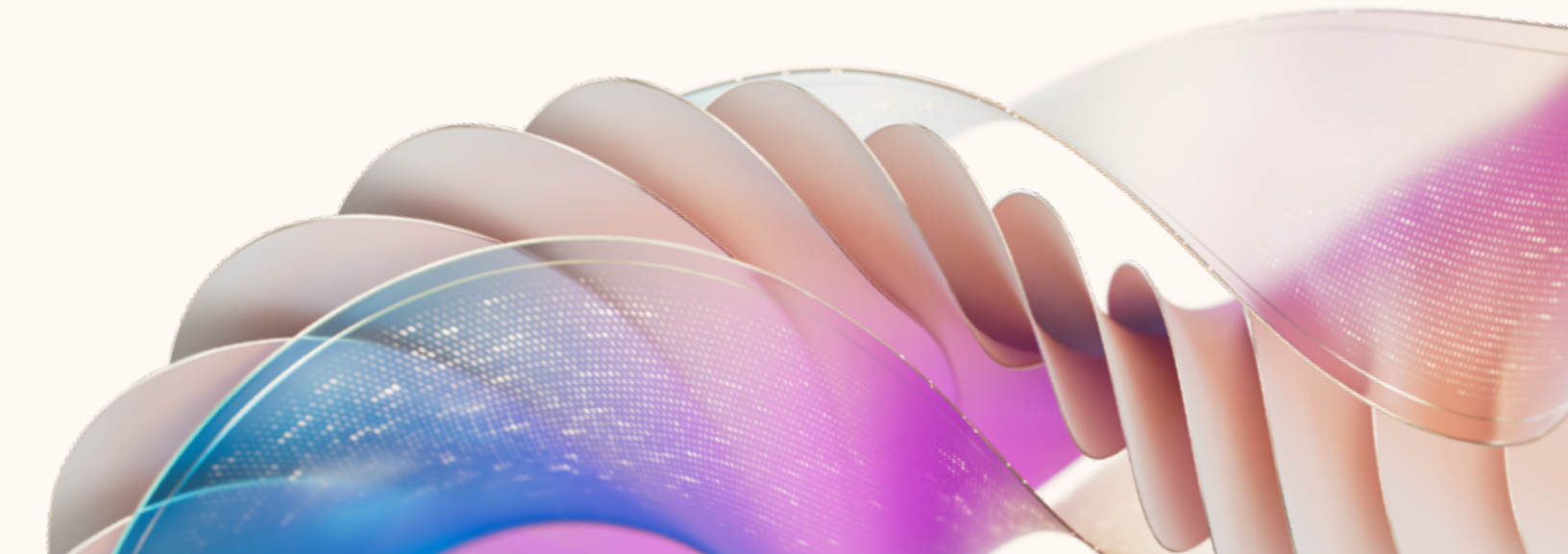
這些風險是可控的，但資安團隊無法單憑一己之力解決。隨著您的 AI 工具與 Agent 規模擴大，治理、可觀察性以及共同控制措施變得更加重要，且資安需要成為一項全面性、共同承擔的責任。開發人員、IT 團隊與資安團隊同樣扮演著關鍵角色，共同負責設定界限、強制執行存取權限，並監控行為。

考慮採取以下步驟，以因應代理型 AI 系統所帶來的獨特風險：

將身分識別管理與存取原則套用至 Agent。Agent 面臨許多與人類相同的身分管理與存取控制問題。隨著 Agent 與您更多系統進行互動，它們需要身分識別、定義明確的權限、資源存取權、生命週期控制，以及對可疑活動的監控。將 Agent 整合至您現有的身分管理系統中，是更妥善保護它們的簡便方法。

建立資料安全性控制。實施一致的資料分類與存取機制、對 AI 及 Agent 行為進行自動化監控與審計，並建立明確的核准與淘汰 Agent 生命周期流程。建立涵蓋法務、資安及合規團隊的跨職能監督機制。

實作所有 AI 應用程式和 Agent 的整合安全控制平面。AI 導入了全新的身分、工具與跨系統整合。集中式的控制台能防止影子 AI、支援最小權限存取，並賦予資安與合規團隊所需的能見度，好在大規模擴展中監控並治理 Agent。



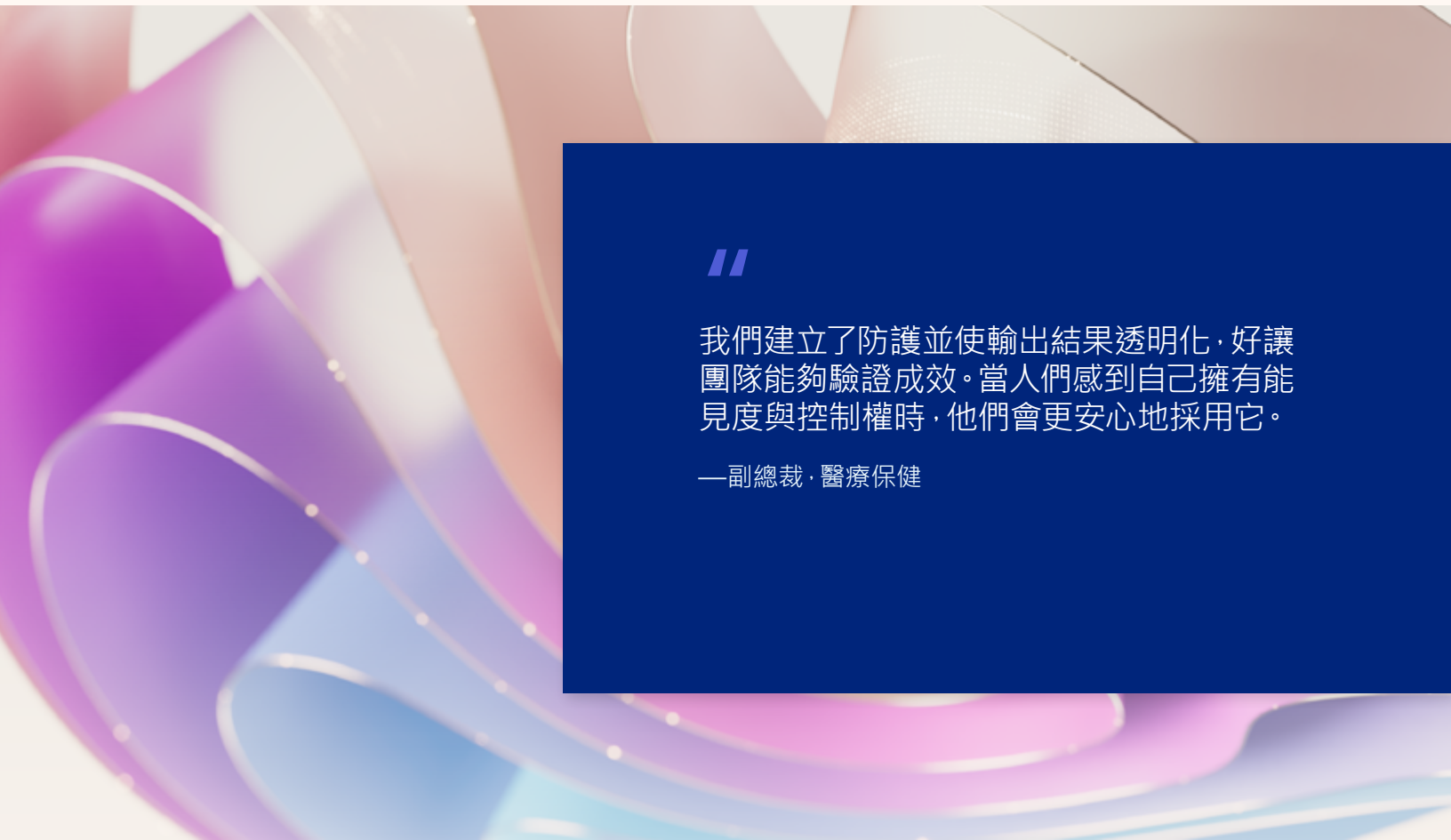
確保您對 Agent 及其行為具備持續監控與即時的可觀察性。代理型 AI 的尖端且複雜功能，可能會導致出乎意圖的行動、不安全的工具呼叫，或是繞過標準安全控制措施的行為。使用自動化偵測系統，才能進行偵測提示詞注入、思考鏈惡意操縱或工具濫用。請實施持續監控，以提早發現可疑行為。

針對每個 Agent 進行部署前的安全評估。資安團隊進行的部署前分析與測試，能防止高風險行為進入正式生產環境。一致且徹底的審查流程，不僅能減少安全事件，還能建立與內部審計團隊、業務利益相關者及法規監管機構之間的信任。

解決隱私權與法規遵循

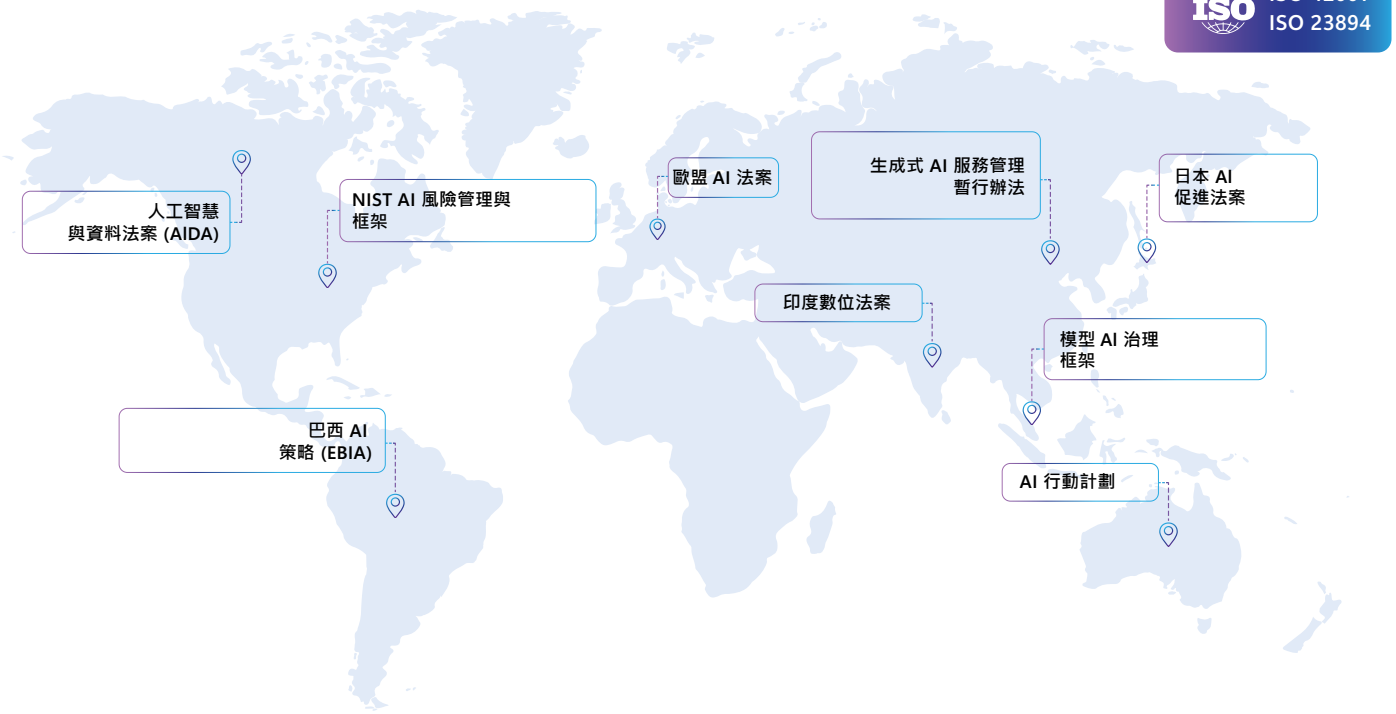
AI 系統仰賴大量的資料，其中通常包含敏感、個人或專有的資訊。Agent 也普遍與多個系統及資料來源進行互動。這些複雜的行為引入了全新的挑戰，您的資料隱私與安全原則必須對此加以管理。

在此同時，法規情勢正在迅速演變。各國政府與監管機構正透過專門針對 AI 的原則來擴大資料保護，這些原則強調透明度、問責制與負責任使用。您越來越被預期不僅要保護敏感資料，還要證明您的 AI 系統如何符合各項原則。



> 我們建立了防護並使輸出結果透明化，好讓團隊能夠驗證成效。當人們感到自己擁有能見度與控制權時，他們會更安心地採用它。
>
> —副總裁，醫療保健

各區域正陸續推出 AI 規範



多個 AI 監管原則架構正在全球各地興起。

為了消除這些顧慮，請將資料隱私、安全與法規合規性深植於您的整體 AI 治理策略中。

- **對所有 AI 與代理性工作負載執行嚴格的資料隱私權控制。**實施相應的控制措施，以防止未授權的存取，並依照新興的 AI 法規保護敏感或受管制的資料。同時，應持續遵循現有的隱私權框架，例如《通用資料保護規則》(GDPR)和《醫療保險隱私權與責任法案》((HIPAA)。
- **定期對 AI 系統進行安全評估，以確認是否符合法規。**透過法律、隱私權與安全團隊的正式評估，能確保 AI 系統在正式上線前符合既定標準。隨後進行的持續性評估，則能維持系統的合規狀態，從而降低法規、商譽及營運上的風險。
- **在 AI 生命週期的每個階段整合法律與合規團隊。**在您的跨部門治理團隊中納入法規專家，協助您持續保持 AI 系統的合規性並履行法律義務。
- **部署自動化模型監控工具。**若未被偵測，模型行為漂移可能導致隱私缺口、輸出不準確、偏頗結果或敏感資料濫用。進行持續監控，協助您及早發現問題並迅速回應。此類監控已成為越來越多司法管轄區的法規要求。

預見障礙

當您將 AI 擴展到更多業務領域時，監控系統行為並建立防護以管理風險，避免阻礙有價值的創新。挑戰不僅僅是增加更多監督，而是打造一套透明、可衡量且負責任 AI 治理，同時保留試驗、學習與改進的靈活性。

提升 AI 系統的可觀察性

可觀察性是 AI 治理的基礎。您無法管理、審查或保護自己未曾察覺的系統，更無法控制那些無法監控或理解的系統。

隨著 AI 應用的普及，提升能見度已成為每個職責角色的首要任務：

- IT 團隊需要了解有哪些 AI 系統存在，以及它們的運作狀態。
- 開發人員必須掌握 AI 工具與 Agent 的運作行為，才能確保系統獲得負責任作業與管理。
- 資安團隊不論這些系統在何處執行或由誰建立，都需要具備探索、測試並保護它們的能力。

一套共享的安全控制措施，例如集中化的 AI 資產清單、一致的存取原則、全球資料保護以及統一的威脅偵測，有助於銜接這些需求。隨著 AI 成為您核心業務的一部分，您需要透過這些控制措施來提供可觀察性基準，以作為您治理策略的建構基礎。



平衡治理與創新

雖然安全與治理不可妥協，但過於嚴格的原則可能會拖慢試驗與 AI 的導入速度。在創新與控制之間取得平衡，是維持動能同時提升 AI 系統信任與安全性的關鍵。

隨著 AI 規模擴大及治理模型成熟，利益相關者之間存在著不同的優先事項。建置 AI 解決方案的團隊，追求快速行動、高度自主與執行彈性。IT 部門需要具備可擴展性、成本效益，並遵循原則的系統。資安團隊希望對 Agent 具備可見性、落實資料保護與存取控制，並確保系統能防範持續演變的威脅。

治理機制不應為迎合特定群體，而犧牲另一群體的推進速度。相反地，應建立共同的防護，讓創新得以持續推進，同時避免出現盲點或未受妥善管理的風險。

您的目標應是將前沿卓越中心轉變為加速中心，在簡化並鼓勵創新的同時，務實地分析風險。在投資防護以安全支援關鍵且高風險使用案例的同時，請平衡優先推動低風險使用案例的初步部署。

達成目標：可信賴且可稽核的 AI

完善的 AI 治理與安全措施，讓企業能夠自信地擴展 AI。隨著規模擴展，RAI 已深植於設計、部署與管理 AI 系統的方式中。治理貫穿了 AI 的生命週期，使 AI 工具與 Agent 具備可審計性與透明度，並與倫理、法規及商業期望保持一致。

在較高的成熟度層級，治理能帶來可衡量的商業效益。它能提升領導階層、員工、客戶與法規監管機構的信任。這套機制也簡化了部署流程，協助您的組織在不失去控制的前提下加快前進步伐。最終將打造出值得信賴且可審計的 AI，進而支持更強大的商業效益。

> 若要自信地擴展 AI 規模，核心限制往往不在於技術本身，而是在於營運模式、治理清晰度以及全企業範圍內的賦能。
>
> —資訊科技總監，零售

Microsoft 身為零號客戶

我們親身經歷的前沿轉型歷程，提供了眾多實務與實地範例，佐證了此藍圖中的核心原則如何在全面規模化時相輔相成。Microsoft 身兼技術提供者與跨多元業務範疇營運的企業雙重角色，透過在內部落實這些策略，進而加速推動自身的轉型步伐。

及早成立前沿卓越中心

我們的內部 IT 組織 Microsoft Digital 於 2023 年成立了第一個 AI 卓越中心，做為支援全公司內部 AI 推動工作的顧問小組。Microsoft Digital 內部的各個團隊開始滿懷熱情地建置工具、工作流程，以及啟用 AI 的解決方案。

轉型動能迅速提升，但我們很快就發現了不同的解決方案在應對相同的問題，且治理成效不一、標準與報告的使用也缺乏一致性。為了在大規模擴展中驅動一致且可衡量的 AI 成果，我們將前沿卓越中心的角色從純粹的「指引」演進為「協調」，藉此協助設定優先順序、定義防護，並將 AI 工作與業務成果直接連結。

我們前沿卓越中心的營運模式採取了刻意簡化的設計。員工只需透過統一的表單即可向卓越中心提報創意構想。隨後，前沿卓越中心團隊會根據四大共同支柱來評估各項計畫，藉此引導團隊跳脫單一專案的局部思維，進而確保所有專案皆能對齊核心業務優先順序、安全地進行規模化、擁有明確的落實路徑，並符合負責任導入規範：

策略支柱聚焦於分析 AI 專案的商業價值與實施心力。

架構支柱定義了我們如何協助團隊擴展 AI 解決方案，同時避免產生資安漏洞、合規問題，或日後必須清除的技術債。

藍圖支柱聚焦於 Microsoft 員工如何與 AI 互動，以確保使用者體驗具備凝聚力，並與我們更廣泛的員工體驗目標相符。

文化支柱確保 Microsoft 全公司對 AI 的採用皆具備目標性、負責性且可持續。它定義了 Microsoft 團隊應如何採用 AI，並將其整合至日常工作之中。



變更 IT 角色

我們自身大規模採用 Agent 的經驗，迫使 IT 的思維模式發生轉變。我們發現將 IT 人員當作守門人並無生產力；相反地，他們需要與開發人員及業務擁有者合作，扮演值得信賴的夥伴。

為了安全且大規模地加速 AI 採用，IT 需要更加主動、具備策略思維並導向平台化，為 Agent 在全企業中穩定運作所需之基礎能力承擔責任。

我們的 IT 團隊聚焦於幾個關鍵領域：

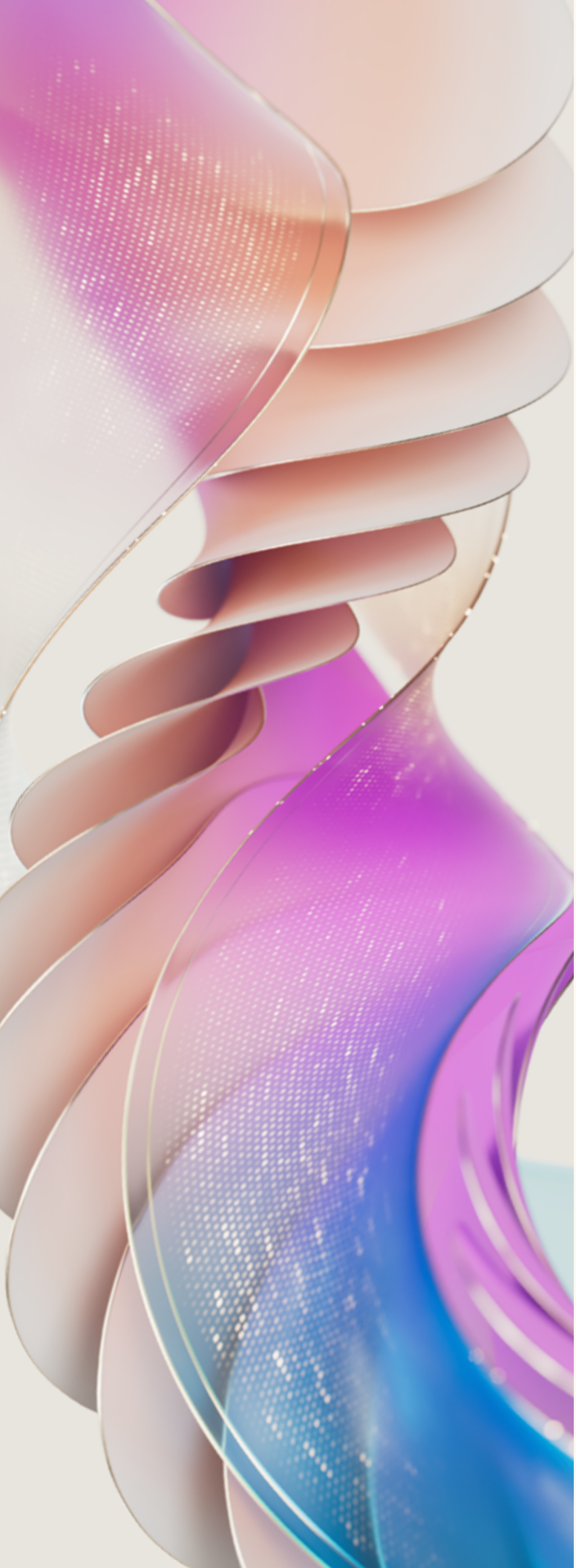
開發與維護 Agent 記憶體系統。Agent 需要持續且具背景關聯的記憶體，才能有效運作。IT 必須確保跨工作負載之記憶體儲存與管理系統，具備高度安全性、合規受控且表現一致。

協調 Agent 與核心系統之間的整合。Agent 的真正價值，取決於其與企業應用程式及業務流程的緊密連結。建構與管理 API、MCP、連接器及事件驅動流程基礎結構，確保 Agent 行動安全且可靠。

統籌策劃並開放經認證的資料來源。對 Agent 而言，資料品質決定了行動品質。IT 的角色從守門人轉變為策展人，負責提供值得信賴、治理完善的資料來源，讓 Agent 能夠自信地使用。這降低了風險，並提升了可靠性。

促使 Agent 從個人應用「晉升」至全企業範圍使用。許多 Agent 最初都是以個人或團隊層級的試驗開始。IT 負責管理 AI 生命週期，以確保具備實用價值的 Agent 在全公司範圍內規模化擴展之前，皆通過驗證、資安審查、整合強化以及營運就緒檢查。





透過經驗建立技能、信任與採用率

Microsoft 很早就意識到，對 AI 的信任是推動轉型的先決條件。我們聚焦於建立清晰的防護、透明的溝通以及一致的使用者體驗。負責任 AI 原則與合規機制，協助我們打造出安全、穩固且符合商業意圖的 AI 系統。

在此同時，我們也希望避免採取會阻礙 AI 使用的過度限制性控制。我們開發了一套「快車」方法，以受控、具備治理的方式來加速 AI 的採用。它聚焦於以下幾點：

- 我們挑選出一批深獲信賴的特定團隊與員工，**在初期便對其全面開放 AI 工具與核心功能的廣泛使用權限。**
- 這種存取權搭配**明確的防護、原則與監督。**
- 鼓勵團隊**嘗試、快速學習並反覆改進。**
- 透過中央治理、**監控與共享標準來管理風險。**

隨著採用的普及，大家對我們系統的 trust 也隨之加深。這使我們得以從打造個人生產力工具，轉向構建能與人類協同工作以創造新能力的 Agent。員工被賦權在受原則治理的生態系統中，去建立、部署並最佳化 Agent，將人類的判斷力與機器智能結合，從而實現大規模的工作流程轉型。

將 AI 整合至文化

我們推動前沿轉型的方法，要求我們必須針對五個關鍵領域進行組織與文化上的改變：

高階主管的支持。AI 轉型由高層親自領導。定義明確的業務與技能提升目標，皆與可衡量的成效保持對齊。領導階層的決策，是由展示採用率、證實 ROI 並指引未來資源配置的遙測資料所驅動。

嵌入式治理與負責任 AI。我們已建立的前沿卓越中心，在各項計畫中驅動著健全的治理、負責任 AI (RAI) 實踐與合規性。員工可使用 Microsoft Copilot Studio 與 Microsoft Foundry 建立 Agent，這些工具整合了我們的治理原則與防護措施。Microsoft Agent 365 提供組織內的管理與可觀察性。

企業級規模的採用與成效衡量。Microsoft 365 Copilot 和代理式 AI 已在全公司部署，並以即時遙測和使用目標追蹤採用情況。

技能培養與遊戲化的學習文化。為了支持持續學習，舉辦有趣的活動和內部競賽，鼓勵團隊爭取獎項與認可 (例如徽章與榮譽標誌)，以強化新行為，並協助將學習轉化為實用技能。

倡導者網路與社群擴展。跨部門的倡導者、實務社群及測試廚房會議，有助於壓力測試並擴大成功的實務做法。



將 AI 治理嵌入整個組織中

為了將治理嵌入整個組織中，將其視為加速器而非限制，我們的 Frontier CoE 推動了工程、安全、合規、資料以及業務主管之間的協作。我們的方法將人類判斷與 AI 驅動的風險分析和監控相結合，並融入了嚴格的資料治理、負責任 AI，以及在設計與部署流程中內建的合規原則。

我們在過程中學到了一些關鍵的課題：

跨領域的治理團隊是基礎。沒有任何單一團隊能有效治理 AI。只有當具備多元專業知識的主管共同加入 AI 治理團隊並攜手協作時，才能取得成功。

人類與 AI 系統協同運作時能發揮最佳效益。雖然決策仍由人類制定，但 AI 系統能強化治理。AI 協助我們分析風險、對應依賴關係、標記潛在的違規行為，並在數千個工作負載中擴展審查規模。

只有正確的資料才應該開放給 Agent。我們了解到，Agent 的生產力與資料整潔度直接相關。如果資料分類不當、重複或過度分享，Agent 就會放大這些問題。

從一開始就嵌入合規與負責任 AI 原則。在我們的 AI 轉型過程中，我們將內部實作與全球隱私權框架以及我們的 RAI 原則保持一致。這些原則已作為防護，嵌入在我們所有的 AI 平台中。



Microsoft 如何協助？

Microsoft 憑藉自身的前沿轉型歷程，以及多年來協助客戶發揮 AI 潛能的深厚經驗，已累積了豐富的實務知識。這包括各種訓練與參考資料、範例、工具與系統，能幫助您更快速且自信地從早期試驗邁向企業規模的 AI 採用。

如果您正在思考 *下一步該怎麼做？*，Microsoft 能提供經實證的方法、指引、平台與加速器來協助您。善用這些資源將有助於您建構分層的智慧基礎、建立可複製的治理與營運節奏，並提升團隊技能以協助他們加速交付解決方案。



企業級 AI 指引與框架

Microsoft 提供全面的指引、框架與資源，以支持您前沿轉型旅程的每個階段。我們汲取自身的企業經驗以及與客戶合作的實務心得，分享結構化方法、經實證的最佳實務和實用工具，協助您從試驗階段邁向具備治理且可擴展的 AI 採用。

- **Microsoft AI 採用**指引提供結構化流程，協助您將複雜的轉型工作分解為一系列更易管理的階段。
- **負責任 AI 工具與實務**
  資源提供一套完整的框架、治理模型、安全控管、評估工具及營運最佳做法，旨在協助您在企業規模下建置、部署、保護、監控及治理安全且負責任 **AI** 系統。
- **AI** 解決方案加速器 **(AI Solution Accelerator)**
  網站提供了範本、範例與指引，能協助您快速建立 AI 解決方案。
- **Microsoft Inside Track 部落格**介紹 Microsoft 如何運用 AI 來解決問題、改進產品並幫助客戶。
- **AI Skills Navigator** 協助您引導全體員工大規模參與結構化的角色導向學習旅程，讓您能夠追踪進度、培養職能並長久維持轉型動能。

建立前沿卓越中心的指引

Microsoft **卓越中心指引**能協助建立前沿卓越中心，做為推動轉型的核心組織團隊。

這份指引概述了前沿卓越中心的角色、職責與參與模式，供您的業務與技術團隊在內部採用。其中包含變更管理與溝通的最佳實務，以及將治理、負責任 AI 和生命週期管理嵌入前沿卓越中心管轄權責下的相關建議。

AI 卓越中心 的學習路徑是協助員工理解卓越中心概念及其優勢的優質資源。



結論

這份藍圖概述了推動 AI 就緒的共同驅動因素，並為您展示了多種可採行的策略與實務做法，以最大程度地提高 AI 為企業帶來重大且正向影響的機會。我們希望這些洞察與指引能協助您以更清晰的思維與信心迎接 AI，進而持續創新並隨著時間推移見證複合價值的增長。

下一步該做什麼？

在前沿轉型之路上邁出下一步。

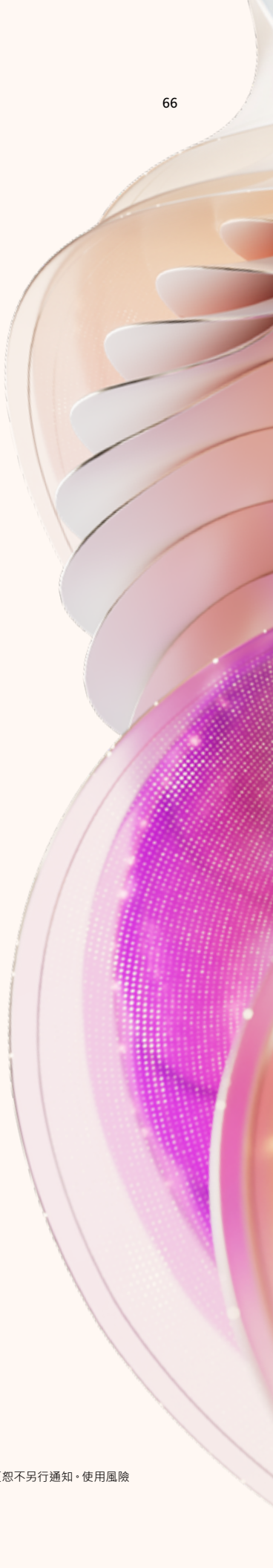
探索 **Microsoft AI**，從試驗階段邁向全企業影響力。

在 **AI Skills Navigator** 上培養規劃、制定策略以及擴展 AI 專案所需的技能。

研究與方法

本電子書背後的研究包括 Emerald Research Group 代表 Microsoft 公司進行的研究。這項研究進行了 70 次深入訪談，對象為參與推動 AI 轉型的 IT 領導者與商業決策者。

為了確保這些研究能涵蓋多元的經驗，Emerald Research Group 篩選了來自不同背景組織的候選人，其中包含已在 AI 領域取得成功者，以及在 AI 採用與使用上較為謹慎或進度落後者。Emerald Research Group 親自挑選來自不同領域及各大產業的人士，以擴大研究結果的範疇與價值。研究人員於 2026 年 2 月 23 日至 2026 年 3 月 13 日期間，進行了多場 30 至 45 分鐘的訪談，以深入探討其組織的 AI 規模化旅程。



©2026 Microsoft Corporation.版權所有，保留一切權利。本文件是以「現況」提供。文中所呈現的資訊和觀點，包括 URL 及其他網際網路網站參考資料，如有變更恕不另行通知。使用風險須自行承擔。本文未賦予您對於任何 Microsoft 產品中任何智慧財產權的任何法律權利。您可以針對內部參考用途，複製及使用本文件。