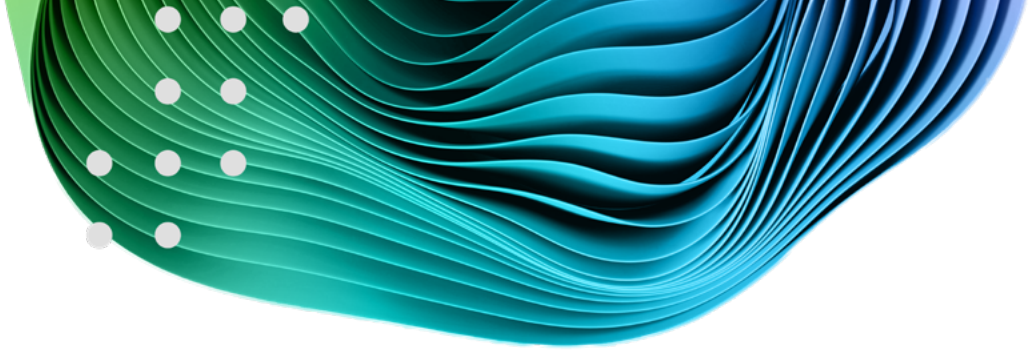
Deloitte.

台灣人工智慧學校
Taiwan AI Academy



企業 AI 治理白皮書

實現 AI 的規模化落地與長期競爭優勢



前言：AI 治理驅動組織轉型與永續成長的關鍵能力

以策略釐清、組織推動、風險管理與人才發展四大支柱，協助企業將AI 潛力轉化為可持續的商業價值

當前全球產業正處於數位轉型與智慧化發展的關鍵階段。隨著人工智慧（AI）技術快速成熟與生成式 AI 的廣泛應用，企業正面臨前所未有的機會與挑戰。AI 不僅能提升營運效率、優化決策品質及創造創新商業模式，更逐漸成為企業強化競爭力與驅動永續成長的重要動能。然而，企業在積極推動 AI 應用的過程中，也同時面臨策略方向不明、組織協作不足、風險管理機制未臻完善，以及人才能力落差等課題，使 AI 的潛在價值難以充分發揮。

面對快速變動的市場環境與技術發展趨勢，企業若要真正實現 AI 價值，不應僅聚焦於技術導入，更需從企業整體經營角度出發，建立兼顧策略發展、組織治理、風險控管及人才培育的系統化管理架構。透過明確的發展藍圖與治理機制，企業方能有效整合資源、降低風險，並將 AI 能力轉化為持續創造價值的核心競爭優勢。

基於上述趨勢，我們期望透過此份《企業人工智慧治理白皮書》報告，協助董事會與高階管理階層從企業經營與價值創造的角度，重新思考企業 AI 治理，並聚焦於四個彼此連動的關鍵面向，以創造長期且永續的競爭優勢：

- 策略釐清：關注的不只是「我們要使用什麼 AI」，而是 AI 將如何支持企業未來的成長策略、競爭定位與價值創造，並據此建立清楚的發展藍圖與投資優先順序。
- 組織推動：將策略轉化為執行能力，透過適當的治理架構、權責分工與跨部門協作，使 AI 不再只是個別部門的創新專案，而能逐步形成企業級能力。
- 風險管理：其核心並非阻止企業使用 AI，而是建立與 AI 風險程度相匹配的管理機制，使企業在資料、模型、資安、第三方及 AI 自主行為等風險可被掌握前提下，加速創新與應用。
- 人才發展: 建立 AI 時代所需要的新型組織能力。企業除了需要 AI 專業人才，更需要讓管理者與員工具備理解、運用、監督及管理 AI 的能力，進一步重新設計人與 AI 的分工與協作模式。

目錄

前言：AI 治理驅動組織轉型與永續成長的關鍵能力 **1**

01 策略釐清：AI × Strategy = Competitive Advantage **3**

02 組織推動 **9**

03 風險管理 **13**

04 人才發展 **19**

結語 **23**

發起與研究團隊 **24**

策略釐清：AI × Strategy = Competitive Advantage

01

在人工智慧時代，企業的成功不僅取決於技術的導入，更仰賴於清晰的策略方向。本章節旨在闡述如何將 AI 發展與企業核心目標深度對齊，透過明確的價值定位、系統性的績效衡量與動態的資源配置，確保每一分 AI 投資都能轉化為可持續的競爭優勢，並在掌握機會與風險之間取得最佳平衡。

AI 策略治理：確保方向一致，掌握機會與風險

在人工智慧時代，策略是確保 AI 投資能有效創造企業價值的關鍵。董事會應關注 AI 發展方向是否與企業整體策略及長期目標一致，並持續監督策略執行成效，確保資源配置能支持核心業務與未來成長。面對 AI 技術快速演進及外部環境變化，董事會亦應協助管理階層掌握新興機會與潛在風險，適時調整發展方向，避免資源錯置或錯失關鍵契機。透過將 AI 納入企業整體策略規劃與持續優化機制，企業得以在風險可控的前提下，強化競爭優勢並創造長期價值，同時提升組織韌性、強化創新能力，並建立面對市場變化的快速應變機制，以支持企業永續發展與穩健成長。

此外，董事會應定期檢視 AI 投資與企業整體經營績效之關聯性，確保各項 AI 計畫不僅著重技術導入，更能實際促進營運效率提升、創新商業模式發展及客戶價值創造。透過建立明確的策略目標、績效指標與追蹤機制，董事會得以掌握 AI 應用的實際效益，並據以評估投資成果與資源運用效率，確保相關計畫能持續為企業創造可衡量的價值。

企業 AI 治理藍圖：董事會監督與管理實務

願景與使命

定義並維護組織的願景與使命宣言，確認其與組織的策略目標及 AI 潛力相符。

策略規劃

維持反覆監控管理層執行 AI 策略計畫的過程，找出最受 AI 影響的核心業務流程。

利害關係人參與

與股東、員工、客戶及其他利害關係人保持透明溝通與參與，討論 AI 的使用與治理。

董事會與管理階層共同作為

資源與資本配置

- 檢視企業 AI 資源投入方向與配置情形
  - 預算
  - 人力
  - 技術
- 確保資源能支持關鍵 AI 策略與成長目標

AI 導入節奏

- 評估 AI 推動速度是否在創新與風險控管之間取得平衡
- 確保發展方向與企業策略目標一致

績效指標

- 掌握關鍵績效指標（KPI），以衡量 AI 推動是否符合企業策略目標
- 依據執行情形適時調整發展方向

市場趨勢關注

- 持續關注 AI 市場趨勢、競爭動態及潛在機會與威脅，作為策略規劃與決策的重要依據。

文化驅動

- 建立負責任 AI 文化及相關責任歸屬機制。
- 規劃 AI 關鍵人才發展策略與能力藍圖。
- 監督AI人才招募、培育、留任及獎懲制度規劃。

機會探索與策略定位

面對 AI 驅動的產業變革，企業應從商業價值、數據、組織文化及應用場景等面向系統化探索機會，並透過治理轉型、數據賦能與人才培育三大策略，逐步實現 AI 價值落地。

透過系統性的機會探索與策略布局，企業不僅能更有效地發掘 AI 所帶來的成長機會，也能在兼顧風險管理與治理要求的前提下，加速 AI 應用落地，提升組織韌性、強化市場競爭力，並建立持續創新與永續發展的能力。



機會探索

商業價值的對齊

- 確保應用場景與核心目標一致
- 優先高報酬與低風險的試點

數據的價值變現

- 盤點核心數據找出業務痛點
- 整合數據開拓新商業模式與營收來源

組織文化的適應

- 推動全體員工的 AI 素養
- 建立快速迭代組織，減少轉型阻力

AI 應用及場景的識別

- 主動探索適合自身發展的創新應用
- 以單點營運流程為單位進行獨立識別與剖析



對應策略

AI 治理與價值轉型

- 建立 AI 治理框架與責任機制
- 推動人機協作流程優化
- 以高價值場景加速落地驗證

數據價值與創新發展

- 建立企業級資料治理機制
- 提升數據資產整合與共享能力
- 發展數據驅動決策與創新商業模式

戰略人才培育需求

- 建立管理層與技術開發的風險認知
- 培植具備 AI 治理與跨界能力的人才

掌握 AI 績效，建立一致且清楚的績效衡量方式

為確保 AI 投資能持續創造價值，企業應建立一致且清楚的績效衡量機制，從財務效益、營運績效及法遵與治理等面向定期檢視執行成果。透過衡量投資報酬、作業效率提升、成本優化及法規遵循情形，企業能更全面掌握 AI 應用成效，作為資源配置與策略調整的重要依據，進而在兼顧創新、風險管理與企業治理的前提下，持續提升營運價值與競爭力。



定期檢視與 AI 投資相關的預算與財務預測，包括投資報酬及成本節省成效等指標。

- 長期資本配置能力： 建立涵蓋建置、規模化到維運的全生命週期成本預估
- 投資邊際效益：定義與衡量 AI 投入對業務淨利潤與資本回報的驅動力
- 資源配置動態性： 快速更迭的技術，企業須有相應的財務預測機制。



持續關注關鍵營運指標，以評估 AI 應用是否提升作業效率與整體成效。

人機協作效率：AI 導入重塑工作結構，達到精實核心資源的效果

- 營運效率的槓桿：AI 精準配置在關鍵的業務或決策瓶頸而提升效率
- 組織適應力成本：評估組織文化轉型與員工素養提升所投入的時間成本



將法規遵循與聲譽管理視為 AI 投資的安全紅線，全面評估技術應用對現行監管要求的衝擊，並在「資訊透明度」與「法律曝險」之間取得戰略平衡，以確保企業建立聲譽防護網。

法規掌握度：董事會應全面掌握 AI 策略涉及的法規監管要求，並確保審查政策能實質支持監督職責。	流程合規性：須評估公司是否已將最新的 AI 法律義務，深度內化至現行的內部政策與作業流程中。	揭露與曝險平衡：評估對外進行自願性揭露時的潛在風險，確保提升透明度的同時，不增加法律與聲譽曝險。

AI 價值實現與投資回報

企業更應建立完整的 AI 價值衡量機制，從財務效益、營運績效、風險管理及策略價值等多元面向，全面評估 AI 導入所創造的成果。透過建立明確的 KPI 與成效指標，持續追蹤、監控及檢視 AI 投資效益，確保 AI 應用與企業策略目標保持一致，提升投資決策的透明度、可衡量性與商業價值。

此外，企業應定期檢視 AI 投資成果與價值實現情形，依據實際成效持續優化資源配置與投資方向，提高 AI 專案成功率，並為後續擴大 AI 應用規模、推動組織轉型及制定未來投資策略，提供客觀、可量化且具證據支持的決策依據。



AI 導入策略規劃藍圖

AI 的戰略價值，在於將企業原本的價值定位無限放大。在導入前的關鍵節點，董事會與 CEO 的核心任務，是透過產業定位、藍圖整合與願景確立，將技術紅利穩健轉化為企業的長期數位壁壘。

企業在規劃 AI 導入藍圖時，應先評估產業成熟度與自身競爭優勢，聚焦高價值應用場景，並將 AI 視為推動營運優化與商業模式創新的重要動能。同時，在資源配置、治理架構、風險管理及人才培育等面向建立一致的推動機制，逐步完成組織轉型與數位資產累積，使 AI 從技術工具提升為驅動企業長期成長與競爭力的重要策略資產。



組織推動：

02

將 AI 策略轉化為組織的具體行動，需要一個強而有力的組織架構來支撐。本章節的核心在於建立一套從上到下權責分明、運作流暢的推動體系，明確界定董事會、管理階層及執行單位的監督與管理職能，確保 AI 在企業內部能獲得一致、高效且負責任的發展。

掌握 AI 發展關鍵時刻，治理能力決定長期競爭力

隨著 AI 逐漸成為企業創新與成長的重要驅動力，企業正迎來關鍵轉型契機，善用 AI 可提升營運效率、優化客戶體驗、加速創新，並創造新的商業價值。然而，唯有透過完善的治理機制，企業才能將 AI 潛力有效轉化為可持續的競爭優勢。若缺乏適當治理，企業可能面臨決策偏誤、資訊安全與合規風險、資源配置失衡等挑戰，進而影響品牌信任、營運穩定及策略執行成效。因此，建立完整的 AI 治理架構，不僅有助於風險管理，更能促進跨部門協作、加速策略落地，讓企業在掌握 AI 機會的同時，持續強化企業長期競爭力。

在治理架構上，企業可由管理階層帶動，串聯 IT、數據、資安、法務及業務等跨部門團隊，建立明確的治理權責。同時，透過 AI 治理的協作、溝通與決策機制，明確規範 AI 應用的評估、導入與管理流程，在兼顧創新與風險的同時，加速 AI 應用落地。

掌握 AI 發展關鍵時刻，治理能力決定長期競爭力



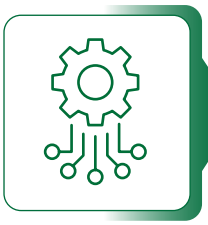
治理架構

隨著 AI 逐步成為企業策略與營運的重要驅動力，企業應建立適當的治理架構，以確保 AI 發展方向、資源投入及風險管理能獲得有效監督，並與企業整體策略目標保持一致。



治理議題溝通機制

AI 議題往往涉及多個部門與管理層級，因此企業需建立有效的溝通機制，確保重要資訊、風險及治理議題能於組織內部充分流通，提升治理透明度與監督效能。



跨職能協作與決策流程

由於 AI 應用涉及業務、技術、資訊安全、法遵及風險管理等多元領域，企業應建立適當的跨職能協作與決策機制，以整合不同專業觀點，提升治理品質與決策效率。

掌握 AI 發展關鍵時刻，治理能力決定長期競爭力

01 **企業監理架構是否需要調整？**

是否需設立新委員會或調整現有分工，以強化 AI 監督能力？

02 **企業是否已建立 AI 治理機制？**

是否具備完整的 AI 治理架構與相關政策，並納入「負責任 AI」原則？

03 **企業內由誰負責 AI 策略的規劃與推動？**

董事會是否清楚掌握負責 AI 策略執行的高階主管、團隊或委員會？

04 **AI 推動的策略與績效如何向董事會報告？**

是否明確界定負責回報 AI 進展與議題的管理階層窗口與報告機制？

05 **AI 是否已納入常態治理與監督機制？**

董事會是否已將 AI 相關風險、投資及重大決策納入定期討論事項？

建立跨部門 AI 治理架構，強化企業監督與決策能力

為有效推動 AI 應用並發揮其價值，企業可考量建立由董事會監督、高階管理階層參與之 AI 治理組織架構，明確權責分工與決策機制。透過治理、決策、推動及應用等層級的協同運作，以強化 AI 發展方向、資源投入及風險管理之監督機制。



AI 治理關注面向

不同企業之 AI 發展階段、應用情境及治理需求可能有所差異，企業可依實際情況，考量關注下列 AI 治理面向：

- AI 策略目標與重大投資規劃
- AI 風險管理及重大事件處理
- 法規遵循、資訊安全與資料治理
- AI 治理機制推動及執行情形
- AI 治理成熟度與持續改善進展

AI 治理架構常見推動挑戰

- 權責分工不清，跨部門協調與決策效率不足
- AI 應用快速增加，治理機制與流程未同步建立
- 法遵、資安與資料治理要求日益複雜
- AI 風險缺乏一致評估標準與監督機制
- 治理認知與投入程度不一

AI 治理協作、溝通與決策機制

AI 治理架構建立後，企業仍須透過常態化的溝通機制與跨職能決策流程，確保各項 AI 應用在推動創新的同時，兼顧風險管理、法規遵循及企業策略目標。

AI 治理議題溝通機制之重要性

AI 治理最大的風險往往不是技術失效，而是重要資訊未能被即時傳遞至適當的管理與監督層級。當 AI 議題橫跨多個部門時，若缺乏正式的溝通機制，容易形成資訊孤島、治理標準不一致及風險管理落差，進而影響企業決策品質及對重大 AI 議題的監督效能。因此，企業應建立制度化的 AI 治理議題溝通機制，透過定期會議、管理報告及議題通報等方式，確保 AI 發展進度、風險評估結果、法規變化及重大議題能於各治理層級間有效傳遞，透過透明且一致的資訊共享，管理階層及董事會得以及時掌握關鍵風險與發展趨勢，並確保 AI 治理方向與企業策略目標及風險承受度保持一致。

跨職能協作與決策流程

AI 應用往往同時涉及業務需求、技術可行性、資訊安全、法規遵循及風險管理等多重面向，其影響已超越單一部門所能評估與管理的範圍。若缺乏明確的跨職能協作與決策機制，容易因權責不清、部門觀點差異或協調不足而產生決策落差，進而影響 AI 治理成效。因此，企業應建立制度化的跨部門協作與決策機制，確保 AI 相關議題能獲得適當評估、審查與決策，並透過明確的權責分工與爭議事件升級流程，提升決策品質及執行效率。

AI 治理運作機制應具備之核心特性

為確保董事會、高階管理階層及各職能單位能有效掌握 AI 發展、風險及重大議題，企業應建立具備下列特性的治理溝通與決策機制，以提升治理透明度、決策品質及監督效能：

原則	說明
透明性 (Transparency)	確保重大 AI 專案、風險與治理議題能被適時揭露與掌握，提升治理透明度。
一致性與標準化 (Consistency & Standardization)	建立跨部門共同遵循之治理標準與管理要求，避免各自為政或重複決策。
問責性與權責分工 (Accountability)	明確界定各治理層級的角色、責任與決策權限，確保責任可歸屬。
及時升級與監督 (Timely Escalation & Oversight)	建立重大風險、事件及爭議事項的升級機制，確保能及時獲得適當監督與決策。
可追溯性 (Traceability)	保留重要決策、審查與風險評估紀錄，以支持後續查核、監督及持續改善。

風險管理

03

隨著 AI 應用日益廣泛，其衍生的風險也變得更加複雜多元。本章節旨在建立一套貫穿 AI 生命週期的整合性風險管理體系，從資料的可信度出發，系統性地識別、評估與應對各類潛在風險，確保 AI 在追求創新的同時，其發展始終維持在企業可控、合規且值得信賴的軌道上。

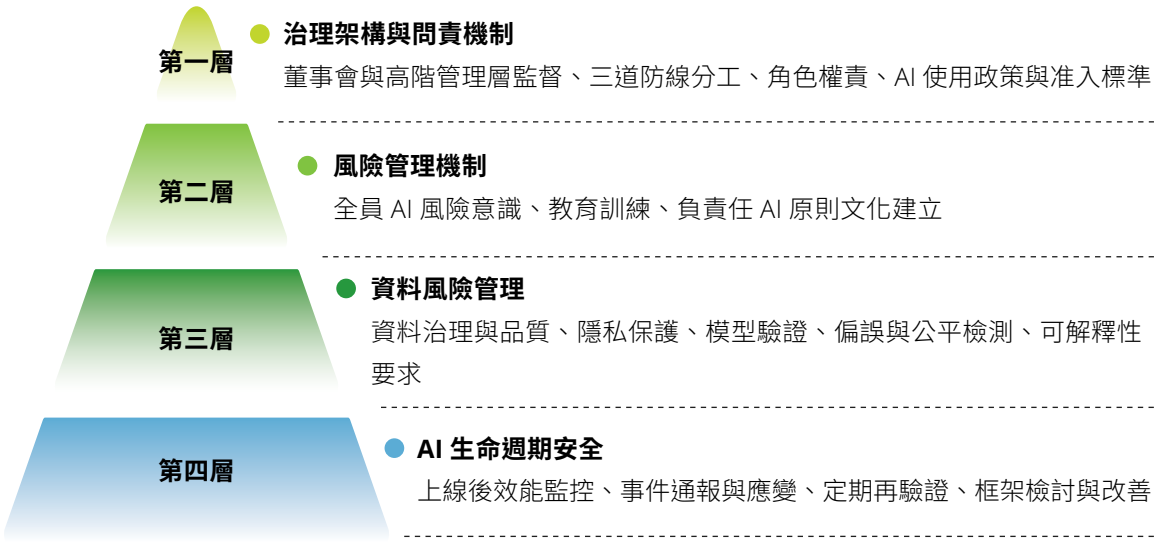
治理驅動：建立可信任的 AI 風險管理體系

企業應建構涵蓋治理權責、風險管理、資料治理及 AI 生命週期安全的多層次防線，並將風險識別、評估、減緩、應變與持續監控納入日常管理流程，形成系統化且可追蹤的風險管理機制。透過董事會、高階管理團隊及相關業務單位的共同參與，明確界定權責分工與監督機制，確保 AI 應用發展方向符合企業風險承受能力。同時，企業應建立定期檢視與改善機制，持續追蹤 AI 模型效能、資料品質及法規遵循情形，以能及時因應技術、業務及外部環境變化所衍生的新興風險。

此外，針對資料品質、合法授權、決策可追溯性、偏誤公平性、資訊安全、隱私保護及產業應用風險等面向，應採取適當且差異化的管控措施，並於 AI 技術開發、部署、營運及監控各階段落實風險管理要求。透過建立透明且可稽核的治理機制，提升利害關係人對 AI 應用的信任度，確保 AI 在推動創新、提升營運效率與創造商業價值的同時，兼顧合規要求、企業聲譽及永續發展目標，打造安全、可靠且負責任的 AI 應用環境。

企業 AI 治理風險管理框架

建立以風險基礎之管理規範，因應 AI 運用風險施予不同程度風險管控措施，建立系統化遵循架構。



AI 風險管理

掌握 AI 風險，確保策略與營運穩健

隨著 AI 逐步成為企業策略與營運的核心工具，其所帶來的風險亦更加多元且複雜，涵蓋策略面、營運面及外部環境等層面。企業管理階層應充分理解並監督 AI 相關風險，確保其已納入企業整體風險管理機制中進行系統性管理。同時，AI 不僅會產生新的風險，也可能放大既有風險，對企業整體策略執行與營運穩定性造成影響，建議透過持續監督與整合性風險管理，確保企業在推動 AI 創新的同時，有效維持風險於可控範圍內，強化組織韌性與長期發展能力。

風險面向

偏見與不公平風險	供應鏈風險	聲譽與信任風險
透明度與可解釋性風險	營運風險	法規遵循風險
資安與濫用風險	模型可靠性風險	治理機制風險
第三方風險	資料隱私風險	策略與競爭風險

AI 風險管理流程

企業應建立完整的 AI 風險管理流程，從風險識別開始，辨識各類 AI 應用可能產生的倫理議題、模型偏誤、透明度不足及法規遵循等風險；接著透過風險評估分析風險發生的可能性與潛在影響，並依據風險程度進行優先排序。在此基礎上，企業應採取適當的控制措施以降低風險，並管理第三方供應商所衍生的相關風險。同時建立事件通報與應變機制，以妥善處理 AI 應用可能引發的各類事件與挑戰。最後，管理階層應持續監控 AI 風險並定期向董事會報告執行情形，透過監督、檢討與改善機制，確保 AI 應用在安全、透明、合規及可信賴的原則下穩健發展。

01 風險識別

辨識各類 AI 風險，如倫理議題、偏見、模型幻覺及透明度不足等。

02 風險評估

評估風險**發生的可能性**與**影響程度**，並進行優先排序。

03 風險抵減

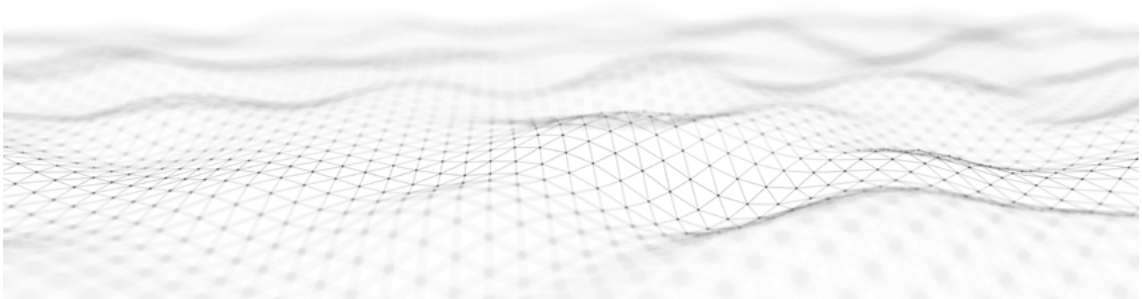
採取適當控制措施降低風險，並涵蓋第三方供應商所帶來的相關風險。

04 應變準備

建立因應機制，以妥善處理 AI 可能引發的各類事件與挑戰。

05 風險監控與報告

- 管理階層應持續監控 AI 相關風險，定期向董事會報告風險管理執行情形，以支持董事會履行監督職責並提升透明度與問責性。
- 應依第三方參與程度建立相應的監督機制，確保外部服務提供者於 AI 應用中的風險亦納入整體治理範疇。



各產業 AI 應用風險曝險焦點

AI 一旦進入決策現場，即同時承擔多重風險，從演算法歧視到解釋性申訴，企業不僅需因應公平性與透明度要求，更必須提升決策可解釋度，以縮小能力落差、化解層層風險，並在挑戰中尋找成長契機。

不同產業的 AI 風險曝險焦點釋例

高度曝險 法規合規	**金融、保險、醫療、能源：專法約束風險** 金融、核保、醫療診斷及能源基礎設施等場景若採用 AI，企業將面臨多重法規疊加，需建立差異影響評估、申訴專責窗口與決策說明機制。
中度曝險 公平聲譽	**人力資源、教育、零售：公平性與聲譽曝險** 履歷篩選、學生評估、動態定價等應用，公平性與品牌信任為主要風險源，負面事件將直接衝擊品牌與市佔。
特定曝險 營業秘密	**製造、物流：營業秘密與專有資訊外洩** 製程優化、預測維護、需求預測等場景，主要風險為資料品質與模型準確性，以及第三方模型使用之資訊外流風險。

產業應用 AI 風險管理行動建議

- **短期 (3~6 個月)：**
  由風險管理單位提出主要風險識別與抵減規劃。
- **中期 (6~12 個月)：**
  建立子構面的內部盤點與分級機制，納入年度風險管理議題
- **長期 (1 年以上)：**
  將完整風險面向納入企業風險儀表板，每年重新校準

資料風險管理——驅動 AI 的資料可信度

AI 的風險與價值皆源自資料。若資料品質、來源或授權不明，即使技術再先進，也可能產生錯誤決策，並放大營運、法遵與聲譽風險。因此，企業應強化資料治理，確保資料正確、合法且可追溯，並使 AI 結果可解釋、可審核及可問責。

信任 AI 的五大資料治理面向

1



資料品質（Data Quality）：避免劣質資料驅動錯誤決策

高品質資料是可信任 AI 的基礎。董事會應督促建立持續性資料品質管理，確保關鍵資料在全生命週期具備完整性、正確性與即時性；否則將導致 AI 誤判，影響營運決策與財務結果。

2



關鍵資料識別（Critical Data Elements, CDE）：資源應集中於真正重要的數據

不是所有資料都需同等治理強度。董事會應確認已識別關鍵資料（財務績效、營運決策與風險、法遵申報），並對其採取更高強度的品質控管、存取限制與監督，避免 AI 建立於不可靠資料之上。

3



資料來源合法性與使用授權（Legality & Authorization）：避免「合法取得但不當使用」

在 AI 時代，風險多來自「超出授權目的的資料使用」。董事會應確認：「蒐集符合法規、同意涵蓋 AI 訓練與推論、 防範機敏資料留存或外洩」。完善資料授權管理，可降低合規與聲譽風險，並維護利害關係人信任。

4



資料追溯與決策回溯（Lineage & Traceability）：讓 AI 決策經得起檢視

董事會有效監督 AI 的前提在於決策是否具備可追溯性；因此，資料治理需確保資料從產生、轉換到被 AI 使用的全流程可追蹤，並在發生錯誤或爭議時能快速溯源，同時讓 AI 產出可回連其數據依據，以支撐可解釋性與問責需求。這不僅是技術議題，更是因應監理、稽核與外部質疑的關鍵防線。

5



資料偏誤與公平性（Bias Source）：避免 AI 系統性放大既有偏差

資料可能隱含偏誤，若缺乏治理，AI 恐放大不公平與歧視。因此，董事會應要求建立偏誤辨識與修正機制，以識別資料中是否存在偏見，並透過數據洗淨與平衡，防止 AI 放大既有的社會偏見或系統性誤差，確保符合企業價值與社會責任。

從生命週期角度管理 AI 風險

此治理框架旨在為企業提供全面性與結構化方法，將風險管理深度融入技術發展的每一個生命週期階段。本架構建立了一套跨越資料、開發、部署與監控的動態治理體系，協助企業在追求卓越創新的同時，構築堅實的信任防線。

監控階段｜持續審計與動態演進

AI 系統部署後需持續監控與優化，透過模型表現追蹤、漂移檢測及使用者回饋管理，確保效能穩定；並建立即時應變機制，於異常或安全事件發生時迅速啟動備援措施，維持系統穩定與業務連續性。

部署階段｜系統集成與防禦壁壘建構

此階段聚焦於 AI 系統上線後的持續監控、效能優化與風險管理，透過模型效能監測、使用者回饋蒐集及持續優化機制，確保系統穩定運作並符合業務需求。風險管理則著重於資安防護、異常監測與合規治理，以降低模型攻擊、資料洩露及法遵風險。

資料階段｜數據資產的奠基與倫理防禦

此階段涵蓋資料蒐集、處理與標註等作業，確保資料品質、完整性與可用性。風險管理核心包含隱私保護與資料偏見治理，透過去識別化、匿名化及公平性檢測等機制，防範敏感資訊外洩與偏誤風險，提升資料合規性與模型可信度。

開發階段｜模型構建與算法透明度控制

此階段是將資料轉化為 AI 能力的關鍵過程，核心範疇包含模型選擇、訓練與驗證。風險管理聚焦於模型公平性與透明度，透過偏差檢測降低性別、地域等因素對決策結果的影響，確保模型輸出更公平一致；同時提升決策邏輯的可理解性與可追溯性，讓業務與管理人員能掌握模型判斷依據，進一步提升模型可信度與治理成效。



人才發展：

04

將人才是落實 AI 治理與實現人機協作價值的根本。本章節將探討在 AI 驅動的轉型浪潮下，企業應如何重新定義工作模式，並透過差異化的培訓策略，系統性地提升員工的 AI 協作能力與風險素養，最終將人力資本轉化為驅動企業前進的核心動能。

建構關鍵能力，支撐 AI 發展與治理落地

AI 治理不僅依賴技術，更需跨域人才，培養與引進關鍵人才，有助於確保 AI 應用在合規與創新間取得平衡，並提升組織整體應對能力。 同時，企業應建立跨部門協作機制，強化管理、業務、法務及技術團隊之間的溝通與整合，以有效推動 AI 治理與應用發展。

企業可從 AI 素養提升、人機協作時代的工作重塑，以及 AI 人才與組織策略三大面向著手，逐步建立支撐 AI 發展與治理落地的核心能力。

1 AI 素養提升：

透過系統性的全體員工培訓，提升全員的 AI 素養，確保每位同仁都能在新的協作架構中發揮價值。

2 人機協作時代的工作重塑：

企業應重新定義工作流程、人才角色與組織運作模式，進而提升營運效率、創新能力與企業競爭力。透過善用 AI 協助處理重複性工作，員工可將更多資源投入高價值決策、創新與客戶服務等關鍵活動。

3 AI 人才與組織策略：

企業必須調整組織架構並制定人才策略，同時應培養具備技術、業務及治理能力的跨域人才，建立長期的人才發展機制，確保 AI 策略得以持續推動並創造實際效益。

AI 素養提升：最有效率的企業轉型是完善人員再培訓機制，透過差異化訓練提升整體人才 AI 水準

企業要成功推動 AI 轉型，最有效的方法不是讓所有人接受相同訓練，而是先補齊 AI 能力落差，再依不同人才成熟度實施差異化培養。

1	**定位轉向**	**「替代者」到「副駕駛」**：政策須明確將 AI 定義為能力增強工具而非人力取代方案
2	**責任賦能**	**保留人類最終決策權**：法律與組織框架下，明確員工擁有最終的裁量權與監督職責
3	**溝通環境**	**建立高信任與低摩擦文化**：打造透明的溝通管道，明確轉型目標在於「價值提升」
4	**參與式推動**	**消除轉型心理阻力**：讓員工參與 AI 導入過程，將「技術壓力」轉化為「參與動力」
5	**激勵機制**	**將效能轉化為自發動力**：建立透明且與技術效能掛鉤的激勵與績效制度

設計再培訓機制，透過差異化訓練提升整體同仁 AI 素養

統一訓練 → 差異化管理

加速轉型人才

能執行 AI 策略與管理 AI 風險的人才接受進階培養，流程重設、人機協作設計、AI champion 培訓

重點投資人才

對於成熟度不足者提升協作能力而謹慎者則有效結合專業判斷與 AI 工具，差異化訓練適配人才

配置轉換對象

AI 能力落差較大，需辨識落差來源後，分配學習資源，縮小 AI 不平等

分階段培訓人

建立 AI 基礎

所有人都要具備 AI 素養，包括使用邊界、常見錯誤、風險與倫理原則，避免在低度掌握下誤用 AI

情境化應用

依職類、角色與實際任務訓練，連動工作場景並嵌入工作，例如 HR 要熟悉招募、人才分析的 AI 使用與風險

角色轉換

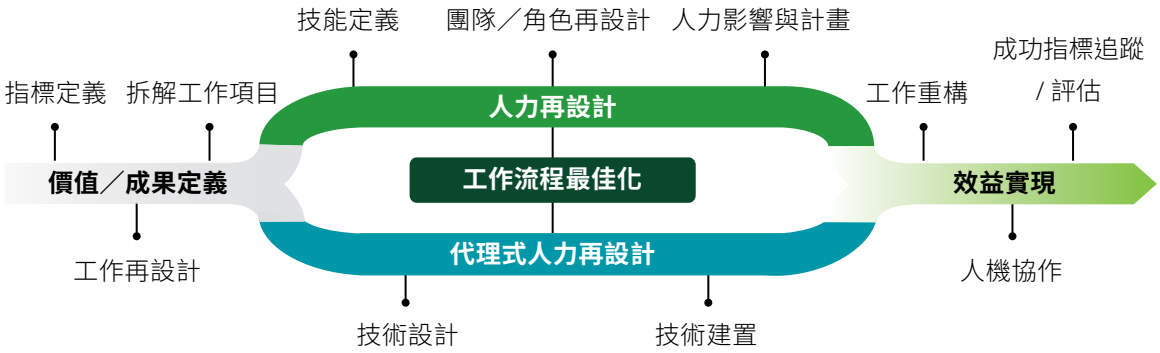
職位的任務結構改變，工作被重新拆解，要訓練轉換角色，從重複作業者轉向跨部門協調與例外處理者

人機協作時代的工作重塑 ：人機協作時代的人才再定義與能力轉型

隨著 AI 快速發展，企業競爭力的核心已從流程效率延伸至人才能力重塑。面對人機協作的新工作模式，企業應重新思考未來人才所需的能力、角色定位與發展路徑。從高價值應用場景出發，盤點關鍵人才缺口，培養兼具商業洞察、數位能力與 AI 協作能力的人才，並建立支持持續學習與創新的組織文化，打造兼具韌性與競爭力的未來人才團隊

未來人才轉型框架

以企業策略與高價值業務場景為基礎，重新定義未來人才所需能力與角色。透過能力盤點、人才發展、角色轉型以及人機協作模式設計，協助員工從執行者升級為價值創造者，全面提升個人與組織競爭力。



人才策略四大重點

高價值 Use Case 識別關鍵人才需求

- 哪些工作將因 AI 而改變？
- 哪些能力將成為未來關鍵競爭力？
- 哪些人才類型最具策略價值？
- 未來需要哪些新興角色？

盤點未來關鍵能力與人才缺口

- 現有人才具備哪些能力？
- 未來能力需求與現況差距為何？
- 哪些關鍵能力需優先培養？
- 哪些人才需重新培訓與轉型？

建立 AI 時代的人才發展機制

- 如何提升 AI 與數據應用能力？
- 如何培育跨域協作與創新能力？
- 如何建立持續學習文化？
- 如何加速人才成長與能力升級？

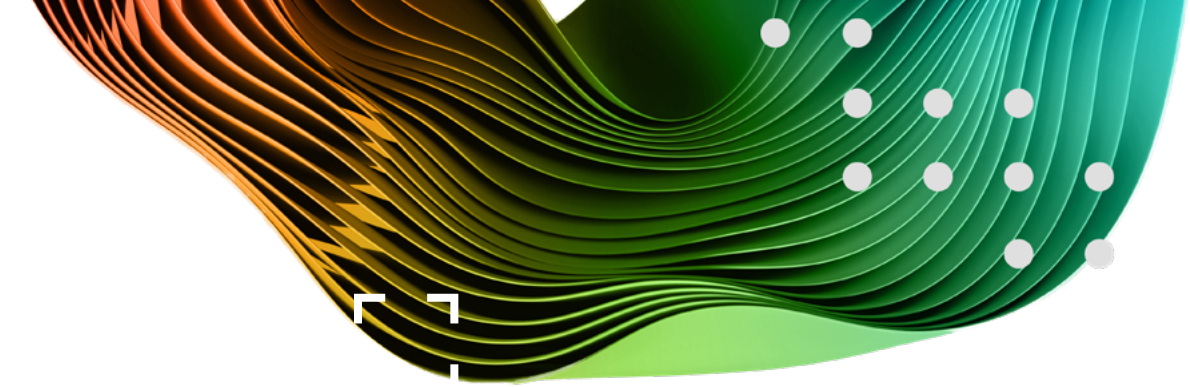
重新設計人機協作與組織模式

- 人與 AI 如何有效分工協作？
- 哪些工作由 AI 支援或自動化？
- 人才應聚焦哪些高價值任務？
- 如何支持新工作模式與職涯發展？

AI 人才與組織策略擬定——現有人才與未來職務需求的能力落差

AI 轉型不只是技術導入，而是人才、工作與組織模式的全面變革。企業需重新調整職位設計、能力架構、工作流程與治理機制，使人才能力能與 AI 賦能的新工作模式相匹配。

		角色轉型	AI 應用素養	AI 判斷與風險意識	AI 治理與責任機制
過去		職位設計、職責、績效假設全由人力完成	有專業能力，但以傳統方式完成任務，未把 AI 納入工作流程	願意使用 AI 且頻率不低，但缺乏驗證與風險辨識，容易直接採信 AI	已開始使用 AI，但組織尚未建立對應政策、責任、績效
轉變		**AI 轉型下互動模式改變，人才要具備 AI 協作能力，職位結構與能力要求需重新配對**			
未來	**AI**	接手部分標準化、可預測、可模板化的工作	廣泛用於資訊搜尋、寫作與基礎分析	風險來自於偏誤資料及 AI 倫理不足	可快速生成初階產出，幫助人更快決策
	人才	參與決策、跨部門協調、業務理解與流程設計	將時間從低價值任務轉移到更高價值工作	驗證 AI 成果並辨識高風險任務，適時進行決策	跨部門協調、價值與倫理判斷及責任承擔
調整方向		職位導向 → 任務 / 技能導向 **重新定位職位**：轉向 AI 不易取代的高判斷、高互動、高責任工作	專業導向 → 價值導向 **培養流程整合經驗**：學會把 AI 嵌入既有工作流程中	應用導向 → 風險導向 **加強 AI 辨識能力**：訓練判斷力 監督力、AI 倫理意識	AI 協作 → AI 治理 **AI 納入治理體系**：承認 AI 使用事實，重新界定人的責任與績效評估



結語

AI 治理的價值，最終不在於增加多少制度與流程，而在於企業能否將治理轉化為支持決策、促進創新與建立信任的日常能力。這項能力並非一次性建置即可完成，而需要隨著技術演進、應用深化及外部環境變化，持續檢視與調整。企業更應將 AI 治理視為持續演進的管理課題，使治理要求能夠落實於策略規劃、資源配置、專案執行及營運監督之中，並在創新發展與穩健經營之間取得適當平衡。

企業可從自身發展階段與關鍵應用場景出發，逐步明確決策權責、建立跨部門協作機制，並由高階管理階層統籌風險、績效與人才等關鍵議題，確保 AI 投資方向與企業策略及長期價值一致。董事會與管理階層亦應持續掌握 AI 所創造的價值與衍生的風險，確保創新的速度與組織的承擔能力相互匹配。

未來，真正形成差異化的，不只是企業採用了哪些 AI 技術，而是能否以清楚的策略、有效的治理、可信的資料及成熟的人機協作模式，將 AI 穩健地融入營運與決策。治理不是創新的限制，而是讓 AI 得以規模化、可信任並持續創造價值的基礎。當治理能力逐步內化為組織文化與管理常態，企業才能在快速變動的技術與市場環境中持續應變，並將 AI 從單一工具或專案，進一步轉化為支持企業成長、組織韌性與長期競爭力的重要能力。

發起與研究團隊

台灣人工智慧學校

勤業眾信聯合會計師事務所



Deloitte 泛指 Deloitte Touche Tohmatsu Limited（簡稱"DTTL"），以及其一家或多家會員所網絡及其相關實體（統稱為"Deloitte 組織"）。DTTL（也稱為"Deloitte 全球"）每一個會員所及其相關實體均為具有獨立法律地位之個別法律實體，彼此之間不能就第三方承擔義務或進行約束。DTTL 每一個會員所及其相關實體僅對其自身的作為和疏失負責，而不對其他行為承擔責任。DTTL 並不向客戶提供服務。更多相關資訊www.deloitte.com/about了解更多。

Deloitte 亞太（Deloitte AP）是一家私人擔保有限公司，也是 DTTL 的一家會員所。Deloitte 亞太及其相關實體的成員，皆為具有獨立法律地位之個別法律實體，提供來自100多個城市的服務，包括：奧克蘭、曼谷、北京、邦加羅爾、河內、香港、雅加達、吉隆坡、馬尼拉、墨爾本、孟買、新德里、大阪、首爾、上海、新加坡、雪梨、台北和東京。

本出版物係依一般性資訊編寫而成，僅供讀者參考之用。Deloitte 及其會員所與關聯機構不因本出版物而被視為對任何人提供專業意見或服務。在做成任何決定或採取任何有可能影響企業財務或企業本身的行動前，請先諮詢專業顧問。對於本出版物中資料之正確性及完整性，不作任何（明示或暗示）陳述、保證或承諾。DTTL、會員所、關聯機構、雇員或代理人均不對任何直接或間接因任何人依賴本通訊而產生的任何損失或損害承擔責任或保證（明示或暗示）。DTTL 和每一個會員所及相關實體是法律上獨立的實體。

© 2026 勤業眾信版權所有 保留一切權利