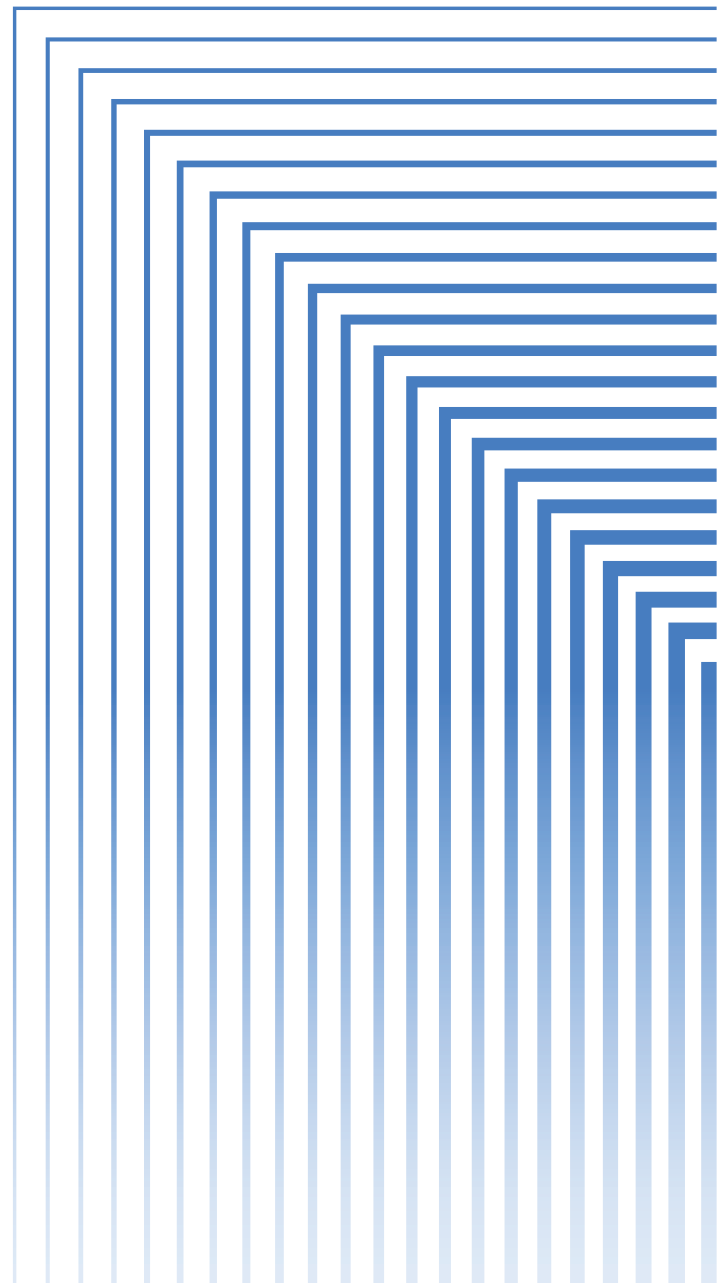


Google Cloud

財團法人人工智慧科技基金會

台灣企業 AI 準備度調查報告



01 前言	3	04 產業案例	40
• 導入 AI 前，企業應該思考哪些問題？	4	• 玉山銀行	41
• 面對熱切的 AI 期望，台灣準備好迎接新一波產業典範轉移了嗎？	6	用資料科學打基礎，玉山銀行讓 AI 成為員工 DNA	
		• 統一資訊	44
		從熟悉的工作中出發，統一資訊用 AI 找出新解方	
02 企業準備擁抱 AI 了嗎？	8	• 遊戲橘子	46
• 2024 企業 AI 準備度整體表現	9	從數位轉型中探尋 AI 市場化機會—遊戲橘子的創新之路	
• 五大能力指標分析	11	• 趨勢科技	50
• 結論	29	必須比駭客更會用 AI，趨勢科技賦能員工因應產業需求	
03 企業 AI 準備度生存指南	31	05 結論與建議	53
• 企業如何導入 AI？策略、人才、運算資源盤點與規劃	32	• 經營策略與組織文化將決定 AI 成敗	54
• 資料治理與風險管理是 AI 治理的關鍵	36		

01

前言

- Google Cloud
導入 AI 前，企業應該思考哪些問題？
- 人工智慧科技基金會
面對熱切的 AI 期望，台灣準備好迎接新一波
產業典範轉移了嗎？

導入 AI 前，企業應該思考哪些問題？

文 / Google Cloud

AI 正以驚人的速度影響著世界：它改變人們與科技的互動與協作的方式、更甚至重塑整個產業、驅動了社會與政策的轉型。根據麥肯錫 2023 年發布的《[生成式人工智慧的經濟潛力](#)》報告，生成式 AI 每年可為全球經濟增加數兆美元的價值。PwC 在 2023 年《[全球人工智慧研究：發掘 AI 革命](#)》中更表示，到 2030 年，AI 將為全球 GDP 增加高達 15.7 兆美元。

然而，儘管企業對 AI 的興趣與需求不斷攀升，實際採用率仍存在巨大差距。麥肯錫的調查顯示，目前僅有 21% 的企業已將人工智慧應用於多個業務領域，且許多企業仍在試驗階段。這也揭示了企業在實現人工智慧的價值方面仍面臨挑戰，包括技術人才短缺、數據質量問題、以及缺乏清晰的策略，而這也使得企業 AI 化程度的落差正在逐步加大，出現強者愈強、弱者愈弱的態勢。

在這幾年與企業接觸的過程中，我們觀察到，不少企業對於 AI 往往懷抱許多美好想像，但當實際著手導入 AI 專案、進行相關佈局時，才發現內部有許多基礎建設的不足之處急需填補。因此，我們與人工智慧科技基金會合作進行「台灣產業 AI 準備度調查」以企業在 AI 佈局與發展需留意的面向出發，分成數據、治理、創新、算力、技術等五大象限，邀請 101 家對於 AI 導入感興趣的企業領導人、高階主管，或 AI 專案負責人參與調查，期待透過本次的結果，深入了解台灣產業在 AI 導入上的困境。

自 2016 年起，Google 便是一家以 AI 為優先的企業，Google 致力於開發人

人都能受惠的 AI 技術，更持續提升服務的簡便性和擴充性，協助企業機構運用 AI 推動創新，並且根據企業的關鍵業務需求打造相應的產品組合。AI 導入是一個複雜的過程，需要企業進行全面的規劃和準備。擁抱眼前 AI 技術的快速革新，我們期待能致力於讓個人、企業、乃至於整個社會都能受惠於 AI 所開闢的嶄新機會，並充分利用 AI 的潛力。在本次發布的《台灣企業 AI 準備度調查報告》中，對於 AI 導入感興趣的企業，可以在進行 AI 佈局之前，先盤點內部能力；已經著手進行 AI 策略佈局的企業，也能藉此掌握 AI 導入的方法論，從中找到新的革新機會。

這份調查報告旨在幫助企業發掘自身於 AI 導入過程中，包含基礎建設、資料平台、治理、技術等面向的準備度，由此了解需補足之處，從而加速推進企業導入 AI 的步伐。在第一部分，我們會說明此次調查的目的與衡量標準；第二部分則針對 AI 準備度調查結果進行分析；第三部分則提供導入 AI 的逐步指南，以及各領域專家的建議心法。最後，我們將深入探討真實案例，瞭解各產業的先驅如何建立自己的 AI 策略，與實際應用及導入過程。

這份調查報告旨在幫助企業進行導入 AI 前的能力盤點，並提供實用的準備指南。我們將探討以下主題：

- 台灣企業目前在 AI 準備度上的表現
- 企業在導入 AI 時需具備的五大能力
- 協助企業導入 AI 的具體建議與做法

- 企業真實案例探討

此外，企業在導入 AI 前，還需要考慮以下因素：

- **AI 策略：**企業需要制定明確的 AI 策略，確定 AI 的應用方向和目標。
- **基礎架構：**AI 需要強大的計算能力和數據存儲能力。企業需要確保自己的基礎架構能夠滿足這些需求。
- **資料：**AI 模型需要大量資料進行訓練。企業需要確保自己擁有高品質的資料。
- **人才：**企業需要具備 AI 技能的人才來開發、部署和管理 AI 模型。
- **安全與治理：**企業需要確保 AI 模型的安全性和合規性。

以下是一些具體的建議：

- **制定 AI 策略：**企業應制定明確的 AI 策略，確定 AI 的應用方向和目標。
- **評估自身需求：**企業應評估自身的 AI 需求，確定需要應用 AI 解決的問題與目標。
- **選擇合適的 AI 解決方案：**企業應選擇合適的 AI 解決方案，以滿足自身的需求。
- **建立 AI 人才團隊：**企業應建立 AI 人才團隊，以開發、部署和管理 AI 模型。
- **確保 AI 安全：**企業應確保 AI 模型的安全性和合規性。

人工智慧 (AI) 正以迅猛的速度改變著我們的世界，並為企業帶來無限可能。AI

技術已在各產業得到廣泛應用，且正成為企業轉型的關鍵驅動力。希望這份調查報告能夠幫助您了解 AI 導入的準備。

面對熱切的 AI 期望，台灣準備好迎接新一波產業典範轉移了嗎？

文 / 人工智慧科技基金會執行長 溫怡玲

2024 年 5 月，賴清德總統與新內閣正式就任，AI 成為新政策的重要亮點；6 月初的台北電腦展 Computex 從 5 月底隨著 NVIDIA 執行長黃仁勳來台，就高潮迭起、彷彿提前熱鬧開幕；接著還有多位世界級科技領導人齊聚一堂，共同發表對 AI 未來的想像。因此，台灣這個以半導體聞名的葛爾小島，成為全球舞台上鎂光燈的焦點。

而在對 AI 未來熱切的期望中，台灣產業擁抱 AI 的現況如何？我們準備好如何迎接這一波產業典範轉移了嗎？這是 Google Cloud 與 AIF（人工智慧科技基金會）合作《台灣企業 AI 準備度調查報告》的初衷。

什麼是 AI 準備度？顧名思義，藉此調查，希望能夠知道目前台灣企業在開始導入 AI 之前做了哪些準備，從基礎設施、數據、人員技能和經營策略等方面的調整。這是衡量組織是否能夠應用 AI 的起點，也是決定是否能夠成功的重要關鍵；不只能應用在企業，也可以用以評估國家。

例如根據 Oxford Insights 公佈的資料，2023 年台灣的 AI 準備度排名全球第 18，這個調查所使用的指標包括政府政策、AI 治理、基礎設施、數據與技術等四大面向。

而英國 Tortoise Media 公布的 2023 年全球 AI 指數排名，則使用「投資、創新與實踐」三大面向來評估全球 62 個國家。美中分居前二名，新加坡第三、

韓國第六，台灣則是排名 26。

不同的指標會影響最終結果，無論是對於國家或企業而言都是如此。若將目光移到台灣產業，目前我們準備好了嗎？與全球國家整體評比不同的是，每個國家有其產業特色，AI 發展路徑並不相同，必須加入對於在地不同產業的了解才能擬出較符合真實的指標。

因此，AIF 從 2019 年即開始進行「台灣產業 AI 化大調查」，初期從企業人才技能評估的角度出發，延伸至企業策略、領導風格以及組織等面向。在 2022 年疫情過後，則轉以企業為主體進行整體 AI 應用能力評估。在參考全球研究相關文獻及分類建議之後，將 AI 應用能力分為經營、人才及技術應用等三大面向，將分數加總平均。依據分數不同分為四個群組，並針對每個群組提供後續導入 AI 的建議方案。

而根據連續兩年「台灣產業 AI 化大調查」的結果，發現台灣企業在導入 AI 應用的比例並沒有想像中那麼高，大約僅有三成左右；同時資通訊產業整體分數領先，與傳產及政府部門的差距相當大。所以，顯然還有許多企業必須從初期的準備起步，盡快展開導入 AI 應用的行動。

AI 準備度調查有哪些面向？根據 Google Cloud 與 AIF 在全球及台灣推動產業 AI 化的經驗，並參考相關研究，AI 準備度包括以下五項：

- **數據力**：企業有足夠數據及完整資料策略，以便發揮資料的最大價值。
- **創新力**：組織文化能夠接受 AI 技術導入時經常面對的錯誤，並能夠及時調整，靈活進行組織調整隨時因應新的分工。
- **技術力**：企業已能將 AI 應用於企業中，具備足夠 AI 人才，並擁有自行建置與維護 AI 模型的能力。
- **治理力**：企業董事會了解 AI 應用的機會與侷限，並能確保 AI 的安全性與隱私，掌握並避免 AI 可能造成的風險與傷害。
- **運算力**：對於發展 AI 的運算環境已有妥善策略與規劃。

每一個面向的概念，都各自發展出具體指標，並透過問卷訪問方式，邀請企業相關部門主管或負責人確實填答。除此之外，再依據問卷結果，我們邀請相關領域專家學者，分析數據所呈現的現象背後各自代表哪些意義，並提出具體建議，希望能夠讓企業在著手準備 AI 技術導入時，有明確的方向感與目標。

在經歷 PC、網際網路、行動裝置、雲端及大數據等不同階段後，台灣一直扮演全球重要的硬體協力夥伴。很多人說，AI 是第四波工業革命，將驅動全球產業的典範轉移，創造全新格局。

過去兩、三年由於生成式 AI 崛起造成的大量需求，台灣 AI 算力供應鏈相關企業突飛猛進。再下一步呢？當 AI 應用創新大量出現之後，台灣的企業應該如何著手準備下個世代的核心競爭力？如何重新找尋在全新生態系中的定位，還

能夠共創新局？這份《台灣企業 AI 準備度調查報告》將是一個重要的起點，也標示著台灣即將邁入一個新的里程碑。

02

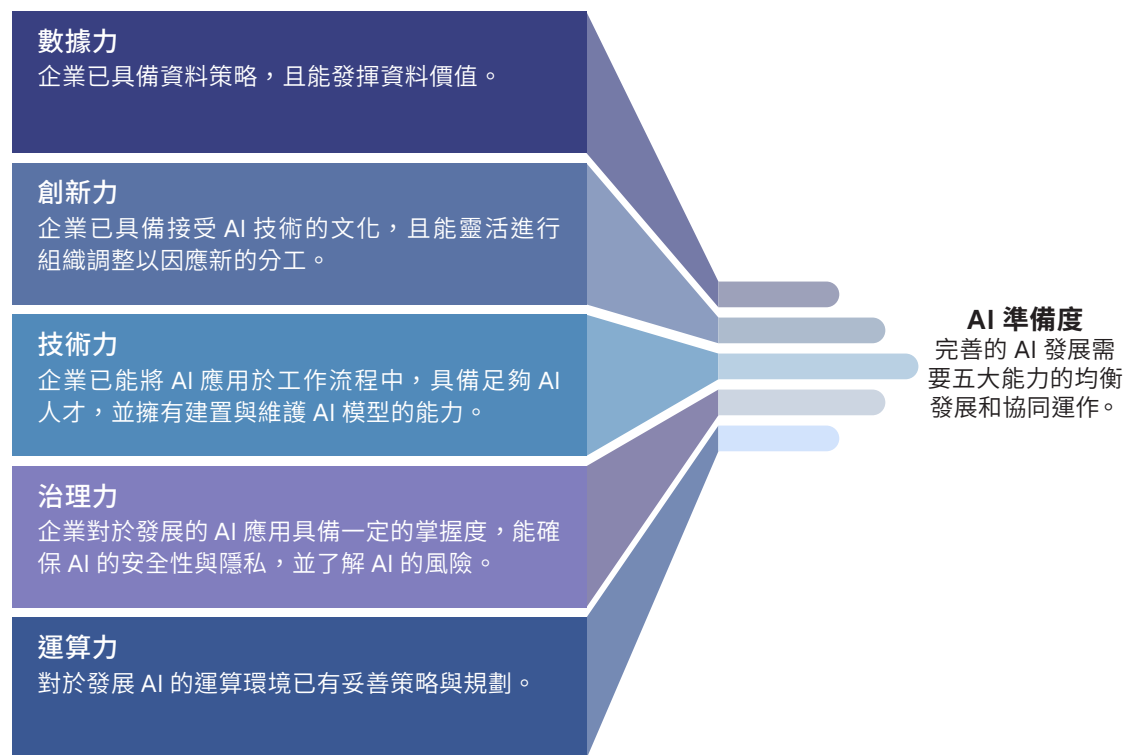
企業準備擁抱 AI 了嗎？

- 2024 企業 AI 準備度整體表現
- 五大能力指標分析
- 結論

AI 準備度五大能力

參考國內外相關調查、文獻，並結合過往產業服務經驗，我們將 AI 準備度拆分為五大能力：數據力、創新力、技術力、治理力、運算力。

五大能力缺少任何一個環節，都可能使得企業的 AI 技術發展和應用面臨發展瓶頸。例如，擁有強大的運算力，卻缺乏足夠而有效的數據，將無法有效進行 AI 模型訓練；而擁有創新力和技術力，但缺乏治理力，則可能引發 AI 應用倫理問題和企業數據外洩等資安隱患。

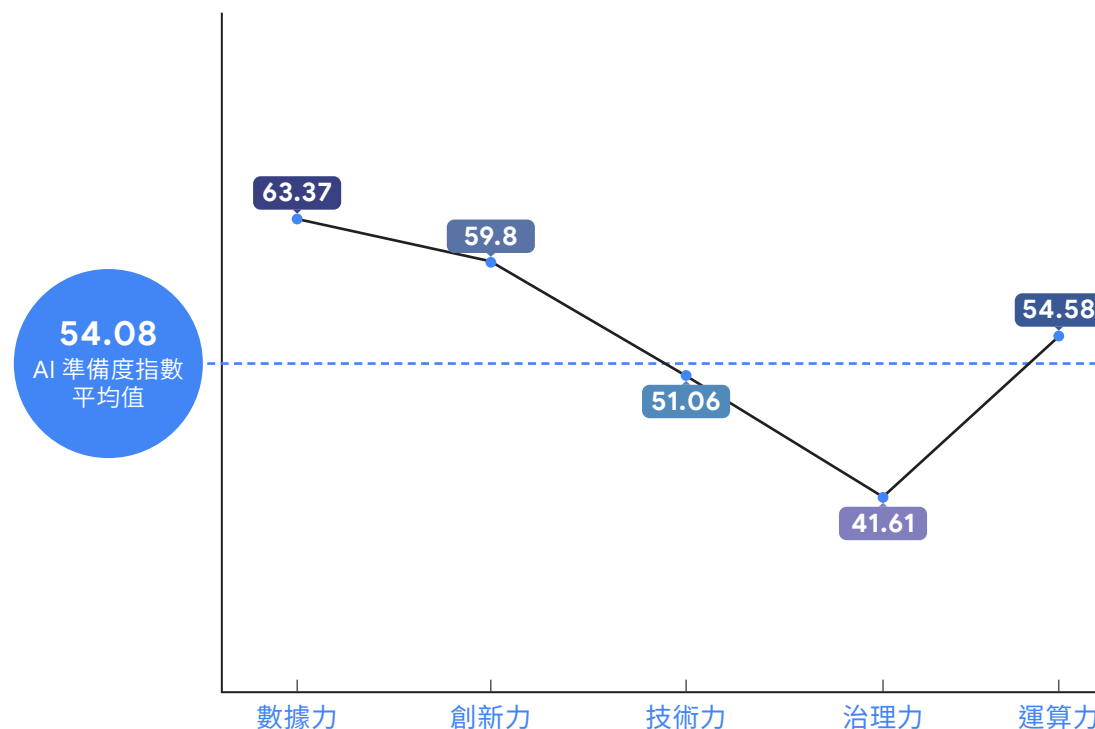


整體 AI 準備度指數

此次調查報告顯示，2024 年企業整體 AI 準備度指數平均為 54.08，該指數為數據力、創新力、技術力、治理力、運算力等五項能力分數加總平均。指數僅為統計台灣企業目前在各能力準備程度的分佈情形。五大能力中，準備程度最高為數據力，最低則為治理力，創新力及運算力雖高於平均值，但進一步分析後發現，多數企業雖意識到人工智慧、算力資源的重要，但並未完全體現在具體執行上，例如意識到人工智慧將帶來變革，卻未有可因應的組織調整。其他如技術能力、人才培育、組織管理、算力資源等方面仍有許多成長空間。

另一方面，治理力準備程度最低，凸顯企業在 AI 策略與風險管理上缺少相關意識，建議企業可加強國際上對於 AI 監管與治理的趨勢，以因應瞬息萬變的情勢。

單位：分 (0-100)



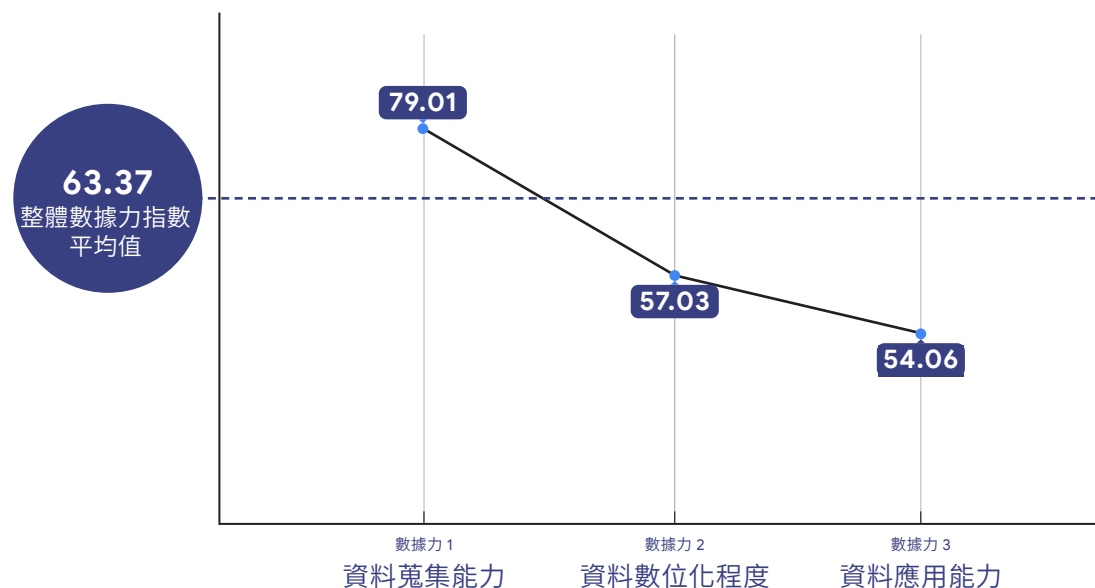
整體「數據力」分析

數據力涉及企業的資料蒐集、整合管理及應用能力。若企業無法整合內部數據管理規則，確保各部門的資料品質與資料處理流程，在數據應用就會受到限制。不少人也許聽過「沒有資料就不會有人工智慧。」而人工智慧是否能達到預期效益，也與資料品質息息相關。

在「2024 企業 AI 準備度」調查中，整體數據力指數為 63.37 分，是五大能力中表現最佳的部分。不僅在資料蒐集能力上獲得 79.01 分，高於 AI 準備度指數平均值（54.08 分），甚至在資料數位化程度上也獲得 57.03，同樣高於整體平均值。由於資料蒐集能力包括資料與應用範圍，結果顯見多數企業或組織皆已意識到資料的重要性，並具備營運資料蒐集能力。但在進一步的資料管理與整合能力上，表現仍有待加強。

目前僅有 6.9% 企業仍以紙本形式管理營運資料。另有逾五成企業已知使用資訊系統，並有 17.8% 企業擁有整合平台，能快速處理不同來源的資料。但在資料的應用上，多用於業務與開發上，建議可關注其他營業單位，如人事、財會等不同單位的需求，並開展相關資料應用。（詳細調查結果將於下三頁中說明）

單位：分 (0-100)



企業皆已具備資料蒐集能力

38.6%

企業由各部門各自蒐集與使用資料

在數據力的 3 項指標中，以「資料蒐集能力」指標表現最好，無論是部門內部使用，或是可以被跨部門使用，幾乎所有企業或組織皆已具備營運資料蒐集能力。但有 7.9% 的企業不知道下一步該如何使用資料。

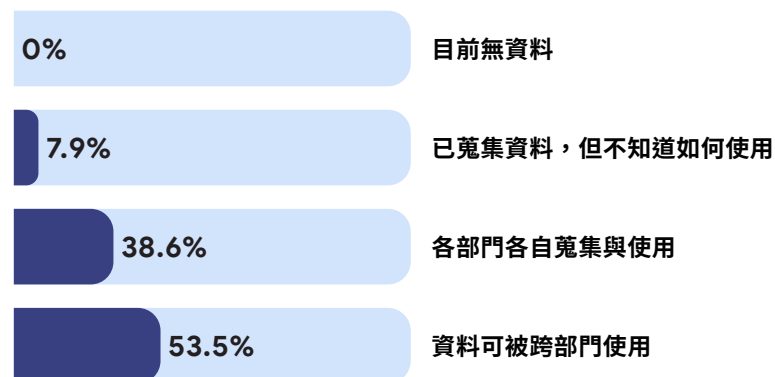
此外，38.6% 的企業由各部門各自蒐集與使用資料，當企業資料分散在不同的部門或系統中時，若沒有一致的資料管理策略，將難以保證資料的一致性和可用性。

有效的數據策略可以整合跨部門的企業資料，並提供統一的存取介面，進而提高資料的一致性和可用性，以利企業能快速從資料中提取洞察力，並做出更明智的決策。

數據力 1 | 資料搜集能力

N=101

Q. 以下哪一個描述最符合貴公司目前「營運資料」的應用狀況？



資料整合能力將是關鍵

17.8%

企業能整合並快速處理不同來源的資料

在數據力的 3 項指標中，企業在「資料數位化程度」方面，超過九成企業具備資料數位化能力，並有逾五成企業使用資訊系統。

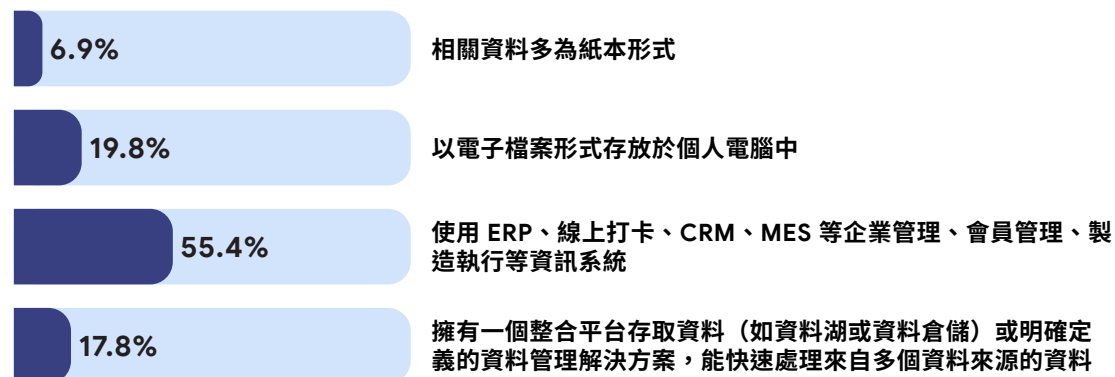
由於企業累積的資料量將逐步增加，在保障資料安全和遵循法規的同時，還必須從中發掘寶貴的洞察，複雜度將有增無減。資料整合能力將是未來企業需要強化的能力，而此次調查中，僅有 17.8% 的企業具有相關能力。

擁有一個資料存取的整合平台（如資料湖或資料倉儲）或明確定義的資料管理解決方案，將能協助企業快速處理來自多個資料來源的資料，整合不同來源的資料，並提供統一的存取介面，讓企業能夠更輕鬆地從資料中獲取價值。

數據力 2 | 資料數位化程度

N=101

Q. 請問貴公司的「營運資料」（如客戶名單、訂單資料、生產資料、人事財務管理等）最主要透過以下哪些方式管理？



資料科學仍是重要課題

在「資料應用能力」方面，企業多數將資料應用於與業務開發面向，如「管理和分析客戶互動和數據」、「整合市場和用戶等數據分析，做為產品開發和創新策略，引導新產品或服務的開發」。

從該題的指數分數來看，多數企業在資料應用面向上，多為 2~3 項應用為主，若想拓展企業更多面向的應用能力，關乎企業成員對於資料的理解程度，以及成員是否擁有自主應用等能力，亦即無需仰賴資訊部門協助，即可依需求分析、應用資料。資料科學仍是 AI 時代必須了解的課題。

企業的數據应用能力與數據治理程度息息相關，當企業各式的數據散落在不同單位或資訊環境中形成數據孤島 (Data Silos) 時，各業務單位無法自主運用資料，且必須仰賴 IT 部門的協助時，就沒有辦法讓有用的資料 (Data) 協助進行決策及運營基礎。

數據力 3 | 資料應用能力

N=101

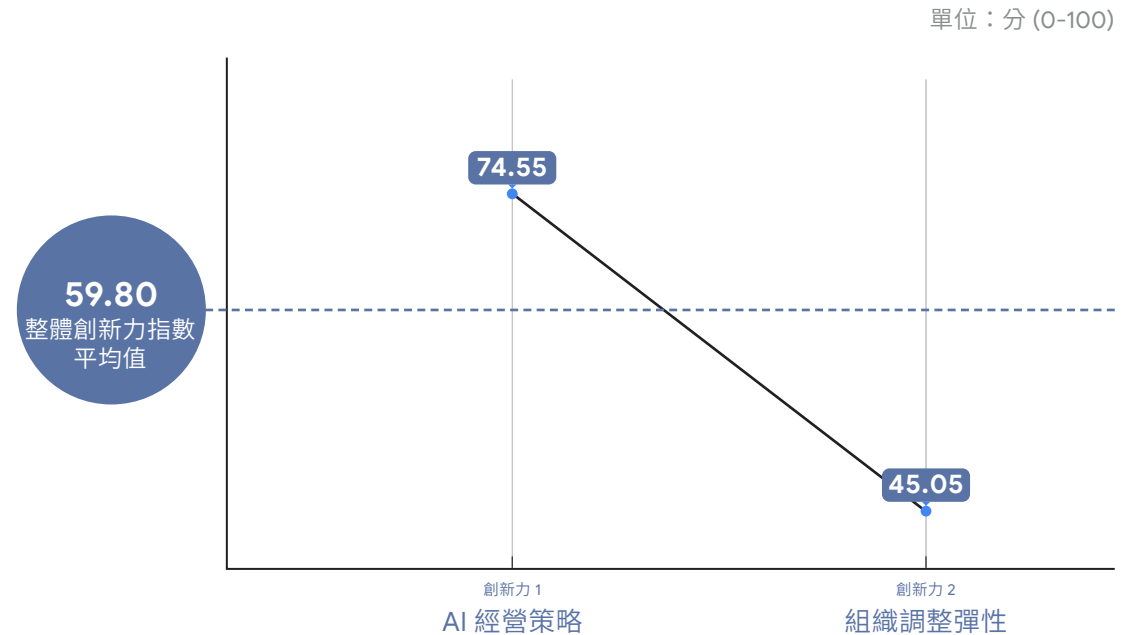
Q. 請問貴公司目前最主要將「營運資料」應用於下列哪些面向？【請依重要程度排序前 5 項】



整體「創新力」分析

創新除了是新工具或新技術的開發與使用外，也是企業對於組織、管理、文化等方面，對於新的變革具備因應能力，且能進一步驅動企業創造出差異化的競爭優勢。

在創新力的 2 項指標中，「AI 經營策略」一題的指數高達 74.55，可以看出，企業多半已將 AI 視為重要的策略；然在「組織調整彈性」上，卻僅有 45.05，顯示多數企業或組織雖然高度認同人工智慧的重要性，但並未隨著 AI 的發展調整組織架構與流程，而這往往是企業應用落地程度偏低的主要原因。



雖認同 AI 但仍在探索階段

35.6%

企業仍在初步探索研究中

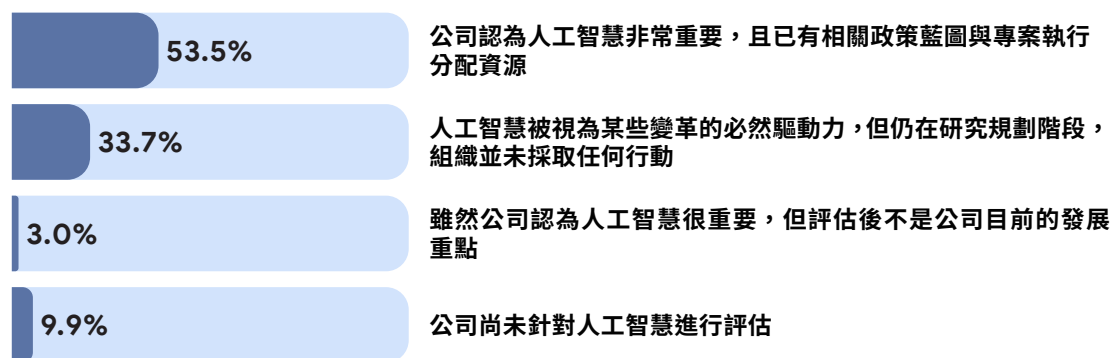
創新力包含了對於新變革所具備的因應能力，因此除了從 AI 經營策略面了解公司對於人工智慧的態度，也必須參照企業應用 AI 的程度，以了解實際落實狀況。

綜合結果可發現，無論有無進一步行動，近九成企業認同 AI 是帶動變革的必然驅動力。超過半數組織認同 AI 非常重要且已有相關政策藍圖，並分配資源。然而，「組織調整彈性」指標表現偏低，約四成 (44.5%) 仍處於尚未應用 (8.9%) 或僅初步探索研究 AI (35.6%) 的階段。

創新力 1 | AI 經營策略

N=101

Q. 以下哪一個描述最符合貴公司目前對於人工智慧的態度？



創新力 2 | 組織調整彈性

Q. 以下哪一個描述最符合貴公司應用人工智慧的程度？



生成式 AI 為首要投資

36.6%

企業將「生成式 AI 應用工具或方案導入」視為優先資源投入面向。

生成式 AI 與以往其他形式的 AI 不同，使用者可以輕鬆透過這項技術解決私人生活和工作中的日常問題。

過往 AI 和機器學習技術大多著重在提高生產效率與成效；但生成式 AI 的出現，使得應用開始偏向「採用完全不同以往的做法」，大眾也開始思考如何應用新工具與技術，用比過去更快速省力的方式處理事務。

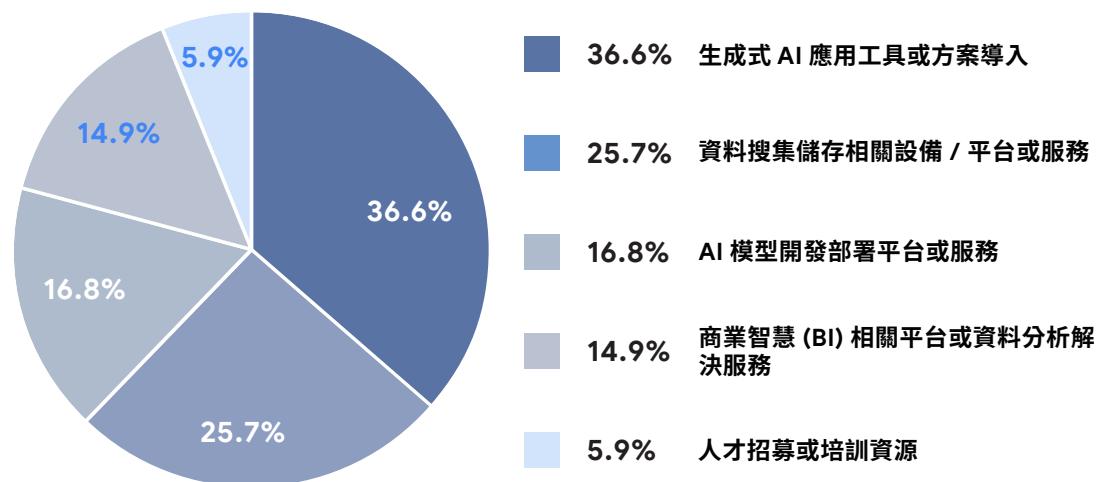
雖然生成式 AI 的確為企業帶來新的改變，但仔細往下解構就會從費用、資安、環境等地方發現，每個環節都有必須克服的問題。

此外，若企業想進一步利用 AI 發展出新服務或對營運產生影響甚至開創新一波發展，生成式 AI 只是起點，必須對於 AI 有更深入的認識，才能夠創造新價值。

趨勢分析 | 因應未來發展，企業資源投入傾向

N=101

Q. 因應貴公司未來三年的整體發展，請問將優先投入資源在哪些 AI 的相關面向？
【請依重要程度排序】

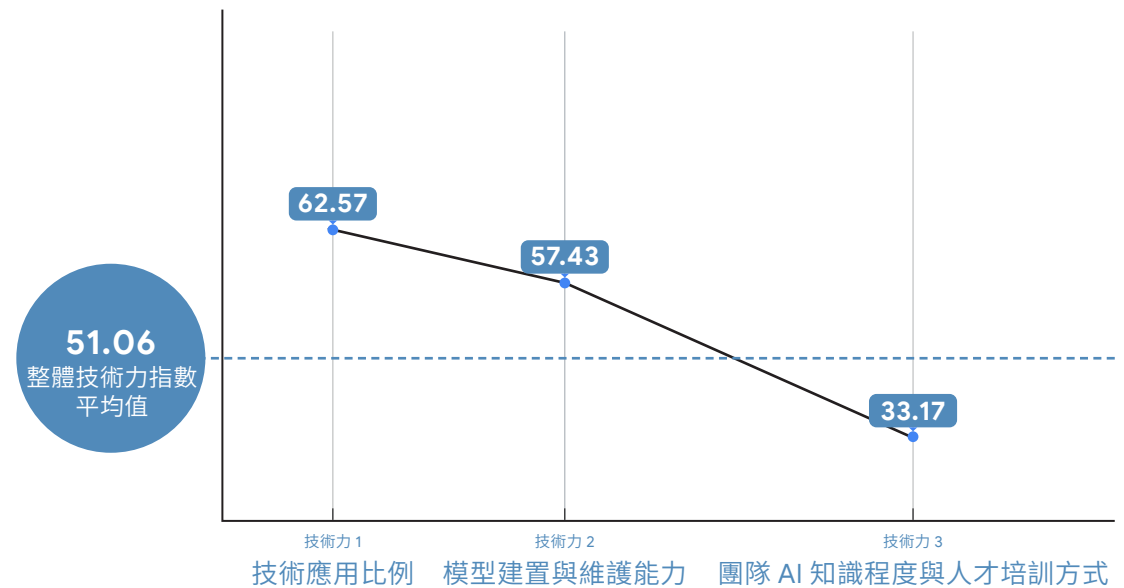


整體「技術力」分析

技術應用比例及模型建置與維護能力高於整體技術力，顯見雖然企業已能將 AI 技術應用於企業中，但僅有特定部門具備 AI 能力，整體企業對於 AI 知識程度的掌握與人才培訓方式仍待加強。

儘管生成式 AI 降低了 AI 的使用門檻，為使用者提供快速的創意，並生成有說服力的文本，但仍須對於 AI 的能力與限制具有一定程度的了解，才能有效提升生產效率。

單位：分 (0-100)



不只應用單一 AI 技術

51.1%

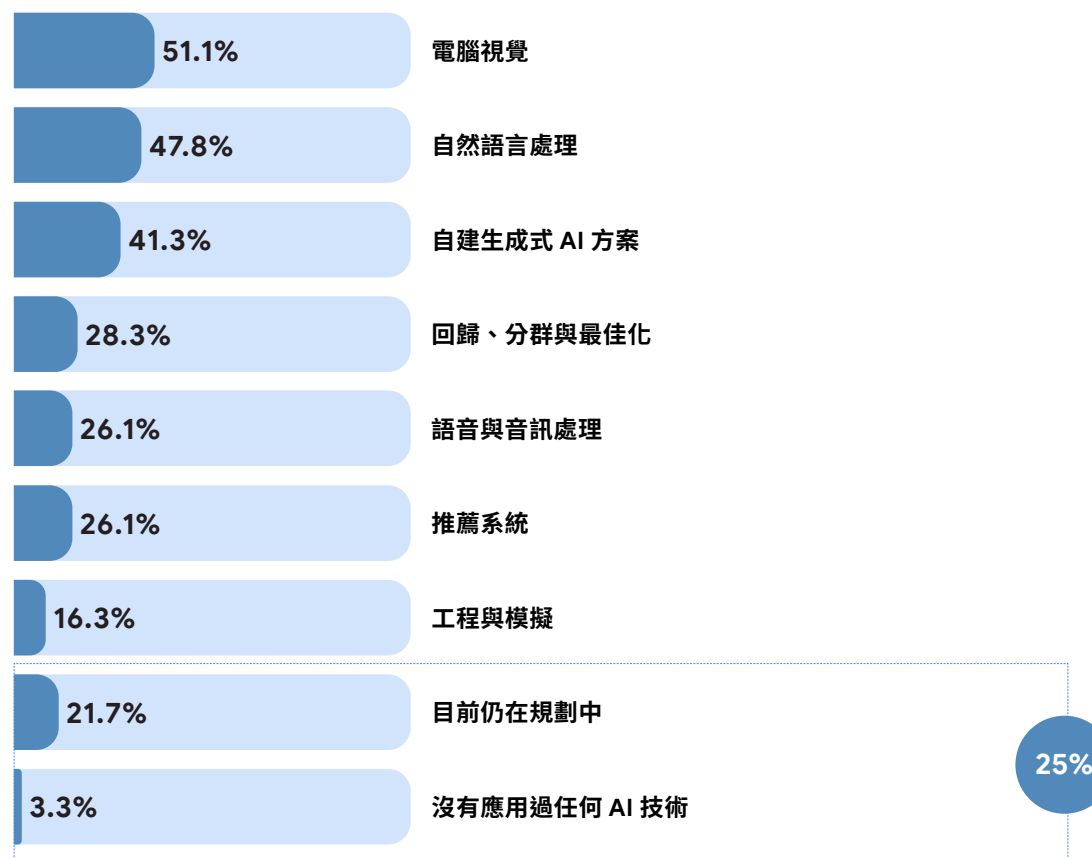
企業將數據應用於電腦視覺，自建生成式 AI 方案者約為 41.3%。

雖有 25% 的組織仍在規劃、或尚未將數據應用在任何 AI 技術上，但超過半數以上企業已使用超過一項以上的 AI 技術應用。生成式 AI 的出現，提供了企業新的技術選擇，而電腦視覺的技術發展則較為快速，其應用範圍也在逐日增加，常見的應用場景如辨識、偵測、追蹤與分割等功能上。其次則是自然語言處理，以及生成式 AI 的方案。

技術力 1 | 技術應用比例

N=101 | 組織有應用 AI，n=92

Q. 請問貴公司曾應用以上數據在哪些 AI 技術領域？(可複選)



AI 專案多為內部自建

54.3%

企業以內部自建 AI 專案為主

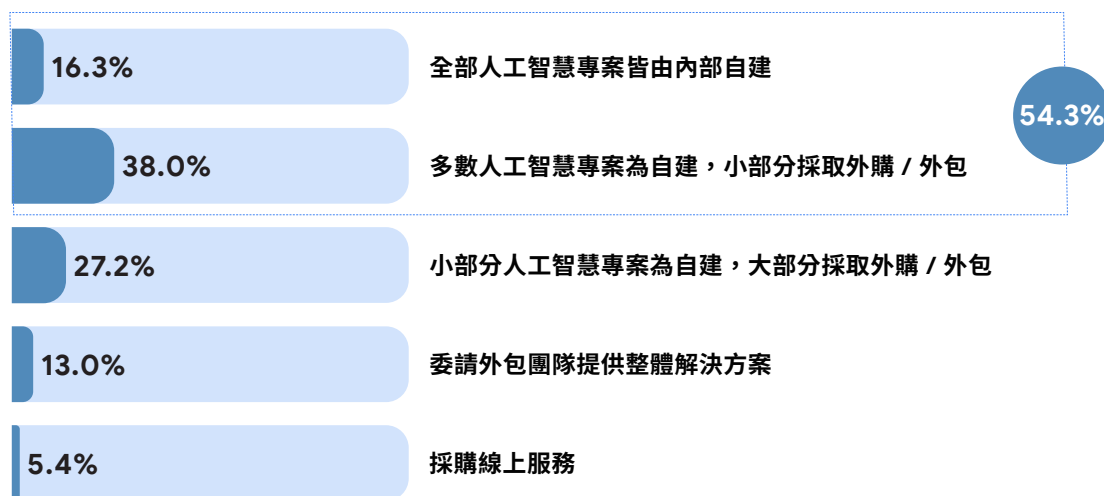
在「模型建置與維護能力」方面，有應用 AI 的組織多數為自建搭配部分外購 / 外包。但可發現近兩成的企業選擇委外或採購服務，包括 13.0% 委請外包團隊提供整體解決方案，以及 5.4% 委請外包團隊提供整體解決方案。

除因近年來提供 AI 服務或產品的公司大幅增長，生成式 AI 工具的出現，也使得企業更願意嘗試使用 AI。但後續是否能對企業經營或是決策流程帶來改變，仍需觀察。

技術力 2 | 模型建置與維護能力

N=101 | 組織有應用 AI，n=92

Q. 以下哪一個描述最符合貴公司目前導入人工智慧專案的方式？



AI 人才培訓是必要投資

69.3%

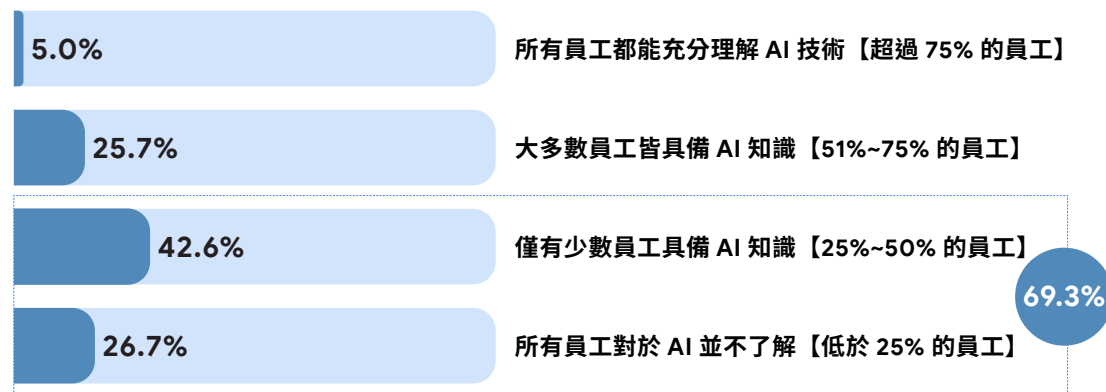
企業表示多數員工對 AI 知識的了解程度偏低

儘管生成式 AI 的出現，吸引許多人的目光，使得大眾對於 AI 的關注度提升；而生成式 AI 雖能提供快速的創意，並生成有說服力的文本，但了解 AI 的能力與限制者，才能有效提升生產效率。尤其高技術工作者更需要在與 AI 協作時，持續運用本身既有的專業，並驗證 AI 的正確性。若企業需要更深入的導入 AI 工具，得提升內部員工對於 AI 的認識，並將 AI 人才培訓納入策略規劃中。

技術力 3 | 團隊 AI 知識程度與人才培訓方式

N=101

Q. 以下哪一個描述最符合貴公司目前員工對於人工智慧的了解程度？

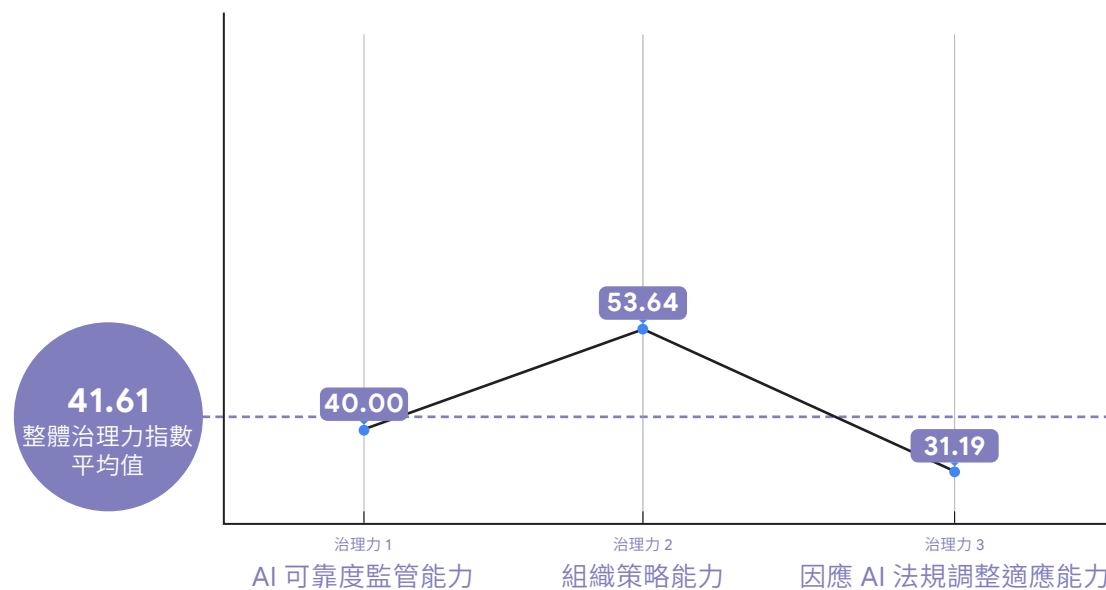


整體「治理力」分析

治理力主要是了解企業在發展 AI 應用上對於風險的掌握度，並能確保 AI 的安全性與隱私。

此次調查結果中，治理力整體指數偏低，其中以「因應 AI 法規調整適應能力」指數最低，主因是許多企業或組織尚未建立機制，以確保符合國際 AI 規範。

單位：分 (0-100)



企業需注意 AI 的可信賴性

17.7%

企業並不清楚或無採用 AI 準則

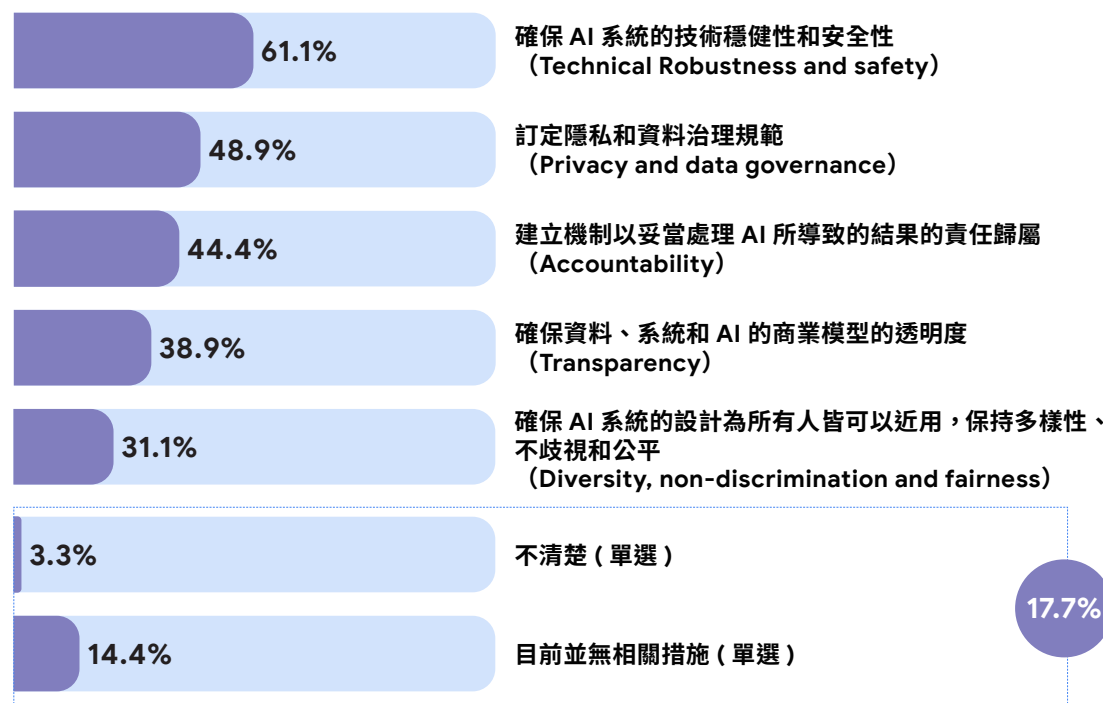
在 AI 發展中注重負責任、可信賴原則的企業，將有助其提供更安全、可靠的產品，以獲得客戶及其信賴。而此處主要參考歐盟議會所發布的《可信賴人工智慧倫理準則》內容，並針對企業 AI 導入情境提出選項。調查發現，仍有 17.7% 並不清楚或未採用 AI 準則。

多數企業主要關注「隱私和資料治理」(Privacy and data governance) 與「技術穩健性和安全性」(Technical Robustness and safety) 等基礎與資安相關準則，然兩者皆屬基礎準則，前者影響系統運作、後者有法遵問題，因此遵循比例明顯較高。

治理力 1 | AI 可靠度監管能力

N=101 | 組織有應用 AI，n=92

Q. 您的組織如何確保人工智慧模型是可信賴的？(可複選)



AI 推動非單一部門問題

32.7%

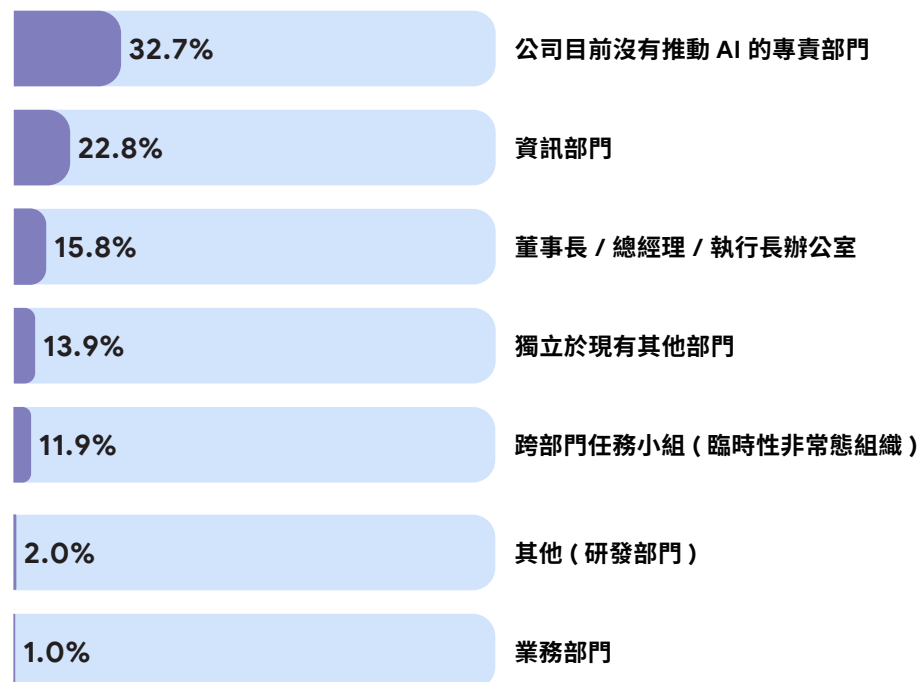
企業沒有推動 AI 的專責部門

AI 在多數企業仍屬單點推動，由於 AI 導入與企業策略相關，並牽涉到企業內部組織結構，建議企業應有整體的規劃與策略。

治理力 2 | 組織策略能力

N=101

Q. 請問貴公司是否有推動 AI 的專責部門？



逾五成企業未有 AI 規範

52.5%

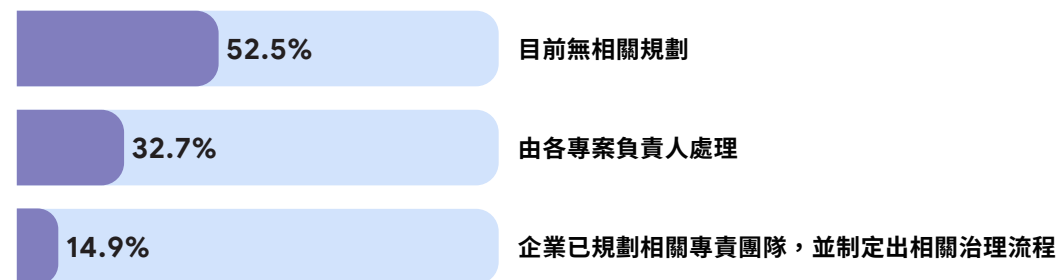
企業沒有規劃機制，以確保 AI 模型符合最新國際規範。

在生成式 AI 工具引發熱潮後，各國已積極透過規範方針或原則，規範 AI 發展及應用。例如 2023 年，美國總統拜登與 OpenAI、Google、微軟、Meta、亞馬遜、Anthropic、Inflection 等七家人工智慧公司的高層共議人工智慧風險防範，承諾以安全、保障和信任為三大基本原則，監督人工智慧的使用方式。而 Google 早在 2018 年即發布 [AI 原則](#)，我們參考客戶和合作夥伴的意見仔細訂下這些原則，並以此為核心規劃及發展自身的 AI 產品與服務，確保自身和客戶都能達到預期成果，並避免這些技術帶來任何意外的潛在傷害。建立成功 AI 的關鍵在於審慎評估，建議企業應及早注意相關議題發展，以因應未來趨勢。

治理力 3 | 因應 AI 法規調整適應能力

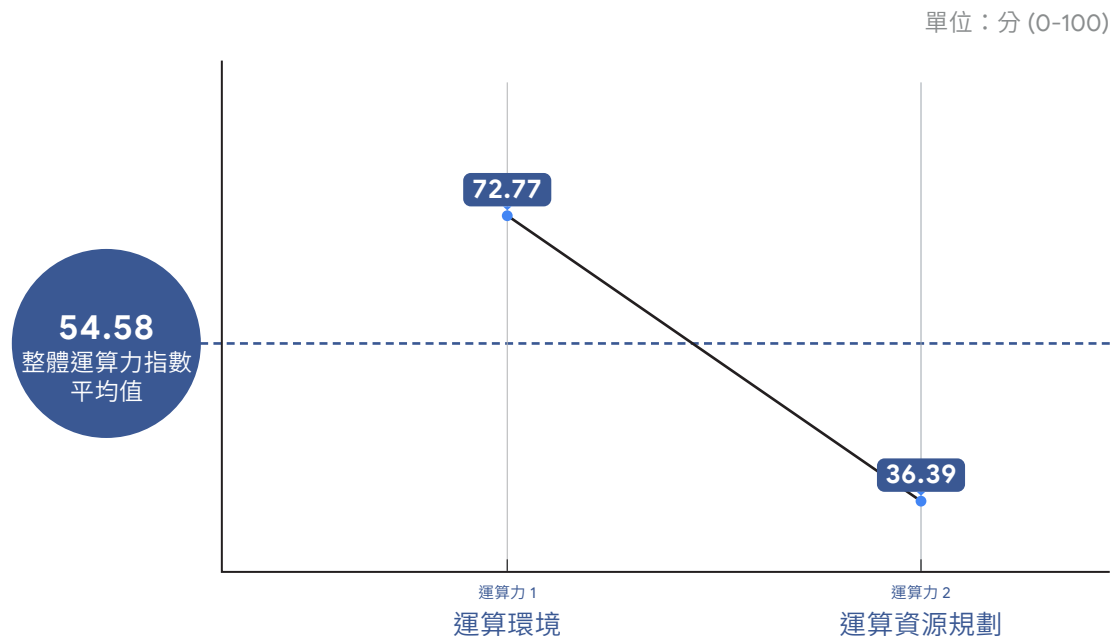
N=101

Q. 請問貴公司如何確保所使用的人工智慧模型能符合最新的國際規範？



整體「運算力」分析

運算力的評估涉及企業對於整體 AI 策略、數據治理、團隊對於雲端經驗的熟悉與否，多數企業或組織雖已知 GPU 等算力資源對 AI 發展的必要，但在進一步的算力架構規劃上，企業除了要考量自家的 AI 策略外，更需要兼具產業知識與算力部署等跨領域人才的投入，協助企業進行整體評估。



算力是 AI 時代關鍵角色

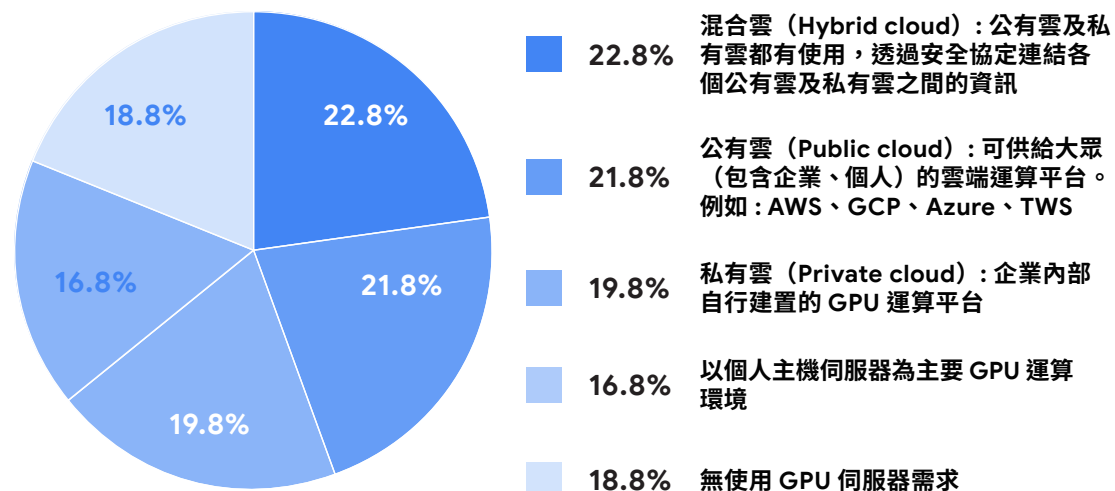
算力在 AI 時代極為關鍵，由於深度學習訓練、圖像生成、自然語言處理等任務，都需要大量而複雜的計算，具備平行運算能力及高速傳輸速度的 GPU 便提供極大幫助。

在「運算環境」的選項中，混和雲、公有雲與私有雲分別各有約 2 成的企業選做主要使用的 GPU 環境。

運算力 1 | 運算環境

N=101

Q. 貴公司目前最主要使用的 GPU 運算環境是？



運算資源涉及企業策略

51.5%

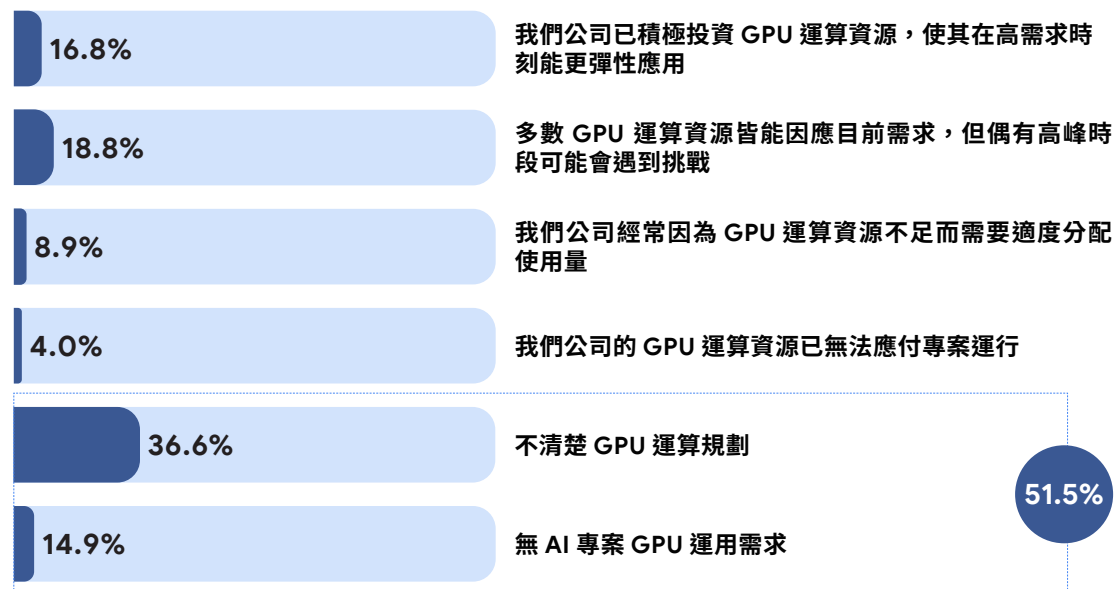
企業仍不清楚規劃或沒有運用需求

隨著數據生成、模型規模和運算需求呈指數增長，現有基礎設施可能無法滿足模型訓練和部署及管理大型語言模型的需求。因此，企業需要合適的 AI 基礎架構，才能確保模型效能出色，並兼顧成本效益。而運算資源的評估選擇涉及企業的策略，以及是否有足夠人才協助評估，尤其在生成式 AI 興起後，若需要充分發揮生成式 AI 的潛力，構建兼具性能、敏捷性和可擴展性的基礎設施更是至關重要。若團隊無相關資源，亦可透過外部專家團隊諮詢，獲得最佳配置。

運算力 2 | 運算資源規劃

N=101

Q. 以下哪一個描述最符合貴公司目前 AI 專案應用 GPU 運算資源的程度？



整體 AI 準備度表現

「數據力」最佳，「治理力」最低

本次受訪企業多半對於 AI 已有一定認識，且半數以上企業皆已於部分專案中試行 AI 相關應用。平均表現由高至低分別為「數據力」、「創新力」、「運算力」、「技術力」、「治理力」。

整體調查結果顯見在 AI 準備度上，企業雖具有資料搜集與整合等能力，但具體落實到企業現場，在技術、人才、組織調整、運算資源等部分仍有許多成長空間。

「數據力」平均指數 **63.37**

**多數企業已具備資料搜集與使用能力；
但資料治理將是企業重要議題**

近九成企業或組織已具備營運資料蒐集能力；僅有 17.8% 企業能整合並快速處理不同來源的資料。

企業資料應用仍與業務開發面向相關，原因可能與企業成員對數據的了解與掌握度相關。有效的數據策略可以整合跨部門的企業資料，並提供統一的存取介面，進而提高資料的一致性和可用性。

「創新力」平均指數 **59.80**

AI 應用實際落地程度偏低，因組織缺乏靈活調適力

目前近九成組織認同人工智慧實為重要，然較多仍在初步探索或試行於部分專案的階段。實際企業落地應用的程度仍偏低。

進一步瞭解，36.6% 企業將「生成式 AI 應用工具或方案導入」視為未來三年優先資源投入面向。

「技術力」平均指數 **51.06**

近七成組織表示員工對於 AI 知識的理解程度偏低

雖然企業已能將 AI 技術應用於企業中，但團隊 AI 知識程度與人才培訓方式不足，使得企業整體技術力表現不佳。

在「模型建置與維護能力」方面，有應用 AI 的組織多數為自建搭配部分外購 / 外包。

「治理力」平均指數 **41.61**

整體 AI 治理能力皆偏低

約三分之一的組織沒有專責推動 AI 的部門，且超過半數目前沒有規劃相關機制，以確保目前所使用的 AI 模型符合最新國際規範。

多數企業主要關注「隱私和資料治理」(Privacy and data governance) 與「技術穩健性和安全性」(Technical Robustness and safety)，然兩者皆屬基礎準則，前者影響系統運作、後者有法遵問題，因此遵循比例明顯較高。

「運算力」平均指數 **54.58**

已知算力資源對 AI 發展的必要，但應用需求偏低

整體各有兩成左右的組織其 GPU 運算環境為混合雲、公有雲及私有雲；然而，仍有一半以上企業表示不清楚 GPU 運算規劃或目前沒有 AI 專案 GPU 運用需求。

03

企業 AI 準備度生存指南

- 企業如何導入 AI ？策略、人才、運算資源盤點與規劃
- 資料治理與風險管理是 AI 治理的關鍵

企業如何導入 AI ？策略、人才、運算資源盤點與規劃

文 / 人工智慧科技基金會



人工智慧科技基金會
常務董事張益肇

人工智慧科技基金會
執行長溫怡玲



人工智慧科技基金會
技術處總監張嘉哲

Google Cloud 台灣
技術總監安致宇



“人工智慧基金會與 Google Cloud 台灣等 AI 領域專家，以自身多年輔導產業進行 AI 轉型與導入經驗，針對想導入 AI 的企業，提供一系列策略、人才與運算資源建議。”

當 AI 工具愈變愈聰明，人們透過日常用語提問就能和 AI 聊天機器人或虛擬服務專員互動，無論是回答問題、創作內容、生成圖片、製作文件摘要等都能在極短的時間內完成。「你可以想像未來五年內，公司 CEO 就像隨時能調動一百個 IQ200 的 AI 同事，」人工智慧科技基金會 (AIF) 常務董事張益肇指出，面對這些新的成員，企業該思考如何借用這些新技術，為公司創造更好的價值。

不只使用工具，而是用 AI 驅動變革

張益肇表示，AI 的定義十分廣泛，但在生成式 AI 引發熱潮前，因為當時的 AI 技術與應用，如瑕疵檢測，僅與企業中特定單位的工作相關，所以其他部門成員對此較為無感。如今，生成式 AI 無論在文件撰寫、程式設計、設計繪圖等方面，幾乎可應用於各部門的工作情境中，因而引起新一波 AI 熱潮。

對企業來說，導入 AI 和僅是使用 AI 工具，兩者的準備程度截然不同，前者光是數據整理與收集的複雜程度就高很多，且就長遠之計，如果企業希望透過 AI 協助整個公司的運行，包括協助客戶開發或是產品開發等，就必須有十分清晰的數據整理，包括用於客戶經營的 CRM 系統與製造管理的 ERP 系統資料也必須打通。而資料整合上需要顧及的面向非常多，包括資料定義與整理、收集規範與原則、客戶隱私保護等等。實際上，跨部門合作與資訊互通極為不容易，尤其部門間如果涉及業務或客戶競爭關係，在資料整合上也會有所顧忌，甚或擔心與顧客間的聯繫資訊會曝光，而這些顧慮在客戶機密的保護上，也極具挑戰性。

而在這次的調查中可以看到，雖然有近九成企業認同 AI 是帶動變革的必然驅動力，但在後續相對應的「組織調整彈性」上，約四成 (44.5%) 仍處於尚未應用或僅初步探索研究 AI 的階段。人工智慧科技基金會執行長溫怡玲觀察，多數企業或組織雖然高度認同人工智慧的重要性，但並未隨著 AI 的導入應用調整組織架構與流程。「這的確是很多企業目前的困擾，因為沒有經驗，也不

敢嘗試，」她說，這也是很多企業 AI 應用落地程度偏低的主要原因。

先從簡單的專案切入，建立手感與信心

AI 導入的第一步往往最為艱難，張益肇建議，一開始先從較為可行、簡單的專案切入，使團隊從中建立信心、逐步熟悉流程，接著再慢慢擴大，例如先從客服回應等應用開始，提升回覆品質。因為這類型專案較常見，且資料量多也較容易規模化，加上目前生成式 AI 因為已經發展得非常成熟，可與客戶進行互動，會是較好的起點；而營運、管理、研發方面的 AI 應用，因為需要針對不同領域訓練 AI 模型，仍有其他努力空間。

在人才和運算資源上，具體仍得視企業需求而定。人工智慧科技基金會技術處總監張嘉哲提醒，易於上手的生成式工具雖然吸引不少關注，提高大眾學習的意願，也降低企業使用 AI 的門檻，但大語言模型並非一般公司可負擔的遊戲，限制也較多，企業大多仍透過 Fine tuning 進行一些小型資料訓練。而大語言模型終究是語言模型，仍是 AI 的範疇，使用原理和限制差距不大，企業仍得需要具備資料及可因應的基礎知識。

對於還沒有開始 AI 轉型的組織，張嘉哲建議，企業不要急著著眼於 AI 應用，可以先檢視企業自身哪些流程、系統或服務會產生資料，再從中觀察合適的應用場景。倘若企業不先從資料著手，僅是天馬行空地幻想有哪些應用，往往會在執行中遭遇現實阻礙，不如實際檢視手中的資料，仔細盤點出對公司重要的

資料，並開始著手蒐集。一開始，可能藉由一般的試算表軟體就能從資料中觀察到些許特徵，接著，再往下深掘更多資訊。當掌握到更為明確的目標與資料後，對於使用 AI 的目的，以及所需的資源與方向將會越來越明確。

技術培訓就像播種，組織文化才是關鍵

人工智慧科技基金會在協助企業賦能 AI 的過程中也觀察到，台灣企業在人才招募與培育上的限制，例如找不到人才的窘境。然而，因應企業轉型升級需求，企業內部勢必得進行結構調整，並開始思考如何培育與賦能現有同仁的能力，透過課程訓練與內部競賽的方式，先在內部孕育出重要的種子部隊，並拓展到其他的部門與團隊，才能帶動整個企業脫胎換骨。

「AI 技術的培訓就像是播種，將 AI 的種子灑到各個企業中，期待能從中啟發有潛力的人，在企業中帶來改變。」張嘉哲說，技術問題脫離不了組織問題，AI 要在企業中落地，需要克服重重困難，除了發展資料驅動需要的資料科學家、工程師等人才，負責發起 AI 專案的人還需要會爭取資源且懂得避開風險，以確保專案的成功率。尤其當員工學習 AI 知識或技術後，返回原本的組織，仍得需要就企業整體共同的目標與共識，才能會做出相應的調整。而組織的文化也是 AI 能否落地的關鍵，企業若能經營合作與分享的文化，避免部門間的隔閡，才能有利於新專案的發想與進行。

隨著科技快速進步，企業如果要適應加速改變的未來，就必須對於人才的培

育進行規劃與投資，提早因應技能重塑的未來。這不只是教育訓練，而是企業建立核心競爭優勢的關鍵策略。

根據企業需求定位，選擇合適的 AI 算力資源

Google Cloud 台灣技術總監安玟宇直言，生成式 AI 的爆紅也隨之帶動起 AI 算力的需求。而當企業在評估運算資源時，也是在為自己定位，究竟是要做為一個 AI 開發公司，例如是否需要發展自己的大型語言模型；或是將 AI 視為驅動企業的成長的工具之一，通過引入第三方 AI 方案來輔助與構建企業的應用場景。

舉例來說，企業若要將生成式 AI 落地到商業場景，常見的問題是直接在大語言模型 (LLM) 上提問，會發現沒有辦法得到針對特定商業場景所需的答案，還需要做提示工程 (Prompt Engineering)，或是建置服務，輸入公司現有資料，再讓大語言模型學習，才會達到最好效果。但真正需要加強的地方依然還是人才，包括很多產業專家的投入，在準備度上也需一段學習曲線。例如想用 LLM 解決醫學或法律的問題，同時需要兼具法律專長與 AI 知識的人，而這樣的人才目前仍是稀缺的。所以大部分第一波的導入大多不涉及核心業務，如客服或線上 QA 應用，待熟悉後再開始啟動核心業務相關的 AI 專案是目前業界主流的進程。

安玟宇分析，企業的運算架構佈局大致可分為自建模型、使用開源模型

(Open Source)，及開源模型加上調整訓練三種選項。自建模型初期需要投入大量的硬體資源，由於企業大多無法在短時間內佈建所需的基礎設施，或無法即時取得新的硬體，這時就會需要雲端服務 (Cloud) 支援。在算力資源選擇上又可考量場景的不同分為兩種選擇，部署專為 AI 訓練優化的特殊加速器，如 Google 提供的 AI 加速器 Tensor Processing Unit (TPU)，或是使用通用型的 GPU。

即使 GPU 已經是當前熱門單字，但企業仍可依成本與效能選擇 TPU 或 GPU。安玟宇認為，一般來說，在人才招募與開源資源豐富度上，基於 GPU 開發的模型較有優勢；然而考量運算成本與效能，如果將 TPU 和 GPU 使用在同一個任務上，TPU 將更能達到較佳的投資效益。但他提醒，真正的問題在於，對於開發時僅考慮在 GPU 上運行的程式碼，如果要移植到 TPU 上進行運算，就需要再投資人力來改寫與優化，才能達到使用 TPU 的最大效益。對此，Google 也積極的支援更多的 AI Framework，如 TensorFlow、PyTorch、JAX/FLAX，降低改寫與開發的門檻。企業是否需要投資更多人力撰寫程式碼，然後使用如 TPU 等進階的硬體進行更高效益的訓練運算，還是選擇一般 GPU 就可以執行的任務把資源投資在其他地方，這是企業必須考量其核心競爭力要做的權衡。

相較於自建模型，使用開源模型 (Open Source) 雖然不需要投入算力進行模型訓練，但安玟宇提醒，企業在這個選項中需要富有產業知識的人才協助，

才能在眾多的開源模型中，評估出適合自己的模型。如果是使用開源模型加上調整訓練的方式，除了評估模型的問題外，更需要有足夠的技術人才調整與優化模型。

他也提到，目前 Google 在 Model Garden 上提供許多受歡迎的第一方與第三方模型；假使企業沒有自建模型的計畫，可從 Model Garden 中選擇適合的模型，並直接在 Google Cloud Vertex AI 平台上開啟使用。而介於兩者中間的開源模型加上調整訓練這個選項，耗費的算力與投入成本屬於中間程度，對於專業領域知識的人才需求又大於僅使用開源模型的企業。

讀再多案例，沒有動手仍是一場空

「不可能做什麼事情，都只有好、沒有壞；或只有成功，沒有失敗。」張益肇說，由於 AI 需要投資，無論設備添購或是使用外部廠商，都需要成本，而領導者的心態十分重要，能接受合理範圍內的失敗，並鼓勵員工勇於「嘗試」。但最重要的是，無論閱讀過多少案例，如果沒有實際執行的話，都沒有用。

另一方面，生成式 AI 的發展加速了 AI 應用產品的出現，在大眾對於人工智慧及其影響了解還不深時，對於市場上產品良莠也無法判斷。張益肇提到，為了幫助社會可以以更安全的方式應用 AI，人工智慧科技基金會正在推動相關認證標準的討論，集結產官學界的看法，透過標準的擬定，持續倡議並落實可信賴 AI 的願景。

資料治理與風險管理是 AI 治理的關鍵

文 / 人工智慧科技基金會



東吳大學資料科學
副教授胡筱薇

人工智慧科技基金會
董事長詹婷怡



“無論是數位轉型或人工智慧發展，資料就是一切的核心。兩位專家從資料治理與風險管理的角度切入，說明導入 AI 不能忽略的兩大關鍵思維。”

隨著生成式 AI 崛起，應用場域快速擴張，企業想要導入 AI，除了技術、人才、運算外，資料與 AI 治理更是不可避免的議題。「數據（資料）治理如果不夠完善，要產出更深更廣的數據應用就會受到一些限制。」東吳大學巨量資料管理學院副教授胡筱薇說。

這裡說的數據（資料）治理就像是打通資料孤島，也可稱作資料的民主性，

胡筱薇說，公司內各部門員工、業務單位都能自主運用資料，而不是任何數據分析或報表的產出都要仰賴 IT 部門協助，如人事部同事可依業務需求，利用公司的資料資源拉出所需的介面或需要的服務。

資料治理是一門研究資料與實務應用的科學：為整個資料生命週期每一階段設定政策和程序

人工智慧科技基金會董事長、前國家通訊傳播委員會主任委員詹婷怡則認為，資料治理與風險管理正是 AI 治理的關鍵。無論從數位轉型或是人工智慧的發展，資料就是一切的核心。詹婷怡指出，一般談及資料問題時，多半聚焦在個資與隱私保護，兩者也的確是重中之重，需要更多的立法與政策溝通，形成風險管理機制與可信任環境。從資料經濟發展的觀點，如何提高資料與數據的分析應用及經濟效率，並創造價值，且兼顧維護隱私保護的初衷，引發諸多相應制度與法規方向發展的辯論與探討，形成了所謂「資料治理」（Data Governance）研究風潮。當前產業對於資料 / 數據治理的概念仍十分薄弱，而資料 / 數據治理的重點在於，資料是活的，「它隨時會更新，收集和分類」。詹婷怡說，資料治理不僅是一門研究的學科，也是一門實務的政策。

「資料治理是指與有效獲取、管理、利用資料相關的一組實踐方法、策略、角色，其目的是確保資料在組織內提供盡可能多的價值。也是指在組織內管理資料的策略，確認資料的品質和安全性，決定誰可以使用什麼資料以及何時使用。」詹婷怡解釋，資料不是存在於單一的時間點，它是由來源、清理、更新、

儲存、分析、傳輸、備份、刪除等步驟所創造出來的。

「為整個資料生命週期每一階段設定政策和程序，才是真正資料治理。」她強調，資料治理就是指組織內管理資料的策略，而這就跟組織的營運制度有關。

儘管組織理論上應擁有許多資料，但依然存在許多問題，最基本的問題就是根本未有資料管理機制、多數都不是格式化資料；且即使有格式化，由於資料來源及組成十分複雜，組織也無法確定資料是否可靠；也因為資料品質不定，而無法依賴資料進行決策。因此，資料治理會是一個，使組織運用資料形成決策變得「變得可靠的過程」，真正有助於數位轉型和 AI 應用。

業務、資料、應用及技術四大層面 構成導入 AI 所需的完整架構

胡筱薇指出，無論要推動資料治理或導入 AI，企業都必須有一個完整架構，而這個公司治理的架構主要可分為業務、數據、應用及技術四個重要層面，形成一個循環且彼此協作，以推進企業的戰略。

業務驅動架構最重要的就是企業的戰略與願景，由於資料應用與公司的銷售、行銷、人資、財會、營運等各業務單位相關，如果企業只由 IT 部門負責導入 AI 應用或服務，可能因為技術人員不熟悉第一線的業務內容，以及各部門的真實需求，而容易發展出銷售與行銷等與公司營收直接相關的應用。

數據架構則要建立企業級的數據管理策略，除了數據收集、儲存、處理、安

全和隱私保護等；更要定義數據標準和數據品質管理流程，以確保數據的一致性、準確性和及時性。同時，還需建立數據治理委員會，負責制定數據治理政策和監督執行情況；以及建立資料字典（Data dictionary）和詮釋資料（Metadata）管理，方便數據檢索和理解。

應用架構必須包括識別企業的關鍵應用場景，並評估 AI 技術的適用性；設計「以用戶為中心」的應用架構，確保 AI 應用能被集結到業務流程中。此外，必須建立應用開發和部署的標準化流程，縮短應用上線時間；並加上應用性能監控和反饋機制，以持續優化應用體驗。

技術架構不只要選擇合適的 AI 平台和工具，以滿足企業技術需求外，還需要設計可擴展、高可用性的技術架構，以確保系統的穩定性和性能。而企業也應該建立數據安全和隱私保護機制，確保數據在採集、傳輸、儲存和使用過程中的安全；以及建立技能培訓和知識管理體系，提升技術團隊的 AI 開發和應用能力。

胡筱薇強調，在規劃相關架構時，企業還需要注意與參考以下重點：

1. 明確企業戰略和業務目標，識別 AI 應用的關鍵領域。
2. 評估現有的數據、應用和技術基礎，找出差距和改進點。
3. 制定業務、數據、應用和技術的發展藍圖，明確關鍵里程碑和交付成果。
4. 成立跨部門的項目團隊，確保各個架構的設計和實施能夠協同推進。

5. 建立數據架構治理機制，持續監控和優化架構的執行情況。
6. 加強與業務部門的溝通與協作，確保架構設計滿足業務需求。
7. 看看別人怎做，學習先進企業的經驗教訓。

有規範和使用準則才能形塑產業，相對健康的樣貌才能形成 Responsible AI，發展 Trustworthy AI

詹婷怡表示，不同於一般的損害主要主張事後回復原狀或損害賠償，在 5G 和萬物聯網的時代，一旦系統出現損害，所帶來的傷害將會極大；加上 AI 的應用中可能潛藏資料與數據偏差、演算法不透明、自主性過高、安全和隱私等風險，在 AI 相關的系統發展及產品設計時，就必須考量到這些挑戰，這也是需要使用與發展準則及評測的重要原因。

「有規範跟使用準則，才有辦法形塑產業，」詹婷怡說，規範對於產業的長成十分重要，也是塑造或重塑產業的關鍵。從全球趨勢來看，在軟體與系統設計時，一直以來即有不少規範指南及行業行為準則。隨著 AI 應用蔚為風潮，如 IEEE 在 2017 年 12 月 12 日全球發布第 2 版「人工智慧設計的倫理準則」白皮書 (Ethically Aligned Design V2) 指出，隨著自主和 AI 系統的應用與影響無處不在，我們需要建立社會及政策方面的指南，從而確保這些系統以人為本，並服務於人類價值和倫理準則，因此提出白皮書。

因應人工智慧的發展，以風險管理的原則來形塑相關規範與制度

美國國家標準暨技術研究院 (NIST) 則提出 NIST RMF (Risk Management Framework)，RMF 是為企業跟組織管理 AI 系統風險提供結構化跟可衡量的流程，遵循這個流程，可以最大限度發揮 AI 系統風險結構化。「可以看到這些準則多半從風險控管的角度出發，」她解釋，風險包含數據偏差、算法不透明度、自主性過高等，在 AI 風險總體架構中，將討論組織如何構建 AI 風險框架及可信賴 AI 系統該具備的特徵，包括透明度、解釋性、公平性和可追溯性。

近幾年，世界各國政府紛紛提出倫理準則與白皮書或至少開始積極討論，例如歐盟人工智慧法 (EU Artificial Intelligence Act) 草案採用「風險原則」(Risk Based Approach)，也就是根據立法者預測 AI 應用的危險程度來管制，並將風險區分為三類：第一類是風險無法接受，這類 AI 由於對人類構成嚴重威脅，因此要全面禁止，包括以行為、社經地位、個人特徵為準的社會評分系統、遠端即時生物特徵辨識系統，以及預測個人會不會犯罪的預防性執法系統等。第二類是高度風險，也就是可能損害人身安全或基本人權的 AI 系統，必須在上市前接受審查，上市後也要持續追蹤，例如交通、醫療、電梯設備等重視安全性的產品。另外，關鍵基礎建設、教育職業訓練、邊防移民、司法和民主程序等，可能牽扯到歧視或基本人權領域的產品也屬於此類。第三類是有限風險，例如爆紅的 ChatGPT 等生成式 AI 就屬於這一類。這類的規範重點是資訊透明，必須標示 AI 生成的內容、必須讓用戶知道自己正在跟 AI 互動。目的是希望 AI 不要被拿來傳播假資訊。此外，如果 AI 系統的訓練過程使用任何有版權的文字、

影像、聲音作品，也必須明確列出。這將有助於著作權持有人要求分潤的機會。最後一類則是風險極低的應用，如過濾垃圾信件、遊戲軟體等等，絕大多數應屬於這類，就不需要面對任何特殊規範。

身為許多國際事務組織的參與者及國際事務推動者，詹婷怡認為，國際經驗的參採十分重要，但前提是文化與思維的轉型，不論國家與政府領導者、規範制定與立法者、或是企業創辦人與經營者，都必須具備數位轉型的理念與行動能力，回到網際網路與 AI 技術與運作本質，了解萬物相連的特質。

除了從風險管理的角度，她更強調，必須想清楚要做什麼，以及如何用 AI 解決對台灣真正有用的議題，大至提升國家競爭力、創造數位發展生態系；也可以是台灣極為重視的 AI 產品與服務。而 AI 的風險管理必須從更高格局，在數位匯流基礎上，思考台灣推動 AI 的目的。詹婷怡再三強調，絕不是只有打入 AI 供應鏈及製造 AI 設備等這麼基本的事，更重要的是讓台灣社會整體資訊素養提升，並具備 AI 應用的正確觀念與方法。

詹婷怡說：「很多科技技術帶動的發展，目前不一定有正確答案，但我們有正確的理念、對話、整合的機制，以及成熟的多方治理模式時，許多答案就會慢慢浮現。」

04

產業案例

- **玉山銀行**
用資料科學打基礎，玉山銀行讓 AI 成為員工 DNA
- **統一資訊**
從熟悉的工作中出發，統一資訊用 AI 找出新解方
- **遊戲橘子**
從數位轉型中探尋 AI 市場化機會—遊戲橘子的創新之路
- **趨勢科技**
必須比駭客更會用 AI，趨勢科技賦能員工因應產業需求

玉山銀行用資料科學打基礎，讓 AI 成為員工 DNA

玉山銀行科技長張智星



面對科技帶來的衝擊與影響，許多大型金融業者很早就積極進行數位轉型，甚至在 AI 領域投入資源。隨著 GenAI 的發展，更多金融場景的想像與應用也隨之而來，企業如何透過科技強化顧客體驗、優化工作流程，提供穩定的服務與系統，除了技術債之外，更重要的是企業對 AI 的態度，以及整體架構的制定。

生成式 AI 帶來的影響，讓企業在 AI 應用更小心

玉山銀行為全台首家將 AI 導入各業務場域的金融機構，早在 2006 年，就在

金控底下設置大數據分析團隊 CRV (Client's Risk & Value)，進行客戶分群分析；直至 2018 年開始佈局金融 AI 發展藍圖，除了率先成立科技長辦公室，更打造自家機器學習即服務 (MLaaS) 平臺，為 AI 落地的關鍵基礎設施之一。2019 年成立智能金融處，做為內部 AI 供應商，將 AI 融入日常業務營運。致力透過科技強化顧客體驗，並提供穩定的服務與系統。2023 年更開始布局生成式 AI，一路發展出多個應用服務，更在今年初正式推出 GENIE 平臺，行員透過 Web 介面即可快速使用生成式 AI 服務，加速各項工作流程。

玉山銀行科技長張智星表示，生成式 AI 的發展使得企業在 AI 的應用上變得更加謹慎小心。由於玉山早在 2023 年初就開始使用相關工具，在應用流程上，不僅資料上傳前需要確保有無機敏資訊，輸出的資訊也需要監測。除了利用內部開發的工具與技術強化資料把關，在內部教育訓練上，也會提醒員工不能將個資及敏感資訊用於外部的生成式 AI 工具上。他補充，目前的應用尚不會與顧客直接接觸，主要仍是擔心回應不夠適當或提供錯誤資訊。

玉山銀行智能金融處主任工程師陳照元解釋，由於金管會現在已經允許金融業將資料上雲，只是需要更為複雜的資料保護與管理權責機制，因此，他們下一步的目標首要是完善雲端隱私的合規面。至於生成出的資料，難免有不穩定的狀況，除了盡力確保輸出格式沒有跑掉，也基於內部的自動化檢核系統，確保內容正確性。

另一方面，生成式 AI 的出現，也降低了企業在文字處理上的成本。陳照元說，之前團隊在處理新聞等文字資訊時，主要透過玉山自建的文字處理模型，但仍

不夠泛用。而生成式 AI 的出現，讓他們在即時新聞資訊擷取與翻譯等資料的整理上，大幅降低了導入成本，不過，在監控的成本上也會提高。後續團隊也預期開始進行多元資料的整合，輔以知識圖譜等技術，發展出更多內部應用。

導入 AI 挫折滿滿，優化員工工作流程才是初衷

張智星提到，玉山投入在資料科學的經營已有十幾年，在培養每個業務單位成員對資料科學的認識上，更是投入不少教育訓練資源。從新人入職開始，智能金融處就會派員協助上課，講解關於人工智慧概覽，與初階資料科學的介紹。透過長期的教育訓練，讓每個部門都具備 AI 及數據的概念。除此之外，針對中階管理人員、高階主管也都有相應的訓練課程。

除此之外，智能金融處也會定期與各部門開會討論，了解當季的專案與執行狀況，同時也會主動與業管單位討論業務流程的調整與新的專案發想，兩邊是否有需要合作的地方。一旦提案與發想成熟，就會進標準化的開發流程中。

智能金融處在成立的 1 年內便推出 AI 研發平台、AI 工具，更將 AI 應用融入日常工作流程，包含推出 GRACE 智能理財來協助理專，提供顧客更完整的配置建議；或是推出智能 IVR 語音導航服務，將客戶撥打客服電話的操作時間縮減 68.3%。甚至現在集團同仁還會主動提出新的 AI 需求，這可以視為是一種對於團隊的肯定，張智星認為，這代表 AI 導入的部分已被其他單位所接受，且證實能提升工作效率，並廣泛運用。

陳照元笑說，團隊在導入 AI 的路上磕磕碰碰，也跌過不少跤，最大的困難則

是，如何讓業務單位知道導入新的流程，或 AI 產品是對雙方都有利，甚至是業務單位受益較多，而不是彼此妥協。他舉例，對理專來說，過往需要耗費多時間自己整理資料，但現在透過 AI 依據研究員提出的市場觀點，快速生成出顧客資產最適化報告後，理專再將報告內容消化後，轉譯成客戶喜歡的互動方式清楚快速傳遞的資訊，更減輕了前期的工作量。

他認為，業務同仁並不擔心被 AI 取代的原因，除了與 AI 協作幾乎已經是玉山常見的工作型態；再者，員工可以專注於需要更高專業性與高價值的工作。例如客服電話中心，「人一定在某些重要的環節內。」陳照元說，AI 可以回覆顧客常見的問題，但在像是債務協商、商機探索等工作，需要更專業且溫暖的溝通技巧，目前的 AI 還無法勝任的，也是銀行的核心價值。

張智星坦言，團隊向來以 AI 落地為目標，但過往導入的 AI 專案，失敗率極高，後來才發現，硬要套入 AI 技術，並發想相關應用非常困難。於是，他們開始朝向如何在既有流程中，提出改善方法。他笑說，有時候可能加入 AI 技術並不是最佳解法，可能需要的是改善整體工作流程或是進行組織調動。直到現在，他們也對 AI 專案有一定的熟悉度，知道該如何提出問題，並且透過價值與效益的評估，才進入開發排序中。但他說，最重要的核心仍是要優化哪些流程，才能對客戶與業務有幫助。

從資料應用到資料治理議題

張智星說，由於智能金融處與傳統銀行的 IT 部門不一樣，會看到大量的真實

顧客個資，並進行資料處理、模型建置，所以在資安隱私的保護環節上需要有很多法務的協助，以及系統上的配套措施。如何設計一個完善的資料庫，讓集團的資料都可以匯入，並由智金處統一收集處理，所需顧及的範疇也就非常的廣泛。

而玉山過去大數據分析團隊 CRV (Client's Risk & Value) 一開始從顧客風險價值出發，探勘既有的客戶 KYC (Know Your Customer) 資料，並細緻地將客戶分群。除了內部資料，甚至整合外部如新聞、財報等資訊，這些經歷也為現在智能金融處奠定了風險控管基礎，並漸漸朝向精準行銷、語音辨識、文字處理等應用發展。同時透過多年豐富數據的累積，整合資料間的關聯性，進而拓展更多的應用。

面對金控內部不同事業體，彼此錯綜龐雜的資料，如何連結整合是個重要的課題，也凸顯企業資料治理的重要性。張智星說，主要是成立跨單位資料小組，由總經理擔任召集人，並將所有的資料分成不同層級，包括可和其他部門共享的協定及列為機密管制的最高層級資料。並將資料重新整理與標準化，當標準訂出來之後，推及到整個集團適用。並且透過隨時的追蹤和判別，確保所有資料標準是被遵循。如果資料有衝突的話，就要提到委員會中討論。

舉辦玉山人工智慧公開挑戰賽，不只吸引人才更希望建立產業生態系

張智星提到，自 2019 年舉辦至今的「玉山人工智慧公開挑戰賽」不僅是企業吸引人才，也是希望透過這個比賽達成金融共好。由於金融業場景的真實資料，

礙於監管關係，十分難以取得，這也使得許多新創難以進入相關領域。但透過公開比賽，玉山將真實金融場景中的資料清洗後釋出，由於資料的稀缺，吸引不少研究學者或是團隊報名參加。甚至有研究學者取得相關資料，並以此進行研究後發表，說明了真實金融資料的珍貴。

參賽隊伍除了考慮資料、演算法外，還要顧及解方必須貼合真實場景。不同於學校教學的 AI 題目都有標準答案，挑戰賽並沒有最佳解方，甚至需要隨著環境變化持續修正。例如信用卡冒用的題目，由於詐騙集團的手法一直更換，永遠都得處於一個競爭的狀態，有可能這週有用的模型，下週就不適用了。張智星說，即使玉山內部已經有許多 AI 專案進行，但依然很難向外界解釋實際面臨的困難。透過比賽，參賽隊伍可以藉此瞭解玉山內部正在進行的事情。

此外，為了確保企業的技術能量可以跟上最新趨勢，玉山也與國內重要研究及學術機構都有建立產學合作機制，確保對於前沿技術的探索。

從熟悉的工作中出發，統一資訊用 AI 找出新解方

統一資訊副總吳聲輝



2023 年的生成式 AI 熱潮，吸引許多企業積極了解相關應用潛力，面對勞動力減少、消費者購物行為改變等因素，更希望能藉由 AI 技術的使用，增加營運與生產效率。

找到 AI 對工作的幫助，說服成員接納新技術

「使用 AI 不是省掉人力，而是協助提升工作效率，還有執行力。」統一資訊副總吳聲輝說，例如企業之前推出的「食安資訊解決方案」，便是透過爬蟲系統快速找出海內外食安相關新聞、案例等資訊，再利用大型語言模型快速整理

摘要，協助人員有效溯源原物料產品，並可在第一時間做出預警與應變。使得更多需要耗費龐大人力整理的資訊，在幾分鐘內就能完成，大幅釋放有價值的人力。該方案更獲得多家食品製造廠與零售通路業者肯定。

團隊也從這個案例開始往外拓展新的專案或想法，嘗試在傳統的作業或是業務流程上，加入 AI 的元素，使其工作效能提升並有效節省成本。不過，吳聲輝也坦言，對企業人員來說，要在習慣的工作模式中加入新的 AI 技術，除了要適應新的技術，更需要投入學習成本，甚至可能會影響到原本的作業流程，這才是企業導入 AI 最大的挑戰。因此，需要與同仁溝通學習新技術之後，後續應用在工作帶來的益處，以利後續 AI 專案的推動。除此之外，他也讓全公司的人都能先接觸並使用 AI 工具後，再將員工的使用心得進行統整，歸納出適用於自家企業的使用方式。

例如，企業如果有海外拓點的計畫，需要花費許多時間撰寫的招募職缺描述，如果可以透過生成式 AI 的協助，很快就能完成；又或是協助文件整理與翻譯，無論是業務開發或是信件溝通上，都能藉由相關技術的使用提高工作效率。於是，內部也開始著手相關工具的開發，先從企業內部成員開始試用，讓企業中每個人都可以用 AI 完成想做的工作，再慢慢往外推廣。

吳聲輝提到，由於市面上許多生成式 AI 工具，企業因為顧慮到資料外流的風險，所以使用上難免有所限制，甚至可能無法使用。在資料的存放與 AI 應用開發上，統一資訊也開始著手私有雲的規劃部署。

資料是關鍵的基礎

至於 AI 開發中關鍵的資料問題，吳聲輝提到，建立資料倉儲 (Data warehouse) 是目前重要的基礎工作，而企業中各部門長期累積下來的資料，整理過程中更有許多問題需克服，包括系統、資料庫、格式、版本等等的不一致需要克服，但他認為，過程中，需要企業由上而下的落實治理策略，並且遵循規範。在統一資訊中，系統支援部門就是負責相關流程、規範的專責單位，以方便其他部門遵循。後續建立的 AI 團隊，也才能從資料中進行延伸的應用。

另一方面，吳聲輝認為，由於政府法規對於個資方面的規定，在資訊安全面必須做把關，無論是資料儲存或是分類都需要符合規範；而在資料清洗與整理上也有一定的流程，並且需避免雲端上資料外洩與被入侵的風險。至於內部溝通上，統一資訊每年都會舉行一個重大的資安會議，並聘請外部顧問一同商討及檢視缺失，並進行改善。他直言，資安的問題必須由上至下，嚴格落實把關，且因為涉及企業形象，因此，即使是一些小缺失，也要想辦法改善。

工作流程已產生改變，企業勢必得擁抱 AI

吳聲輝笑說，AI 導入真的會對工作流程帶來改變。例如公司有 70% 的人需要寫程式，過往工程師需要讀懂別人的程式，並且進行團隊開發。但導入生成式 AI 工具後，不僅 PM 可以透過提示詞自己寫出一段程式；對於一些特殊的程式碼，工程師過往需要花費一至兩天時間找資料或是解決 Bug，有了工具之後，僅需要五到十分鐘就能快速寫出符合需求的程式碼，大大提升了開發效率，甚

至對整個流程帶來破壞性的改變。這些改變與效率的提升，也讓他們更確定企業未來的策略勢必得擁抱 AI。

但也因為技術的進步速度越來越快，吳聲輝認為，雖然不會對企業的整體策略帶來劇烈改變，但新技術的出現與資源的投入評估更需要與時俱進。許多大型語言模型的出現，使得企業在評估資源與成本後，便放棄自行開發語言模型的計畫，轉而以應用的開發為主。甚至多模態模型的出現，則可能為集團帶來新的應用，例如結合集團內部的物流，往倉儲自動化方面佈局。目前多以人力進行倉儲揀貨，可能可以用機器人取代，包括機械手臂或是影像控制等技術的導入。

從熟悉的事業出發，找出解決方法

吳聲輝強調，目前已知的方向是透過了解企業的痛點，想辦法找出解決方法，而不是利用 AI 去做出一個事業。因此，團隊主要還是在熟知的事業中，嘗試透過 AI 技術的導入進行改變。

至於後續可能產生的風險議題，吳聲輝表示，公司內部的法務也已經開始注意到相關資訊，並且在內部推動教育訓練；而國際的法規趨勢，也開始受到關注。他認為，下一步的 AI 策略是希望整個公司的成員都能善用 AI，且可應用 AI 提高工作效率。同時，他們正規劃往海外發展，也募集並運用相關的海外人才，甚至將本地的經驗帶往海外。

從數位轉型中探尋 AI 市場化機會——遊戲橘子的創新之路

橘子集團大數據與資料科學研發處處長蘇緯倫（左）
遊戲橘子數位科技集團策略長陳冠宇（右）



從遊戲到泛娛樂產業，遊戲橘子已悄然佈局 AI 市場

遊戲橘子數位科技近年除了持續深耕遊戲營運，更同步積極經營網路電商、媒體影音、支付工具、社群平台、IP 孵育、及雲端資安等市場，從原本的遊戲主業往泛娛樂產業佈局，成功拓展及堆疊遊戲外的多元事業營收。

橘子集團策略長陳冠宇表示，集團各產業累積的豐厚使用者數據、輪廓，是橘子發展全生態娛樂科技的關鍵能力。例如遊戲事業部擁有龐大數據量體，可協助其他事業部進行關聯性分析，像是某遊戲玩家在遊戲裡儲值消費的行為，是否能轉化至電商應用；而各事業部對使用者的畫像分析則能補足遊戲事業部

對該玩家的理解。

由上至下貫徹 AI 轉型目標，技術團隊與各事業單位激盪出創新火花

藉由 AI 進行數位轉型，已成為橘子內部從上至下強力貫徹的任務，集團執行長劉柏園要求，各事業部必須定期向他匯報當前 AI 專案進程。陳冠宇說：「執行長要求，各事業部優化營運方向必須以數據分析為依據，且將透過 AI 提升營運績效，做為核心目標之一。」

即使有明確的指導方針，但實際導入 AI 最大的挑戰是，各業務單位不一定了解 AI 技術能帶來的幫助。因此，集團數據中心透過營運單位外部與內部驅動雙管齊下，讓業務與技術單位互相理解。外部驅動部分，數據中心定期主動與營運單位訪談業務策略及痛點，給予導入 AI 的建議及技術支援；而內部驅動部分，由於集團各單位都有獨立的數據分析師，透過分析師與各業務單位營運同仁進行大量日常領域知識交流，最後再回到數據中心協同共創 AI 需求研發。

「讓技術人員了解特定業態的業務模式與痛點，同時加強營運單位對 AI 的認識，才能激盪出真正可為營運單位創造價值的 AI 解決方案。」橘子集團大數據與資料科學研發處處長蘇緯倫說。

建構靈活的資料框架是推動集團 AI 轉型的關鍵

「發展 AI 數據，最重要的事就是數據要能統一管理、整合，」蘇緯倫解釋。由於集團內部各事業部門的業務類型和用戶不同，數據格式也各異，因此首要打造一個集中管理的大數據系統做為基礎。

蘇緯倫指出，要建構良好的大數據平台，必須做好數據梳理和監管，否則後續 AI 應用無法產生效益。由於集團囊括眾多產業，各自關注的重點和運作方式也不同，因此，他花了大量時間理解各產業需求及未來策略，定義出一個靈活、可擴展，橫跨產業都能通用的具體框架，讓過往累積的數據轉換到新框架下，而各單位也能理解彼此數據，並在框架內自由運用和收集更細緻的大量數據。他強調，AI 時代的核心在數據，只有建立良好的基礎設施，才能為 AI 轉型提供可能。

經過三年佈局，遊戲橘子集團內部已成功提供數十個 AI 解決方案，以下為集團內不同產業公司應用案例。

客服公司：透過深度學習 100% 覆蓋對話監控，提升客服服務品質

對客服公司來說，對話監控的覆蓋率是重要評估指標，目前市場上的客服公司多由真人進行對話品質監控，礙於人力，僅能抽驗監控，覆蓋率約 5%-8%。蘇緯倫說，團隊以深度學習方法偵測語音對話內容，並檢視客服人員的回應與禮儀是否合宜、有無高風險對話等。一旦偵測出錯誤回應內容或服務品質不佳的通話，再由真人進一步判定。這個專案的開發不僅協助客服公司顯著提升效率，更因可達 100% 的覆蓋率，也幫助客服公司爭取到與國外客戶的合作機會。

點數公司：多技術結合，協助精準打擊詐騙連續行為

蘇緯倫解釋，詐騙型態快速變化，過去主要利用寫定的專家規則過濾詐騙，但這個方法不僅容易打擾客戶，也常將一般客戶認定為詐騙，間接影響營

收。集團的點數公司希望將 AI 運用於詐騙偵測上，因此團隊利用 Topology Learning 與 Time Series Analysis 輔以 Anomaly Detection 等技術多管齊下，對疑似詐騙的連續行為做風險分級，配合驗證機制，在只影響 0.5% 用戶下，抓出 91% 的詐騙，精準打擊詐騙行為。

媒體公司：透過深度學習與強化學習，協助模擬專業投手投廣

在廣告投放領域，廣告操盤手投遞廣告策略的經驗直接影響廣告成效。集團數據中心整理長期累積的廣告資料，並運用深度學習技術分析廣告圖文與影音資訊。透過強化學習 (Reinforcement Learning) 模擬專業廣告操盤手的投放方式，最後使用生成式 AI 總結行動，向操盤手提供建議。這項技術有效減少操盤者的經驗誤差，使廣告投放成效更趨向專業操盤者。

社群與電商平台：減少社群人力成本、增加電商轉化率

過往社群經營人員需要花費大量時間管理不實資訊，透過深度學習技術分析圖、文、影音，以 AI 巡邏可自主抓出約 95% 的不合適內容（色情、暴力、詐騙或廣告），準確率高達 98%，大幅減少重複性工作人力。而電商公司利用 AI 技術優化使用者購買體驗，幫助消費者更快找到所需商品。蘇緯倫說，AI 技術結合 UI/UX 改善，大幅增進電商網站的轉化率達 17 倍、平均客單成長 30 倍。

三大階段佈局，協助市場上其他企業跟上 AI 浪潮

「在集團執行長的支持下，過去幾年集團廣招資料科學家，持續研發 AI 對外

服務專案，並研擬出橘子集團後續的 AI 佈局。」陳冠宇說，未來其他企業也有機會使用到橘子的 AI 服務。

陳冠宇觀察，台灣許多企業難以回應這波 AI 浪潮有五大主因：一、發展 AI 需要龐大經費，二、缺乏人才團隊，三、重新佈建基礎建設費時又費力，四、大部分 AI 工具都從技術切入，提出單一解決方案，但各產業都有專屬領域知識，產業人員無法將工具應用於工作中，五、從業人員擔心 AI 衝擊本業。

他透露，未來橘子的 AI 願景是協助其他企業跟上 AI 浪潮，為此，後續佈局可分為三階段，第一階段透過自家開發的 AI 工具，協助集團內各單位有效提升營運績效，或成本控制；第二階段則從集團內不斷發展的 AI 專案中，找到市場化的機會，透過客製化專案服務外部廠商；第三階段是將所有的 AI 服務模組化 (AlaaS)，置於合作平台方銷售，其他企業可以在平台上選擇適用的產品模組，協助沒有 AI 團隊的企業透過提供的 AI 服務解決營運問題。陳冠宇說，目前發展正處於第二階段，預期明年將發展至第三階段。

兩大類型客製化專案打頭陣，先行服務市場

近期橘子正在研發幾套可對外服務市場的客製化專案，其中兩大類型專案：客服機器人、IP 為核心的變現工具，雖尚未正式對外行銷但已吸引許多外部合作機會。

客服機器人：蘇緯倫說，該機器人主要利用自家研發的 D-RAG (Distilled Retrieval Augmented Generation) 技術，核心關鍵在於模型可自動整理用戶

上傳的原始資料，降低用戶清整資料的痛點，也提升資料產出的精準度。相較一般的 RAG 架構再提升 40% 的精準度，也因資料能被精準梳理，更能有效掌握基礎風險，避免 AI 幻覺問題。同時也提供後台讓廠商可以進行人為的資料干預，再次針對高風險議題進行管控，另外，機器人還能依據真人反饋自主學習問答。該系統已應用在線上大型遊戲客服上，機器人的自主解決率達 83%，且上線後維持零風險問答，並整合集團各項資源，提供一條龍服務，如真人服務、客服系統串連、大數據廣告推送等。

IP 為核心的變現工具：為放大創作者的原創價值，團隊透過 AI 技術結合 IP 使用場景，發展出不同 IP 應用專案，如 AI 風格創作工具及偶像分聲。

蘇緯倫提到，團隊針對圖像創作者，開發一套 AI 風格創作工具，主要是在 Diffusion Model 上疊加技術，加強臉部細節，讓臉部更符合 IP 風格。同時，也讓創作者們參與 AI 模型的訓練，並獲得一套自己風格的 AI 創作工具。透過這套應用可為創作者的粉絲們帶來全新互動體驗，未來更進一步延伸到客製化周邊商品的製作，為創作者們帶來更多變現機會。

此外，團隊也提出偶像分聲專案，主要利用深度學習技術，在 Bert-VITS/GPT-SoVITS 基礎上自主研发語調、語氣、語速模型，發展出學習聲音及捕捉情緒的 AI 聲紋工具，甚至能支援技術難度更高的台語語音，讓影音創作者或藝人 (如：偶像、聲優、網紅、Vtuber 等 ...) 訓練屬於自己的 AI 分聲模型。

不陷入大模型角力：聚焦垂直應用，解決產業問題

陳冠宇與蘇緯倫共同表示，大型語言模型的出現不該是讓所有人都投入自建行列，而是能藉此開發出垂直產業的新工具。對遊戲橘子而言，更重要的責任是「深入產業，解決業界問題。」當大模型越強，企業就有更強大的能力提供更好的服務、解決業界更深層的問題。

必須比駭客更會用 AI，趨勢科技賦能員工因應產業需求

趨勢科技台灣區總經理洪偉淦



生成式人工智慧技術持續成長，不僅改變了許多企業的服務與使用體驗，更對資料隱私安全帶來莫大威脅。面對潛藏的資安危機，趨勢科技執行長陳怡樺曾在受訪時提到，因應生成式 AI 的可能威脅，公司同仁必須比駭客更會用 AI。面對 GenAI 帶來的挑戰，趨勢科技如何透過行動賦能，協助員工進行技能提升，以面對時代的轉變？

2022 年底興起的生成式 AI 熱潮，讓不少人誤以為 AI 就只是生成式 AI。趨勢科技台灣區總經理洪偉淦強調，AI 技術很早就被廣泛運用在資安領域中，而趨勢科技早在 2018 年前，就已經將 AI 技術應用在如垃圾郵件的判斷與偵測上，

過程中最大的挑戰就是，雖然擁有許多資料，但是得從許多紀錄 (log) 和遙測數據 (telemetry data) 中提取出惡意和可疑的行為。而在 GenAI 技術大幅躍進之後，公司內部就開始推動相關計畫，全面鼓勵員工認識並思考如何在日常工作中運用 AI。

為了賦能員工新技能，特意舉辦一場長達半年的競賽

轉型最大的困難其實是技能的轉變。對於企業來說，如何協助員工技能轉換，由內向外應變產業環境的最新需求是個重大議題。洪偉淦說，為了賦能員工新的技能以適應新的時代，公司甚至舉辦大規模且長達半年的 AI 競賽：AI contest。

這場活動的主要目的就是希望透過有趣的方式為員工賦能，過程包含一連串 AI 專業知識及商業應用發想的練習，並邀請各界 AI 專家於內部舉辦專題演講及專業課程，最後還舉辦全球黑客松比賽，期待藉此激發出更多的創意與想法。因為只要兩人就能組隊，也沒有應用主題限制，因此，吸引許多跨部門的團隊報名，如業務搭配 RD 或行銷，報名參賽的隊伍數高達近千組，過程十分激烈，最後篩選出近百組隊伍到日本進行決賽。

這場比賽也可以視為企業內部啟動 AI 專案的開始。洪偉淦強調，比賽只是個形式，重點在於如何激發公司同仁的學習氛圍，面對新的科技演變，不論任何職務專才都必須「Get ready for this kind of change。」

「未來無論在公司營運或客戶服務的領域中，都可以使用 AI。因此，企業成

員應該要有基本的應用知識，才有機會發想與思考任何可能的 AI 應用。」洪偉淦說，每個人使用 AI 的方式都不相同，不只可用 AI 自動完成部分工作，更可以藉助 AI 之力做到更多事情，為自己創造價值。

透過生成式 AI 啟動知識管理

洪偉淦說，除了透過生成式 AI 協助工程師撰寫程式碼，提升開發效率；同時，還有些專案是希望能降低技術支援的比例，更進一步來說，是利用 GenAI 進行企業知識管理。由於趨勢科技的產品十分廣泛，許多說明都放在內部維基百科上，若能透過大型語言模型學習產品及各類技術知識，並利用簡單的介面快速取得相關的技術說明，後續無論是在 RD、技術支援、業務行銷上，都能廣泛應用。

知識管理應用過往在搜尋方面並不是那麼順暢，但透過大型語言模型的強化效果，內部團隊也可以了解到哪些資料容易透過這種方式取得，以及還有哪些資料不方便使用，由於演算法推陳出新的速度十分快速，即使專案暫時遇到困難，團隊也必須時刻做好準備。

此外，還有針對客戶成功（Customer Success）的應用，也就是利用客服紀錄、產品使用紀錄，以及會員系統上的紀錄，統整分析出客戶目前的階段與類型，提供適切的服務以提高滿意度。例如大型企業剛導入產品時，需要的可能是部署的知識，系統會通知相關人員，客戶目前所需的執行方案，以利人員後續提供服務。或是在人力支援較不足的情況下，可以提供線上的訓練課程，協

助客戶使用。

過去雖然已有相關研究，但較偏向人工方式進行，並已開始進行資料集的整理。「資料彙整的部分，並不是當 AI 來時才開始進行，」洪偉淦說，團隊很早就開始相關議題的研究。但目前遇到的難題除了有部分資料無法被彙整之外，還要考量資料敏感性的問題，因此，資料分級將是接下來要考慮的議題。

另一方面，團隊也在產品的設計上加上生成式 AI 的應用，由於資訊安全產業中有許多專業的名詞，許多企業在使用上較難理解相關說明，於是透過 Chatbot 的設計，以口語的方式讓使用者可以快速理解說明並執行後續動作。

至於如何利用生成式 AI 進行更多後端的分析，洪偉淦說，目前主要分為兩大部分，其中一個就是風險評估。「資安要做好，必須要先理解面臨的風險是什麼，」他解釋，風險包括熟知的漏洞、錯誤設定等等；而風險緩解並不是等到遭受駭客攻擊了，才趕快進行回應，而是希望在駭客攻擊前，就已經掌握企業內外部可能會被攻擊的潛在弱點，針對風險進行緩解措施。但風險的防護並非壁壘分明，當中雖然有一定的規則進行分析，但目前團隊也在嘗試利用生成式 AI，讓風險評估可以做得更完美，效果也更能被客戶接受。

而另一個部分就是零信任（Zero Trust）的概念，由於零信任涉及信任推論，也就是所有訊息如資料存取請求都不能相信，必須以風險程度進行評估標準，以判斷是否允許後續的存取與信任機制。

除了 AI for Security，更要 Security for AI

「導入 AI 是有風險的，」洪偉淦說，包括隱私、完整性，以及幻覺與準確度判別等問題，甚至可能常聽到的 Prompt Injection，也就是透過 Prompt 取得不應揭露的機敏資訊；以及資料污染等問題。即使透過各式的規則與指引，提醒內部員工在 AI 使用上需要注意的規則，依然無法全面防止資料或機密外洩。即使沒有駭客攻擊，人工智慧本身就存有隱私與資安的問題，更遑論其他有心的攻擊。因此，未來企業在導入 AI 上，更需要注意資安問題，例如導入過程中，必須確保資料的安全；並避免有心人士透過 Prompt 取得敏感的機密資料。

洪偉淦提到，Security for AI 是趨勢未來極為重視的方向。在使用 AI 應用時，資安的問題總是伴隨而來。因此，必須認真看待相關議題，例如如何管理企業使用的熱門 AI 應用工具、使用過程中如何避免資料外洩、企業開發 AI Apps 的安全架構等。至於如何管理，當中涉及到如 Application Control、Access Control、Data Filtering，或是 Data Scanning 等技術，這些與趨勢過去累積的知識經驗都很相近，只不過發生新的平台或服務上。

無論企業導入 AI 的程度多少，使用雲端或是本地的 AI，都必須要有資安的解決方案，以協助企業在進入 AI 領域的過程中，不致發生資料外洩的狀況。未來，趨勢也會正式投入 AI Security 領域。「我們相信市場在 AI 熱潮之下，將有非常多的應用會陸續出現，」他強調，這是未來的目標也是重要的發展路徑（Roadmap）。

為了推動整體的 AI 生態系，趨勢科技也陸續與相關廠商進行合作及討論，知名的雲端廠商也都是重要的合作夥伴。洪偉淦認為，未來將會有更多各式各樣的網路架構出現，如何在不同的平台上提供解決方案，將是重要的一環，並期待能與更多的協助客戶導入 AI 的系統整合廠商進行合作。

05

結論與建議

- 經營策略與組織文化將決定 AI 成敗

經營策略與組織文化將決定 AI 成敗

文 / 人工智慧科技基金會

生成式 AI 的蓬勃發展，吸引不少企業開始在組織中使用相關工具，期待加快業務程序，更能進一步為組織帶來新的成長。然而，因為生成式 AI 出現而順利導入 AI 應用的企業有哪些？或是因此而帶動公司轉型？

在這一次的 AI 準備度調查中，可以發現，企業雖具有資料搜集與應用能力，但在技術、企業文化、工具資源上仍有許多成長空間，尤其不少專家都指出，組織與文化是 AI 導入的關鍵。例如組織文化能否接受 AI 技術導入時，可能出現的失敗或錯誤，並及時調整，靈活進行組織調整，隨時因應新的分工等與組織創新能力相關的衡量。

創新與 AI 時代的來臨

創新，是大多數人都十分熟悉的字眼，更是很多企業進入 AI 時代積極追求的目標：惟有創新，才能突破既有的框架與限制，才能夠創造新的價值，並持續發展出企業的成長動力。

但究竟什麼是創新？財團法人人工智慧科技基金會執行長溫怡玲表示，只要翻開企業管理或營運策略相關書籍都可以看到，創新有幾種不同的類型與路徑，例如：

1. 漸進式創新 (Incremental Innovation)：指的是針對現有產品、服務或流程進行局部或小幅度的改進。日本與台灣都擅長的持續打磨、優化製造細節，或者不斷降低成本，增加效率、優化流程或創造更大的客戶價值，

都屬於這類。

2. 破壞式創新 (Disruptive Innovation)：這種創新通常由資源較少或初入市場的小公司發動，他們提供價格便宜、性能或許較少或較簡單的產品或服務，來吸引原本市場龍頭不在意的客群，挑戰並改變現有市場的規則，甚至逐步取代市場上的主導公司。

3. 根本性創新 (Radical Innovation)：相較前項，這種創新的影響力更大，可能會創建新產業或徹底改造現有產業。例如蘋果推出 iPhone，不僅顛覆舊有手機的商業模式與生態，甚至改寫許多人的生活型態。又如這兩年的生成式 AI，預期將對不同產業生態系帶來衝擊，當然，這仍是現在進行式。

溫怡玲分析，不同創新類型的差異，主要在於對現有市場和技術的影響程度。漸進式創新通常是小步驟的改進，而破壞式和根本性創新，則可能帶動產業與消費市場的重大變化，當然，影響範圍大小與時間長短不同。

「創新絕對不只是產品的問題，」她舉例，美國創新大師賴瑞·基利 (Larry Keeley) 多年研究製造業和服務業的創新，發現 95% 的創新以失敗收場。所以他深入研究成功企業的創新方法，希望以系統化的方式將創新轉變為可驗證、有方法論的科學，並出版《創新的 10 個原點》一書。

賴瑞·基利根據多年觀察企業成敗的經驗，整理出十種創新類型及其相對應的關鍵作法，分別為獲利模式、網絡、結構、流程、產品性能、產品系統、服務、

通路、品牌以及顧客參與等不同的創新環節。可以脫穎而出的創新，通常能夠產生出，難以在短期內被競爭對手模仿的優勢，並創造新的成長曲線。

值得注意的是，雖然每一種創新類型都可以發展出新的創新策略，也可以選擇幾項加以組合，但如何選擇、組合，必須依照企業本身的目標、資源和既有的條件。所以最關鍵的不是新產品或新技術，而是企業的發展目標與營運策略是否足夠明確，並且整個組織能夠提供足夠的支持讓創新產品與服務發展完整。

「這樣的原則跟企業推動 AI 化是一樣的，」溫怡玲點出，新技術、新產品或新服務當然很容易令人興奮，但其實單點的創新是不夠的，必須考慮更大的整合流程，不只是跨部門、跨領域的整合，更重要的是必須思考如何從根本的組織架構與流程、人才培育、到新產品或服務研發、行銷等關鍵環節，全部囊括在內，才會為企業創造出最適合的價值。

當然，要理解和運用企業不同類型的創新，需要更多更深入的觀察與研究，但也需要有個起點。溫怡玲指出，這次與 Google Cloud 合作的調查中，就以「AI 經營策略」與「組織調整彈性」開始，理解企業如何準備 AI 技術的導入。前者指的是企業理解 AI 的重要性並有明確策略，後者則是已具備接受 AI 技術的文化，且能靈活進行組織調整以因應新的分工。

在創新力的兩項指標中，「AI 經營策略」一題的分數高達 74.55 分，53.5%

企業已有 AI 策略藍圖，更重要的是，有近九成企業認同 AI 是帶動變革的必然驅動力。由此也可以看出，大部份企業已將 AI 視為重要的經營策略一環，並根據這樣的策略藍圖分配資源。

然而，在後續相對應的「組織調整彈性」上，卻只有 45.05 分，約四成（44.5%）仍處於尚未應用或僅初步探索研究 AI 的階段。整體而言，這意味著多數企業或組織雖然高度認同人工智慧的重要性；但並未隨著 AI 的導入應用調整組織架構與流程。「這的確是很多企業目前的困擾，因為沒有經驗，也不敢嘗試，」溫怡玲說，這是很多企業 AI 應用落地程度偏低的主要原因。

在這波新科技帶動新商業模式的巨浪中，「由上而下推動是必要的，」溫怡玲說 AI 導入的影響非常深遠。表面上看起來，要成功首先需要有足夠的資料、AI 相關人才，並且找到有價值的題目。但實際上，光是要做到這些，企業不僅要有創新思維，還要有實施創新的策略和流程，「董事會跟高階經營者必須扮演關鍵角色，」包括鼓勵創意、給予真正的支持、接受風險、促進跨部門合作等，都屬於企業治理範疇。當然，也牽涉到企業的核心競爭能力與成長可能性。

「人工智慧是改變我們所做一切事情的執行環境」。人工智慧不僅提供新的做事方法，也正在改變經營公司的概念，包括如何營運及如何競爭，都將展現出截然不同於以往的面貌。而創新除了新工具或新技術的開發與使用外，也考驗企業是否能夠因應組織、管理、文化的快速變動，並且能進一步驅動企業創

造出具有差異化優勢的競爭門檻。

2019 年 6 月出版的《人工智慧在台灣》，是第一本從台灣產業觀點出發的產業 AI 化的專書。作為共同作者，溫怡玲表示當時因為預見 AI 將帶來一波翻天覆地的變化，於是選擇以「紅皇后的領地」做為全書主軸。如今看來，台灣產業的確已經走入其中，「如果你想前進，至少要跑得比現在快兩倍！」

面臨複雜難題，或需要進一步的 AI 轉型或策略顧問服務，
歡迎透過以下連結與我們聯絡。

AIF

Google Cloud

需要更多啟動 AI 專案詳細資訊，或是資源運用，歡迎與
[Google Cloud 銷售專員](#)聯絡，或是[按此](#)取得支援。

