Deloitte.

勤業眾信

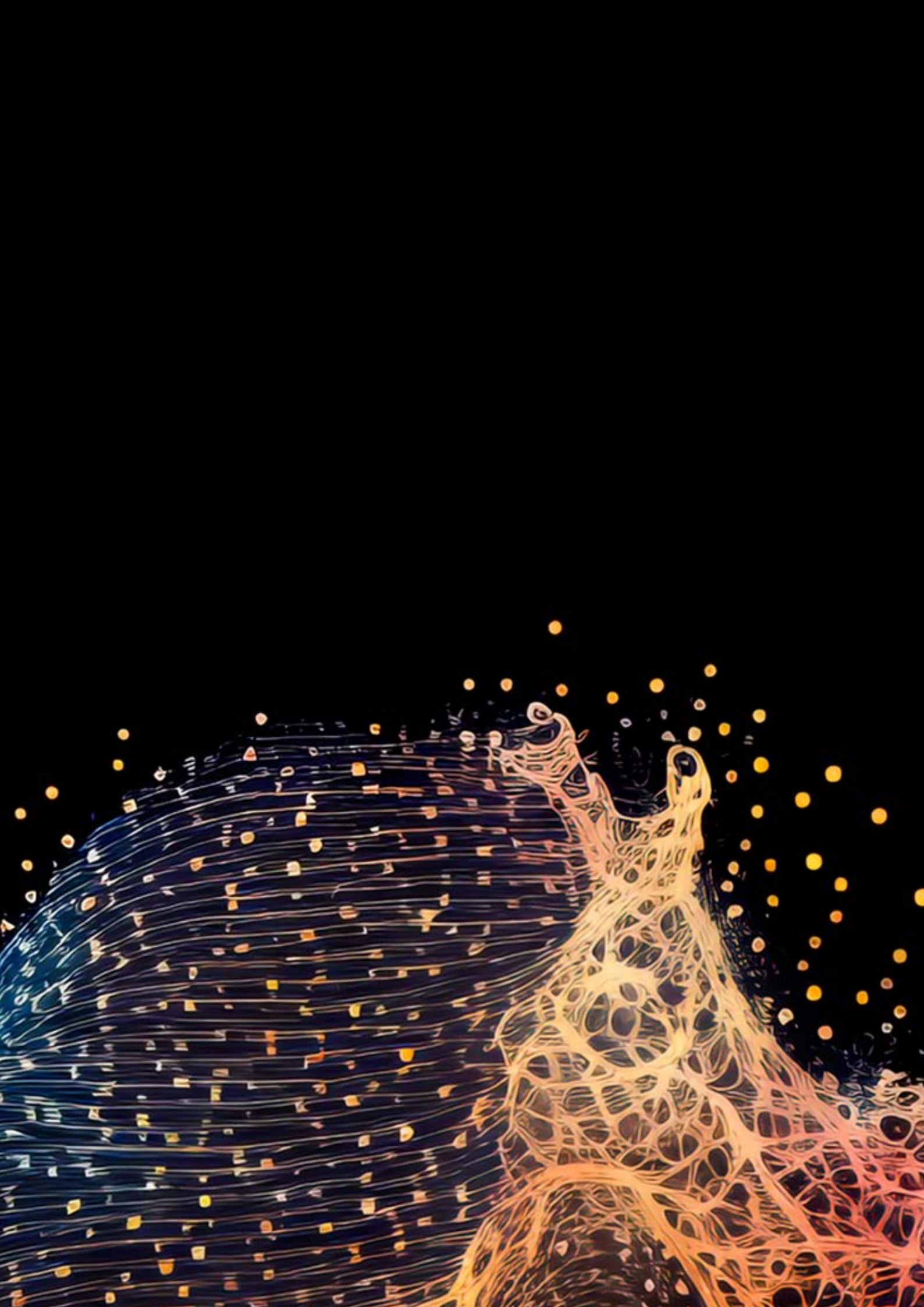
Deloitte
Access Economics

人工智慧 (AI) 的關鍵轉捩點

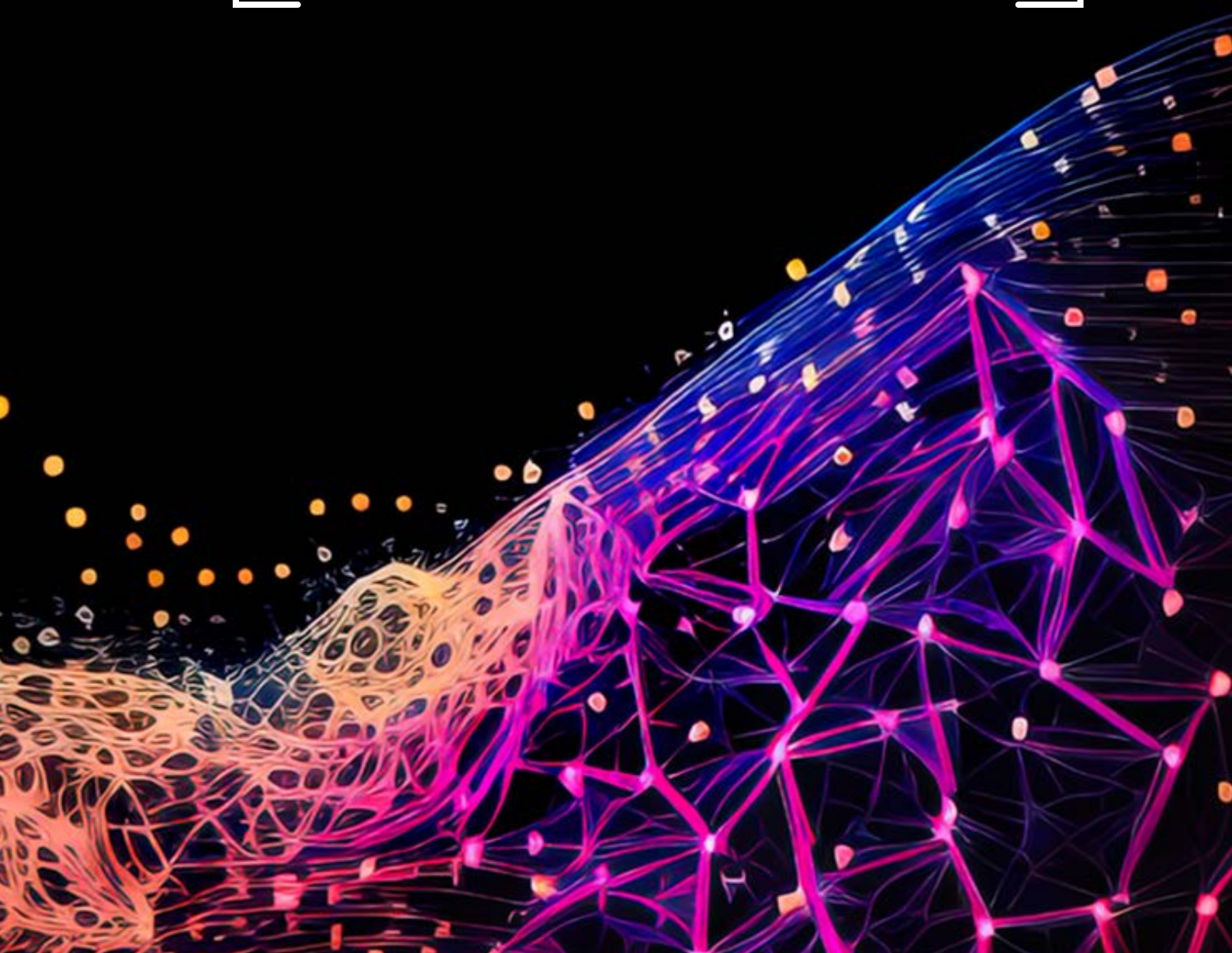
以信任作為企業擴展基礎

Deloitte亞太區 | AI研究院

MAKING AN IMPACT THAT MATTERS since 1845



目錄



概述

本報告由Deloitte Access Economics研究機構與Deloitte AI研究院(Deloitte AI Institute)共同撰寫,旨在為亞太地區的企業高階主管與資訊科技主管提供觀點,以協助其建立人工智慧治理框架與組織架構,進而發展出更值得信賴的人工智慧(AI)解決方案。

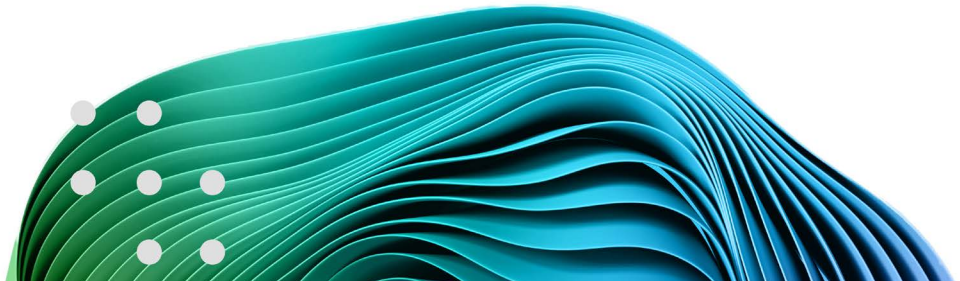
Deloitte建立了一套「可信任AI框架」,提出組織建立可信任AI解決方案時須具備七大面向,包括:透明和可解釋性、公平與公正、健全與可靠、隱私性、安全和防護、負責任和當責性。

然而,組織需要具備哪些條件才能實現可信任AI?答案便是良好的AI治理。

對於企業高階主管與董事會成員而言,在眾多優先事項中推動並支持有效的AI治理措施可能充滿挑戰。為協助企業解決此需求,本報告透過「AI治理成熟度指標」以定義良好的AI治理在管理實務的全貌。這是一套由Deloitte開發並用來評估組織AI治理成熟度的指標,本次運用該指標調查近900位來自澳洲、中國大陸、印度、印尼、日本、馬來西亞、紐西蘭、菲律賓、新加坡、南韓、台灣、泰國與越南等國家的高階主管。調查涵蓋多個產業、不同規模的組織以及公部門機構。

本次調查旨在了解各組織AI治理的成熟程度,並識別推動有效AI治理的關鍵因素,同時評估AI治理為組織帶來的效益。

1. 透明和可解釋性
2. 公平與公正
3. 健全與可靠
4. 隱私性
5. 安全和防護
6. 負責任
7. 當責性



AI的關鍵轉捩點：
信任作為企業擴展基礎

當高階主管將AI解決方案從測試階段轉向實際部署時，組織往往會面臨安全漏洞、隱私與法律等多項關鍵風險議題。儘管AI解決方案可為企業提供較佳的生產力，但若未能妥善管理這類工具的風險，恐將導致資料外洩、聲譽受損、營運中斷，甚至發生違反法令導致裁罰之情形。

令人擔憂的是，有超過一半的科技工作者並不認為自身具備能有效應對AI風險的能力。為探討有效的AI治理如何協助解決風險並釋放更多的AI潛力，Deloitte針對亞太地區13個地點、近900位高階主管進行調查，是迄今針對AI治理成熟度最全面的評估之一。

各行各業因使用AI而引發的事件數量正在不斷攀升

超過25%的組織在上一財務年度曾經歷的AI相關事件數量增加

上一財政年度AI事件數量增加之情形（按產業分類）

良好的治理能促進更廣泛的AI應用並帶來更高的經濟收益

企業內使用AI解決方案的員工數量**增加28%**

在研發、營運與生產以及顧客服務、行銷與銷售等領域使用AI解決方案的可能性**提高3倍**

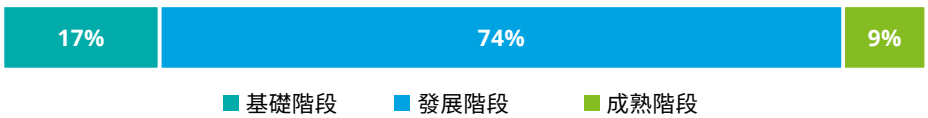
AI解決方案帶來的**營收成長率**增加4.6個百分點

45%的高階主管認為良好的治理能**提升企業形象**

然而，超過90%的組織仍有改善AI治理的空間

Deloitte的AI治理成熟度評估使用12項指標來評估組織的AI治理狀況。

亞太地區AI可信任指標的分佈情況



建立可信任AI的行動措施

1. 優先考量AI治理以實現AI能帶來的效益
2. 了解並善用更廣泛的AI供應鏈
3. 培養風險管理者，而非風險迴避者
4. 溝通並確保AI轉型準備就緒

01
掌控快速採用AI所帶來的風險

在亞太地區，AI的應用正持續改變著商業環境。生成式AI（Generative AI, GenAI）的迅速崛起更進一步加速了此過程，亞太地區對AI的投資金額預計至2030年將比2022年成長近五倍，達到1,170億美元。[1]生成式AI已迅速成為此地區成長最快的科技。

快速採用的背後推手則是員工，其往往比領導者更先開始使用。根據Deloitte先前關於「AI世代」的研究，超過40%的員工已在工作中使用生成式AI，年輕員工更是其中的先驅。[2]

如此快速且大規模採用AI，意味著領導者在測試和推廣這項科技時，正面臨著與AI相關的風險。

根據本報告針對近900位高階主管的調查，顯示在AI相關的風險中，安全漏洞（86%）、監控（83%）及隱私（83%）是高階主管最關注的幾項重點（圖1）。自生成式AI出現以來，上述風險日趨顯著。生成式AI能力的躍升以及更為友善的使用者介面，讓更多人能夠運用這些強大的工具，同時進一步放大了相關風險。

> 「根據Deloitte的研究，超過半數的科技從業者認為其工作場所缺乏識別或應對AI相關風險的適當機制。」[3]

AI解決方案或其使用的大量資料可能導致安全漏洞，並可能成為資料竊取或外洩的目標，進而造成巨額的損失。2024年，全球資料外洩事件的平均成本已接近500萬美元，相較前一年增加了10%。[4]對大型組織而言，此成本可能更為高昂。

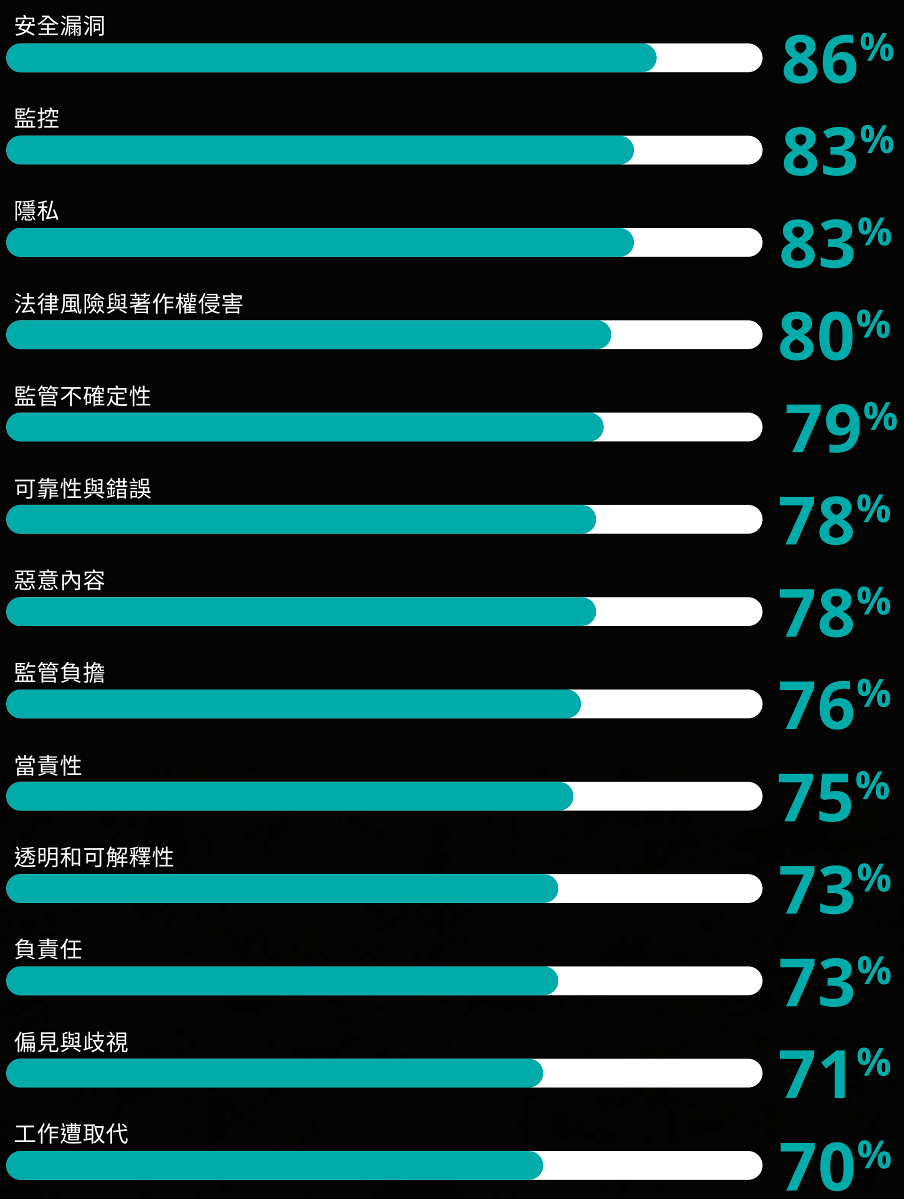
此外，亦存在更多難以量化的成本，例如對品牌的傷害與顧客流失等。而消費者信心的流失以及對品牌聲譽的負面衝擊將帶來長遠的影響，因此，企業如何有效管理AI與網路安全變得相當重要。同時，消費者對於使用AI時遵守道德倫理規範（如保持高度透明）的企業表現出強烈偏好。根據Capgemini Research Institute的研究顯示，62%的消費者更信任其AI互動符合道德倫理規範的公司，並有53%的消費者更願意購買此類產品和服務。[5]

組織也必須確保自身在運用AI方面符合不斷變化的法律與監管要求，這也是高階主管所列最常見的風險之一。儘管亞太地區各國政府專注於制定與實施相關法規與立法，但現有的監管要求通常僅規定組織需要達到的最低標準，而非全面的最佳實踐。因此，高階主管必須針對自身組織制定、採用並執行AI解決方案與系統的信任標準。[6]

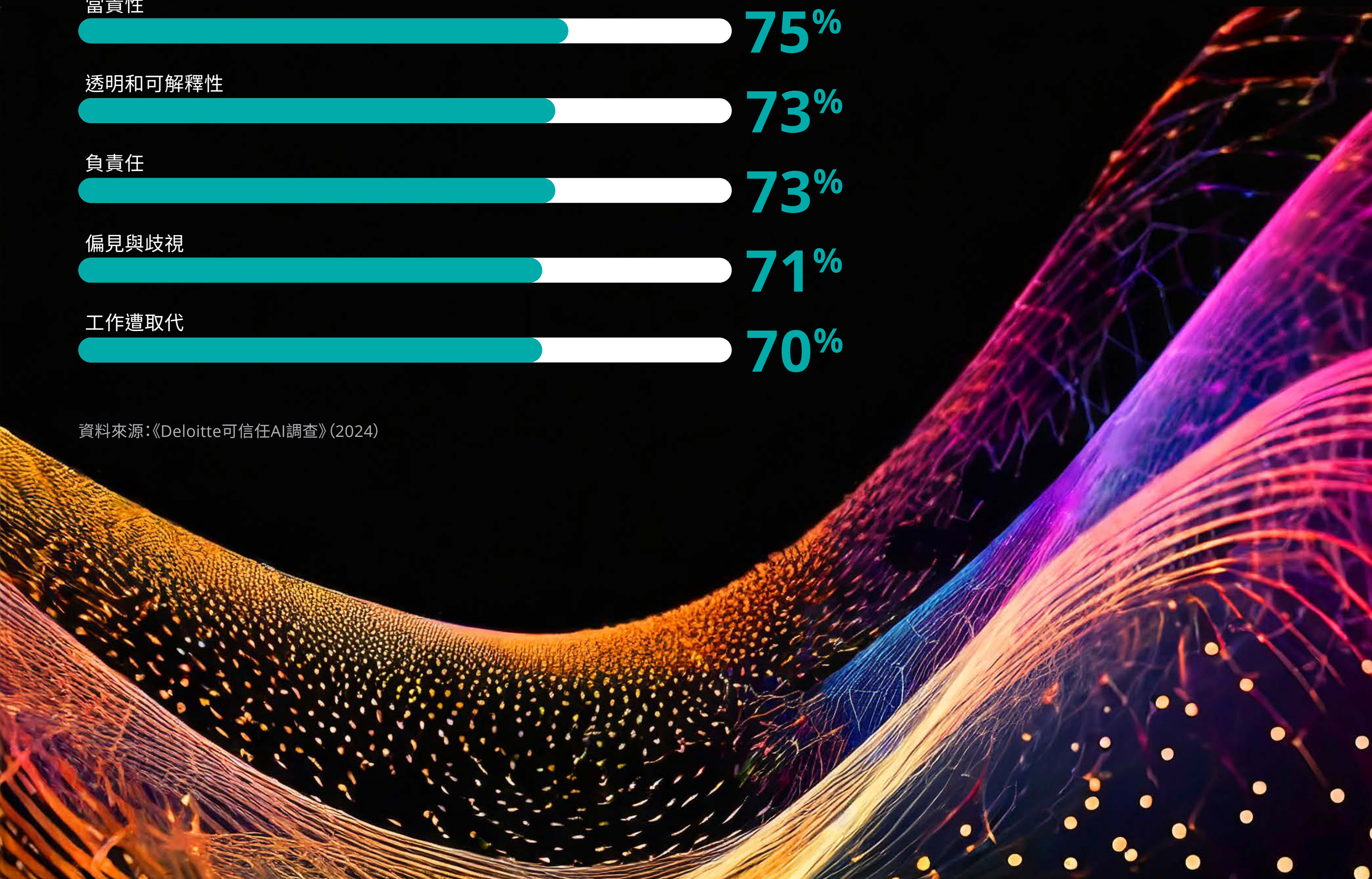
應對AI相關風險相當重要：若未能妥善管理風險，可能會導致顧客關係緊張、遭受監管機構處罰或引發民眾負面觀感。此外，對於相關風險的擔憂也可能阻礙組織使用AI。根據Deloitte AI研究院2024年第三季《智慧紀元，洞察未來：生成式AI前瞻解析》報告中指出，開發與使用AI工具面臨的四大挑戰中，其中三項便是風險、監管及治理問題[7]，突顯在管理AI所帶來的道德倫理與營運風險，以及充分發揮其科技潛力方面，有效治理皆有其重要性。

圖1

使用AI時主要考量的潛在風險



資料來源:《Deloitte可信任AI調查》(2024)

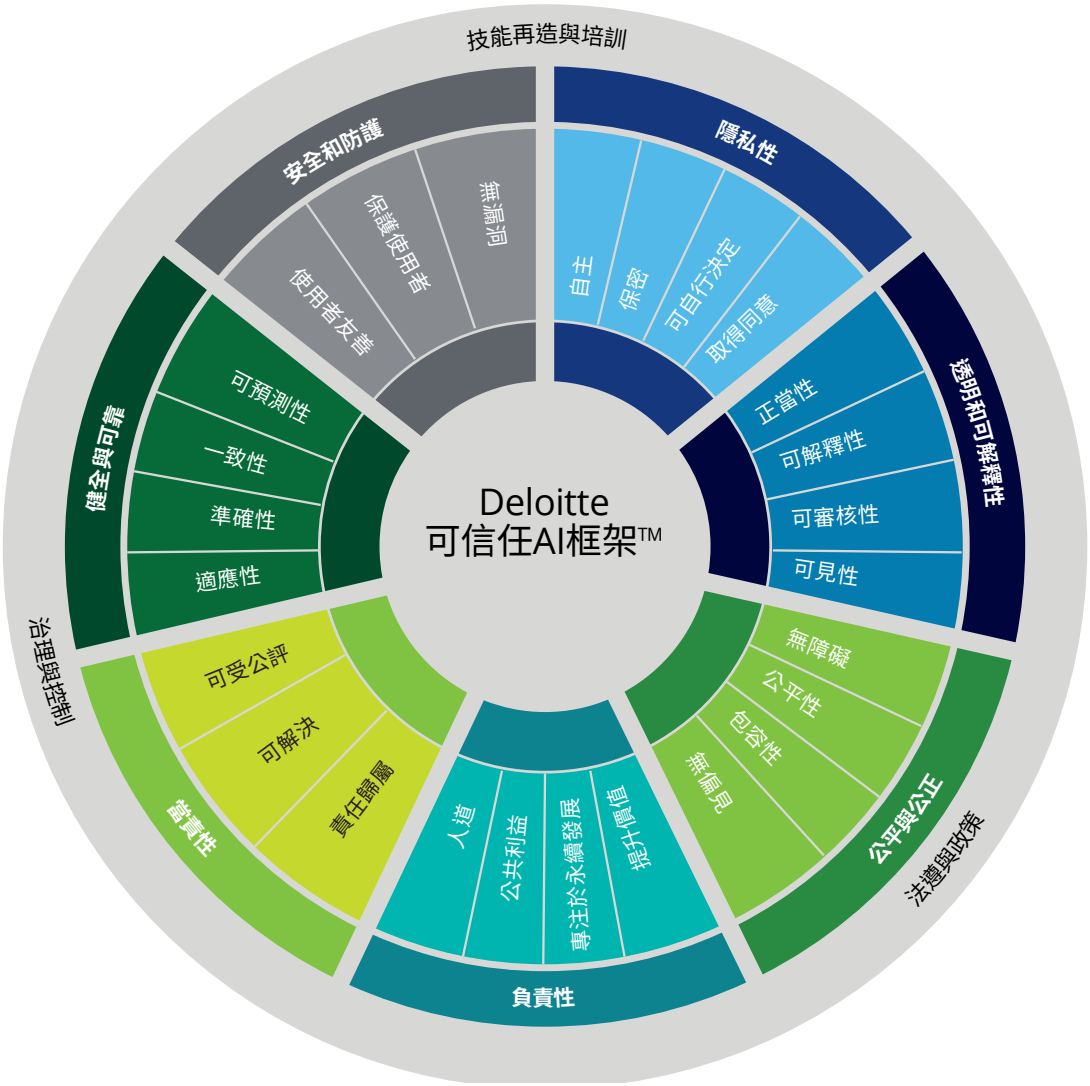


02
良好AI治理的樣貌為何？

開發可信任AI解決方案對高階主管而言至關重要，這不僅有助於成功應對快速採用AI的風險，也能全面接納並整合此革命性科技。可信任AI為科技的道德倫理、合法性與技術穩健性提供一定程度的保障，並增強高階主管對於在整個組織內部使用AI解決方案的信心。

Deloitte所開發之「可信任AI框架」，概述了為AI解決方案建立信任所需的七個關鍵面向：(1) 透明和可解釋性、(2) 公平與公正、(3) 健全與可靠、(4) 隱私姓、(5) 安全和防護、(6) 負責任與 (7) 當責性 (圖2)。此框架及其標準涵蓋AI解決方案的所有過程，包含構思到設計、開發、採購與部署。

圖2：Deloitte可信任AI框架



資料來源：Deloitte (2024)

AI解決方案要符合可信任AI框架的七個關鍵面向並非輕而易舉。組織必須具備健全的AI治理架構，藉此為AI解決方案提供結構化框架，以確保其符合原則。

良好的AI治理本質上需要涵蓋AI生命週期所有階段，並融入科技、流程及員工培訓。治理規劃需根據AI解決方案的成熟度、所在地區及產業特定的監管要求，以及組織內部政策與標準進行調適。

AI治理常因目標不斷變動而顯得難以掌握。為協助組織採取實際步驟實現可信任AI，本報告特別設計了AI治理成熟度指標，作為評估依據。

此指標基於五大核心要素：「組織結構」、「政策與原則」、「程序與控制」、「人員與技能」以及「監測、報告與評估」，並於其下劃分出12項關鍵指標，以評估組織的AI治理成熟度（表1）。根據上述指標，進一步將組織的AI治理成熟度分類為「基礎階段」、「發展階段」或「成熟階段」。有關此指標及相關評估項目的詳細資訊，請參見附錄B。

表1：Deloitte AI治理成熟度指標

五大核心要素	基礎階段	發展階段	成熟階段
組織結構	未明確配置AI治理的角色與職責。	已配置部分個人與群體在AI治理中的角色與職責。	已明定董事會的問責機制，並指派管理階層之角色與職責，以支援全組織的AI治理。
政策與原則	未針對AI治理制定政策或指導原則。	已制定基本政策或草案，包含指導AI治理的通用原則。	依據AI發展策略，已明確定義治理執行原則，為組織量身打造符合AI治理的健全政策。
程序與控制	未針對AI系統的開發、部署或使用制定風險管理程序或控制措施。	針對AI系統的開發、部署或使用之風險管理程序和／或控制措施正在開發中。	現有的風險管理程序和／或控制措施足以指引AI系統的開發、部署或使用。
人員與技能	未提供資源或培訓讓員工負責任地使用AI。	正在為員工尋求所需資源，以使其負責任地使用AI。	已為員工提供資源，包括使用指引與培訓，以使其負責任地使用AI。
監測、報告與評估	未制定監測或報告AI系統運行狀況的機制。	正在開發監測或報告AI系統運行狀況的機制與工具。	已建立用於監測或報告AI系統運行狀況的機制與工具。

資料來源：Deloitte (2024)

下圖顯示DeloitteAI治理成熟度指標中的每項核心要素，如何作為協助組織實現可信任AI的基礎。此外，此指標也指出組織應採取的實際規劃與行動，以實現可信任AI框架中強調的七個關鍵面向。

圖3：Deloitte AI治理成熟度指標

資料來源：Deloitte (2024)

AI治理並無放諸四海皆準的方法。根據產業、監管環境、AI願景及所採用的AI解決方案類型，其所需的具體治理架構皆有所不同。例如，用於提供員工諮詢內部人資政策的AI聊天機器人，與直接面對顧客的銀行AI信用申請解決方案兩者之間，其控制流程即存有顯著差異。比較AI治理的共通特性，則可協助組織找出其治理標準中需要改善的領域。

值得注意的是，AI治理成熟度較高並不意味著必然可實現可信任AI。若已制定治理程序，但未能有效執行、員工無法充分理解，或未配合業務背景與策略，則仍可能無法達成可信任AI的目標。有效AI治理在每個組織裡的樣貌都是獨一無二的；因此，組織應持續評估並精進自身的AI治理框架，確保其規模適合自身的獨特需求以及不斷變化的監管要求。

賦能未來：
Energy Queensland對負責任AI與永續創新的承諾

Energy Queensland是澳洲最大的國營電力公司，服務超過230萬名客戶，並在其配電、零售與綜合能源解決方案業務中僱用了逾9,300名員工。

Energy Queensland資訊長Sharyn Scriven表示：「AI科技改變了遊戲規則，隨著其逐漸成熟，這項科技將幫助我們的業務和員工實現公司的願景與2032年企業策略。」

Energy Queensland客戶與新興平台總經理Josh Gow指出，整合AI科技是Energy Queensland推動卓越經營並提升客戶體驗的重點之一，亦是該組織宏觀策略之發展支柱。Energy Queensland已使用AI多年，其應用範疇已從特定的專業用途，轉變為更廣泛的應用案例評估與部署。

制定AI政策對於Energy Queensland而言相當重要，可在引入新AI解決方案之前，確保已建立適當的政策和設置。包括制定AI政策和在整個組織中推出應用案例的策略，同時採取必要行動以建置適當的防護措施。為確保AI政策符合業界最佳實踐並能正確實施，Energy Queensland除了進行內部審查，也委託外部機構對該政策進行獨立審查。Josh解釋道：

「AI環境變化快速，產業標準與指引也不斷成熟，因此我們的AI政策是動態的文件，不斷進行審查並滾動調整。我們的AI指導委員會也包括了高階主管，並且每個月都會召開會議，定期討論AI的進展、風險與機會。」

在全面實施之前必須先測試與試行AI應用案例，這是Energy Queensland AI策略的重要特點。根據Josh的說法，在企業內部試行AI應用案例是策略性的選擇，目的是在創造「以測試和學習為重點的環境，以逐步評估風險與機會」。此過程包括試行企業工具並構建AI平台服務，初期目標是為需處理大量文件、會議及電子郵件的企業使用者提供支援。

有效且負責任地使用AI，需要擁有適當能力的團隊成員與強大的AI解決方案相互輔助。為此，Energy Queensland進行並審查「限制範圍的試點部署」計畫，讓不同職位的員工在有限範圍內參與測試及評估、教育和培訓計畫，作為進一步部署前準備。

「重要的是確保我們能把握進一步採用AI所帶來的價值與機會，並持續管理其風險。AI在更多技術領域中被廣泛應用已是大勢所趨，這已成為必定會發生的事情，只是時間早晚的差異。然而，並非每個人接觸到的AI系統都是相同類型或相同功能，有些AI可能隱藏在背後運作，對使用者而言不見得可察覺到它的存在。因此我們需要依據組織需求量身打造AI解決方案，確保其以有效、負責任且具價值的方式幫助公司。」

打造可信任AI的關鍵要素

- 人工智慧政策
- 人工智慧指導委員會
- 組織內部試點並試行人工智慧計畫
- 人員培訓規劃

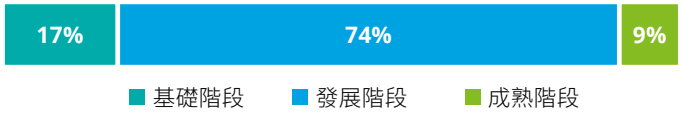
03
亞太地區的AI治理

在亞太地區中，僅有不到一成的組織具備實現可信任AI所需的治理架構。根據AI治理成熟度指標的分類，91%的組織目前具有「基礎階段」或「發展階段」的AI治理架構，顯示AI治理尚有顯著的改善空間（圖表1）。

而檢視AI治理成熟度指標的五大核心要素，亞太地區的組織在「政策與原則」以及「程序與控制」兩方面有較大的改善空間。目前，分別有31%與23%的組織在此兩核心要素中落在「基礎階段」中。在「組織結構」以及「監測與評估」核心要素的表現則相對較佳，有超過90%的組織達到至少「發展階段」的水準。

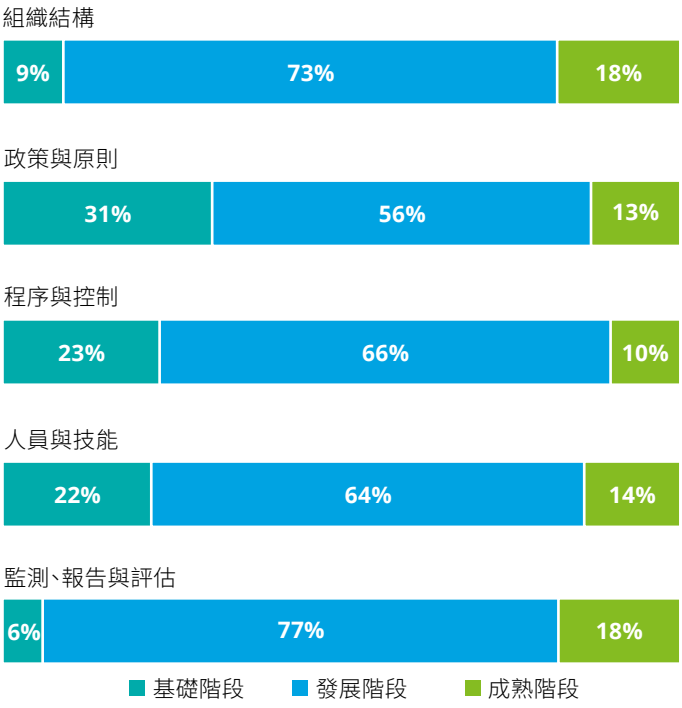
總體而言，要實現AI治理成熟度指標的「成熟階段」狀態，需要在所有五個核心要素上都表現出色。雖然有將近五分之一的組織在其中一個核心要素中達到了「成熟階段」狀態，但只有一半的組織在整體AI治理方面實現了「成熟階段」。這凸顯了組織需要從整體角度考慮AI治理的重要性，以發展出可信任AI所需的條件。

圖表1：亞太地區AI可信任指標的分布情況



資料來源：《Deloitte可信任AI調查》（2024）

圖表2：可信任AI指標在各核心要素中的分布情況



資料來源：《Deloitte可信任AI調查》（2024）

過度自信所造成的偏誤

領導者可能會高估AI治理的成熟度。根據Deloitte AI研究院2024年第三季《智慧紀元，洞察未來：生成式AI前瞻解析》報告顯示，23%的組織領導者認為其風險管理程序與治理已高度準備就緒。然而，本次更為詳細的研究深入探討了AI治理的基礎結構，發現實際上僅有9%的組織達到「成熟階段」的治理水準。[8]儘管兩項研究的問題設計與樣本有所不同，但研究結果的顯著差異表示，高階主管需要深入了解其AI治理的實際成熟度。此點尤為重要，因為過度自信可能成為改善AI治理的阻礙。如果領導者認為已具備足夠的機制來管理AI風險，就不太可能主動探索進一步改善的方法。

核心要素1

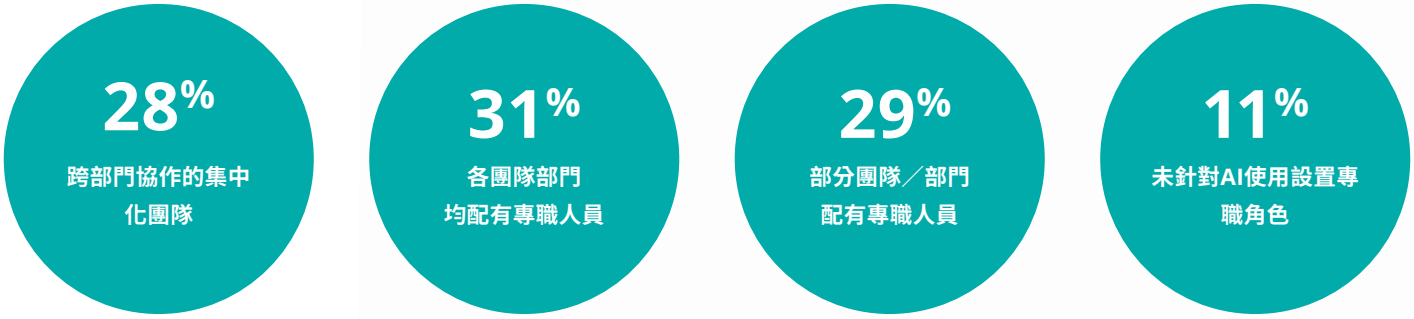
組織結構

在組織內明確界定負責管理AI標準的角色，有助於妥善處理AI相關的新問題。根據調查，多數組織將此責任歸於高階管理團隊，其中91%的組織明確指定了一位董事會成員或高階主管負責此項工作。另有7%的組織指定非高階的AI負責人管理風險與標準，而不到2%的受訪者則表示無法在其組織內找出負責此工作的主要角色。

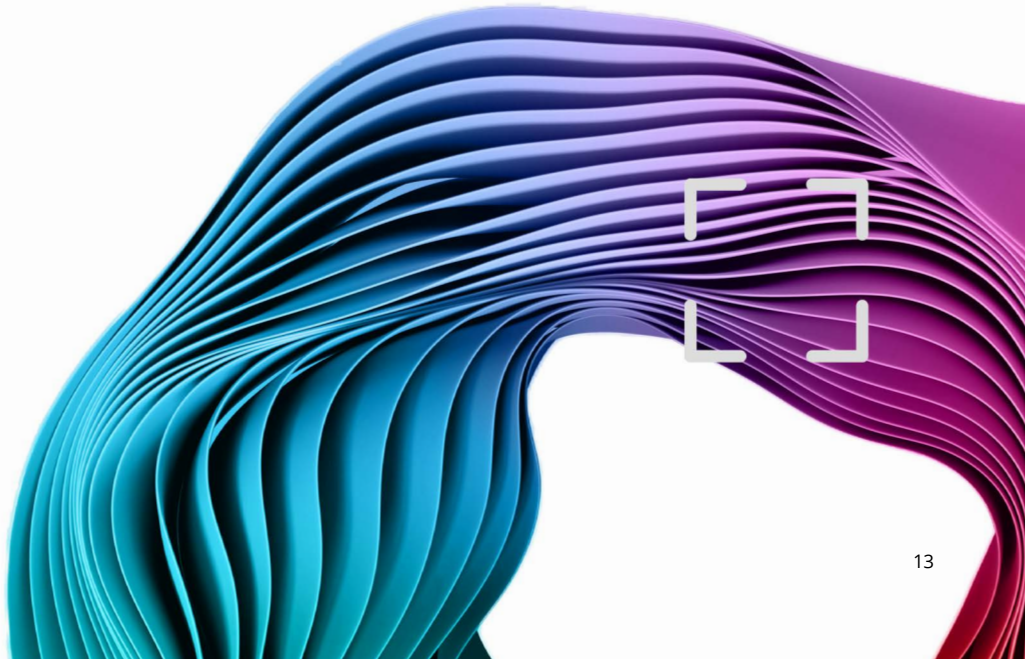
組織在建構負責AI相關道德倫理、法律及監管法遵的團隊上可能有所不同。僅有28%的組織設有集中化的道德倫理與風險團隊，負責監測趨勢並偵測AI使用相關風險，而61%的組織則在全部或部分部門或團隊中設有專職人員（圖表3）。其餘組織則僅在部分團隊中設有專職人員，或完全沒有針對AI使用設置專職角色。

相較於團隊架構，更重要的是對AI標準設有明確的責任與問責機制。然而，這在較小型的組織中相對罕見；在擁有超過1,000名員工的組織中，則只有3%未設有專職的AI風險管理角色；而在少於100名員工的組織中，此比例則高達23%。

圖表3：負責AI相關道德倫理、法律及監管法遵的團隊架構



資料來源：《Deloitte可信任AI調查》(2024)



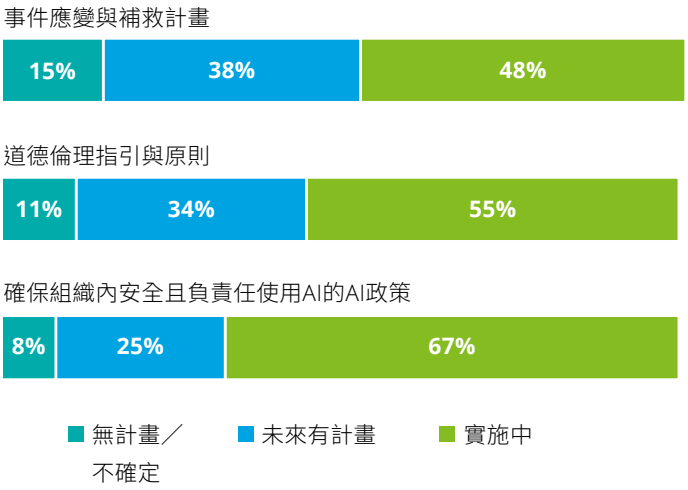
核心要素2

政策與原則

清晰且多數人皆可理解的政策與原則，是實現有效AI治理的基本前提。AI政策與AI策略並不相同，後者涵蓋更廣泛的元素，例如與AI相關的願景以及衡量進展的關鍵指標。儘管亞太地區大多數組織已制定AI策略，許多組織的AI政策中仍缺乏良好治理的關鍵要素。超過半數的AI政策缺乏實現AI治理目標的時間表，或未包含與AI相關的道德倫理指引與原則。

在AI政策中納入治理要素，對於讓員工理解其價值相當重要。在已制定整體AI策略的組織中，30%表示並非所有員工都能認同該策略的價值。然而，當AI政策中包含明確的監測或審核事項（風險胃納、應變計畫以及與組織整體政策整合的補救計畫等）時，員工更有可能認同該策略的價值。

圖表4：可信任AI政策的實施



資料來源：《Deloitte可信任AI調查》(2024)

核心要素3

程序與控制

第三個核心要素主要探討組織中管理AI相關風險與標準的日常實踐，包括識別和管理AI相關風險的評估程序、對使用中的AI解決方案進行全面盤點，以及減緩使用AI解決方案所造成的風險之控制框架。在此核心要素中，已歸類為「成熟階段」的組織數量最少，因此在本核心要素的推動將成為提升整體性可信任AI的關鍵。

有效AI治理的關鍵要素之一，是為員工提供當遭遇使用AI所遇到之相關問題或事件的通報系統，然而，40%的組織尚缺乏此類通報機制。具備通報機制的組織收到的問題數量是其他組織的五倍，通報的事件數量也高出兩倍，表示缺乏此類通報機制的組織可能無法察覺與AI相關的新興風險。有鑑於與AI相關的問題和事件數量正節節攀升，使得此問題在亞太地區尤為迫切（圖表5）

圖表5：2024度與2023年相比，AI相關事件數量的變化

資料來源：《Deloitte可信任AI調查》(2024) 註：不包括「不確定」的回答 (6%)

核心要素4

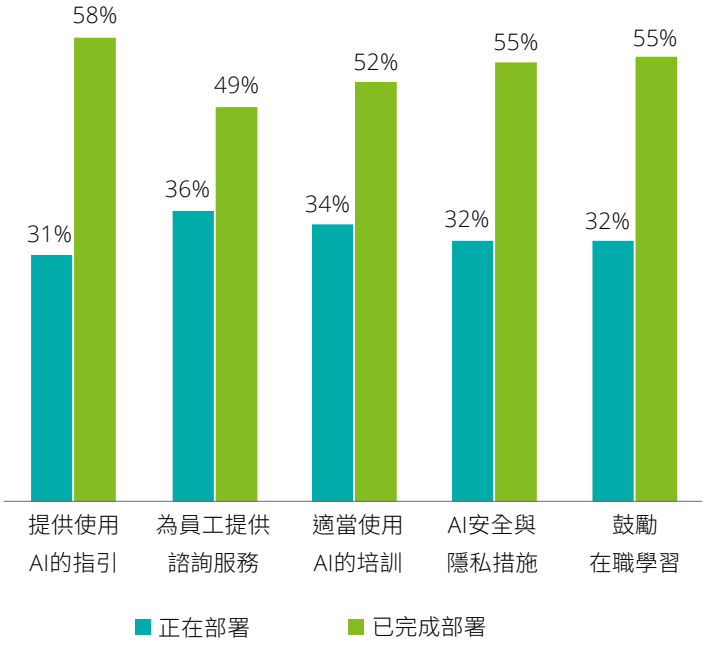
人員與技能

員工在實施可信任AI機制扮演著關鍵角色，這對許多組織來說仍是挑戰，目前平均僅有56%的員工具備負責任使用AI的技能與能力。

培訓是彌補此差距的有效工具。提供給員工AI培訓計畫的組織，其具備安全使用AI能力的員工比例較未提供培訓的組織高出27%，然而，目前僅有52%的受訪組織提供此類培訓計畫。而在尚未提供培訓的組織中，有72%正積極為其團隊開發相關計畫。

大多數組織確實提供負責任使用AI的指導方針，其中55%鼓勵員工透過在職學習與實際探索或應用AI來掌握技能，49%的組織則設有為員工提供諮詢服務的部門或機構。私人企業在提供AI使用指導方針與培訓方面處於領先地位，而公部門組織則更傾向於專注於安全措施，並鼓勵在職學習。

圖表6：為支持員工使用AI而提供的資源



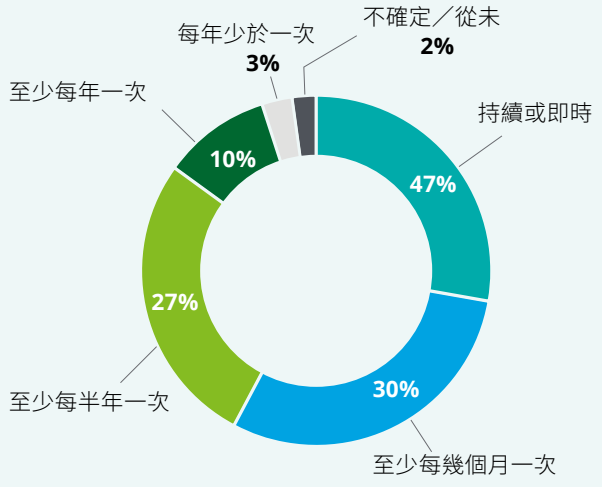
資料來源：《Deloitte可信任AI調查》(2024)

核心要素5

監測、報告與評估

擁有能夠應對變化需求和新興問題的AI治理系統，對於確保組織能及時應對風險與事件相當重要。整體而言，組織在此核心要素中的表現相對良好，有18%的組織達到「成熟階段」，為最高比例之一。85%的組織至少每六個月根據內部標準評估其AI治理（包括每六個月、每三個月或即時進行評估）。監測並評估AI治理是否符合監管要求的變更，是此核心要素的另一項重要內容。近75%的組織至少每六個月審視法律與監管要求是否有所變動。

圖表7：AI系統根據內部組織標準進行評估的頻率



資料來源：《Deloitte可信任AI調查》(2024)

可信任AI在各產業中的表現如何？

AI治理成熟度指標及各核心要素評估結果因產業而異。依據本報告調查結果，高科技、金融服務與專業服務等產業在可信任AI上具備較高比例的「成熟階段」組織。而公部門、生技醫療產業的比例則相對較低。以下將針對四個關鍵產業提供相關摘要。亞太地區主要地點的相關摘要可參見附錄D。

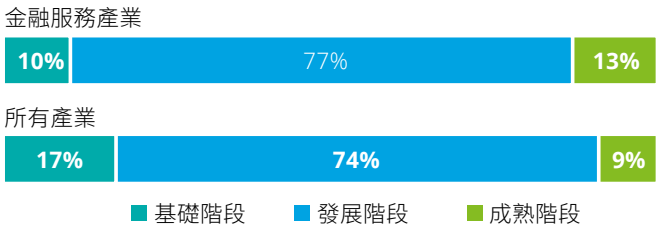
聚焦

金融服務產業

作為知識與資料密集型產業，金融服務產業一直是數位創新的領先採用者。由於此產業的受監管程度相對較高，且掌握敏感的金融資訊，因此金融服務產業組織的治理環境需要快速發展，以應對新的創新。

本研究的AI治理成熟度指標顯示，金融服務產業的成熟度高於其他產業。隨著金融服務的需求持續成長，尤其更年輕且具科技素養的消費者群體持續增加，良好的治理將會是此產業未來成長的重要基礎。在金融服務產業持續採用AI科技的過程中，遵守監管要求與保護客戶資料將成為關鍵議題。

AI治理成熟度指標



註：由於四捨五入，總和可能不等於100%。

有效的AI治理所帶來的前三大預期**效益**

- 提升對AI解決方案的產出或結果的信任度（57%）
- 由於信任度提高而更廣泛應用AI解決方案（47%）
- 更快速地在組織內部署AI解決方案（47%）

使用AI所帶來的前三大**風險**關注點

- 可靠性與錯誤（92%）
- 法律風險與著作權侵害（88%）
- 安全漏洞（87%）

使用或導入AI的前三大**阻礙**

- 對監管、法律、道德倫理、法遵及其他風險的擔憂（45%）
- 導入的技術挑戰（38%）
- 缺乏創新意願和／或探索不足（32%）

70% 的金融服務機構設有讓員工反映問題的通報機制

57% 的金融服務機構員工具備足夠技能以符合道德倫理和合規的方式使用AI解決方案

42% 的金融服務機構表示上一財務年度收到的AI事件數量有所增加

68% 的金融服務機構正在提升員工的能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：金融服務產業的樣本數量＝60

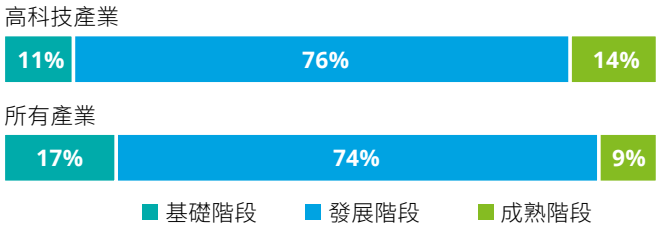
聚焦

高科技產業

高科技產業位於AI變革的最前線，同時也是其他產業開發AI解決方案的重要推手。作為AI解決方案的長期使用者，此產業的治理環境較其他產業更為完善，因此在AI治理成熟度的表現也更為出色。

根據Deloitte AI 研究院2024年第三季《智慧紀元，洞察未來：生成式AI前瞻解析》報，高科技產業的員工在將生成式AI融入工作流程方面處於領先地位，使此產業能夠快速應對新發展。然而，此產業在管理用於科技解決方案的數據時，面臨法律與保密風險的重大挑戰。由於高科技產業為其他產業提供技術支持，謹慎的治理將成為維護顧客信任的首要任務。

AI治理成熟度指標



註：由於四捨五入，總和可能不等於100%。

有效的AI治理所帶來的前三大預期**效益**

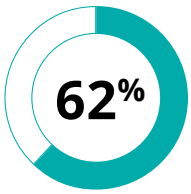
- 由於信任度提高而更廣泛應用AI解決方案（58%）
- 提升對AI解決方案的產出或結果的信任度（54%）
- 更快速地在組織內部署AI解決方案（53%）

使用AI所帶來的前三大**風險**關注點

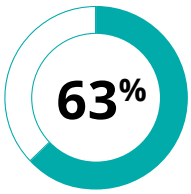
- 法律風險與著作權侵害：法律義務與責任（84%）
- 法律風險與著作權侵害：法律義務與責任（84%）
- 安全漏洞：駭客網路攻擊、未經授權的存取或濫用AI系統的風險（81%）

使用或導入AI的前三大**阻礙**

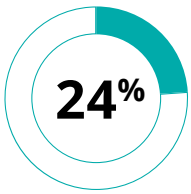
- 導入的技術挑戰（39%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（34%）
- 對技術及其潛力的理解不足（33%）



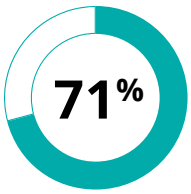
的高科技企業設有讓員工反映問題的通報機制



的高科技企業員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



的高科技企業表示上一財務年度收到的AI事件數量有所增加



的高科技企業正在提升員工的能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：高科技產業的樣本數量＝160

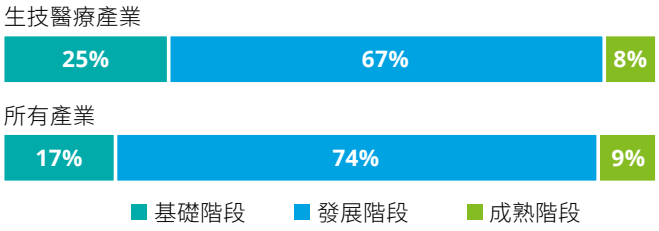
聚焦

生技醫療產業

生技醫療產業的AI解決方案通常需要使用如病歷及人口統計資訊等個人資料，且這些個人資料需要嚴格的隱私與安全標準。此類資料的特性使安全漏洞成為生技醫療產業關注的主要風險之一。患者在同意將其資料用於AI解決方案之前，需要確保資料被使用的安全性，因此，提升口碑、獲得社會大眾認可成為提升AI治理帶給生技醫療產業的主要效益之一。

生技醫療產業中處於「基礎階段」組織比例相對較高，此現象與生技醫療產業在接受數位轉型方面較為緩慢，且員工中存在一定程度的抗拒有關；此亦可能顯示，除非AI治理獲得改善，否則生技醫療產業可能無法充分利用AI解決方案。

AI治理成熟度指標



註：由於四捨五入，總和可能不等於100%。

有效的AI治理所帶來的前三大預期**效益**

- 提升口碑（44%）
- 在使用AI解決方案上獲得社會大眾認可（42%）
- 更高的法規遵循程度（42%）

使用AI所帶來的前三大**風險**關注點

- 安全漏洞：駭客／網路攻擊風險（86%）
- 監控：因全面性監控導致的隱私侵害（86%）
- 監管負擔：使用AI解決方案所要求的相關報告及流程（83%）

使用或導入AI的前三大**阻礙**

- 對技術及其潛力的理解不足（39%）
- 缺乏高層的承諾與決心（33%）
- 缺乏實施AI的策略與願景（33%）

55% 的生技醫療產業設有讓員工反映問題的通報機制

51% 的生技醫療產業員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案

31% 的生技醫療產業表示上一財務年度收到的AI事件數量有所增加

61% 的生技醫療產業正在提升員工的能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：生技醫療產業的樣本數量＝36

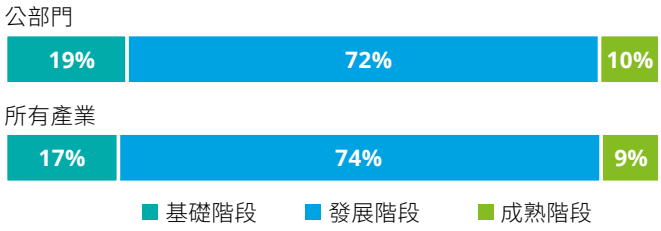
聚焦

公部門

亞太地區的公部門組織在AI的監管與道德倫理使用方面面臨主要挑戰。公部門保持靈活並迅速應對圍繞AI科技使用的問題，是在不斷變化的環境中保持領先的首要任務。

AI具有提升公部門向民眾提供數位服務效率的潛力，但在此過程中，必須確保資料安全以防範網路攻擊風險；為了達成此目的，也導致關注安全漏洞與監控的公部門組織比例相對較高。

AI治理成熟度指標



註：由於四捨五入，總和可能不等於100%。

有效的AI治理所帶來的前三大預期**效益**

- 提升對AI解決方案的產出或結果的信任度（56%）
- 由於信任度提高而更廣泛應用AI解決方案（54%）
- 更快速地在組織內部署AI解決方案（48%）

使用AI所帶來的前三大**風險**關注點

- 安全漏洞：駭客／網路攻擊風險（87%）
- 監控：因全面性監控導致的隱私侵害（83%）
- 惡意內容（82%）

使用或導入AI的前三大**阻礙**

- 導入的技術挑戰（39%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（34%）
- 對技術及其潛力的理解不足（33%）

65% 的公部門組織設有讓員工反映問題的通報機制

57% 的公部門組織員工具備足夠技能以符合道德倫理與合規方式使用AI解決方案

28% 的公部門組織表示上一財務年度收到的AI事件數量有所增加

69% 的公部門組織正在提升員工的能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：公部門的樣本數量＝172

公部門之定義來自於該部門內組織的所有權，其他產業則以其生產的特定商品或服務界定。公部門中的組織經營於多個產業，例如醫療與金融。

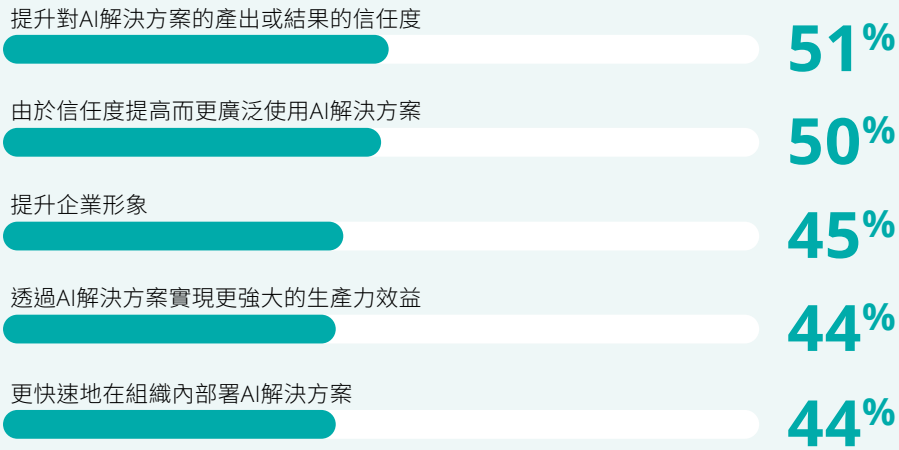
04

良好AI治理所帶來的效益

投入於提升AI治理成熟度的組織正獲得顯著的效益，同時高階主管已意識到，唯有建立對AI產出結果的信任，才能有效發揮AI所帶來的機會。

圖表8

可信任AI的前五大效益



資料來源：《Deloitte可信任AI調查》(2024)

AI治理最常見的效益之一是**提升對AI解決方案產出或結果的信任度**，約半數(51%)的高階主管予以認同(圖表8)。根據電機電子工程師學會(Institute of Electrical and Electronics Engineers, IEEE)國際期刊內的研究顯示，透明的AI系統能使用者的信任度提升30%，進而提高採用與使用此AI系統的可能性。[9]

AI治理措施下提供的具體行動提升了對AI產出結果的信任程度，並減輕高階主管面對使用AI時面臨的風險。例如，實施事件應變與補救計畫可讓領導者對問題的妥善管理更具信心。達到AI治理成熟度「成熟階段」的組織對於安全、隱私或法律風險等關鍵問題的擔憂較少(圖表9)。處於「發展階段」與「基礎階段」的組織對風險的擔憂程度相近，突顯了在各核心要素中實施有效AI治理，以解決AI使用上相關的問題之重要性。

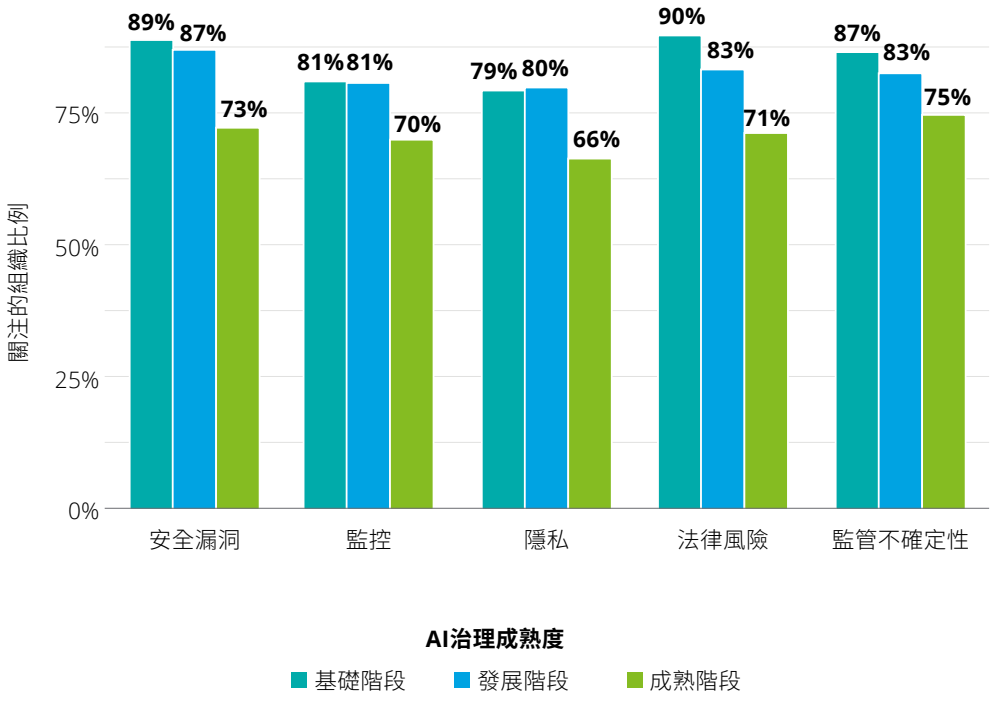
半數的高階主管表示，**在整個組織內更廣泛地使用AI解決方案**是有效的AI治理所帶來的另一項關鍵效益。根據計量經濟模型獲得的驗證結果顯示，AI治理成熟度指標中達到「成熟階段」的組織，與僅處於「基礎階段」的類似組織相比，已在其內部的三個額外業務領域部署AI解決方案[10]。例如，**「成熟階段」組織在顧客服務、行銷與銷售、營運與生產以及研發等方面，使用AI的可能性是其他組織的三倍**。

此外，建立AI治理也能提升AI解決方案在部署領域內的**使用範圍**。平均而言，達到「成熟階段」的組織中使用AI工具的員工比例比「基礎階段」的組織高出16個百分點，相當於**平均每個組織的AI使用人數增加了28%**。

即使將針對在相同領域（例如行銷與銷售或研發）部署AI解決方案的組織進行比較，此結果仍然成立。此說明了可信任AI整體上能提升員工對AI解決方案的接受度。有關本調查結果的更多細節，請參見附錄C。

「本研究調查結果顯示，有效的AI治理能同時提升AI解決方案在組織內的應用廣度（跨部門使用）與深度（更多員工使用）。」

圖表9：不同階段的AI治理成熟度組織對主要風險的關注程度



資料來源：《Deloitte可信任AI調查》(2024)

顧客對AI應用的道德倫理與資料隱私的關注日益增加。事實上，僅有一半的消費者認為，從線上服務獲得的效益超過對資料隱私的擔憂。[11]有效的AI治理能展現組織對AI價值的承諾，進而提升其**企業形象效益**，其中有45%的高階主管對此表示認同。

傳統AI與生成式AI工具皆已證明能顯著提升生產力。根據Deloitte對11,900名「AI世代」的年輕員工與學生的分析，每日使用生成式AI者每週可節省5.3小時的工作時間。[12]未來隨著使用者對AI的熟悉度提升與科技能力的進一步發展，此數字可能會繼續增加。

另外，MIT麻省理工學院史隆管理學院的研究顯示，採用AI解決方案的組織其營運效率與生產力提升了15%。[13]**本研究調查顯示，44%的高階主管表示有效的治理框架可以使AI解決方案更具生產力**。此外，根據本調查結果，可信任AI指標上取得較高水準的組織，其過去一年的營收成長表現更為突出。即使在控制AI的使用程度下，當可信任AI指標每增加15分，組織的營收可成長4.6%。對於擁有超過1,000名員工的大型組織而言，若該組織在2024至2025年收入成長了1億美元，擁有較高的可信任AI水準之組織的營收將額外460萬美元。對於中位數組織（去年營收成長19.5%）而言，則相當於近25%的增幅。有關本調查結果的更多詳細資訊，請參見附錄C。

「完善的人工智慧治理能提升AI解決方案的效率。即使考量AI解決方案的使用程度，

具較高的AI治理成熟度對於企業帶來正面的營收效益。」

大多數的人可能誤以為AI治理將造成組織內部的業務流程更加繁瑣，從而減緩了AI被採用的速度。事實上，有效的AI治理反而能透過建立明確的程序與控制措施，進而簡化AI解決方案的部署流程。本研究調查顯示，44%的高階主管認為有效的AI治理能加速AI解決方案在組織內的部署。另一項研究顯示，擁有強大AI治理框架的組織之AI解決方案的部署速度比缺乏AI治理框架的組織快20%。

05

建立可信任AI的基石

當組織欲將AI解決方案整合至營運與商業模式時，有效的AI治理至關重要。如前幾章所述，有效的治理能促進更廣泛的科技應用並增加商業價值，同時協助管理風險。

那麼，組織領導者目前可以採取哪些關鍵步驟來改善AI治理呢？

根據調查分析結果，在此提出以下四項具重大影響力的行動建議：

建議1

優先考量AI治理，以實現AI帶來的商業價值

1

AI治理成熟度指標顯示，大多數組織在AI治理方面仍有顯著改善空間。本研究顯示，AI對企業而言是一種極具影響力的科技，而強化AI治理並非「可有可無」，而是協助企業更有效地運用AI的關鍵推動力。優先考量AI治理的第一步是了解目前的起點。

AI治理成熟度指標規劃了五大核心要素：「組織結構」、「政策與原則」、「程序與控制」、「人員與技能」以及「監測、報告與評估」，上述要素可用於協助組織評估其自身系統並識別需要改善的領域。

本研究指出，許多組織應將重點放在「政策與原則」以及「程序與控制」兩核心要素上。

為了因應與AI相關的新興風險或解決方案部署過程中的風險，持續性地評估AI治理的成效也有其必要性。針對特定地區和產業的監管變化，亦促使企業必須保持在AI治理水準上保持領先地位。

建議2

了解並善用更廣泛的AI供應鏈

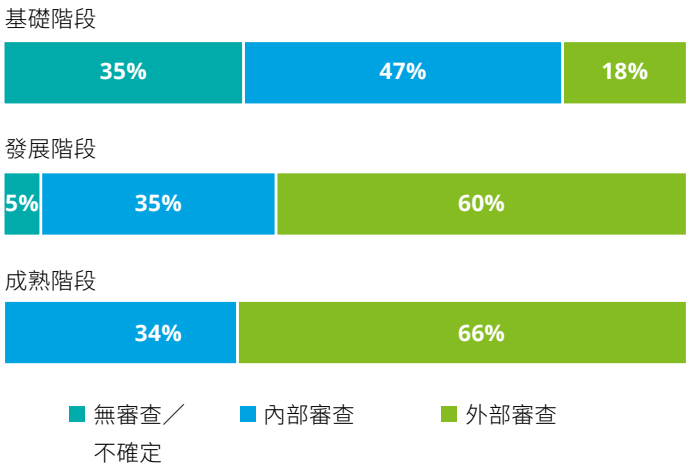
2

了解組織自身對AI的使用情形，以及組織與更廣泛的AI供應鏈中各角色（如：開發者、部署者、監管機構、平台提供商、終端使用者及顧客）的互動情形，將有助於組織對AI治理要求形成更全面的理解。例如，15%的高階主管表示，其組織同時使用外購現成的AI解決方案、內部開發的AI解決方案，以及公開可用的AI應用程式。而面對上述之不同來源的AI應用，都需要量身訂做不同的治理方法。

AI供應鏈中各角色通常具備相關的專業知識與不同的觀點，因此高階主管也可以善用更廣泛的AI供應鏈來改善其AI治理內容。越來越多的組織希望透過引入外部審查機構，為其治理框架建立「第三道防線」。

為了使外部機構發揮作用，審查需要涵蓋AI解決方案的整個生命週期。值得注意的是，聘請外部機構審查AI解決方案實施情形的組織，其可信任AI指數較高（圖表10）。而歸類為「成熟階段」的組織中，約有六成曾委託外部機構審查其AI解決方案的實施情形。本研究調查結果也發現，與相關產業協會合作，有助於組織了解AI治理在不同產業或組織的獨特性要求或規範。

圖表10：不同階段的AI治理成熟度組織審查AI實施情形的類型



資料來源：《Deloitte可信任AI調查》（2024）

建議3

培養風險管理者，而非風險規避者

3

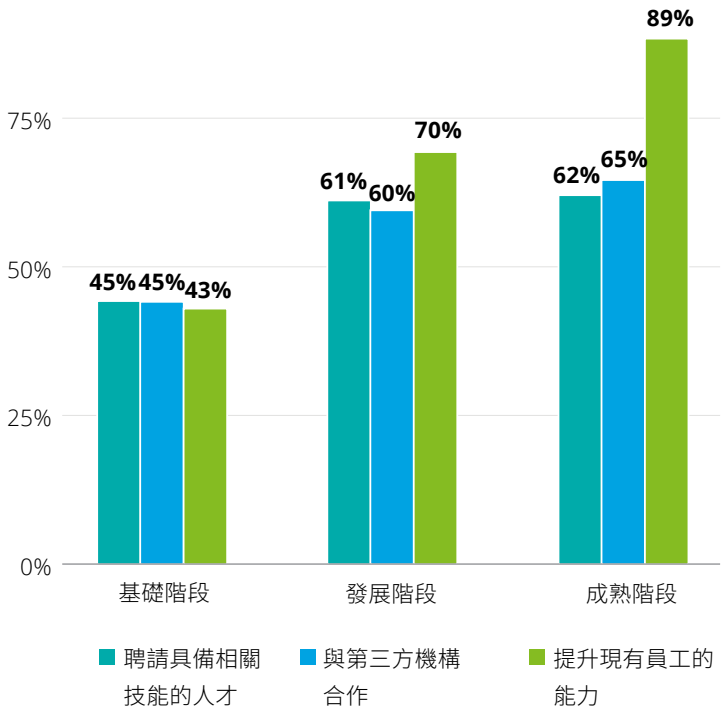
人員的專業判斷與回應對於成功的AI治理至關重要。無論是設計、部署或是使用AI解決方案的員工，其對於AI功能性及使用時可能產生的潛在風險都能提供寶貴的見解。更重要的是，培養員工的技能可協助識別、評估並管理風險，進而預防或減緩風險，而非選擇規避或忽視風險。有鑑於此，「人員與技能」成為AI治理成熟度指標中的關鍵核心要素之一。然而，儘管此要素的重要性如此突出，「人員與技能」仍是組織在平均得分中最低的部分。

本研究調查顯示，近90%的「成熟階段」組織正在提升現有員工的能力，以縮小符合道德倫理與合法使用AI所需的技能差距。此結果顯現，達「成熟階段」的組織較積極的培養員工之技能與能力，以確保員工能以符合道德倫理且負責任的方式使用AI。

相較之下，僅有43%的「基礎階段」組織正在提升現有員工的技能以縮小該差距。「成熟階段」的組織也較高比例的與具備適當技能的第三方機構合作（65%），並聘請具備相關技能的員工（63%）。

「培養風險管理者，而非風險規避者」對縮小AI技能差距產生了實質影響，且隨著技術能力和監管環境的不斷演進，持續更新與強化員工的AI治理技能將變得至關重要。根據本調查結果顯示，在「成熟階段」的組織中，有73%的員工具備符合道德倫理和合法使用AI的技能與能力，而處於「基礎階段」組織的員工，此比例僅佔40%。

圖表11：不同階段的AI治理成熟度組織縮小AI治理所需技能差距的方法



資料來源：《Deloitte可信任AI調查》（2024）

建議4

進行內部溝通並確保AI轉型準備就緒

4

有效的溝通對於AI治理的日常管理作業而言相當重要，也是帶領員工踏上AI旅程的必要條件，這包括保持長期AI策略的透明度、業務的效益與風險分析、提升團隊使用AI模型的技能，以及對於未來可能因AI取代其工作的相關人員培訓新技能。同時，確保所有利害關係人理解與AI相關的風險與效益，並能就其使用做出明確決策及提出疑慮，是不可或缺的。為達到良好的AI治理，需要清晰且透明的溝通，並且願意展開積極對話，組織可採取的相關實際行動包括：針對高風險事件進行情境規劃，讓領導者和員工能夠以可信任、人性化的方式說明新興科技的角色與帶來的影響，並進行危機演練，以測試是否已為非預期的嚴重事件做好準備。

「建立良好的AI治理通常需要組織內部思維的轉變。在最初的討論中，部分人員會質疑AI治理是否僅僅是IT部門的問題。透過多次討論後，理解AI如何從IT、網路安全橫跨至風險管理和法遵等各業務領域，促使所有人意識到良好的AI治理是所有團隊的共同責任。」

—— 電信服務提供商的數據長

附錄

附錄A
調查方法

本報告於2024年9月至10月，針對來自亞太地區13個地點、899位高階管理階層進行調查。此次調查旨在評估AI治理結構的成熟度，並了解良好AI治理所帶來的效益。

受訪對象以高階管理階層為主，如風險長、法務長與數據長。組織涵蓋公部門、私人企業及非營利組織等多個領域，並涉及金融、教育、生技醫療及高科技等多個產業。

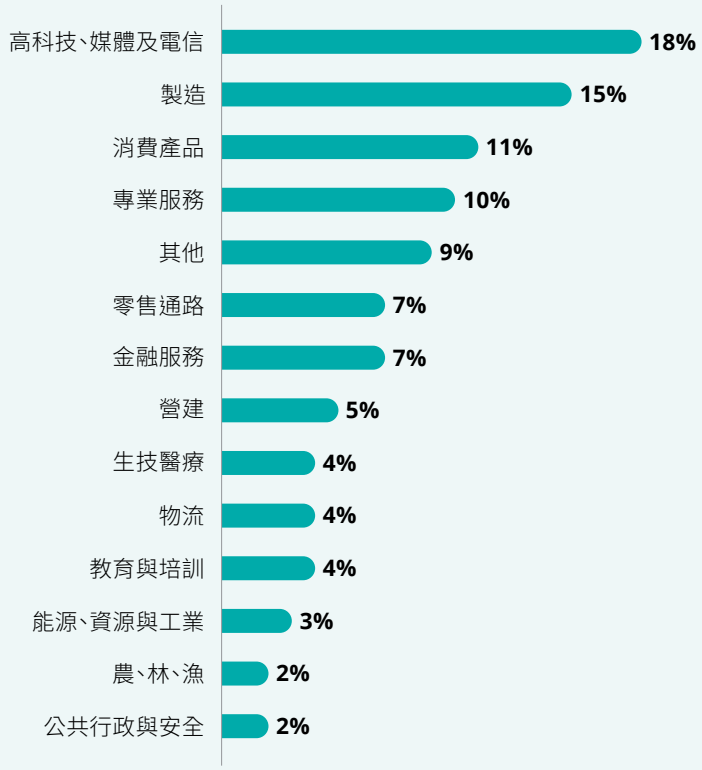
附表A1顯示亞太地區各地點的受訪者數量；附表A2和A3分別說明受訪者所屬產業及其職務分布。

附表A1：各地受訪者數量

地點	受訪者數量
澳洲	112
中國大陸	103
印度	102
日本	104
紐西蘭	53
東南亞	321
印尼	64
馬來西亞	51
菲律賓	52
新加坡	51
泰國	51
越南	52
南韓	52
台灣	52
總計	**899**

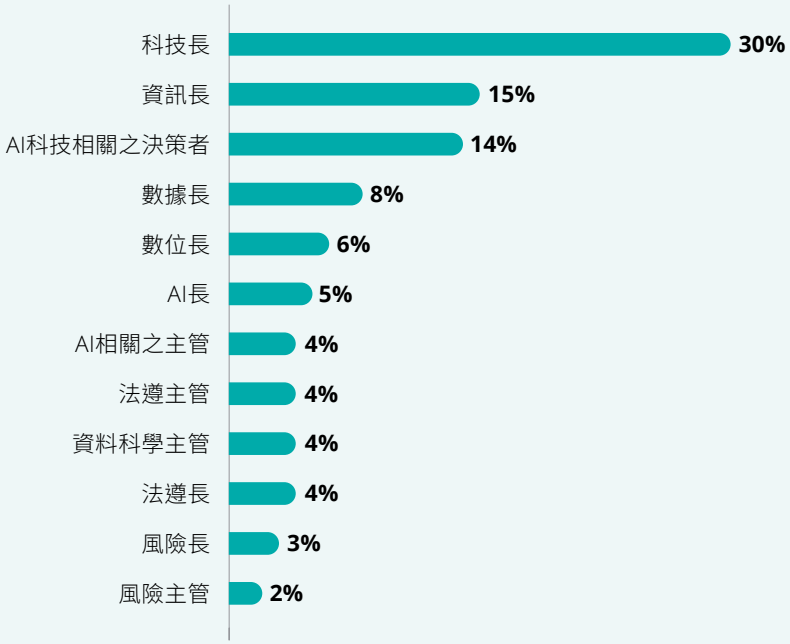
資料來源：《Deloitte可信任AI調查》(2024)

附表A2：受訪者所屬產業



資料來源：《Deloitte可信任AI調查》(2024)

附表A3：受訪者職務



資料來源：《Deloitte可信任AI調查》(2024)

附錄B
Deloitte AI治理成熟度指標

AI治理成熟度指標為Deloitte於本研究中所開發，以12個問題（部分問題包含多個子問題）的回答為基礎，並以下列五個關鍵核心要素為區分依據。
本方法論透過問卷調查方式，蒐集近900家組織的AI治理情形，藉以評估組織在AI治理的成熟度。

組織結構

1) 在貴組織中，主要負責確保AI道德倫理、法律及技術標準明確實施並進行評估的是誰？

可能的回答：董事會、執行長、技術長、數位長、數據長、法遵長、資訊長、風險長、AI長、高階管理團隊、法遵主管、AI業務之主管、部門主管／總經理／高階經理、AI開發團隊、其他。

2) 下列與AI使用相關的組織結構元素，哪些已經在貴組織中實施？

a. 董事會監督的AI治理運作結構

b. 負責監督AI治理的AI委員會，包括來自法律、法遵、IT、人資及其他相關部門的代表

c. 明確定義AI治理在AI生命週期中的角色與責任，例如：業務負責人、AI系統負責人、資料負責人、領域架構者等

3) 下列哪項最能描述貴組織中負責AI相關道德倫理、法律及監管規範團隊的結構

a. 沒有負責該任務的角色

b. 部分部門／團隊有專責該任務的專業人員

c. 每個部門／團隊都有專責該任務的專業人員

d. 備有中央團隊負責該任務，在組織內監測趨勢並檢測AI使用相關風險

e. 以上皆非

f. 不確定／不願回答

政策與原則

1) 下列敘述何者最符合貴組織在運用AI方面的策略?

a. 目前沒有AI策略，也未針對策略制定採取任何步驟

b. 目前沒有AI策略，但正在積極制定

c. 部分部門／團隊有各自的AI策略

d. 有涵蓋全組織範圍的AI策略，但並非所有人都認同其價值

e. 有涵蓋全組織範圍的AI策略且為優先事項，但並未追蹤進度

f. 有涵蓋全組織範圍的AI策略，其中包含明確定義的流程，用於設定優先順序與衡量分析計畫的價值

g. 不確定／不願回答

2) 下列哪些元素包含在您的AI策略或治理框架中？

a. 確保組織安全且負責任使用AI的AI政策

b. 道德倫理指導方針與原則

c. 明確界定組織的AI風險胃納

d. 實施AI治理目標與流程的時間表

e. 實施治理計畫的資金支持

f. 監測與審核流程

g. 事件應變與回應計畫

h. 關鍵績效指標

i. 與其他相關政策（隱私、資料治理與網路安全）或組織的策略目標整合

3) 下列哪些元素已在貴組織中使用或部署的AI系統中落實？

a. 明確分配監督和持續監測AI系統的角色與責任

b. 針對使用AI系統所做出或導出的決策進行明確的責任分配

c. 設有保護措施以確保AI系統不會使用超出其預期和聲明用途的資料

d. 使用者了解AI系統如何做出對其產生影響的決策

e. 設有檢測和減緩偏見的機制，以確保AI系統的公平與公正

f. AI系統以負責任的方式設計與運作，並注重人類、社會與環境的福祉

g. AI系統的設計與運作旨在產生一致且準確的產出結果，能夠承受錯誤並快速從無法預期的中斷中恢復

h. AI系統受到保護，以防止未經授權的存取與遭受攻擊者的利用

i. 設有資料匿名化和假名化措施以保護個人和敏感資訊

序與控制

1) 是否已設置能讓員工對AI使用及產出提出問題的系統？

可能的回答：是、否、備有設置系統的計畫、不確定

2) 下列哪些與AI使用相關的實踐、程序或控制措施已在貴組織中落實？

a. AI風險分類，用於定義AI解決方案的風險組合

b. AI風險評估程序，於開發、測試及實施過程中協助識別和管理AI相關風險

c. AI控制框架，用於減輕與AI解決方案使用相關的風險

d. 組織目前使用的AI解決方案清單，包括內部開發或外部採購的解決方案

e. AI治理平台，用於評估和監測AI系統活動的風險及法遵情況

f. 用於收集AI生命週期各階段資訊以協助獨立第三方審核之系統

g. 客戶或其他利害關係人等外部各方於使用AI時的風險或申訴處理程序

人員、技能與文化

1) 貴組織具備下列哪些可供員工使用的資源，以協助員工以符合道德倫理、法律和監管規範且正確的方式使用AI？

a. 提供有關如何在工作中適當使用AI的指引

b. 開發諮詢服務或諮詢機構，讓員工能向具有風險和法遵經驗的團隊成員諮詢AI各個方面的使用問題

c. 提供有關如何在工作中適當使用AI的培訓，了解與之相關的道德倫理、法律和監管規範風險

d. 針對AI系統的使用導入資料加密和存取控制等安全與隱私措施

e. 鼓勵員工的獨立實驗、實踐社群、團隊成員之間的討論等在職學習

2) 根據您的估計，有多少比例的員工具備以合法和符合道德倫理的方式使用AI所需的技能和能力？

監測、報告與評估

1) 為保護權利和防止濫用，貴組織檢視與工作中使用AI的相關現有法律或監管要求之頻率為何？

a. 至少每隔幾個月一次

b. 至少每六個月一次

c. 至少每年一次

d. 少於每年一次

e. 以上皆非

f. 不確定／不願回答

2) 您多久評估一次AI系統，以確保其符合貴組織對AI的標準?

a. 持續或即時

b. 至少每隔幾個月一次

c. 至少每六個月一次

d. 至少每年一次

e. 少於每年一次

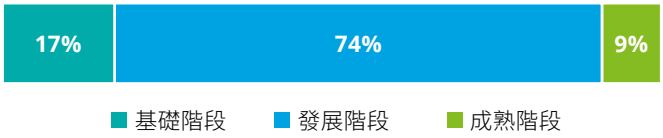
f. 以上皆非

g. 不確定／不願回答

每個答案皆給予0到100之間的分數，並將每個問題的「最佳」答案評為100分。例如，若該組織回答「有涵蓋全組織範圍的AI策略，並制定了流程來確定優先順序和衡量價值」，則該題會獲得100分；如果回答「只有部分部門有AI策略」，則獲得60分。每項核心要素的分數是該核心要素內所有問題的平均分數，整體指標則為各核心要素的平均分數。

分數低於50分者歸類為「基礎階段」，分數介於50至90分者歸類為「發展階段」，分數高於90分者歸類為「成熟階段」。該分數的類別分布呈現如附表B1：

附表B1：AI治理成熟度指數分數分布



資料來源：《Deloitte可信任AI調查》(2024)

下表為各核心要素的平均分數、中位數，以及獲得「基礎階段」或「成熟階段」評分的組織比例。

AI治理成熟度指標 核心要素	平均分數	中位數	基礎階段 (%)	成熟階段 (%)
整體指標	70.8	68.0	9%	17%
組織結構	73.9	72.0	9%	18%
政策與原則	58.4	66.3	31%	13%
實踐、程序與控制	64.8	67.5	23%	10%
人員、技能與文化	67.2	70.0	22%	14%
監測、報告與評估	76.0	80.0	6%	18%

附錄C
計量經濟模型

使用普通最小平方法進行迴歸分析，估算良好的AI治理實踐與企業績效衡量指標之間的關係。為了降低遺漏變數偏誤的風險，因此納入組織的關鍵特徵作為控制變數，該控制變數列於下表：

控制變數	詳細內容
總部所在地	依據調查回饋的總部所在國家，共13個選項
產業別	依據調查回饋的《紐澳行業標準分類》(1碼)，共19個選項
員工人數	依據調查回饋的全職當量員工人數，共4個選項
部門別	公部門、私人企業，或非營利部門
營業收入	依據調查回饋的2023-2024年度收入(連續資料，按2024年10月匯率換算為美元)

兩個應變數分別為：受訪者表示已「完全導入」AI解決方案的業務領域數量(共10個選項)，以及在業務中使用AI解決方案的員工比例(介於0至100之間)

關鍵的自變數是Deloitte AI治理成熟度指標，其計算方式如上附錄所述；該指數同時使用「數值」與「三類別劃分」的方式進行估算。

此外，考量組織的AI採用程度可能與誤差項及自變數存在相關性，因此將使用AI的員工比例納入控制變數。該變數的納入並未顯著改變主要參數的估計值。在以使用AI的員工比例作為自變數的模型中，完全實施AI解決方案於業務中的領域數量則用作控制變數。

透過下列迴歸模型進行估算：

1) 使用AI的員工比例 $= \beta_0 + \beta_1 \times$ 指數得分 $+ \beta_2 \times$ 具備AI工具的業務領域數量 + 控制變數

2) 具備AI工具的業務領域數量 $= \beta_0 + \beta_1 \times$ 指數得分 $+ \beta_2 \times$ 使用AI的員工比例 + 控制變數

3) 營收成長 $= \beta_0 + \beta_1 \times$ 指數得分 $+ \beta_2 \times$ 使用AI的員工比例 + 控制變數

以下提供迴歸模型的摘要表。需注意，應謹慎解讀模型；由於資料是由調查回饋取得，因此可能存在未觀察到且同時與解釋變數和誤差項相關的因子，該因子將使估計產生偏差。結果應僅作為相關性分析解讀。

模型1：應變數——使用AI的員工比例

變數	估計值	標準誤差	p值
指標得分	0.30543	0.0646	<0.00001
具備AI工具的業務領域數量	2.02022	0.3996	<0.00001
判定係數	0.1978		
調整後的判定係數	0.1510		

型2：應變數——使用AI的員工比例

變數	估計值	標準誤差	p值
指標類別：發展階段	8.27383	2.865	<0.00001
指標類別：成熟階段	15.7533	4.123	0.004
具備AI工具的業務領域數量	2.257	0.393	<0.00001
判定係數	0.1881		
調整後的判定係數	0.1394		

模型3：應變數——具備AI工具的業務領域數量

變數	估計值	標準誤差	p值
指標得分	0.0555	0.0061	<0.00001
具備AI工具的業務領域數量	0.0197	0.0039	<0.00001
判定係數	0.3352		
調整後的判定係數	0.2965		

模型4：應變數——具備AI工具的業務領域數量

變數	估計值	標準誤差	p值
指標類別：發展階段	1.3557	0.283	<0.00001
指標類別：成熟階段	3.0569	0.396	<0.00001
具備AI工具的業務領域數量	0.0226	0.004	<0.00001
判定係數	0.3120		
調整後的判定係數	0.2707		

模型4：應變數——具備AI工具的業務領域數量

變數	估計值	標準誤差	p值
指標得分	0.0031	0.0018	0.0884
使用AI的員工比例	0.0017	0.0011	0.1355
判定係數	0.0677		
調整後的判定係數	0.004769		

附錄D
各地區焦點

聚焦 澳洲

澳洲人口：2710萬 | GDP：1.7兆美元

有效的AI治理所帶來的前三大預期**效益**

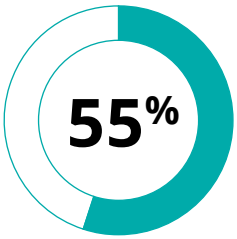
- 提升對AI解決方案的產出或結果的信任度（47%）
- 由於信任度提高而更廣泛使用AI解決方案（46%）
- 更高的法遵能力（42%）

使用AI所帶來的前三大**風險**關注點

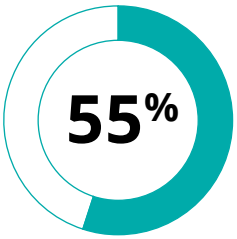
- 監控：因全面性監控導致的隱私侵害（88%）
- 隱私：敏感、機密或個人資料由AI系統外洩的風險（88%）
- 安全漏洞：駭客／網路攻擊風險（85%）

使用或導入AI的前三大**阻礙**

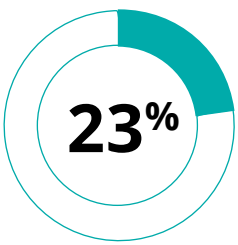
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（44%）
- 對技術及其潛力的理解不足（34%）
- 缺乏人才和或技術技能（29%）



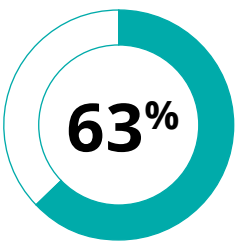
位於澳洲的組織設有讓員工反映問題的通報機制



位於澳洲的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於澳洲的組織表示上一財務年度收到的AI事件數量有所增加



位於澳洲的組織正在提升員工的能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

 註：澳洲樣本數＝112

聚焦

中國大陸

中國大陸人口：14.19億 | GDP：18.2兆美元

有效的AI治理所帶來的前三大預期**效益**

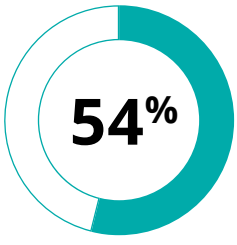
- 由於信任度提高而更廣泛使用AI解決方案（52%）
- 透過AI解決方案實現更強大的生產力效益（51%）
- 更快速地在組織內部署AI解決方案（50%）

使用AI所帶來的前三大**風險**關注點

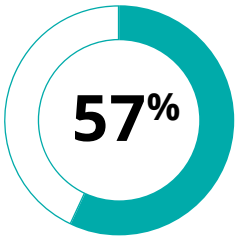
- 安全漏洞：駭客／網路攻擊風險（86%）
- 法律風險與版權侵害（80%）
- 監管負擔：使用AI解決方案所要求的相關報告及流程（80%）

使用或導入AI的前三大**阻礙**

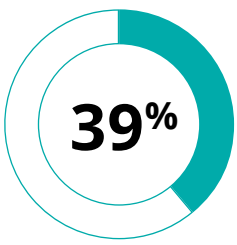
- 技術導入挑戰（38%）
- 缺乏創新意願和或實驗不足（36%）
- 缺乏人才和／或技術技能（34%）



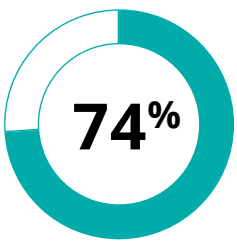
位於中國大陸的組織設有讓員工反映問題的通報機制



位於中國大陸的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於中國大陸的組織表示上一財務年度收到的AI事件數量有所增加



位於中國大陸的組織正與第三方機構合作，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：中國樣本數＝103

聚焦

印度

印度人口：14.51億 | GDP：3.95兆美元

有效的AI治理所帶來的前三大預期**效益**

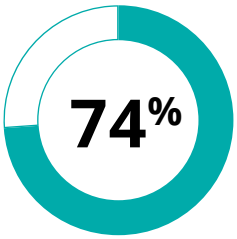
- 提升對AI解決方案的產出或結果的信任度（63%）
- 提升口碑（60%）
- 由於信任度提高而更廣泛使用AI解決方案（57%）

使用AI所帶來的前三大**風險**關注點

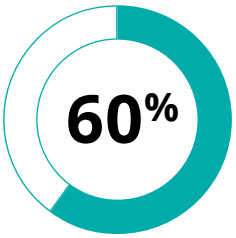
- 安全漏洞：駭客網路攻擊風險（92%）
- 隱私：敏感、機密或個人資料外洩的風險（91%）
- 監管不確定性：變動的要求可能導致對義務的不了解（89%）

使用或導入AI的前三大**阻礙**

- 技術導入挑戰（50%）
- 對技術及其潛力的理解不足（35%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（32%）

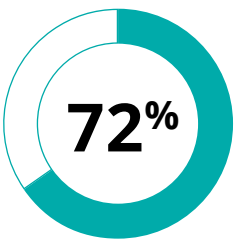


位於印度的組織設有讓員工反映問題的通報機制



位於印度的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案

位於印度的組織表示上一財務年度收到的AI事件數量有所增加



位於印度的組織正在聘請具備相關技能的員工，以縮小符合道德倫理與合規的方式使用AI所需的技能差距

 註：印度樣本數＝102

聚焦

日本

日本人口：1.238億 | GDP：4.1兆美元

有效的AI治理所帶來的前三大預期**效益**

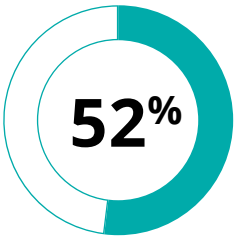
- 提升對AI解決方案的產出或結果的信任度（51%）
- 提升口碑（49%）
- 由於信任度提高而更廣泛使用AI解決方案（45%）

使用AI所帶來的前三大**風險**關注點

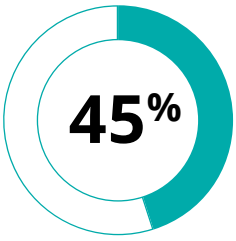
- 安全漏洞：駭客網路攻擊風險（88%）
- 監控：因全面性監控導致的隱私侵害（85%）
- 隱私：敏感、機密或個人資料外洩的風險（83%）

使用或導入AI的前三大**阻礙**

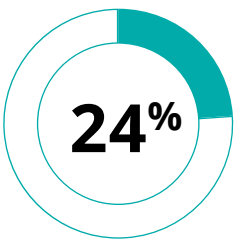
- 技術導入挑戰（38%）
- 缺乏創新意願和或實驗不足（36%）
- 缺乏人才和／或技術技能（34%）



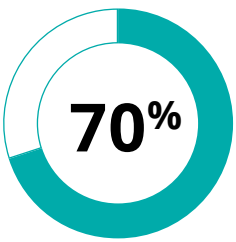
位於日本的組織設有讓員工反映問題的通報機制



位於日本的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於日本的組織表示上一財務年度收到的AI事件數量有所增加



位於日本的組織正在提升員工能力，以縮小符合道德倫理與合規的方式使用AI所需的技能差距

註：日本樣本數＝104

聚焦

南韓

南韓人口：5180萬 | GDP：1.7兆美元

有效的AI治理所帶來的前三大預期**效益**

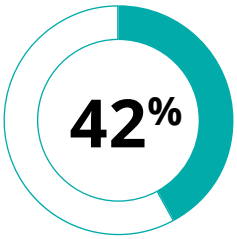
- 由於信任度提高而更廣泛使用AI解決方案（46%）
- 更高的法遵能力（42%）
- 更快速地在組織內部署AI解決方案（40%）

使用AI所帶來的前三大**風險**關注點

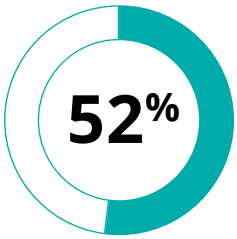
- 安全漏洞：駭客／網路攻擊風險（85%）
- 監控：因全面性監控導致的隱私侵害（85%）
- 監管負擔：使用AI解決方案所要求的相關報告及流程（83%）

使用或導入AI的前三大**阻礙**

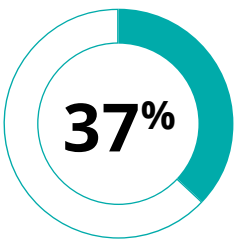
- 技術導入挑戰（35%）
- 缺乏實施AI的策略與願景（33%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（31%）



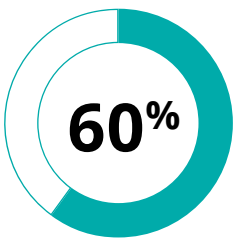
位於南韓的組織設有讓員工反映問題的通報機制



位於南韓的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於南韓的組織表示上一財務年度收到的AI事件數量有所增加



位於南韓的組織正在聘請具備相關技能的員工，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

 註：南韓樣本數＝52

聚焦
紐西蘭

紐西蘭人口：520萬 | GDP：2530億美元

有效的AI治理所帶來的前三大預期**效益**

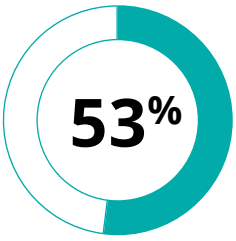
- 由於信任度提高而更廣泛使用AI解決方案（51%）
- 透過AI解決方案實現更強大的生產力效益（42%）
- 提升口碑（38%）

使用AI所帶來的前三大**風險**關注點

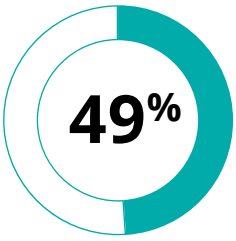
- 可靠性與錯誤（87%）
- 安全漏洞：駭客／網路攻擊風險（85%）
- 隱私：敏感、機密或個人資料由AI系統外洩的風險（85%）

使用或導入AI的前三大**阻礙**

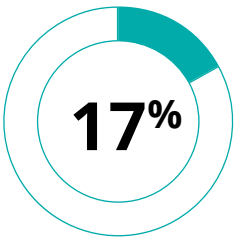
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（40%）
- 對技術及其潛力的理解不足（38%）
- 資金不足（36%）



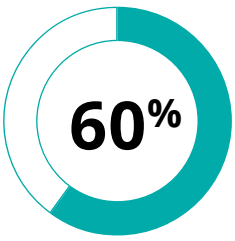
位於紐西蘭的組織設有讓員工反映問題的通報機制



位於紐西蘭的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於紐西蘭的組織表示上一財務年度收到的AI事件數量有所增加



位於紐西蘭的組織正與第三方機構合作，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：紐西蘭樣本數＝53

聚焦 台灣

台灣人口：2340萬 | GDP：7565.9億美元

有效的AI治理所帶來的前三大預期**效益**

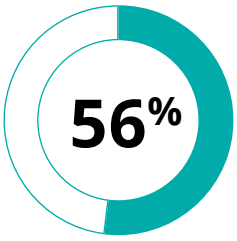
- 透過AI解決方案實現更強大的生產力效益（64%）
- 更快速地在組織內部署AI解決方案（48%）
- 提升口碑（44%）

使用AI所帶來的前三大**風險**關注點

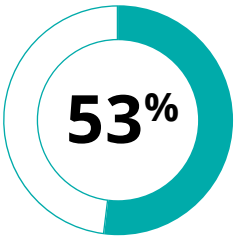
- 安全漏洞：駭客／網路攻擊風險（85%）
- 監控：因全面性監控和資料收集能力導致的隱私侵害（85%）
- 監管不確定性：變動的要求可能導致對義務的不了解（81%）

使用或導入AI的前三大**阻礙**

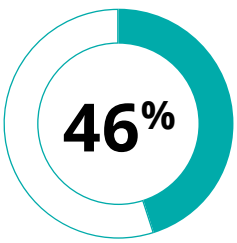
- 技術導入挑戰（40%）
- AI使用的案例和投資與策略脫節（40%）
- 缺乏創新意願和／或實驗不足（37%）



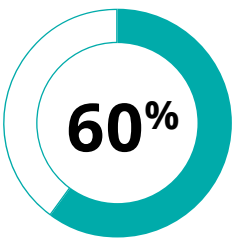
位於台灣的組織設有讓員工反映問題的通報機制



位於台灣的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於台灣的組織表示上一財務年度收到的AI事件數量有所增加



位於台灣的組織正在聘請具備相關技能的員工，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

 註：台灣樣本數＝52

聚焦

新加坡

新加坡人口：580萬 | GDP：5010億美元

有效的AI治理所帶來的前三大預期**效益**

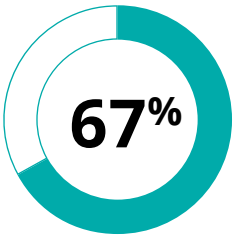
- 提升口碑（43%）
- 提升對AI解決方案的產出或結果的信任度（43%）
- 更高的法遵能力（39%）

使用AI所帶來的前三大**風險**關注點

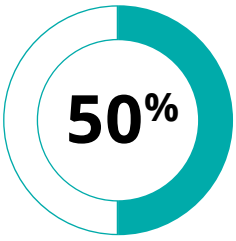
- 安全漏洞：駭客／網路攻擊風險（96%）
- 隱私：敏感、機密或個人資料由AI系統外洩的風險（94%）
- 可靠性與錯誤（94%）

使用或導入AI的前三大**阻礙**

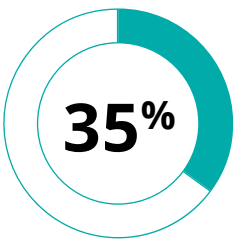
- 對技術及其潛力的理解不足（41%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（37%）
- 技術導入挑戰（31%）



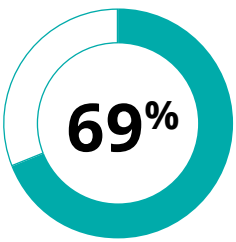
位於新加坡的組織設有讓員工反映問題的通報機制



位於新加坡的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於新加坡的組織表示上一財務年度收到的AI事件數量有所增加



位於新加坡的組織正在聘請具備相關技能的員工，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：新加坡樣本數＝51

聚焦 印尼

印尼人口：2.787億 | GDP：1.37兆美元

有效的AI治理所帶來的前三大預期**效益**

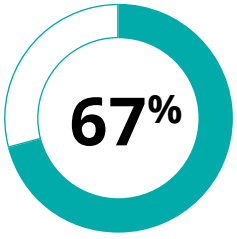
- 提升對AI解決方案的產出或結果的信任度（67%）
- 更快速地在組織內部署AI解決方案（63%）
- 由於信任度提高而更廣泛使用AI解決方案（61%）

使用AI所帶來的前三大**風險**關注點

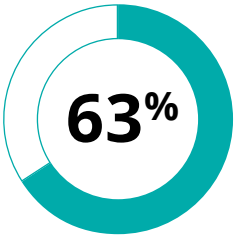
- 安全漏洞：駭客／網路攻擊風險（88%）
- 監控：因全面性監控導致的隱私侵害（84%）
- 法律風險與著作權侵害：與AI解決方案使用資料相關的法律責任或義務（83%）

使用或導入AI的前三大**阻礙**

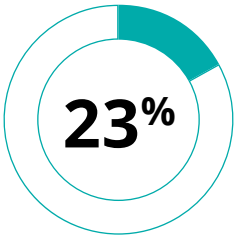
- 對技術及其潛力的理解不足（41%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（38%）
- 技術導入挑戰，例如：維護、與現有系統的整合（36%）



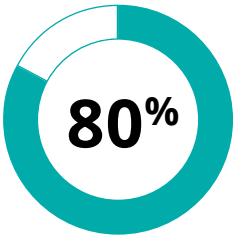
位於印尼的組織設有讓員工反映問題的通報機制



位於印尼的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於印尼的組織表示上一財務年度收到的AI事件數量有所增加



位於印尼的組織正在提升員工能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

 註：印尼樣本數＝64

聚焦

馬來西亞

馬來西亞人口：3340萬 | GDP：4000億美元

有效的AI治理所帶來的前三大預期**效益**

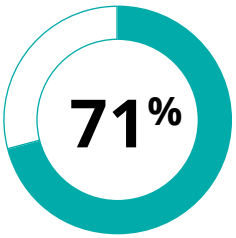
- 提升對AI解決方案的產出或結果的信任度（65%）
- 由於信任度提高而更廣泛使用AI解決方案（63%）
- 更快速地在組織內部署AI解決方案（53%）

使用AI所帶來的前三大**風險**關注點

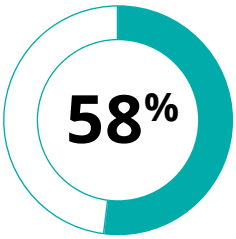
- 安全漏洞：駭客／網路攻擊風險（90%）
- 監控：因全面性監控導致的隱私侵害（84%）
- 隱私：敏感、機密或個人資料由AI系統外洩的風險（82%）

使用或導入AI的前三大**阻礙**

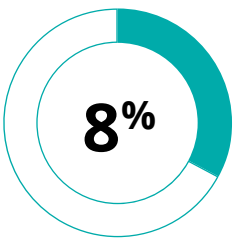
- 技術導入挑戰，例如：維護、與現有系統的整合（51%）
- 對技術及其潛力的理解不足（37%）
- 缺乏人才和或技術技能（33%）



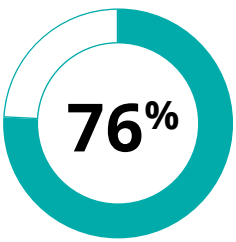
位於馬來希亞的組織設有讓員工反映問題的通報機制



位於馬來西亞的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於馬來西亞的組織表示上一財務年度收到的AI事件數量有所增加



位於馬來西亞的組織正在提升員工能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距。

註：馬來西亞樣本數＝51

聚焦
越南

越南人口：1.003億 | GDP：4300億美元

有效的AI治理所帶來的前三大預期**效益**

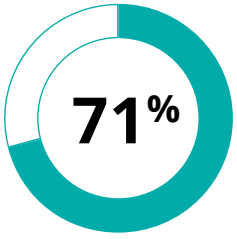
- 提升口碑（67%）
- 透過AI解決方案實現更強大的生產力效益（65%）
- 提升對AI解決方案的產出或結果的信任度（62%）

使用AI所帶來的前三大**風險**關注點

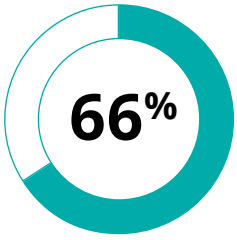
- 隱私：敏感、機密或個人資料外洩的風險（81%）
- 負責任：AI系統開發者和使用者缺乏責任感，可能導致疏忽或不符合道德倫理的使用（81%）
- 可靠性與錯誤：錯誤的產出、不可預測性以及發生故障或意外行為（例如：AI幻覺）（79%）

使用或導入AI的前三大**阻礙**

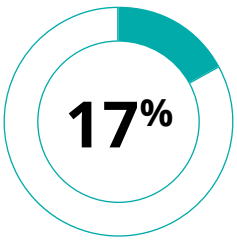
- 缺乏人才和／或技術技能（56%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（40%）
- 缺乏實施AI的策略與願景（37%）



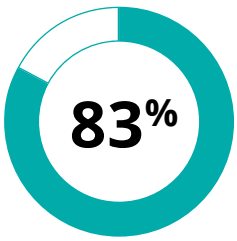
位於越南的組織設有讓員工反映問題的通報機制



位於越南的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於越南的組織表示上一財務年度收到的AI事件數量有所增加



位於越南的組織正在提升員工能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

 註：越南樣本數＝52

聚焦
泰國

泰國人口：6610萬 | GDP：5150億美元

有效的AI治理所帶來的前三大預期**效益**

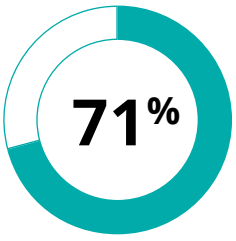
- 提升對AI解決方案的產出或結果的信任度（55%）
- 由於信任度提高而更廣泛使用AI解決方案（51%）
- 更快速地在組織內部署AI解決方案（43%）

使用AI所帶來的前三大**風險**關注點

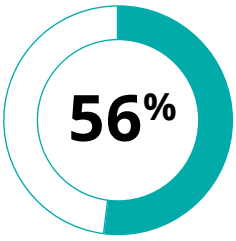
- 安全漏洞：駭客／網路攻擊風險（76%）
- 監控：因全面性監控導致的隱私侵害（75%）
- 法律風險與著作權侵害：與AI解決方案使用資料相關的法律責任或義務（71%）

使用或導入AI的前三大**阻礙**

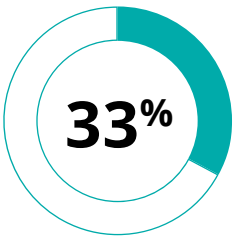
- 對技術及其潛力的理解不足（41%）
- 技術導入挑戰（37%）
- 對監管、法律、道德倫理、法遵及其他風險的擔憂（35%）



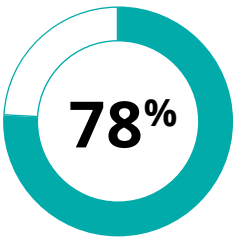
位於泰國的組織設有讓員工反映問題的通報機制



位於泰國的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案



位於泰國的組織表示上一財務年度收到的AI事件數量有所增加

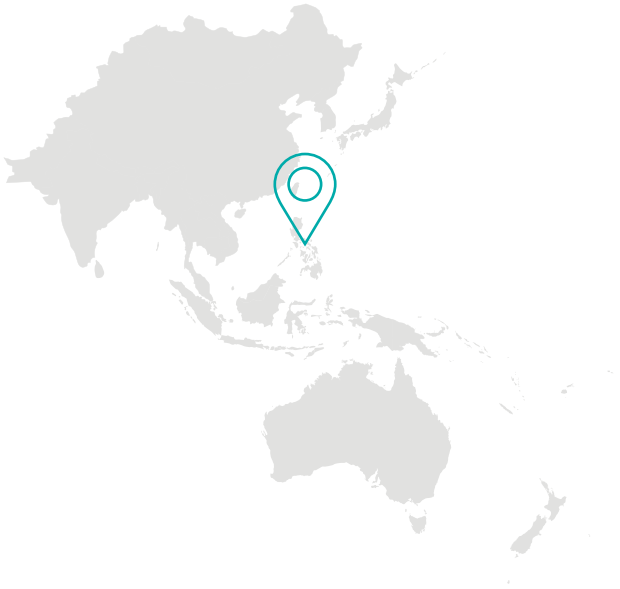


位於泰國的組織正在提升員工能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

註：泰國樣本數＝51

聚焦

菲律賓



菲律賓人口：1.158億 | GDP：4370億美元

有效的AI治理所帶來的前三大預期**效益**

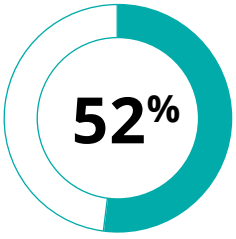
- 提升對AI解決方案的產出或結果的信任度（67%）
- 由於信任度提高而更廣泛使用AI解決方案（52%）
- 提升口碑（48%）

使用AI所帶來的前三大**風險**關注點

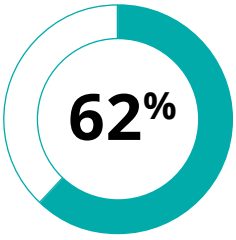
- 監控：因全面性監控導致的隱私侵害（90%）
- 安全漏洞：駭客／網路攻擊風險（85%）
- 隱私：敏感、機密或個人資料由AI系統外洩的風險（83%）

使用或導入AI的前三大**阻礙**

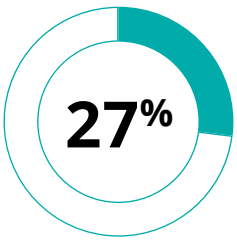
- 缺乏人才和／或技術技能（38%）
- 技術導入挑戰（37%）
- 缺乏實施AI的策略與願景（33%）



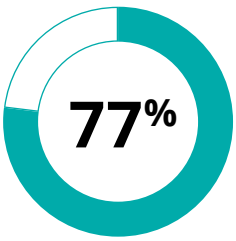
位於菲律賓的組織設有讓員工反映問題的通報機制



位於菲律賓的組織員工具備足夠技能以符合道德倫理與合規的方式使用AI解決方案

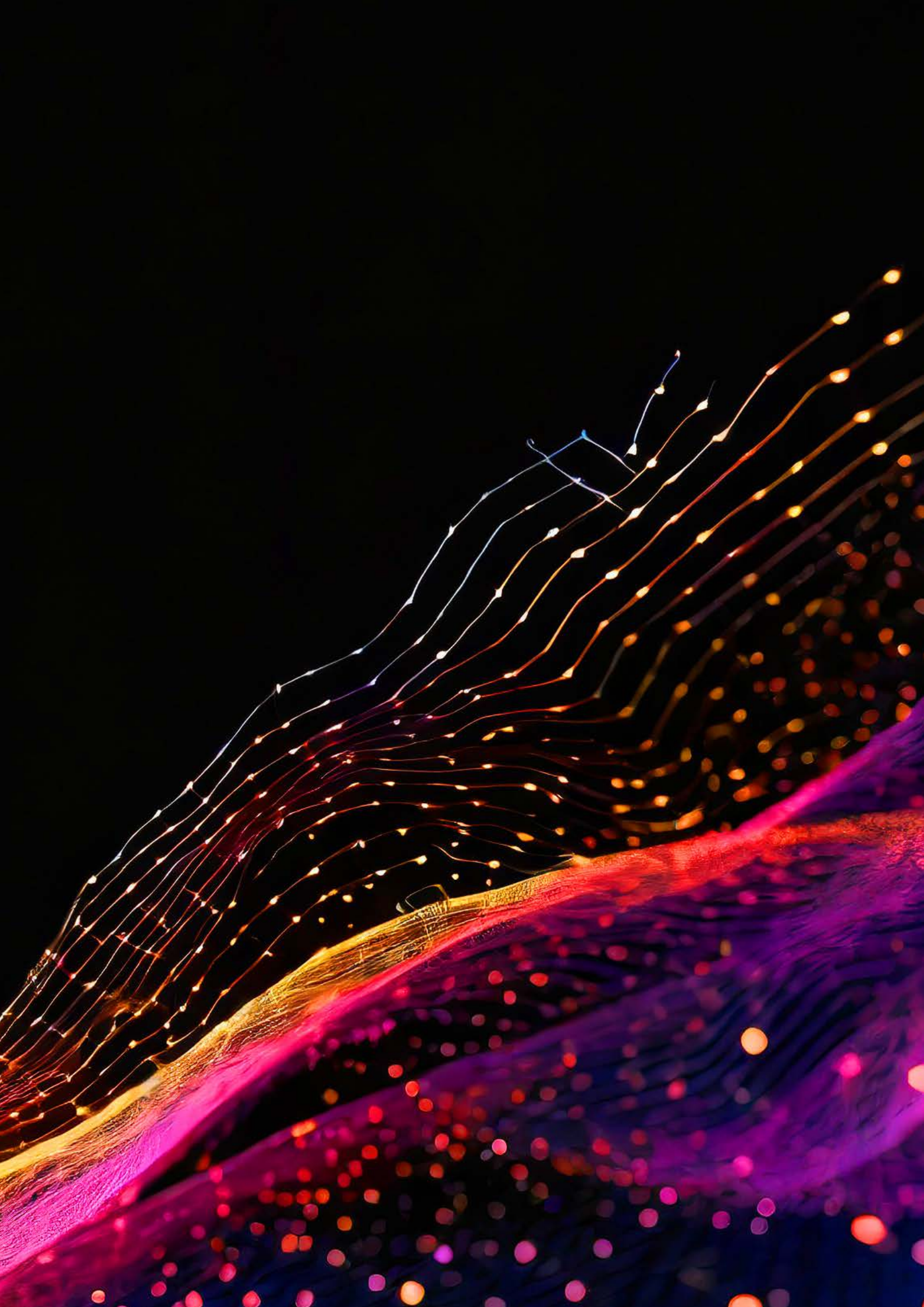


位於菲律賓的組織表示上一財務年度收到的AI事件數量有所增加



位於菲律賓的組織正在提升員工能力，以縮小符合道德倫理與合規的方式使用AI所需之技能差距

 註：菲律賓樣本數＝52



參考資料

1. Deloitte (2024) “Generative AI in Asia Pacific”, https://www.deloitte.com/nz/en/services/consulting/perspectives/generative-ai-in-asia-pacific-may-2024.html
2. Ibid
3. Deloitte Access Economics (2024) “ACS Australia’s Digital Pulse 2024: Decoding the Digital Decade”, https://www.deloitte.com/au/en/services/economics/perspectives/acs-australias-digital-pulse-decoding-the-digital-decade.html
4. IBM (2024), “Cost of a data breach Report”, https://www.ibm.com/reports/data-breach
5. Capgemini Research Institute (2020), “AI and the ethical conundrum” Report, https://www.capgemini.com/news/press-releases/ai-and-the-ethical-conundrum-report/
6. Deloitte Centre for Regulatory Strategy (2024), “Generative AI: Application and Regulation in Asia Pacific”, https://www.deloitte.com/au/en/Industries/financial-services/analysis/generative-ai-application-regulation-asia-pacific.html
7. Deloitte (2024) State of AI in Enterprise, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf
8. Deloitte (2024) State of AI in Enterprise, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf
9. Haresamdram et.al, IEEE Access (2023), “Three levels of AI transparency”, https://ieeexplore.ieee.org/document/10042109
10. Ten areas of the business were presented to senior leaders: operations and/or production, marketing and sales, finance, human resources, customer service, research and development, information technology, management and administration, legal and compliance and logistics.
11. Deloitte (2023), Data privacy and security worries are on the rise, while trust is down. Consumer data privacy and security | Deloitte Insights
12. Deloitte Access Economics (2023), “Generation AI: ready or not, here we come!”, https://www.deloitte.com/content/dam/assets-zone1/au/en/docs/services/economics/deloitte-au-generation-ai-2023-160524.pdf
13. Schrage, M. et. Al, MIT Sloan Management Review (2023), “AI is helping companies redefine, not just improve, performance”; https://sloanreview.mit.edu/article/ai-is-helping-companies-redefine-not-just-improve-performance/
14. The third level of defense refers to a managing risks where the first level of defense are business users or direct managers, the second level of defense is risk and compliance teams and third level of defense is independent assurance

亞太地區各團隊代表與作者群

如需了解更多資訊請聯繫以下各地區之相關代表:

亞太地區各團隊代表

Chris Lewin
Artificial Intelligence
Lead Partner, Asia Pacific
chrislewin@deloitte.com

Dr. Elea Wurth
Trustworthy AI Lead Partner,
Asia Pacific and Australia
ewurth@deloitte.com.au

John O' Mahony
Deloitte Access Economics
Partner, Australia
joomahony@deloitte.com.au

Stuart Scotis
Transformation with Disruptive
Technology, Partner, Deloitte Global
sscotis@deloitte.com.au

Silas Hao Zhu
Trustworthy AI, Partner,
China
silzhu@deloittecn.com.cn

Toyohiro Sometani
Trustworthy AI Partner,
Japan
toyohiro.sometani@tohmatsu.co.jp

Jessica Kim
Trustworthy AI Partner,
South Korea
jessicakim@deloitte.com

Amy Dove
Trustworthy AI Partner,
New Zealand
amydove@deloitte.co.nz

Jayant Saran
Trustworthy AI Partner,
South Asia
jsaran@deloitte.com

Dishell Gokaldas
Trustworthy AI Partner,
Southeast Asia
dgokaldas@deloitte.com

Chris Chen
Trustworthy AI Partner,
Taiwan
chrisachen@deloitte.com.tw

作者群

Nick Hull
Director
nhull@deloitte.com.au

Jennifer Wright
AP Eminence Director
jenniwright@deloitte.com

Sanjukta Mukherjee
AP Head of Research
sanjumukherjee@deloitte.com

Tory Rowley James
Senior Manager
trowleyjames@deloitte.com.au

Maud Dumont
Senior Analyst
madumont@deloitte.com.au

Dominic Behrens
Analyst
dobehrens@deloitte.com.au

Tara Naidu
Analyst
tarnaidu@deloitte.com.

Angela Watzdorf
Analyst
awatzdorf@deloitte.com.au

Deloitte.

Designed by CoRe Creative Services. RITM1974548