

從 AI 治理到提升企業競爭力

首席顧問：利錦文

解決企業痛點・完整解決方案・符合經濟效益



《人工智慧基本法》正式施行

2026 年 01 月 14 日

台灣首部 AI 專法正式上路

■ 核心定位：台灣 AI 治理的根本大法

確立了台灣在人工智慧發展與應用的基本原則，為後續各項具體法規與標準提供最高指導方針。

■ 關鍵影響：兩年內完成子法修訂

優求各部會（例如：金管會、衛福部、數發部）必須在兩年內，依據基本法精神完成相關子法與產業指引的制定或修正。

主管機關權責

行政院國家人工智慧戰略特別委員會

（院長召集，統籌協調國家人工智慧事務）

國科會（中央主管機關）

統籌AI事務、科研預算、政策方向

數位發展部（技術治理）

制定風險分類框架，評估驗證工具

各目的事業主管機關（金管會、衛福部、勞動部、經濟部、交通部.....）

依據風險分類框架，再各自管轄領域訂定具有法律拘束力的管理規範。

七大核心治理原則

01



永續發展與福利

確保 AI 發展促進社會共好、環境永續，並提升人類整體福祉。

02



人類自主

AI 系統應輔助而非取代人類決策，保障人類的自主權與尊嚴。

03



隱私與資料治理

嚴格保護個人資料，建立完善的資料治理機制，防止濫用與外洩。

04



安全與韌性

確保 AI 系統具備抵禦攻擊的能力，並在異常情況下維持安全運作。

05



透明性與可解釋性

AI 系統的運作邏輯與決策過程應具備適當的透明度。

06



公平與不歧視

避免 AI 系統產生或加劇偏見，確保所有群體獲得公平對待。

07



問責

明確界定開發者、部署者與使用者的責任歸屬，確保可追溯性。

風險分級框架 — 企業合規的核心



高風險應用

應用場景

- 醫療診斷與輔助決策
- 自動駕駛與交通控制
- 金融徵信與信用評分

企業應對行動

- ✓ 強制合規審查與第三方驗證
- ✓ 導入 ISO/IEC 42001 標準



中風險應用

應用場景

- AI 客服與對話機器人
- 生成式內容與行銷文案
- 內部流程自動化系統

企業應對行動

- ✓ 落實透明度標示 (標示為 AI)
- ✓ 建立人工介入機制 (HITL)



低風險應用

應用場景

- 垃圾郵件與惡意訊息過濾
- 遊戲 AI 與娛樂應用
- 基礎文書排版與潤飾工具

企業應對行動

- ✓ 企業內部自律管理
- ✓ 遵守一般個資與資安規範

ISO/IEC 42001 — 企業合規的國際標準避險方舟



AI 管理系統 (AIMS)

ISO/IEC 42001 是全球首個針對人工智慧管理系統的國際標準。它提供了一個結構化的框架，協助組織在開發、提供或使用 AI 系統時，能夠負責任地管理相關風險。

透過建立 AIMS，企業能有效應對 AI 帶來的倫理、透明度與安全性挑戰，並將法規要求轉化為標準化的內部流程。

台灣推動現況與進展



驗證標準確立

ISO/IEC 42006 已於 2025 年 7 月發布，為驗證機構提供明確的審查準則，依據組織角色進行稽核。



首家企業取得認證

翱騰國際科技於 2026 年 1 月正式取得 RvA 認證，成為台灣第一家通過 ISO/IEC 42001 認證的企業。



企業行動建議

系統導入通常需要 6 至 12 個月，建議企業應立即啟動 AI 系統盤點、風險分級與 AIMS 導入計畫。

當 AI 進入競爭力公式

How AI Reshapes Create × Satisfy

競爭力

=

創造顧客

+

滿足顧客

×



AI

AI 不是新增一欄應用 — 而是讓公式本身加速運轉的催化劑

總覽：AI 在兩側的作用地圖

每項傳統工作都有對應的 AI 升級路徑

🎯 創造 × AI

洞察需求

→ 搜尋 / 社群 / 行為 LLM 分析

價值創新

→ 生成式設計、合成使用者測試

市場開拓

→ ICP 建模、個人化落地頁

試驗迭代

→ 自動 A/B、Bandits、AI 實驗員

❤️ 滿足 × AI

品質可靠

→ AI 視覺品檢、異常偵測

交期準確

→ 需求預測、動態排程、預測性維護

服務用心

→ RAG 知識庫客服、情感分析

持續改善

→ 自動根因分析、客訴分類聚類

資料飛輪：AI 如何讓兩側互相強化

每一次顧客互動都產生資料；資料訓練模型；模型讓下一次創造與滿足更精準



飛輪怎麼轉

① 創造吸引顧客

AI 幫你找對客群、講對故事

② 互動產生資料

每一次點擊、對話、交易都是訊號

③ 滿足兌現承諾

AI 品檢、預測維護、AI 客服

④ 學習回饋模型

新資料 → 再訓練 → 下一輪更準

沒有資料 → 沒有飛輪 → AI 只是工具，不是競爭力。

從「猜需求」到「算需求」

創造顧客的瓶頸向來是「資訊」——AI 大幅降低了取得與處理顧客真實訊號的成本

議題	AI 之前 (憑感覺)	AI 之後 (用資料)
需求發現	焦點團體、年度調查、業務直覺	百萬則評論 / 搜尋 / 對話的 LLM 摘要與分群
原型設計	一次迭代 4-8 週、依賴少數設計師	AI 生成方案、合成用戶、當天完成多輪
市場定位	依歷史市占與人口統計	ICP 模型、個人化內容、動態區隔
實驗文化	大賭注、怕失敗、慢驗證	自動化 A/B 與 Bandits，以速率取代直覺

四大行動怎麼配 AI



洞察未被滿足的需求

AI 工具：LLM 摘要、社群 / 評論爬蟲、搜尋量趨勢、客服對話分群

把「聽到一兩個聲音」變成「聽到整個市場」



創造新的價值主張

AI 工具：生成式設計、設計變體 A/B、合成使用者訪談、原型生成

在進實體打樣前，先在數位空間跑 100 次



開拓新市場與區隔

AI 工具：ICP 分群模型、LLM 在地化、動態個人化落地頁、潛客評分

針對每個客群都像是「為你量身打造」



持續學習與試驗

AI 工具：自動 A/B、Multi-armed bandits、AI 實驗員、feature flag + AI

實驗速率從一季 2-3 次，變成一週 20 次

從「被動反應」到「主動預測」

滿足顧客的瓶頸是「即時性」與「一致性」——AI 把兩者同時拉到 24/7 × 全數檢查的水準

議題	AI 之前 (反應式)	AI 之後 (預測式)
品質控制	抽樣檢驗、客訴後才發現	AI 視覺全檢、異常即時警示
設備維護	定期保養、壞了再修	預測性維護、故障前就換料
顧客服務	營業時間回覆、標準話術	24/7 AI 客服、情感辨識、個人化回應
問題改善	月報、季報、RCA 要開會	客訴自動分類 / 聚類 / 生成根因假設

四大面向怎麼配 AI



品質可靠

AI 工具：AOI + 深度學習、製程參數最適化、異常偵測、統計 + ML 雙軌

從「抽樣檢」升級為「全檢 + 早期警示」



交期準確

AI 工具：需求預測、動態排程、預測性維護、物流路徑最適化

準交率提升、呆滯庫存與加班同步下降



服務用心

AI 工具：RAG 知識庫客服、語音轉文字 + 情感分析、個人化推薦

7×24 一致回應、複雜案件平順轉真人



持續改善

AI 工具：客訴自動分類 / 聚類、AI 產生 RCA 假設、趨勢異動警示

改善週期從「月」縮短到「當週」

AI 成熟度 × 競爭力的三個階段

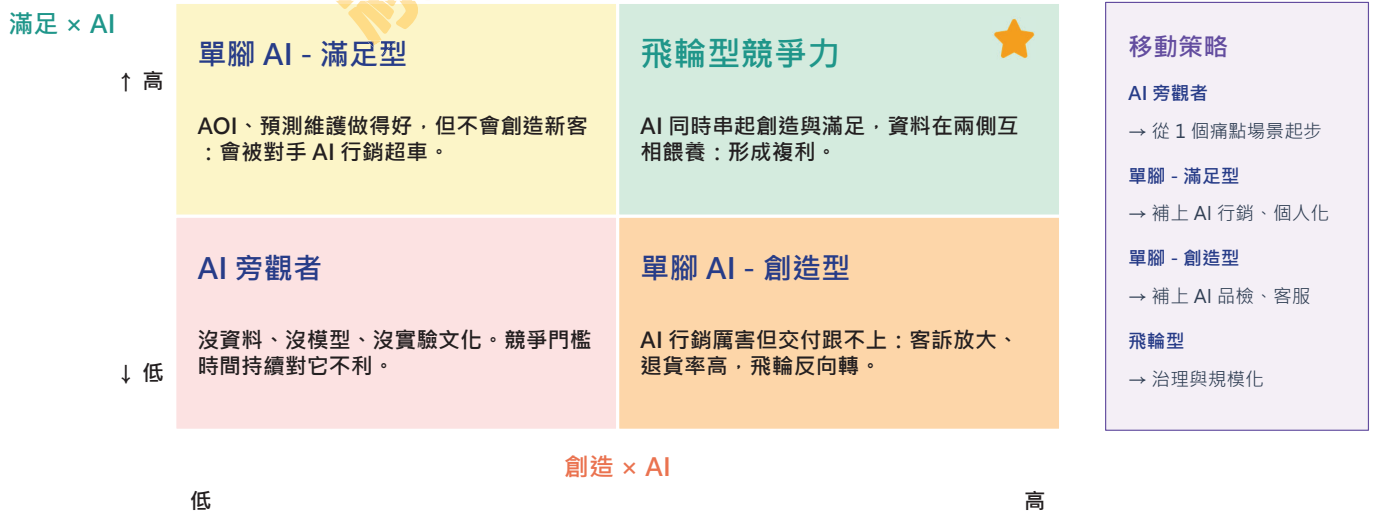
每一階段帶來不同深度的競爭力——也對應不同的組織準備度要求

STAGE 1 規則型	STAGE 2 預測型	STAGE 3 生成 / 代理型
<i>Rule-based</i> 依專家規則與統計模型；人訂條件、機器執行。 創造側： 問卷分析、簡單 RFM 滿足側： SPC 管制圖、規則式 AOI	<i>Predictive</i> 以歷史資料訓練 ML；機器學出「會發生什麼」。 創造側： 需求預測、流失預警、個人化推薦 滿足側： 預測性維護、品檢 CNN、動態排程	<i>Generative / Agentic</i> LLM 生成內容與方案；AI Agent 自主決策與行動。 創造側： 自動撰寫、合成用戶、LLM 分群 滿足側： RAG 客服、AI 填單、Copilot 改善

競爭力深度：效率優化 → 差異化 → 結構性領先

2×2 升級：AI 如何把組織往右上推

關鍵不是「有沒有 AI」，而是「AI 有沒有串起兩側」



AI 帶來的新風險與失敗模式

AI 放大公式的正向效果，同時也放大負向效果——治理必須同步



幻覺傷信任

LLM 一句話講錯，顧客對整個品牌的信任打折。

滿足側風險



偏誤誤判市場

訓練資料有偏差 → 看錯客群、誤判需求方向。

創造側風險



模型漂移

資料分布變了，模型沒再訓練：品質與預測悄悄衰退。

兩側皆有



過度自動化

全流程無人化後，複雜案件無人承接，失去「人的溫度」。

滿足側風險



資料外洩與合規

顧客資料進入模型訓練、跨境傳輸：GDPR / 個資法 / AI Act。

治理風險



單點依賴

鎖死在單一模型供應商：一旦漲價、停服或策略變，整條飛輪卡住。

策略風險

所有上線模型都要有「監控 + 人在迴路 + 治理」——這是 AI 時代的新 ISO。

指標升級：AI 時代要量什麼

除了業務指標，還要量「AI 的運轉狀態」與「飛輪的旋轉速度」



創造側 (AI 加持後)

Insight-to-action 週期

資料 → 決策的時間

實驗速率 / 月

一個月跑幾次 A/B

個人化覆蓋率

多少 % 流量走 AI 分群

新客 AI 佔比

AI 貢獻的新客比例



滿足側 (AI 加持後)

預測準確度

需求 / 故障預測命中率

首問解決率 (AI)

AI 客服一次解決比例

全檢覆蓋率

AI 品檢的產品 %

平均回應時間

從顧客問到收到回覆



飛輪 / AI 健康度

模型上線數 / 在用數

落地規模

模型漂移率

效能衰退速度

資料覆蓋率

可訓練資料 / 全場景

AI 治理事件數

異常、客訴、合規

把 AI 嵌入公司的五項準則

這些原則比選哪個模型、哪家廠商重要十倍

- | | | |
|----|---------|-----------------------------------|
| 01 | 先資料、後模型 | 沒有好資料，就沒有好 AI。資料品質、標籤與平台是前置工作。 |
| 02 | 兩側並進 | 不能只做一邊。AI 行銷沒品質守不住口碑；AI 品檢沒客流沒人買。 |
| 03 | 人機協作 | AI 做大量、重複、即時的判斷；人做例外、創意與責任的判斷。 |
| 04 | 治理同步上線 | 模型上線的同一天就要有監控、人工覆核與回退機制。 |
| 05 | 飛輪思維 | 每個 AI 專案都問：它產出的資料有沒有回饋下一輪？ |

AI 產業變化已由技術展示走向落地應用

自動化 AI

2016年以前

- 取代重複性作業。
- 導入對象多集中於大型企業或標準化程度高的產業。

預測型 AI

2017-2022年

- 應用延伸至需求預測、品質檢測等情境。
- 多數中小企業仍面臨成本高、人才不足等限制。

生成式 AI

2023年-未來

- 基礎模型與通用工具成熟。
- AI 可支援內容生成、知識問答、流程協作與任務執行。

企業關注焦點已由「要不要導入 AI」轉為「如何更快找到可用情境並完成驗證」。

AI 推動重點在建立多數企業都能進入的支持機制

國際經驗的共同點，不在技術展示，而在讓更多企業敢進入、能試做、可複製

01



先降低導入門檻

應從企業可理解、可低成本試行的應用場景切入

02



建立顧問陪跑機制

透過需求診斷、工具導引與試作驗證，降低導入不確定性

03



形成持續擴散模式

由單次培力走向落地應用，並透過案例與網絡帶動後續擴散

中小企業 AI 導入現況及面臨共同挑戰

中小企業家數

171.6 萬

占全體企業 98.87% 以上

就業人數

919.4 萬

占全國就業人數近 8 成

AI 導入率

7.4%

明顯低於大型企業

缺乏 AI 人才

84.5%

導入能量仍待補強

中小企業特性



企業樣態差異大

從偏鄉小微企業、地方特色產業，到小巨人與磐石企業



決策與執行高度集中

多由經營者或少數核心人員同時負責決策與執行



痛點不易明確化

往往知道要轉型，但不易具體說出優先導入場景

面對樣態多元、決策集中的中小企業結構，政策推動重點在於提供可理解、可試行、可驗證的導入支持。

資料來源：2025 年中小企業白皮書

現階段推動做法與成果

透過三類措施，推動中小企業由理解 AI 走向驗證與擴散

策略一



建立基礎能力

讓企業「知道從哪裡開始」

先讓企業看得懂 AI、知道從哪裡開始

- 中小企業網路大學校 AI 課程
- 基礎 AI 工具實作課程
- AI 快診與場景盤點

策略二



推動應用落地

讓企業「用得起 AI、看得到成效」

讓企業先做小型驗證，降低導入風險

- 產業場域實作教案
- 法人實作專班
- 顧問陪跑機制

策略三



促進生態擴散

讓企業「用 AI 創造價值」

把已驗證的做法，透過公協會、地方網絡與案例交流擴散到更多企業

- 公協會帶動擴散
- 地方服務網絡串接
- 主題式產業 AI 推動

基本法給產業的政策工具

不只是原則宣示，而是有法源依據

財政補助與獎勵

AI基本法第8條

政府應積極推動 AI 研發、應用及基礎建設，辦理補助、委託、出資、獎勵、輔導等措施，彙整年度成效報告制度。

租稅優惠

產創條例第10-1條（已三讀）

AI產品或服務納入投資抵減項目，支出金額上限提高至18億元，適用期延長至118年底。企業投資AI可直接抵減營所稅。

創新實驗環境（沙盒）

AI基本法第9條

各目的事業主管機關得建立AI創新實驗環境，鬆綁學術研究限制。研發階段不適用高風險問責規定（第17條）。

資料共享機制

AI基本法第13條

政府應建立資料開放、共享級再利用機制，提升 AI 使用資料的可利用性。去識別化產業資料共享可破解中小企業數據不足的困境。

這些工具已有法源基礎，不再只是政策宣示－企業應主動盤點可用資源

台灣各產業的應用地圖

金融業

導入率 58%

智慧客服、反洗錢偵測、信用評分、理賠自動化。

高風險 (涉及個人權益自動化決策)

製造業

導入率 45%

AOI影像檢測、預測性維護、製程優化、能源管理

中~高 (大廠深入、中小廠觀望)

科技業

導入率 39%

晶圓缺陷檢測、良率預測、AI資安

中 (本身為AI供應鏈)

醫療業

導入率 —

眼底病變、腦出血辨識、胸腔X光篩檢

高風險 (法規門檻最高)

零售業

導入率 28%

聊天機器人、商品推薦、行銷文案生成

低~中 (多用現成雲端工具)

四大核心場景總覽

製造業運用 AI 的關鍵在於解決現場痛點，而非為了導入而導入。



智慧檢測

品質控制 AI-AOI

深度學習視覺模型
降低漏檢率與過殺率



預測性維護

Predictive Maintenance

IoT 感測器 + AI
最大化零件使用壽命



製程最佳化

永續轉型

黃金參數組合
降低碳排與能耗



供應鏈韌性

動態排程 APS

精準銷售預測
提升準時交貨率

政府 AI 補助全景

2026 年政府各部會釋出多項 AI 研發與轉型補助



經濟部技術司 | 科專補助 156 億元

聚焦五大信賴產業與 AI 新十大建設，推動深科技與前瞻技術研發，厚植國家 AI 基礎實力。



經濟部產發署 | 韌性特別預算研發轉型

針對製造業與科技業提供實質補助，個案最高補助 500 萬元、聯盟型計畫最高可達 4,000 萬元。



經濟部商業署 | 服務業 AI 升級方案

提供多層次補助：單店最高 10 萬元、連鎖型業者最高 300 萬元、企業整合型最高 2,000 萬元。



經濟部中企署 | 中小企業網路大專校計畫

降低微型企業轉型門檻，單一企業最高補助 15 萬元、聯合申請最高可達 30 萬元。

企業行動建議

建構跨領域風險治理能力：既懂 AI 七大原則，也懂 S2 四大支柱

1

盤點 AI 應用風險

檢視內部已導入的 AI 工具（探盤查、ESG 數據蒐集、授信評估等），對照風險分類框架進行自評。

2

整合雙框架揭露

將 AI 治理納入 S2 的「治理」與「風險管理」支柱揭露，說明 AI 技術部屬如何影響探排績效。

3

培養 AI 治理人才

董事會層級需要有人同時掌握 AI 法規、氣候變遷與財務揭露邏輯，跨領域而非單一部門。

4

建立資料治理機制

依第13條建立資料共享與再利用機制，同時確保 S2 所需的範疇三數據品質與一致性。

AI 不改寫公式，它改寫公式的速度

創造 × 滿足 依然是本質；AI 讓這條公式 24/7 不停轉，且每轉一次都更準。

CREATE × AI

01

找一個「猜需求」痛點

導入 LLM 輿情 / 分群，把一週的洞察變成每天的洞察。

SATISFY × AI

02

找一個「被動回應」痛點

導入預測或 AI 客服，把修復從事後變事前。

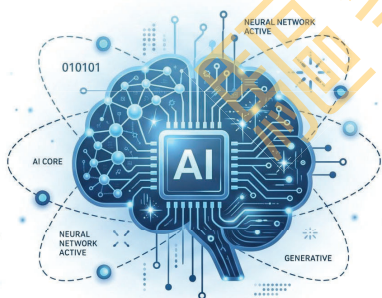
FLYWHEEL

03

把兩側的資料接起來

建立顧客 360° 資料流，讓滿足資料回饋創造模型。

$$\text{競爭力} = (\text{創造顧客} + \text{滿足顧客}) \times \text{AI}$$



謝謝聆聽



如有任何問題，歡迎隨時提問