AISO AI for Sovereignty

企業 AI 基礎設施的 2027 決策指南 執行摘要

在決定買什麼之前，先確認我們該問什麼

企業 AI 專案的成敗不在模型，在治理 —— 而治理無法事後補上。

17%

已實際部署 AI Agent 的組織，相對於兩年內計畫部署的逾 60%

Gartner 2026 CIO 調查

40%

將因生產事故後才發現的治理缺口，而降級或停用自主 Agent 的企業

Gartner 2026 年 5 月

2027/12

歐盟高風險 AI 系統義務生效日

Regulation (EU) 2026/1744

卡住的不是執行力，是找錯了原因

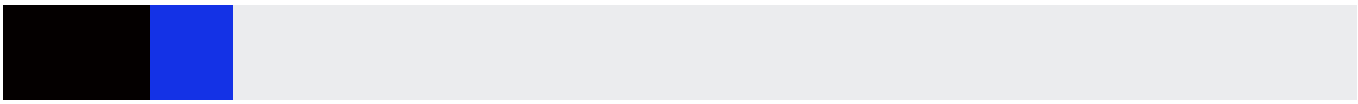
錢在暴衝，落地在停滯 — 而卡住的地方不在模型。

全球企業｜Gartner 2026 CIO 調查，受訪者為企業 IT 決策主管

兩年內計畫部署 AI Agent **>60%**



已實際部署（■ 色段為生產就緒的11%） **17%**



Gartner 2026 CIO 調查；Deloitte，2026

在地對照

台灣 230 家前 2000 大企業中，**74%** 正積極規劃或推動 AI 專案，但只有 **48%** 進入部門級試點或生產環境；另一份調查顯示 **56%** 仍將安全、合規與隱私視為擴大 AI 的主要限制。

Nutanix 委託 DIGITIMES 執行，2026 年 7–9 月；Dell 2026 現代化企業就緒度調查（台灣）。
兩份皆為廠商委託調查。此處 48% 與上方 17% 定義不同，不可直接相比。

當我們的 AI 專案停在試點、遲遲無法進入正式環境，這並不罕見，多數企業都卡在同一段路上。

回頭看那些被取消的 AI 專案，原因反覆是同樣三項：**成本失控、商業價值說不清楚、風險控制不足**。
沒有一項是模型不夠強。

治理的缺口通常不會在試點階段出現，往往要等到正式上線、出了事才被發現。
Gartner 預估到 2027 年，約四成企業會因治理不足衍生的資安風險，因此降級或直接停用自主 Agent，到那時才補，代價最高。

所以下一步最值得投入的，未必是更強的模型，而是在擴大導入之前，先把治理放進規劃。

三股控制不了的外力

它們分別回答：為什麼該做、為什麼是現在、不做的後果何時到期。

推論經濟

233億美元

2026 年全球推論支出，首度超越訓練的 190 億。

推論是穩態負載，適合擁有而非租用。以公有雲為主要推論環境的企業比例，一年內從 56% 降至 41%。

記憶體供給

+125%

2026上半年伺服器成本漲幅。

約七成記憶體產能流向 AI 資料中心，報價窗口縮短至 1–30 天。
今年核定的預算，執行時可能只買得到七成規格。

法規時鐘

2028/01

台灣各目的事業主管機關完成法規調適的期限。

規範要的不是政策宣示，是證據。而證據不能事後回溯補 —— 2027 年是準備年，不是觀望年。

2026/01
台灣《人工智慧基本法》施行

2027/12
歐盟高風險 AI 規範開始適用

2028/01
台灣各部會產業規範完成

哪些 AI 會被要求說明與留痕？

依《人工智慧風險分類框架》，若 AI 應用可能**對國家安全、人民基本權利、生命安全、財產保障、社會秩序或生態環境**造成嚴重危害，主管機關應認定為高風險應用。

判斷以應用本身的客觀特性為準 —— 只要有造成危害的可能即成立，不以實際發生損害為必要。
對我們而言，這代表不能等到出事才確認。
盤點時，就要先找出哪些應用可能落入這個範圍，以及需要為它們保留哪些紀錄。

Gartner, 2026/08；Gartner／TrendForce, 2026；人工智慧基本法；Regulation (EU) 2026/1744

三股力量的時間軸不同，最後卻落在同一件事上：我們 2027 年的導入計畫與預算。
推論每天都在跑，AI 的成本會從一次性的專案支出，變成固定的營運支出。記憶體的供給緊縮是結構性的，延後採購，同樣的預算只會買到更少。法規則是三者中唯一有確定日期的，它要的是最難臨時補齊的東西 —— 證據。

三條路，同一個缺口

沒有一條路徑把治理與稽核證據當作預設交付內容。

公有雲、自建、整合式方案各有真實的優勢，但它們缺的是同一樣東西：治理與稽核證據。

	公有雲	自建	整合式方案
快速起步	●	○	◐
資料主權	○	●	●
成本可預測	○	◐	◐
供給穩定性（2026–27）	●	○	◐
治理內建	○	**需自建**	**多為選配**
稽核證據可交付	○	**需自建**	**需自行設計**

整合式方案：由單一廠商預先整合硬體與軟體、交付到第三方專業託管機房並自行管理。

● 具備 ／ ◐ 部分具備 ／ ○ 不具備

三條路各有真實優勢。
公有雲起步最快，適合仍在驗證的應用；自建的控制權最完整；整合式方案成熟且供應鏈穩固。

但最後兩列是關鍵。
它們或者不提供治理，或者要求採用方自行建構 —— 而依前述四成企業降級或停用代理的數據，這恰好就是原因。

前面提到，Gartner 預估約四成企業會因上線後才發現的治理缺口，而降級或停用自主 Agent。這類缺口最常出現的地方，就在這兩列：**治理沒有內建，稽核證據也得由我們自己設計**。

這並非哪一家廠商的疏失。多數方案的設計起點是「如何讓 AI 跑起來」，AI 治理則常被留給採用方自行補上。但上線之後，要向董事會、主管機關與客戶交代的，是我們。

因此比較方案時，我們需要把 AI 治理列為與效能、成本同等重要的評估項目。
下一頁的八個問題，就從這裡開始。

那我們該問的是另一組問題

當 AI 從回答問題變成代替我們執行，要問的就不只是規格。

上一頁的三條路，缺的都是同一層。
既然如此，我們評估供應商該問的問題，也得跟著換。

過去我們問的	2027 年我們該問的
這台機器能跑多大的模型？	六個月後，我們還能還原某一次 AI 輸出的完整依據嗎？
每 Token 多少錢？	我們看得到哪個部門、哪個 Agent 花了多少，並設上限嗎？
支援哪些模型？	換模型需要停機嗎？我們會不會被單一供應商綁定？
有沒有 RAG 功能？	回答能不能附出處？文件更新後會不會還拿舊版回答？
資料存在哪裡？	哪些資料絕對不出企業網路，是強制執行還是設定選項？
有沒有權限管理？	不同風險等級的 Agent，能套用不同強度的規則嗎？
這個 Agent 能做什麼？	這個 Agent 不能做什麼，是由誰、用什麼方式強制？
什麼時候可以交機？	報價有效期是多久？價格調整機制是什麼？

右欄這八題問的都是**「能不能證明營運績效」**，而不只是「有沒有這個功能」。
這些答案都不在規格表上，而在 AI 被管理的方式裡。也正是在這裡，許多企業踩進同一個誤區。

不是所有 Agent，都該用同一套規則

共用一套底座，但依風險分級訂規則。

最常見的誤區，是讓所有 Agent 套用同一套規則。
訂得太鬆，高風險的 Agent 會失控；訂得太嚴，低風險的應用也推不動。

《人工智慧風險分類框架》也已將代理超出授權範圍列為風險類型 B6「AI 自主代理之授權外行為」：Agent 可能在目標不完整或環境改變時，逐漸偏離原始的指令，甚至取得超出授權的權限；多個 Agent 系統更可能因彼此觸發，引發沒有人預料到的連鎖反應

要同時避開這兩種結果，可行的做法是把「共用的部分」與「分開的部分」拆成兩層。。

上層：所有代理共用

控制平面（統一）

一套身分體系・一套稽核事件格式・一套用量與成本帳本・一個政策執行點

下層：依風險分級管理

L1 只看不動	L2 會動到內部系統	L3 代表公司對外行動
檢索、問答、摘要	寫入內部系統、產生正式文件	對外通訊、觸發交易、跨組織委派
資料範圍限制 輸出附出處	具名核准人 寫入前預覽、可回溯	逐筆核准 額度上限、雙人覆核

底座統一，才看得見全部；規則分級，才管得住風險。

這個分級和各國法規的風險分級邏輯是同一套，合規可以建立在同一個結構上。
不過這些都需要時間 —— 好消息是，這些都不必等到採購完成才能開始。

不必買任何東西
現在就能開始的四件事

無論最後選擇哪一條路徑，
我們都可以先完成以下四項盤點，作為 2027 年導入規劃的基礎。

依《人工智慧基本法》第 16 條授權訂定之《人工智慧風險分類框架》（數位發展部，2026 年 7 月）所列風險類型整理，對應其中 A2 缺乏透明性或可解釋性、A5 影響隱私與違反個資法規、B6 AI 自主代理之授權外行為等項目。

- [ ] **AI 系統盤點**
  公司裡到底有哪些 AI 正在被使用？包括各部門自行採購的工具。
  第一階段
  輸出：一份 AI 系統清冊

- [ ] **資料分級**
  哪些資料可以交給 AI 使用？界線由系統把關，還是靠大家自律？
  第二階段
  輸出：分級標準與強制執行點清單

- [ ] **AI 權限現況**
  Agent 的限制寫在權限設定裡，還是只寫在提示詞裡？
  第三階段
  輸出：Agent 風險分級表

- [ ] **稽核軌跡缺口評估**
  如果明天被要求說明，我們拿得出紀錄嗎？
  第四階段
  輸出：缺口清單與補救優先序

稽核缺口的三個測試題

1. 三個月前某一次特定輸出，是由哪個模型、依據哪些資料產生的？
2. 過去一個月，各部門的 AI 用量與費用分別是多少？
3. 某位員工在特定日期使用 AI 存取了哪些資料？

答不出來的題目，就是我們最該先補的地方。

這四項不需要先做採購決策就可以開始，而且做完之後，任何採購評估的品質都會提高。

如果只記得三件事

01 讓 AI 真正上線的關鍵，往往不在模型，而在我們管不管得住它。

02 法規要看的是證據，而證據只能從今天開始累積。

03 在決定買什麼之前，先確認我們想要什麼。

我們可以先從第 7 頁的四項盤點開始，再依目前的評估進度，選擇以下資源。

還在評估階段

看看三種實踐方式與完整脈絡

aisoportal.com

想看具體方案

AISO 一體機：依產業情境的方案選擇

aisoportal.com/bundled-solution

AISO 是 AI for Sovereignty 的縮寫。
AI 代理技術仍在快速演進，治理的方法也還在成形。現階段的最佳實踐，並非一套固定不變的標準。我們必須持續檢視自身的業務需求與核心競爭力，據此建立適合自己的治理方式。

技術會一直升級。能不能為它負責，才是留下來的那個問題。

service@aisoportal.com