AI GOVERNANCE FRAMEWORK

企業 AI 治理檢查表

Enterprise AI Governance Checklist

10 項 AI Governance Checklist，快速檢視企業 AI 治理成熟度。
在導入 ChatGPT、Claude、Gemini 或各種 AI Agent 之前，先確認您的企業是否具備足夠的治理能力。

10	20	3–5
治理檢核構面	滿分級距	分鐘完成評估

你的企業真的準備好導入 AI 了嗎？

越來越多企業開始使用 ChatGPT、Claude、Gemini 或各種 AI Agent 提升工作效率，但如果缺乏治理機制， 也可能面臨資料外洩、權限濫用、成本失控及法規遵循等風險。

本檢查表協助企業快速評估目前 AI Governance（AI 治理）成熟度，了解哪些能力已建立、哪些仍有改善空間。

完成時間：約 3–5 分鐘

評分方式

每一大題（共 10 大題）底下列出數個檢核小項，請依「實際勾選的小項目數量」換算為該題分數：

評分	說明
2 分	已完成，並持續執行（該題多數小項皆已勾選）
1 分	已開始推動，但尚未完善（該題部分小項已勾選）
0 分	尚未建立（該題小項皆未勾選）

註：每一大題下方皆附有對照換算標準（例如「勾選 3–4 項 = 2分」），10 大題加總即為總分。

總分：20 分

1 是否建立企業 AI 使用政策？

- [ ] AI 使用規範（AI Usage Policy）
- [ ] 明確定義可使用的 AI 工具
- [ ] 員工了解哪些資料不可輸入 AI
- [ ] 定期更新 AI 使用政策

目的：建立一致的 AI 使用原則，降低 Shadow AI（未經授權的 AI 使用）風險。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

2 是否建立 AI 身分與權限管理？

- [ ] AI 平台統一登入
- [ ] API Key 集中管理
- [ ] 不同部門採不同權限
- [ ] 離職或異動人員可立即停用權限

目的：避免權限濫用與 AI 憑證外洩。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

3 是否保護企業敏感資料？

- [ ] 禁止輸入客戶個資
- [ ] 禁止輸入商業機密
- [ ] 禁止輸入原始碼
- [ ] 建立資料分類規範

目的：降低資料外洩與機敏資訊暴露風險。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

4 是否能追蹤 AI 使用紀錄？

- ☐ 使用者紀錄
- ☐ 使用模型紀錄
- ☐ 使用時間紀錄
- ☐ Token 使用紀錄
- ☐ 操作稽核（Log）

目的：建立完整 Audit Trail，符合企業內控與稽核需求。

評分對照：勾選 4–5 項 = 2分｜1–3 項 = 1分｜0 項 = 0分

5 是否管理 AI 使用成本？

- ☐ Token Cost 統計
- ☐ 各部門成本分析
- ☐ 模型成本比較
- ☐ 成本異常通知

目的：避免 AI 使用成本快速增加而無法追蹤。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

6 是否建立 AI 安全防護？

- ☐ Prompt Injection 防護（提示詞注入攻擊，惡意指令偽裝操控 AI）
- ☐ Jailbreak 防護（越獄攻擊，誘導 AI 繞過安全限制）
- ☐ 惡意 Prompt 偵測
- ☐ AI 回覆內容安全檢查

目的：降低 AI 遭受攻擊或輸出不當內容的風險。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

7 是否管理 AI Agent 可存取的資源？

- [ ] 採用 Least Privilege（最小權限原則）
- [ ] AI Agent 僅能存取授權系統
- [ ] 可限制工具（Tools）與 MCP Server 存取
- [ ] 可隨時撤銷 AI Agent 權限

目的：避免 AI Agent 擁有過度權限而造成橫向風險。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

8 是否集中管理 AI 模型？

- [ ] ChatGPT
- [ ] Claude
- [ ] Gemini
- [ ] 開源模型
- [ ] 其他 AI 平台皆可統一管理

目的：避免各部門自行管理模型，造成治理困難。

評分對照：勾選 4–5 項 = 2分｜1–3 項 = 1分｜0 項 = 0分

9 是否符合企業治理與法規需求？

- [ ] AI 使用可追蹤
- [ ] 操作紀錄可保存
- [ ] 具備稽核能力
- [ ] 符合企業內控或法規要求

目的：建立可治理、可追溯、可稽核的 AI 環境。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

10 是否持續監控 AI 風險？

- [ ] 異常 Token 使用警示
- [ ] 未授權模型使用警示
- [ ] 異常操作偵測
- [ ] AI 安全事件監控

目的：從被動管理提升至持續性風險監控。

評分對照：勾選 3–4 項 = 2分｜1–2 項 = 1分｜0 項 = 0分

評分結果

18–20

AI Governance Leader

恭喜！您的企業已建立完整的 AI 治理能力，建議持續優化治理流程，並擴展至更多 AI 應用與 AI Agent 場景。

14–17

AI Ready

已具備基本 AI Governance 架構，但部分能力仍有改善空間，例如權限管理、稽核紀錄或成本管理。

8–13

Need Improvement

企業已開始導入 AI，但治理機制尚未成熟，未來可能面臨資料外洩、權限管理及 AI 成本控制等挑戰。

0–7

High Risk

目前 AI 使用缺乏必要治理能力，建議優先建立 AI Governance Framework，再逐步擴展 AI 應用。

建議優先改善方向

如果您的分數低於 14 分，可優先建立以下能力：

- 建立企業 AI 使用政策
- 集中管理 AI 存取權限與 API Key
- 建立 AI 操作稽核與 Audit Trail
- 導入 Prompt Guardrails
- 管理 Token 使用成本
- 建立 AI Agent 最小權限機制
- 建立 AI 安全監控與異常警示

ACROSS 如何協助企業建立 AI Governance？

企業 AI 治理不只是限制 AI 的使用，而是在確保安全與合規的前提下，讓 AI 能夠被有效管理、持續使用並創造價值。 ACROSS 提供企業所需的核心治理能力，協助企業在不影響使用效率的情況下， 建立兼顧安全、治理與營運效率的 AI 管理架構。

AI Gateway
多模型統一管理

RBAC
Role-Based Access Control

Virtual Key
虛擬金鑰管理

Prompt Guardrails
提示詞安全防護

Audit Trail
AI 操作稽核

Token Cost Analytics
成本分析儀表板

AI Agent 權限控管
最小權限存取

安全事件監控
即時風險警示

Governance Dashboard
治理儀表板

極風雲創（股票代碼 7826）是台灣專注於全域安全與企業 AI 治理的解決方案供應商，整合國際頂尖資安品牌，打造從網路層到 AI 使用層的完整防護架構。我們以資安基因驅動自研平台 Across，協助企業安全導入 AI、建立合規治理機制。

讓 AI 成為企業的生產力，而不是新的風險來源。

算完分數了嗎？讓 Across 協助您補齊治理缺口

預約免費 30 分鐘 AI 治理健檢，我們將依據您的檢查表結果，提供客製化的改善建議與導入規劃。

立即預約諮詢 →