aitokenking

AI • TOKEN • KING

企業 AI 導入
合規解決方案提案書

從採購發票、資料脫敏到內控標準
為金融機構與企業客戶量身打造的 AI 治理架構

適用對象：金融機構 • 交易所 • 受監理產業 • 上市櫃企業

aitokenking

企業級 AI 聚合與合規服務平台

aitokenking.com.tw

文件版本 • v1.0

2026 年 4 月

00 目錄

本提案書整合企業導入 AI 過程中最常遭遇的三項合規難題，並提出可立即落地的整合架構。

01 執行摘要 P. 03

02 三大企業合規難題現況分析 P. 04

03 解決方案總覽 · 三層治理架構 P. 05

04 難題一：代理商法律義務與發票責任 P. 06

05 難題二：脫敏與聚合平台架構選擇 P. 07

06 難題三：法規未到位的內控標準作業 P. 09

07 aitokenking 三重角色定位 P. 11

08 投資配置與方案比較 P. 12

09 實施建議與下一步 P. 13

10 附錄：國內外標準對照 P. 14

11 聯絡我們 P. 15

使用對象說明 ｜本提案書供企業採購、法務、法遵、資訊安全與資訊主管之內部評估使用。內容涵蓋產業最佳實務與在地法規參考，惟具體合約條款與法律意見仍應由企業內外部法律顧問審酌。

01 執行摘要

企業導入 AI 真正卡關的不是技術，而是採購流程、資料外洩風險與內控標準三條合規線。

EXECUTIVE SUMMARY

2024 至 2026 年間，台灣企業導入生成式 AI 的最大障礙並非技術選型，而是**採購合規、資料安全、內控治理**三條防線同時要過關。在《AI 基本法》尚未立法、個資法 AI 應用補強條款仍在研議的空窗期，企業必須自建可被律師、會計師、稽核單位採信的內控標準。

本提案針對企業實務上最常被問到的三大難題，提出一套整合性架構：以**「在地代理 + 技術加值 + 多模型聚合」**三重定位，補足原廠 Enterprise 方案在企業產品端嵌入 AI 的合規空缺。aitokenking 在此架構中同時承擔法律責任、技術執行與業務韌性三層角色，與原廠方案並存互補，協助企業以最低風險完成 AI 治理落地。

本提案三大核心主張

1

採購合規
用在地合約解決

透過在地代理商雙層合約架構，由本國法人開立統一發票、承擔個資法第 27 條委託機構責任，並提供中華民國法律管轄。

2

資料安全
用工程手段解決

透過前置脫敏層、Guardrails 與完整 Prompt 級稽核日誌，將法律承諾轉為可被驗證的工程實作，律師會計師可直接查核。

3

內控標準
用國際框架補位

在台灣法規尚未到位前，採 ISO/IEC 42001 、 27001 、 27701 與 NIST AI RMF 組合自律，建立企業可立即實施的 SOP。

適用對象

本方案專為對**合規敏感度高、需在地發票、有完整稽核需求**的企業設計，包括：金融機構、虛擬資產服務業（VASP）、證券期貨、保險、醫療、法律事務所、會計師事務所、上市櫃公司，以及任何處理客戶個人資料、商業機敏資料的企業。

02 三大企業合規難題現況分析

企業導入 AI 不是「買誰的 API」這麼單純，而是採購、合規、技術三條線同時要過關。以下三題是企業內部跨部門會議中最常出現的爭點。

難題一 ｜ 採購與發票合規

企業要導入 AI 工具，若直接向境外原廠（Anthropic、OpenAI、Google）訂閱，會立即遇到：**海外發票無法抵稅、合約準據法為境外、上市櫃供應商管理流程過不了、個資法委託機構責任無法明確歸屬**。對於需要正式採購流程的企業，這通常導致 PoC 做完後，正式採購階段卡住超過半年。

難題二 ｜ 資料脫敏與架構選擇

金融機構與交易所對「客戶資料不得進入 AI 模型」的紅線非常清楚。但**「自己做脫敏 + 用聚合平台 API」是否能取代原廠企業方案？**這是法遵與資訊主管最常爭論的問題。答案不是 Yes / No，而是要分清楚不同工作負載的特性，採取互補架構。

難題三 ｜ 法規未到位的內控標準

《個資法》尚未針對 AI 訓練資料外洩有明確規範；金管會 2024 年「金融業運用 AI 核心原則」僅為指導原則，無罰則細則；國科會《AI 基本法》草案仍在立法院。但**律師與會計師最在意的是：客戶資料一旦因 AI 應用外洩，民事賠償與信譽損害立即發生，不能等法律到位才動作。**企業必須自建一套可被獨立第三方採信的內控 SOP。

> ***核心觀察*** ｜ *三題看似獨立，實際上互相牽動。採購若沒在地化，個資法責任歸屬就有缺口；脫敏若沒工程實作，內控標準就只是紙上承諾；內控若沒國際標準對齊，律師會計師就無法簽字。三題必須一次解決。*

03 解決方案總覽 • 三層治理架構

本方案以三層架構整合企業 AI 治理：上層由企業自訂治理政策，中層由 aitokenking 執行技術加值，下層連接多家模型供應商。

▲ 治理層 | GOVERNANCE LAYER

企業自訂｜資料分級政策、AI 使用 SOP、稽核流程、廠商風險管理、ISO 42001 對應

◆ AITOKENKING 加值層 | VALUE-ADDED LAYER

核心

前置脫敏 • Guardrails • Prompt 級稽核 • 多模型路由 • 在地發票 • DPA 與在地法律管轄

▼ 模型層 | MODEL LAYER

多家供應商｜Claude (Anthropic) • GPT (OpenAI) • Gemini (Google) • 自架 Llama / Qwen • Embedding 服務

架構設計三大原則

原則	內容
互補不取代	原廠 Enterprise 方案保留給員工互動式使用，aitokenking 加值層服務企業產品端嵌入 AI，兩條路徑各司其職，合規鏈不斷裂。
分層解耦	政策層、技術層、模型層彼此獨立。模型供應商可隨業務需求切換，不影響上層治理政策；治理政策可演進，不影響底層技術實作。
可驗證	每一層都可被獨立稽核：政策可檢視、加值層可實測、模型供應商有 DPA 與承諾書。律師會計師可逐層查核，不留模糊空間。

AITOKENKING 的關鍵定位

原廠 Claude Enterprise 解決**員工「使用」AI** 的合規；
aitokenking 解決企業**產品「嵌入」AI** 的合規。
兩者並存，互補而非替代。

難題一 • PROCUREMENT

04 代理商法律義務與發票責任

企業向境外原廠採購 AI 服務，會在採購、財會、法務、法遵四個環節遭遇結構性阻礙。本節提出「在地代理 + 雲端代理合約」雙層解法。

企業實務痛點

層面	痛點細節
發票與會計	海外電子發票無法抵稅、無法走國內企業採購流程、會計帳上認列困難。
法律管轄	原廠合約準據法常為美國加州或愛爾蘭，台灣企業若有爭議幾乎無法主張。
個資法責任	境外原廠不易被認定為個資法第 27 條下可究責的「委託機構」，企業自負全責。
採購法遵	上市櫃、金融、政府標案要求供應商在地化、ISO 27001、可稽核合約對象。

解決方案 ｜ 雙層合約架構

由 aitokenking 作為在地代理，與企業簽訂中華民國法律管轄合約，承擔開票、合規、稽核責任；aitokenking 再向原廠承接技術服務並回溯部分義務。企業面對的法律對象單一、明確、在地。

代理商承擔的法律義務

義務類型	具體內容
個資法委託機構責任	個人資料保護法第 27 條、施行細則第 12 條規範之安全維護義務，包含資料保管、人員管理、設備維護、技術安全與事故通報。
統一發票開立	含營業稅、可抵扣、符合台灣會計處理流程，支援企業採購系統整合。
在地法律管轄	合約準據法為中華民國法律，第一審管轄法院為臺灣台北地方法院。
資料保護承諾	不將客戶資料用於模型訓練、不轉售、明定資料留存與銷毀政策、Zero Data Retention 條款。
稽核配合	配合企業內外部稽核、金管會檢查、提供 SOC 2 / ISO 27001 報告與必要文件。
損害賠償	明定服務瑕疵或資料外洩之賠償責任範圍與上限，並於合約中載明保險安排。

AITOKENKING 的角色

核心執行者｜不只是發票通道，同時提供難題二（脫敏與聚合架構）與難題三（內控執行）的技術加值層。
一份合約，同時解決採購、合規、技術三件事。

難題二 • ARCHITECTURE

05 脫敏與聚合平台架構選擇

「自己做脫敏 + 走聚合平台 API」是否能取代原廠企業方案？答案是可以並存，但角色要分清楚——對非敏感工作負載成立，對核心合規工作負載必須採互補架構。

三種架構比較

架構	適用情境	優缺點
A ｜ 純原廠 Enterprise	員工日常使用 chat、Claude Code	原廠 audit log 完整、合規鏈直接；無在地發票、單一模型、海外管轄。
B ｜ 純聚合平台 API	開發實驗、非敏感應用	多模型、成本優化、本地發票；若無專業脫敏層，等於把資料直接送出。
C ｜ 並用架構（推薦）	所有合規敏感企業	員工互動走原廠、產品嵌入走 aitokenking，兩條路徑互補，合規鏈不斷裂。

三條業務分流（推薦並用架構）

使用情境	建議路徑	選擇理由
員工日常 chat、寫文件、做研究	原廠 Enterprise（已訂閱）	原廠 audit log 直接涵蓋。
工程師 IDE 內寫程式	Claude Code（Enterprise seat）	原生整合、稽核完整。
客服系統嵌入 AI	aitokenking API	需脫敏 + Guardrail + 多模型備援。
KYC / AML 報告生成	aitokenking API	高敏感資料、需 prompt 級稽核。
內部知識庫 RAG	aitokenking API	需路由策略、成本優化。
法遵函詢回覆草稿	aitokenking API	需脫敏 + 模型比對 + 在地稽核。

aitokenking 加值層四大模組

模組	功能說明
① 前置脫敏	自動偵測並 tokenize 台灣本地敏感資料：身分證、統編、信用卡、銀行帳號、手機、住址、護照、錢包地址；雙向映射確保使用者體驗無感。
② Guardrails	Prompt injection 偵測、輸出端幻覺與機敏關鍵字過濾、政策違規攔截（如金管會紅線：不得做投資建議、不得保證收益）。
③ 統一稽核	Prompt-level 完整日誌（誰、何時、問什麼、哪個模型、回什麼、是否觸發 guardrail），對接 SIEM（Splunk / Datadog / Elastic）。

模組	功能說明
④ **在地化營運**	統一發票、新台幣計價、中文 dashboard、個資法與金管會 VASP 規範對應的留存政策模板、SLA 與在地法律管轄。

難題二 續 • USE CASES

05 金融業實際業務場景

以下為交易所與金融機構最常見的六大 AI 應用場景，皆已在現有客戶生產環境中驗證。

業務場景	AI 應用內容	建議架構
KYC ／ 開戶審核	證件 OCR 與真實性比對；風險敘述生成；脫敏層處理身分證、地址、生日。	aitokenking + Gemini + Claude
AML ／ 交易監控	STR / SAR 可疑交易報告草稿；鏈上交易圖譜的中文化解釋；多模型比對撰寫。	aitokenking + Claude + GPT
客戶服務（最大量）	7×24 多語客服（繁中／簡中／英／日）；FAQ 自動分流；嚴守金管會紅線。	aitokenking + 智能路由
幣種上架審查	白皮書摘要、團隊背景查核、鏈上活動分析；長文件 Claude、視覺 Gemini、結構化 GPT。	aitokenking 多模型
內部研發與資安	Code review、智能合約審計、API 文件生成；走原廠 Claude Code Enterprise。	原廠 Enterprise
法遵與監理回應	金管會函詢回覆草稿；季報年報重點摘要；內部 SOP 文件版本管理。	aitokenking + 嚴格稽核

多模型路由策略

aitokenking 並非「都接給你選」，而是依工作負載特性自動路由至最合適的模型，降低成本同時提升品質：

場景特性	主用模型	策略說明
法遵文件、長合約審閱	Claude Opus	長 context 與細膩推理強
結構化輸出（JSON、function call）	GPT-5	structured output 較成熟
多模態（KYC 證件、合約截圖）	Gemini	視覺與超長 context 優勢
高頻低複雜度（FAQ、分類）	Haiku / GPT mini	成本可降 5–10 倍
極敏感資料（內部風控模型）	自架 Llama / Qwen	完全不出本地

AITOKENKING 的角色

互補而非替代｜不取代客戶現有的 Claude Enterprise 訂閱，而是補足原廠在「產品內嵌 AI」這條路徑上的合規空缺，並提供 Fallback、智能路由、A/B 測試與統一 rate limit 管理。

難題三 • INTERNAL CONTROL

06 法規未到位的內控標準作業

在台灣 AI 專法與個資法 AI 修正案完成立法之前，企業必須自建可被律師、會計師、稽核單位採信的內控 SOP。本節提出國際標準組合 + 五大支柱的具體作法。

建議參照的國際與在地標準

ISO/IEC 42001:2023
AI 管理系統（AIMS），目前最權威的 AI 治理國際標準。

ISO/IEC 27001 + 27701
資訊安全管理 + 隱私資訊管理系統。

NIST AI RMF 1.0
美國國家標準技術研究院 AI 風險管理框架。

OECD AI Principles
經濟合作暨發展組織 AI 原則，國際組織共識。

金管會 AI 核心原則
2024 年金融業運用 AI 核心原則，在地監理參考。

EU AI Act
歐盟 AI 法案高風險系統條款，跨國業務必須對齊。

企業內部 SOP 五大支柱

支柱	實施內容
① 資料分類與處理政策	分為公開、內部、機敏、極機敏四級；每級對應 AI 使用權限；極機敏資料禁用外部 LLM；建立資料盤點清單。
② 脫敏與最小化原則	上 LLM 前必執行 PII 偵測與替換；採 tokenization（雙向）或 redaction（單向）；自動化掃描報告 + 抽樣人工複核 + 第三方稽核。
③ 完整稽核軌跡	每筆 prompt 與 response 留存（時間、使用者、模型、tokens）；留存期對齊金管會要求（金融業通常 5 年）；對接 SIEM 即時告警。
④ 模型輸出治理	Prompt injection 偵測、機敏關鍵字過濾、違規內容攔截（金管會紅線：投資建議、保證收益）、幻覺偵測與信心分數。
⑤ 廠商風險管理	簽 DPA；確認模型供應商不用客戶資料訓練（zero retention）；定期供應商稽核；異常事件 72 小時通報。

難題三 續 • VERIFICATION

06 「驗證脫敏到位」的五種手段

這是律師與會計師最常追問的問題。企業可採以下五種手段組合，建立可被獨立第三方採信的證據鏈。

驗證手段	說明
自動化掃描報告	每批送出資料的 PII 偵測命中率與替換紀錄，可自動化產出月報。
紅隊測試	委託資安團隊嘗試從 LLM 回應反推原始資料，驗證脫敏強度。
樣本人工複核	法遵部門按月抽樣檢視 prompt / response，建立人工審核紀錄。
第三方驗證	ISO 42001 / SOC 2 認證單位查核，取得可對外公示的證明。
供應商書面承諾	取得書面 zero-retention 與不訓練聲明，作為法律救濟基礎。

AITOKENKING 的角色

技術執行層｜上述五大支柱中的「② 脫敏」、「③ 稽核」、「④ Guardrail」三項，aitokenking 直接以工程手段實現，不需企業自建。
法遵部門寫好政策，技術層由 aitokenking 落地——這是大多數企業最缺的中間層。

內控導入的常見誤區

- **只靠合約承諾、不做技術驗證：**合約是事後救濟，技術才是事前防護。律師會計師會要求兩者並行。
- **把 audit log 等同於 prompt log：**原廠 audit log 多為 metadata 級，不含 prompt 內容；要做完整稽核需 Compliance API 或 aitokenking 加值層。
- **單一供應商風險：**金管會明確要求關鍵服務需有備援；單一 LLM 供應商不符監理期待。
- **忽略本地化義務：**個資法、金管會檢查、訴訟管轄都是本地義務，境外原廠無法直接承擔。

AITOKENKING • TRIPLE ROLE

07 aitokenking 三重角色定位

aitokenking 在企業 AI 治理中同時扮演採購、技術、業務三條防線的中間層。以下分述其角色、重要程度與對應決策者。

角色一 | 在地代理商 ★★★★★

定位：採購合規必要層。承擔個資法第 27 條委託機構責任，開立統一發票，提供中華民國法律管轄。

解決：發票抵稅、合約管轄、個資法責任歸屬、上市櫃供應商審核、政府標案資格、ISO 27001 與 SOC 2 文件提供。

關鍵決策者：採購部、法務部、財會部、稽核部

角色二 | 技術加值層 ★★★★★

定位：資料安全核心層。前置脫敏 + Guardrails + Prompt 級稽核 + 多模型路由。

解決：把法律承諾變成可被驗證的工程實作，律師會計師可逐筆查核；補足原廠 Enterprise audit log 不含 prompt 內容的盲點。

關鍵決策者：法遵長、資安長（CISO）、技術長（CTO）、研發部

角色三 | 多模型聚合 ★★★★☆

定位：業務韌性與成本優化層。Fallback、智能路由、A/B 測試、統一 rate limit。

解決：單一模型供應商當機時業務不中斷；同一 endpoint 自動依工作負載挑選最具成本效益的模型，月帳單可降 40–60%。

關鍵決策者：產品部、營運部、技術長（CTO）

三重角色的整合價值 | *單獨任何一個角色，市場上都有競品；但三個角色一次到位、且在同一個 API endpoint 與一份合約之下，這是 aitokenking 的差異化定位。對企業而言，這代表「一次過關」的合規路徑。*

INVESTMENT

08 投資配置與方案比較

aitokenking 提供三層方案，依企業規模、合規強度與業務量階梯式配置。實際報價依用量與客製需求由業務團隊評估提供。

STARTER

基礎方案

適用於：中小企業、新創、AI 試點階段；資料敏感度中低、月用量有限。

- ✓ 多模型 API 統一介接
- ✓ 基礎 PII 脫敏（標準規則）
- ✓ 用量 dashboard 與月報
- ✓ 統一發票（新台幣計價）
- ✓ Email 客服支援
- — 客製脫敏規則
- — SIEM 整合
- — SLA 保證

推薦

PROFESSIONAL

專業方案

適用於：上市櫃公司、中大型企業、有合規與稽核需求；大量生產環境使用。

- ✓ 多模型 + 智能路由 + Fallback
- ✓ 進階脫敏（含客製規則）
- ✓ Prompt 級完整稽核日誌
- ✓ Guardrails 政策引擎
- ✓ SIEM 整合（Splunk / Datadog）
- ✓ 99.5% SLA + 業務時間支援
- ✓ DPA + ISO 27001 文件
- ✓ 季度合規報告

ENTERPRISE

旗艦方案

適用於：金融機構、交易所、保險、醫療等強監理產業；極高合規要求。

- ✓ 專屬租戶 + 私有部署選項
- ✓ 完整客製脫敏與 Guardrails
- ✓ 5 年留存 + 即時告警
- ✓ 金管會稽核配合
- ✓ 紅隊測試 + 第三方驗證
- ✓ 99.9% SLA + 7×24 緊急支援
- ✓ ISO 42001 對應導入顧問
- ✓ 專屬客戶成功經理（CSM）

定價說明 ｜aitokenking 採「平台月費 + 用量計費」雙軌模式。平台月費對應方案規格與支援等級；用量計費透明對應底層模型 token 成本（依市場匯率調整）。實際報價依企業預估月用量、客製需求與合約期，由業務團隊評估提供。**提供 30 天試用期，零風險導入。**

IMPLEMENTATION

09 實施建議與下一步

建議分四階段導入，每階段約 2–4 週，可於季度內完成全面切換。

PHASE 01 · 第 1–2 週

需求盤點與架構規劃

aitokenking 與企業法遵、資安、技術三方聯合盤點：現有 AI 應用清單、資料分級、稽核需求、預算與 SLA 期望，輸出客製化導入藍圖與報價。

PHASE 02 · 第 3–4 週

合約簽訂與環境建置

簽訂雙層代理合約（含 DPA、SLA、賠償條款）；建立 aitokenking 專屬租戶、設定 PII 偵測規則、配置 SIEM 整合、開通在地統一發票流程。

PHASE 03 · 第 5–8 週

試點業務上線

選擇 1–2 個低風險業務情境（如內部知識庫、客服 FAQ）優先上線；建立 Prompt 級稽核日誌、執行紅隊測試、產出第一份脫敏驗證報告交法遵部門簽核。

PHASE 04 · 第 9–12 週

全面切換與標準化

將 KYC、AML、研究等核心業務逐步遷移；對齊 ISO 42001 內控架構；建立月度合規報告制度；訓練內部使用者與制定 AI 使用 SOP。

後續配套

項目	內容
季度檢視	每季召開合規檢視會議，更新風險清單與 SOP。
年度稽核	配合企業內外部年度稽核，提供完整文件與測試報告。
法規追蹤	持續追蹤台灣 AI 基本法、個資法修正、金管會函釋進度，第一時間更新合約與技術配置。
應變支援	設立 7×24 緊急應變窗口，重大事件 1 小時內啟動。

PROPOSAL CONCLUSION

原廠 Claude Enterprise 解決員工用 AI 的合規
aitokenking 解決企業產品嵌入 AI 的合規

兩者並存，互補而非替代，缺一不可

APPENDIX

10 附錄 • 國內外標準對照

本附錄整理企業在 AI 治理過程中可參照的主要國內外標準、法規與指導原則，供法遵與稽核部門參考。

國際標準

標準	適用範圍	發布年份
ISO/IEC 42001:2023	AI 管理系統（AIMS），組織建立、實施、維護與持續改進 AI 治理之國際標準。	2023
ISO/IEC 23894:2023	AI 風險管理指引，補足 42001 的風險視角。	2023
ISO/IEC 27001:2022	資訊安全管理系統，AI 治理的資安基礎。	2022
ISO/IEC 27701:2019	隱私資訊管理系統，個資保護國際標準。	2019
NIST AI RMF 1.0	美國 AI 風險管理框架，企業可採行的治理結構。	2023
EU AI Act	歐盟 AI 法案，全球首部 AI 綜合性法律。	2024
SOC 2 Type II	美國服務組織控制報告，雲端服務商必要證明。	—

台灣在地法規與指導原則

法規／原則	適用範圍	狀態
個人資料保護法	個人資料蒐集、處理、利用之基本法律規範。	現行有效
個資法施行細則	第 12 條規範安全維護義務，含技術與組織措施。	現行有效
金管會 AI 核心原則	金融業運用 AI 核心原則（公平、隱私、可解釋等）。	2024 發布
VASP 專法	虛擬資產服務業之專屬監理規範。	研議中
AI 基本法	國科會草案，AI 發展與治理基本原則。	立法院審議中

產業最佳實務參考

- **OECD AI Principles**｜經合組織 AI 原則，38 國共識
- **Singapore AI Verify**｜新加坡 AI 治理測試框架
- **UK AI White Paper**｜英國 AI 監理白皮書
- **金管會 RegTech 指引**｜金融科技監理指引（含 AI 應用）
- **銀行公會、證券公會自律規範**｜各金融業同業公會發布之 AI 應用建議

aitokenking

AI • TOKEN • KING

讓 AI 合規不再卡住業務

想了解如何將本提案套用到您企業的實際情境？
我們提供免費的需求盤點會議與 30 天試用，
由產品團隊與您的法遵、資安、技術主管直接對話。

WEBSITE
aitokenking.com.tw

BUSINESS
contact@aitokenking.com.tw

SALES INQUIRY
sales@aitokenking.com.tw

SUPPORT
support@aitokenking.com.tw

立即預約需求盤點會議