

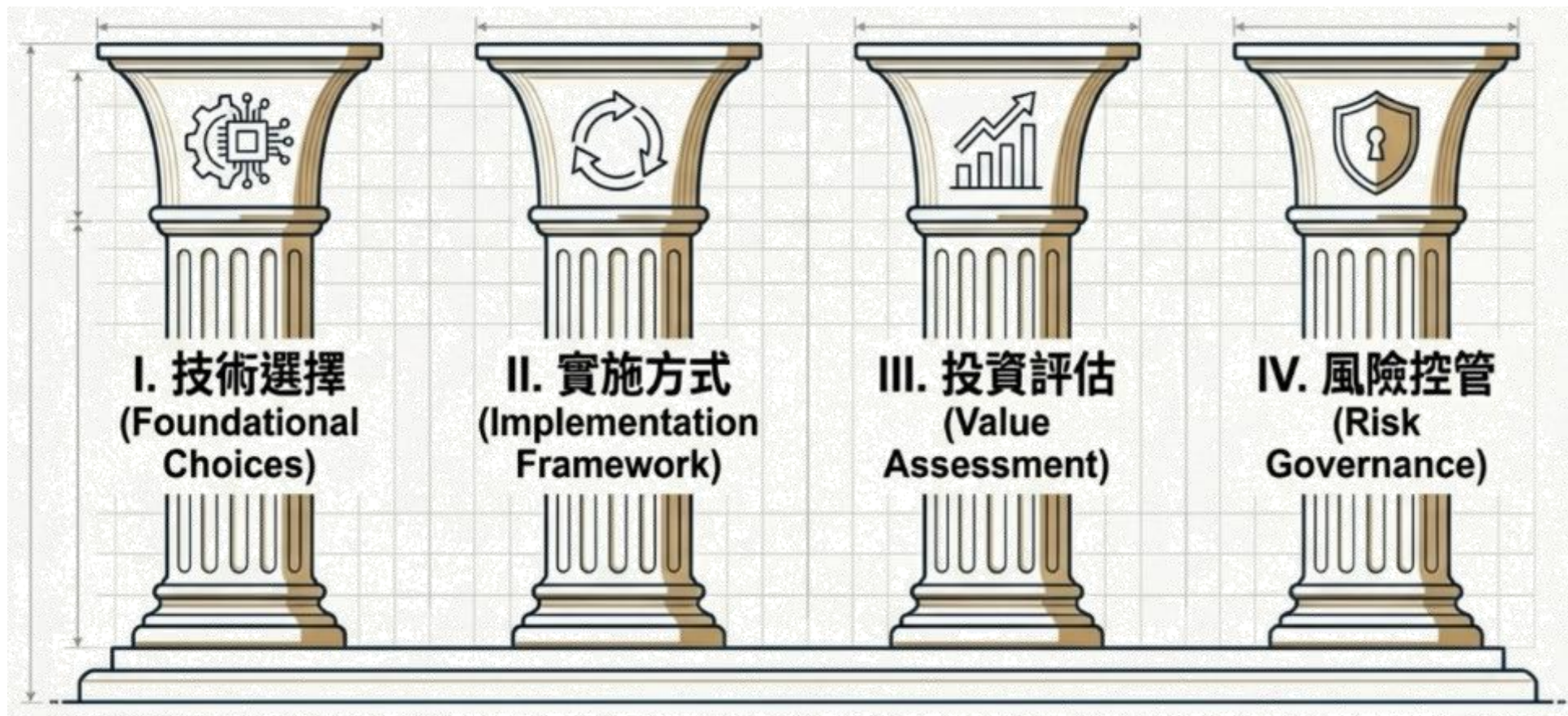


生成式AI落地產業應 用的挑戰

盧志浩 合夥人兼董事長
資誠創新諮詢 PwC Consulting Services

企業考慮GenAI落地的四大挑戰

儘管導入GenAI的趨勢明確，企業仍然面臨眾多挑戰，我們列舉了四個重要的挑戰與建議



從基礎設施、模型選擇、到微調都具備各種不同的評估需要考量

對於初步導入的企業，採用最容易入門與最簡單的架構，應該是最好的選擇



1. 基礎設施的抉擇：公有雲 vs. 私有雲

簡述：在運算能力、資料機密性與模型效能之間取得平衡。



2. 模型的策略：自訓練 vs. 採用現有模型

簡述：評估內部資料資產、成本承受度與投入風險。



3. 效能的優化：微調的投資與模式

簡述：探索符合成本效益的RAG模式與客製化潛力。

生成式 AI 有兩條重要但不同的價值創造途徑

決定在每條路徑上投資多少取決於組織的戰略要務和能力。至關重要的是，不要忽視該技術規模較小但仍然強大的應用，例如改進日常任務和流程，以及更具開創性的應用。



增量生產力的增強功能

此路徑側重於「現成」的解決方案，這些解決方案可以提高所有知識工作者和業務流程的生產力。

突破性的雄心勃勃使用案例

此路徑涉及實施「定製」的大規模變革性解決方案。它需要更長期的探索，以實現「大爆炸」的突破。

大語言模型的學習方式

企業選擇投入的領域，會有各種不同的技術困難需要克服與挑戰



價值實現飛輪（Value Realisation Flywheel）使需求（使用案例和模式）與供應（工具、解決方案、成本與碳排放、部署）決策更加一致

推廣規模

創造規模並探索模式的鄰近性，以最低的成本和努力將部署拓展到其他使用案例，以推動規模成本的下降

佈署與迭代

在受控流程中的初步部署和學習迭代，以及重新評估風險和治理

成本與碳排

評估開發和部署的成本以及相關的碳影響

解決方案

開發適當的解決方案和/或插件，以在各種模式中創造最大化的規模收益



價值假設

根據組織的資產負債表和與行業平均水平的比較，對價值和執行的風險/收益進行評估

使用案例

開發與價值假設相關的關鍵使用案例，以確保工作重點的優先排序

通用模式

將優先使用案例（需求方）與設計/建構（供應方）的通用模式對齊

工具

評估和開發適當的工具，以避免未來被擱置的技術債務（如許多特定領域的人工智慧解決方案或基於個別使用案例）

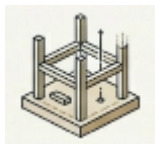
負責任AI的方法

根據負責任AI的架構與可信任AI的實施方法

超越傳統ROI: 全面性評估GenAI的投入與潛在價值

導入GenAI是一項驅動轉型的策略性投資, 必須從財務、策略、營運等多維度進行評估

投資面: 三大成本結構



一次性投入成本

- 需求探索與方案設計
- 資料準備
- 系統整合
- 模型選型與落地
- 安全與合規
- 產品與體驗設計
- 組織與人才



持續性營運成本

- 模型推論費用
- 向量化與檢索
- 計算資源
- 儲存與網路
- 模型維護與升級
- 監控與品質
- 安全防護
- 人工作業



隱性成本

- 幻覺與錯誤修正
- 模型漂移與更新
- 資料品質
- 變革管理
- 高效能目標

實現價值: GenAI在五大核心領域的商業效益

評估效益需同時關注量化指標(如成本降低、營收成長) 與質化效益(如顧客滿意度)



營運效率

自動化資料擷取與處理，縮短流程時間、降低人力投入。



提升準確性 與風險管理

分析大量資料以預測風險，辨識潛在詐欺行為。



客戶體驗與 個人化

量身打造產品與服務，提升顧客滿意度與忠誠度。



預測分析與 決策支援

提供預測洞見，協助企業提前掌握變化、制定策略。



法規遵循與 風險緩解

分析交易資料偵測潛在錯誤，降低違規罰則風險。

GenAI風險全景圖：四大面向的潛在威脅

企業領導人對AI的創新感到興奮,但同時也對網路安全、法律責任、聲譽損失與錯誤資訊傳播等風險感到擔憂



企業營運風險 (Risks to the Enterprise)

- 數據隱私、安全與智慧財產權洩露
- 員工不當使用未經批准的工具



AI能力風險 (Risks to Gen AI Capabilities)

- 幻覺 (Hallucination) 與錯誤資訊導致決策失誤
- 提示注入攻擊 (Prompt Injection)
- 數據投毒 (Data Poisoning)



惡意AI風險 (Risks from Adversarial AI)

- 惡意軟體與勒索軟體自動化
- 高複雜度的網路釣魚與社交工程
- 深度偽造 (Deepfake) 與身份冒充



市場風險 (Risks from the Marketplace)

- 法規不確定性與合規挑戰
- 供應商鎖定與技術過時
- 運算資源與能源消耗壓力

駕馭GenAI浪潮的四大關鍵戰略



1. 戰略思維：啟動「價值實踐飛輪」

拒絕盲目試錯，從高價值POC開始，逐步擴展以達規模效益。



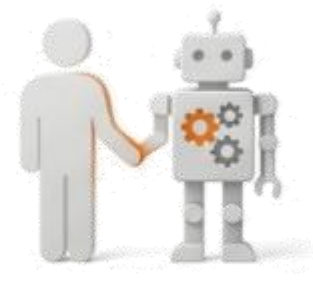
2. 治理核心：將「負責任的AI」轉化為競爭壁壘

將信任嵌入設計，建立問責制，保護企業聲譽與資產。



3. 資源配置：建立動態的全生命週期投資視角

重新定義ROI，納入隱性成本，由財務長與技術長緊密合作。



4. 組織賦能：強化「人機協作」下的流程再造

重視員工培訓與變革管理，保留人工審核機制，釋放自動化潛力。

Thank you