

課程名稱：18494_企業 AI 合規與資料治理實戰 課程摘要

本摘要由 Gemini AI 協助生成，僅供參考

1. 適合對象與能力門檻

- **適合族群：**企業經營者、高階主管、法務與合規人員、新創團隊、行銷/研發/人資/財務等欲在企業內部導入 AI 的業務單位人員，以及金融業從業人員。本課程幫助企業釐清在商業運作與創作中使用 AI 時，可能面臨的民事責任、智慧財產權（著作權）與個人資料保護法上的風險，並提供風險控管與指引實務。
- **能力門檻：**入門。無須具備深厚的法律背景，課程會從 AI 的運作機制（如訓練資料、黑盒子現象）開始逐步引導，進而剖析實際法律案例與規範。

2. 課程核心大綱與架構圖

- **章節架構：**
 - **章節一：前言與實際法律案例分析** — 引言背景、美國律師誤用 ChatGPT 虛構案例裁罰案、三星企業機密外洩風波。
 - **章節二：人工智慧的運作機制與發展** — AI 學習過程與技術軸線（圖靈測試等）、三波 AI 發展史（從符號推理、專家系統到深度學習）、資料品質（Garbage in, Garbage out）與黑盒子現象之法律意涵。
 - **章節三：全球 AI 法治現況** — OECD 指引、美國去管制化趨勢、歐盟嚴格管制（人工智慧法）、臺灣 AI 基本法草案與政策進程。
 - **章節四：AI 產品與應用的民事法律責任** — 責任歸屬鏈分析（開發商、製造商、經銷商到使用者）、自駕車事故案例分析（過失認定困難、風險分配失衡與消保法無過失責任）、監督測試義務與動物/僱用人責任之類比。
 - **章節五：著作權法與個人資料保護法風險** — AI 生成內容的著作權歸屬（智慧財產局函釋）、插畫/音樂/漫畫/翻譯/新聞摘要侵權案例、個資法風險（輸入敏感資料、推論性個資、模型訓練資料

刪除困難）與 ChatGPT 資料隱私條款拆解。

- **章節六：企業因應機制與風險控管** — 四大核心要素（風險評估、安全措施、持續監控、問題修正）、治理框架建立（教育訓練、部門風險識別、使用指引）、技術流程控管（前端輸入、後端輸出、供應商管理、審核與契約條款）。
- **章節七：政府與金融業 AI 使用指引導讀** — 行政院生成式 AI 使用參考指引（10 條原則）、金管會「金融業運用人工智慧指引」深度導讀（六大章節：治理問責、公平以人為本、隱私保護、系統穩健安全性、透明與可解釋性、永續發展）。

3. 必備前置知識清單

- **基本 AI 工具使用經驗**：對通用型生成式 AI（如 ChatGPT、Gemini 等）有基本操作概念。
- **基本商業營運與合規意識**：具備企業內部業務流程（如採購、行銷、人資、研發等）與基本合約/保護商業機密觀念。

4. 專有名詞與概念辭典

- **黑盒子現象 (Black Box Effect)**：指 AI 透過海量資料自動歸納關聯性得出結論，但其內部決策過程對人類而言並不透明、難以回推。在法律上會造成過失認定困難與責任歸屬鏈斷裂的疑慮。
- **可解釋性 AI (Explainable AI / XAI)**：旨在訓練模型的過程中提升決策過程透明度，讓人類能理解 AI 推理邏輯，藉此明確劃分法律責任並減少偏見與錯誤。
- **可合理期待之安全性**：消費者保護法（消保法）第 7 條規範企業經營者的責任要件。由於 AI 技術屬新興科技且缺乏統一產業標準，企業舉證其產品符合當前科技水準將面臨挑戰。
- **監督測試義務**：在立法健全前，要求 AI 開發者或使用者於部署前及營運期間進行定期檢測、追蹤系統變化與記錄備查，作為認定是否已盡民法「注意義務」的具體標準。
- **純 AI 創作 (AI-generated works)**：智慧財產局函釋指出，若創作過程完全由演算法功能獨立產出文字或影象，無人類實質精神創作投入，則

不受著作權法保護。

5. 課程學習職能對照

- **對應職能名稱：**企業法務與合規專員 / 數位轉型法規顧問 / AI 系統治理與風險管理師
- **主要工作任務/能力指標：**
 - **法律風險識別與評估能力：**能剖析企業導入 AI 時於民事侵權、消費者保護法、著作權與個資法（如敏感資料外洩、推論個資）上的潛在責任與風險點。
 - **企業 AI 治理與指引制定能力：**能參考行政院及金管會指引，為企業建構內部 AI 使用規範、進行前後端輸入輸出控管，並完成委外廠商（供應商）合約的風險條款設計。