

課程名稱：18505_資策會_公司資安治理與稽核 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（董事會成員/老闆）、總經理、資安長（CISO）、資訊/資安主管、MIS 系統管理員，以及內部稽核人員。課程協助管理者區分資安治理與管理的權責，並指導如何在有限預算下平衡稽核與實務防護。
- **能力門檻：**入門。無須精通高深的駭客攻擊或程式逆向工程技術，課程重點在於資安治理架構、法規遵行、風險評估與資安教育推動。

2. 課程核心大綱與架構圖

- **章節架構：**
 - **章節一：資安發展趨勢與挑戰** — 剖析供應鏈聯網風險、數位轉型威脅與老舊漏洞（如十年未修補漏洞）問題。
 - **章節二：相關資安法規與指引導讀** — 解析資通安全法（管理、技術、人員面）、半導體資安標準（SEMI E187）與上市櫃公司資安指引。
 - **章節三：資安治理架構與技術部署** — 界定企業核心系統、進行資產盤點、資安評級（Setuup/NIST SP-800）與 98%~99% 基本防護技術地圖。
 - **章節四：資安稽核實務與自動化** — 分析內部/第三方稽核、解決「有做不等於做好」及紙上作業（Paperwork）困境，導入電腦自動化稽核。
 - **章節五：資安教育訓練與廉價高效益投資** — 針對辦公室、IT 與產線/OT 人員因材施教，透過社交工程演練與教育訓練補足最後 1% 的資安缺口。

3. 必備前置知識清單

- **企業營運與組織架構概念：**了解公司內部部門分工（如董事會、總經理、MIS、產線/業務單位）之權責關係。

- **基礎網路與資訊設備常識**：對常見設備與服務（如 Firewall 防火牆、Web Server、PLC/OT 裝置、防毒軟體）有基本概念。

4. 專有名詞與概念辭典

- **資安治理 vs. 資安管理**：治理是從董事會/高層視角確認公司是否有執行資安防護與策略；管理則是總經理/資安長落實資安防護措施與技術執行。
- **核心系統**：企業無論如何都不能中斷、維持營運生命線的關鍵系統（如製造業的 ERP、MES）。
- **零信任 (Zero Trust)**：基於「不信任任何裝置與人員」的原則進行身分與設備驗證，常用於供應鏈伺服器與外部連線，但無法直接套用於封閉式 OT/PLC 產線。
- **自動化稽核**：利用電腦系統自動比對 Raw Data 與備份完整性，取代傳統人工抽查與紙上作業（Paperwork），解決不懂技術的稽核人員驗證困難的問題。

5. 課程學習職能對照

- **對應職能名稱**：資訊安全管理師 / 企業資安治理顧問 / 內部資安稽核員
- **主要工作任務/能力指標**：
 - **資安策略與治理架構規劃能力**：能盤點企業資產、區隔核心系統、建立資安組織並對標政府/產業資安法規與標準。
 - **資安稽核與風險控制能力**：能評估資安評級，設計有效的稽核專案與自動化稽核流程，避免流於紙上作業。
 - **資安文化與教育推動能力**：能針對不同職種（IT、行政、產線）設計專屬資安語言的教育訓練與社交工程演練。