17388_企業資訊安全認知（一） 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**：
  - **中小企業主與二代接班人**：面臨數位轉型、員工居家辦公及供應鏈資安要求，需規劃企業資安政策與合規策略者。
  - **企業資訊（IT）主管與資安專員**：需要了解上市櫃/公開發行公司資安法規（如重訊公告、年報揭露）、ISO/內控規範及端點防護者。
- **能力門檻**：初學者至普通。無須具備資工程式開發或駭客攻防經驗，課程從高階管理角度、法規導覽與實務控管清單切入解說。

📚 2. 課程核心大綱與架構圖

- **章節架構**：
  - **章節一：資訊安全趨勢與五大挑戰** — 剖析數位轉型與疫情遠距辦公下的資安威脅，歸納降低攻擊、雲端安全、異質系統整合、資安人才缺乏及兼顧便利與安全五大挑戰。
  - **章節二：資安主管機關法規與合規要求** — 導覽資通安全管理法、金管會金融資安行動方案、上市櫃資安指引、年報揭露規定及產創新條例資安投資抵減政策。
  - **章節三：上市櫃資安管理指引與架構設計** — 拆解由上而下推動之資安組織、核心業務/資產識別、弱點掃描/原碼掃描、通報應變與教育訓練。
  - **章節四：企業強化資安之五大實務面向** — 涵蓋內控設計（ Need-to-know 最小授權）、資安控管（密碼強度/職責區隔/網路區隔）、資安韌性（備份與勒索軟體因應）、工具安全（多因子認證 MFA）與資料安全（盤查與加密）。
  - **章節五：國內外常見資安資源與平台** — 介紹 TWCERT/CC、資通安全會報、HITCON 駭客年會等國內資安防護與情資分享資

源。

🛠️ 3. 必備前置知識清單

- **基礎企業資訊系統認知**：對企業內部的電腦、網路、伺服器或 ERP 系統運作有基本概念。
- **基礎管理思維**：了解企業內控制度或職責區隔（如管錢不管帳）之基本邏輯。

📖 4. 專有名詞與概念辭典

- **Need-to-know（最小授權原則）**：權限控管核心概念，僅給予員工執行工作所必需的最低系統與資料存取權限，避免過當授權造成資安風險。
- **資安韌性（Cyber Resilience）**：企業面對資安事件時的防禦與迅速復原能力；核心在於即使遭受攻擊或勒索軟體感染，也能在最短時間內恢復正常營運。
- **多因子認證（MFA）**：登入系統時需提供兩種以上的驗證管道（如密碼 + 手機動脈驗證碼），以強化帳號防護安全。
- **TWCERT/CC（台灣電腦網路危機處理暨協調中心）**：提供企業資安事件通報、資安漏洞諮詢與資安威脅情資分享的國家級防護平台。

💼 5. 課程學習職能對照（對標經濟部產業職能基準/iPAS）

- **對應職能名稱**：資訊安全管理師、企業法遵與風險管理師
- **主要工作任務/能力指標**：
  - **資安策略與合規規劃能力**：能依據上市櫃資安指引與年報規範，制定企業資安政策、推動資安內控並規劃投抵申請。
  - **資安風險評估與防護部署能力**：能識別企業核心資產、推動最小授權與多因子認證，並建立資安事件通報與備份復原機制（資安韌性）。