課程名稱：18563_ISO.IEC 27001 資訊安全風險評鑑操作實務 課程摘要

🎯 1. 適合對象與能力門檻

- **適合族群**：
  - **企業經營者與高階主管**：了解資安治理（27014）、內部風險等級劃分與整體資安資源分配者。
  - **資訊、資安與法遵部門主管/工程師**：需實際推動 ISO 27001 驗證，執行資安資產盤點與風險評鑑者。
  - **內部稽核人員與驗證推動小組**：需要熟悉 ISO 27000 系列標準、風險矩陣制定與附錄 A 93 項控制措施實施者。
- **能力門檻**：**普通**（不需程式編寫經驗，但建議對企業營運流程、IT 基礎設施或資安合規有基本情境理解）。

📚 2. 課程核心大綱與架構圖

- **章節架構**：
  - **章節一：ISO 27000 族群標準與 27001 高階架構（HLS）** — 解析 27000、27002、27003、27004、27005 與稽核認證群架構，以及 PDCA 高階架構（4-10 章）。
  - **章節二：資訊安全（IS）與管理系統（ISMS）之層次差異** — 釐清保護資料標的（IS）與系統化制度（ISMS）差異，並比較 4.1/4.2 組織風險與 6.1.2 資安風險評鑑。
  - **章節三：風險評鑑前置兩大關鍵（邊界範圍與資產盤點）** — 界定 ISMS 邊界（地點、部門、流程），以及盤點軟硬體、資料、服務與人員等資訊資產。
  - **章節四：風險識別（6 大面向）與 CIA 三要素衝擊分析** — 從資產、威脅、脆弱性、法規、流程與衝擊等 6 面向識別風險，並執行第一輪 CIA 門檻篩選。
  - **章節五：兩輪篩選機制、風險矩陣與控制措施對接** — 說明第二輪嚴重性（1-5 分）× 可能性（1-5 分）風險矩陣評分，對接

6.1.3 處理對策與附錄 A 93 項控制措施。

🛠️ 3. 必備前置知識清單

- **基礎商業與資安觀念**：對企業常見資訊資產（報價單、客戶個資、機房、伺服器、出貨流程）有基本認知即可。
- **無須程式語言背景**：課程著重於管理架構、條文解讀、表單設計與評估準則之建立。

📖 4. 專有名詞與概念辭典

- **CIA 三要素**：資訊安全的三大核心柱石：**機密性**（Confidentiality，未授權者看不到）、**完整性**（Integrity，資料未被竄改/破壞）、**可用性**（Availability，授權者需要時拿得到）。
- **兩輪風險篩選機制**：第一輪針對 CIA 三要素計算衝擊門檻（篩出顯著風險）；第二輪將顯著風險進行「嚴重性 × 可能性」計算風險等級（篩出不可接受風險）。
- **附錄 A 93 項控制措施**：ISO 27001:2022 附錄所列之資安控制項目，分為組織（37 項）、人員、實體與技術（34 項）四大類別。
- **適用性宣告（SoA）**：企業針對附錄 A 93 項控制措施進行逐項適用性列表之官方文件，若排除特定項目須詳細說明理由。

💼 5. 課程學習職能對照

- **對應職能名稱**：資訊安全管理師 / ISMS 內部稽核員 / 數位風控專員
- **主要工作任務/能力指標**：
  - **分析與決策能力**：能精準界定 ISMS 認證範圍、執行兩輪風險評鑑篩選，並劃分不可接受風險之優先處理等級。
  - **工具操作與執行能力**：能進行企業資訊資產盤點、設計符合公司情境之風險評估準則表單，並對接附錄 A 93 項控制措施撰寫 SOP 與適用性宣告（SoA）。