

中國科技大學補助教師參加校外研習心得報告

研習報告：ISO/IEC 27001：2022 資訊安全，網路安全及隱私保護 - 資訊安全管理系統主導稽核員培訓

一、研習目的與背景

在金融產業高度數位化（FinTech、AI、雲端）趨勢下，導入 ISO/IEC 27001:2022，有其必要性，因為隨著金融科技發展，產業面臨數據驅動決策、雲端金融、開放銀行三大結構性變化，產生，如個資外洩、金融詐欺、系統中斷等代表性風險，因此，ISMS 已從「IT 部門議題」升級為「公司治理核心」。

二、重點說明

本次研習聚焦於 ISO 27001:2022 核心精神 Confidentiality（機密性）、Integrity（完整性）、Availability（可用性）以及2022版重要更新，相較2013版，主要變化，控制措施由114項 → 93項（重整），新增：Threat Intelligence（威脅情報）、Cloud Security（雲端安全）、Data Masking（資料遮罩）、Secure Coding（安全開發），更貼近 FinTech 與 AI 應用環境。

三、架構與應用

- (一) 高階架構（HLS）ISO 27001採用標準化結構
- (二) PDCA 循環（核心邏輯）
- (三) 金融實務應用

四、企業案例與實務觀察

- (一) 國際案例
 - 1.HSBC 導入 ISMS 強化全球資安治理，建立跨國資安標準
 - 2.JPMorgan Chase，投入數十億美元於資安，建立 AI 資安監控系統
- (二) 台灣案例
 - 1.台灣積體電路製造公司高度重視資安（營業機密），導入 ISO 27001保障供應鏈安全
 - 2.中華郵政金融與物流整合，強化個資與交易安全五、研習心得與教學應用
- (三) 實務觀察（重點整理）
 - 1.資安已成為「成本 → 投資」
 - 2.金融機構高度依賴外包與雲端
 - 3.AI 導入帶來「新型資安風險」
 - 4.人為因素仍為最大漏洞（社交工程）

五、研習心得與教學應用

- (一) 研習心得（學術觀點）1.資安=風險管理的延伸 2.ISO 27001與財務管理高度整合 3.數據治理將成為金融核心能力 4.AI 與資安需同步發展（AI Governance）
- (二) 教學應用（課程設計）：可導入以下課程：財務管理 → 加入「資安風險」、投資學 → 資安事件對股價影響、金融科技 → 資安架構設計、公司治理 → ESG+資安以及 PBL 教學案例
- (三) 跨域能力培養：財務分析 資安事件財務影響，資訊素養 基本資安概念，風險管理 ERM 整合，ESG 思維 公司治理

六、結語

在 AI 與金融科技快速發展下，ISO/IEC 27001:2022不再只是資訊部門工具，而是：企業治理核心制度,金融風險管理關鍵架構,ESG 評價重要指標，對財務金融人才而言，未來關鍵能力將是：「財務×資安×AI」三位一體能力

備註：

- 一、研習心得報告請用電腦繕打。
- 二、研習結案報告請先上傳（校園入口網→其它類 E 化系統→研討會心得上傳），連同補助教師校外研習申請表、研習相關資料影本(4頁以上)及研習心得報告，並經主管簽章後，送人事室核銷。

報告人簽章	單位主管簽章	人事室主任簽章
年 月 日	年 月 日	年 月 日