中國科技大學補助教師參加校外研習心得報告

資訊是一種資產，對組織的業務至關重要，需要受到適當地保護。資訊可以以多種形式存在電腦、平板電腦、智慧型手機、網路傳輸的封包、雲端、印刷品、紙本、相片影像、縮微膠捲音頻器具上。資訊安全是透過建立管理系統來保護資訊，包括選擇適當的控制措施，以保護資訊免於各種威脅、確保業務持續性、最大限度地減少財務損失並最大限度地提高投資回報和商機。

ISO/IEC 27001 : 2022 資訊安全、網路安全及隱私保護 – 資訊安全管理系統標準為組織提供用以建立、實施、維持及持續改善資訊安全管理系統(ISMS)，採用 ISMS 為組織之策略性決策。組織的 ISMS 之建立及實作受組織之需要及目標、安全要求事項、所使用之組織過程與組織之規模和結構所影響，預期所有此等影響因素將隨時間改變。其內容包括範圍、規範性參考文獻、術語與定義、組織背景、領導作為、規劃、支持、運作、績效評估和改善，並附錄 A-(規範性)資訊安全控制措施參考。

本人於115年4月11日至115年4月25日參加由法國標準協會集團貝爾國際檢驗認證(AFNOR Group)的 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課程(ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management System)(ISMS)，此課程架構包括 ISMS 理論講述、練習含角色扮演、作業實作，其目標旨在說明 ISMS 優勢、認證/註冊管理系統的益處、評估對 ISMS 和 ISO27001:2022要求的理解、資訊安全概述、概念及術語、ISMS 基本原則、ISO27000系列標準、ISO27001:2022 PDCA 方法、風險管理和風險評鑑、組織的稽核背景、稽核條文5至10要求、附錄 A 概述(控制措施)、稽核(含稽核意義、類型、階段、流程、原則、方案)、稽核員的能力與評估、稽核活動、稽核規劃、稽核發現、現場稽核、稽核檢查清單、稽核證據、稽核結束和關閉 NC、課程與意見回顧並舉行測驗 (本人已通過測驗取得證書，並取得40小時研習時數)。

本次研習尚含括案例觀摩和稽核案例演練，提供企業案例之組織背景、業務範圍、主要部門業務和服務及稽核情境描述，藉此討論提出資訊安全稽核發現(發現類型、發現內容和具體描述)、稽核證據(文件證據、訪談證據、觀察證據等等) 、對照條文要求，風險識別、分析和評鑑，資訊安全風險處理嘗試提出改善措施(不符合事項及矯正措施)並應持續改善資訊安全管理系統以符機密性、完整性和可用性。上述提供缺乏相關實務經驗者循序漸進的理解以建立清晰且明確的概念，不僅有助於本校現正引入 ISMS 之推動，且將之融入相關通識課程，促進本校師生了解 ISMS 的重要性和內涵，並符應和遵循現行法規，建立應備職能。

報告人簽章	單位主管簽章	人事室主任簽章
張賴妙理 115年5月13日	年　月　日	年　月　日