中小企業資訊安全診斷之個案研究

田效文,陳秀玲,黃文聰,顏榮甫
科技管理學系
管理學院
swt@chu.edu.tw

摘要

本研究是以個案研究方式比較兩個行業別相近的中小企業規模零售業，參考ISO 27001 所發行之標準的11個管理領域、39個控制目標、133個控制要點，以模糊德爾菲之專家問卷的統計分析結果排除業務和法令規章無關之控制項目制定一份以60個控制措施評量的資安檢核表，調查、分析與評估目前企業現有問題與資訊安全管理機制，以讓業主了解如何提升其資訊安全等級，研究過程中該企業提出目前急迫改善的控制項進行資訊安全診斷服務，並比較診斷前後實施改善的成果，提出該企業未來制度面與人員資訊安全能力提升的建議與未來資訊安全系統功能架構改善建議，最後，針對個案的兩個零售業公司的資訊安全觀念及落實推動上，分析其資訊安全各控制措施達成率。

關鍵字：ISO 27001、資訊檢核表、資訊安全管理、資訊安全診斷