

# 以ISO27001為基礎校園資訊安全管理之研究

林志勇、楊豐兆

E-mail: 9800785@mail.dyu.edu.tw

## 摘要

本研究以ISO27001 資訊安全評核規範為基礎且彙整了國內外相關研究，將校園資安環境區分為「組織內部」、「外在環境」、「資訊科技」等三大構面，並加以探討資訊安全構面因素與各項評估指標，以提供學校於建構資訊安全系統時之重要參考依據。本研究發現，影響「組織內部」資訊安全管理機制的關鍵因素，分別為安全政策、安全組織、主管支持、人員安全、資產分類及控制、設備及環境安全等因素；在影響「外在環境」資訊安全管理機制的關鍵因素，分別為符合性、委外廠商等因素；在影響「資訊科技」資訊安全管理機制的關鍵因素，分別為存取控制、資訊開發及維護、通訊及作業管理、資訊安全事故管理、業務永續運作管理等因素。

關鍵詞：BS7799、ISO27001、資訊安全管理、資安事件

## 目錄

中文摘要	iii
英文摘要	iv
誌謝辭	v
內容目錄	vi
表目錄	vii
圖目錄	viii
第一章 敘論	1
第一節 研究背景與動機	1
第二節 研究目的	6
第三節 研究問題	7
第四節 研究範圍	7
第五節 研究流程	8
第二章 文獻探討	10
第一節 資訊安全	10
第二節 ISO27001資訊安全管理規範	32
第三節 ISO27001模組化流程	43
第三章 研究方法	49
第一節 ISO27001模組化	49
第二節 研究架構	50
第三節 研究對象	53
第四節 問卷內容設計	53
第五節 統計分析方法與工具	53
第四章 資料分析	55
第一節 問卷回收率分析	55
第二節 受訪學校基本資料分析及交叉分析	55
第三節 問卷信度與效度分析	62
第四節 資訓安全現況分析	63
第五章 結論	78
第一節 研究結論與建議	78

第二節 研究貢獻與限制 . . . . .	83
參考文獻 . . . . .	85
附錄A 研究問卷 . . . . .	92

## 參考文獻

- 一、中文部分Clyde, R. A. (2002), 資安著重管理架構, 資訊傳真周刊, 4, 46-47. ITtoolbox(2007), 企業資訊科技調查[線上資料], 來源: <http://it.toolbox.com/>[2006, January 12]. Kenneth, C. L. (2003), 管理資訊系統:管理數位化公司(周宣光譯), 台北:東華書局(原文於2002年出版)。行政院主計處電子處理資料中心(2007), 電腦應用概況調查[線上資料], 來源: <http://www.dgbas.gov.tw/ct.asp?xItem=17966&CtNode=4920>[2007, May 24]. 何瀛州(2007), 區域級學術網路組織之資訊安全風險評估 - 以宜蘭縣學術網路為例, 佛光山大學資訊管理研究所未出版之博士論文。吳琮璠, 謝清佳(2003), 資訊管理理論與實務, 台北:智勝出版。吳俊德(2002), ISO17799資訊安全管理關鍵重點之探討, 國立中正大學企業管理研究所未出版之碩士論文。吳明隆(2005), SPSS統計應用學習實務 - 問卷分析與應用統計(2版), 台北:知城數位科技。林進財, 黃旭男, 陳啟斌, 鄭信一(2000), 現代企業資訊安全之研究, 科技管理學刊, 5(1), 105-123。邱皓政(2002), 社會與行為科學的量化研究與統計分析(2版), 台北:五南圖書出版。財團法人資訊工業策進會(2006), 經濟部IT IS計劃[線上資料], 來源: <http://www.iii.org.tw/#>[2007, May 24]。李順仁(2007), 資訊安全, 台北:文魁圖書。徐廣寅(2003), 資訊安全管理導論(初版), 台北:金禾資訊。陳祥輝(2000), 資訊系統的安全管理與鑑識軌跡設計 - 基於MIB與資料庫之探討, 中國文化大學資管系未出版之碩士論文。孫思源(2007), 以分析層級程序法探討企業導入BS7799之關鍵成功因素, 國立中山大學資訊管理研究所未出版之博士論文。國際數據資訊(2005, January 11), 台灣資訊安全市場由單點防護走向整合性之資安解決方案[線上資料], 來源: [http://www.idc.com.tw/report/news\\_050105.htm](http://www.idc.com.tw/report/news_050105.htm)[2006, January 11]。張芳珍(2005), 以BS7799落實資訊安全管理 - 管理類資訊資產分類與控管, 國立中央大學資訊管理研究所未出版之碩士論文。郭志賢(2002), 以BS7799為基礎評估大學資訊中心之資訊安全管理 - 以淡江大學為例, 淡江大學資訊管理學系未出版之碩士論文。黃亮宇(1992), 資訊安全規畫與管理, 台北:松崗電腦圖書。黃亮宇(1992), 資訊安全規畫與管理, 台北:松崗電腦圖書。黃烜儀(2000), 臺灣地區不同類型金融機構在全球資訊網路安全考量因素之研究, 國立中正大學資訊管理學系未出版之碩士論文。黃芳銘(2002), 結構方程模式理論與應用, 台北:五南書局。黃俊英(2004), 多變量分析, 台北:華泰書局。黃士銘, 張碩毅, 蘇耿弘(2005), 企業導入BS7799資訊安全管理系統之關鍵成功因素 - 以石化產業為例, 資訊管理學報, 7。劉智勇(2003), 由BS7799看資訊安全部署, 台北:麟瑞科技。劉國昌, 劉國興(1998), 資訊安全, 台北:儒林圖書公司。樊國楨, 方仁威, 林勤經(2003), 資訊安全管理系統驗證作業之研究, 資訊安全論壇研討會, 13, 26-43。賴溪松, 何全德(2003), 公開金鑰基礎建設與憑證管理中心, 行政院國家科學委員會科學技術資料中心, 94-95。謝惠玲(2007), 資訊安全機制規劃及建置之現況調查與分析 - 以國內大學校園系統為例, 靜宜大學資訊管理研究所未出版之博士論文。
- 二、英文部分British Standards Institution(2000). Information security management-part 1: Code of practice for information security management. (BS 7799-1:2000). BS: British Standards Institution.British Standards Institution(2002). Information security management systems-part2: Specification with guidance for use. (BS 7799-2: 2002). BS: British Standards Institution.Caminada, M. (1998). Internet security incidents a survey within Dutch organizations. Computers and security, 17, 417-433.DeVellis, R. F. (1991). Scale development: Theory and applications. California: Sage.Ernst & Yong LLP(2007). Global Information Security Survey[Online]. Available: <http://www.ey.com>. [2007, May 24]Eric M. (2004). Network Security: A Beginner's Guide (2nd ed.). New York: McGraw-Hill.Finne, T. (2000). Information Systems Risk Management: Key Concepts and Business Processes. Computers and Security, 11, 55-76.Gartner Dataquest(2007). Gartner Dataquest The U.S. Security Services Market Forecast. New York: McGraw-Hill.Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate Data Analysis (5th ed.). New Jersey: Prentice Hall.Hong, W., Thong, J. Y. L., Wong, W. M., & Tam, K. Y. (2002). Determinants of User Acceptance of Digital Libraries: An Empirical Examination of Individual Differences and System Characteristics. Journal of Management Information Systems, 18(3), 97-124.Hofer, C. W., & Schendel, D. (1978). Strategy Formulation: Analytical Concepts. New York: West Publishing.Hutt, A. E. (1995). Management's Role in Computer Security Computer Security Handbook. New York: Wiley.Huang, H. Y., Hwang, H. G., & Yen, D. C. (2000). A Study on Internet Security Factors of Different Financial Institutions in Taiwan, Proceedings of the International Conference of Pacific Rim Management. New York: USA.Icove, D., Seger, K., & Vonstorch, W. (1999). Computer Crime. California: O'Reilly and Associates.International Organization for Standardization(2005). Information technology Security techniques Information security management systems Requirement. (ISO/IEC 27001: 2005). ISO: Information technology.Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. International Journal of Information Management, 23(2), 139-154.Karen, D. L., Houston, H. C., & Mellerrill, E. W. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly, 8, 173-186.Martin, P. L., William, L., & Robert, R. (2007). Computer Crime and Security Survey Computer Security Institute. California: San Francisco.Norifusa, M. (1998). Internet Security: difficulties and solutions. International Journal of Medical Informatics, 49, 69-74.Nunnally, J. (1978). Psychometric Theory(2nd ed.). New York: McGraw-Hill.Olnes, J. (1994). Development of Security Policies. Computer and Security, 13, 628-636.Osborne, K. (1998). Auditing the IT Security Function. Computer and Security, 17(1), 34-41.Powell, D. (1993). To Outsourcing or not to Outsourcing? Networking Management, 9, 56-61.Schneier, B. S., & Lies, L. (2000). digital Security in a Networked World. New York: John Wiley and Sons.VonSolms, R. (1996). Information security management: the second generation. Computers and Security, 15(4), 281-288.