業資訊資產之資訊安全風險管理 : 以某銀行為例

江芷佑、曹偉駿

E-mail: 322137@mail.dyu.edu.tw

摘 要

隨著金融自由化與國際化，銀行業的經營環境面臨到急速變遷與激烈競爭的挑戰，其顯然已成為高度風險的行業。在競爭越趨激烈下，銀行要處理的風險不僅呈現多樣化，同時要更加複雜化，在此情形下，銀行若能充分瞭解資訊資產之風險管理的重要性，且謀求適當而有效的管理方法，則將可提升經營的安全。目前針對銀行業資訊資產風險管理的相關研究極少，大部分的研究著重於風險分析對企業重要性及建立企業風險評估模式，因此本研究著重於銀行業資訊資產風險管理研究，基於ISO27001標準中的控制項、ISO27005的風險流程及OCTAVE 操作性關鍵威脅、資產與弱點評估，以銀行為個案進行專家問卷，在根據其結果作風險分析，以評估資訊資產的現有價值、相關威脅、弱點與風險等級。本研究提供使用者瞭解其資訊資產價值與該資產面臨的風險值，並讓銀行在資訊資產的資訊安全風險上有參考的依據，同時也為後續的相關研究提供一些建議的方向。

關鍵詞 : 資訊安全、風險管理、ISO27001、ISO27005

目錄

參考文獻

一、中文部份 陳志誠，林淑瓊，李興漢，許派立(2009)，資訊資產分類與風險評鑑之研究—以銀行業為例，資訊管理學報，16(3)，55-84。 樊國楨，傅雅萍，黃健誠，楊中皇，王演芳(2010)，資訊安全風險評鑑:根基於給水廠之氯氣處理系統(資通安全專論，T98002)，台北:行政院國家科學委員會。 梁定澎(1997)，資訊管理研究方法總論，資訊管理學報，4(1)，1-6。 吳琮璠(1997)，資訊管理個案研究方法，資訊管理學報，4(1)，7-17。 樊國楨、林樹國、鄭東昇(2005)，資訊安全保證框架標準初探:根基於ISO/IEC 17799: 2005-06-15之12.6.1節，台北:行政院國家科學委員會科學技術資料中心。 謝安田(2006)，企業研究方法論(第三版)，彰化:著者發行。 張淑清(2006)，基於COBIT與ISO 27001建構資訊安全治理-以健保局為例，私立大葉大學資訊管理學系碩士班未出版之碩士論文。 二、英文部份 Alberts, C., & Dorofee, A. (2003). Managing information security risks, the OCTAVE approach. New York: Addison Wesley, 25-63. Bakry, S. H. (2004). Development of e-government: A STOPE view. International journal of network management, 14(5), 339-350. Broderick, J. S. (2006). ISMS, security standards and security regulations. Information Security Technical Report, 11(1), 26-31. Brown, A. E., & Grant, G. G. (2005). Framing the frameworks: A review of IT governance research. Communications of the association for information systems, 15, 696-712. Chivers, H., Clark, J. A., & Cheng, P. C. (2009). Risk profiles and distributed risk assessment. Computers & Security, 28, 521-535. CNS 27001: 2007 (2007). Information technology - information security management system – requirements, Chinese National Standard. Taipei: Author. CNS 27002:2007 (2007). Information technology - information technology - security techniques - code of practice for information security management. Chinese National Standard, Taipei: Author. Esteves, J., & Joseph, R. C. (2008). A comprehensive framework for the assessment of e-Government projects. Government Information Quarterly, 25(1), 118-132. Halliday, S. (1996). A business approach to effective information technology risk analysis and

management. Computer & Security ,4, 27-28. ISO 27001: 2005. (2005). Information technology - Security techniques - Information security management systems - Requirements. International organization for standardization. Geneva, Switzerland: Author. ISO 27002: 2005. (2005). Information technology - security techniques - code of practice for information security management. International organization for standardization. Geneva, Switzerland: Author. Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. Computers & Security, 27 , 224-231. Pasquinucci, A. (2007). Security, risk analysis and governance: A practical approach. Computer Fraud & Security 7, 12-14. Rok, B., & Borka, J. B. (2008). An economic modelling approach to information security risk management. International Journal of Information Management, 28, 413-422. Saleh, M. S., Alrabiah, A., & Bakry, S. H. (2007). Using ISO 17799: 2005 information security management: A STOPE view with six sigma approach. International Journal of Network Management, 7(1), 85-97. Schultz, E. E., Proctor, R. W., & Lien, M. C. (2001). Usability and security an appraisal of usability issues in information security methods. Computer & Security, 20(7), 620-634. Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management 46, 267-270. AS/NZS 4360:2004 (2004). Risk management. Standards australia & Standards new zealand, Sydney: NSW. Von Solms, R. (1996). Information Security Management: The Second Generation. Computer & Security, 15(4), 281-288.