

Information Security Risk Management for Banking 's Information Assets – Evidence from Some Bank

江芷佑、曹偉駿

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

ABSTRACT

With the liberalization and internationalization of financial, the banking operation must face a lot of fierce challenges and competition, and it has become highly risky apparently. In the competition, the risks that financial institutions must deal are not only various but also more complex now. The result of banking asset risk management can improve the safety of operation. The current research is almost focused on analyzing the enterprise risk and establishing risk assessment model. In this research, we first classify the information assets of a financial institution, and further assess their risk. The expert questionnaire method is adopted in this research and the questionnaires are designed based on the guidelines of information security management of ISO 27001, ISO 27005 and OCTAVE. The research derives methods for evaluating the assets, threats, vulnerabilities and risk levels. Owing to the lack of the related approaches on the classification of information assets and the assessment of their risk in banking, we affirm that the results of our research can contribute to the risk management of the information assets.

Keywords : information security、risk management、ISO27001、ISO27005

Table of Contents

中文摘要	iii	英文摘要	iii
iv 誌謝辭		v 內容目錄	
vi 表目錄		vii 圖目錄	
viii 第一章 緒論	1	第一節 研究背景與動機	1
1 第二節 研究目的	3	第三節 研究限制	3
3 第四節 研究流程	4	第二章 文獻探討	4
7 第一節 資訊安全	7	第二節 資訊資產	7
9 第三節 風險管理	11	第四節 風險管理標準	11
13 第三章 研究方法	27	第一節 研究架構	27
27 第二節 研究對象	27	第三節 風險分析	27
32 第四章 研究結果	38	第五節 結論與未來發展方向	38
46 參考文獻	47	附錄A	47
51 附錄B	55		

REFERENCES

- 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。 吳琮璿(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., & Borca, 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.