建置銀行業私有雲之資訊安全治理-以某銀行為例

胡雯婷、曹偉駿

E-mail: 364845@mail.dyu.edu.tw

摘 要

隨著資訊科技的進步，銀行業對資訊技術的依賴無可取代。其營運方式不再像過去只有少數的功能，在網路普遍的情況下其商品不斷增加多樣性，使得業務變得更加繁雜，而且面對資訊安全威脅不斷衍生，使得銀行業成為高度風險的行業，因而必須投入基礎設施、資訊技術研發與資安防護等龐大成本。 雖然雲端運算環境擁有高效能、高彈性以及可降低成本等諸多優點，但仍有許多企業對雲端資訊安全感到疑慮而不敢投入此環境。因此，本研究探討銀行業導入雲端運算之資訊安全的問題，並提出建置銀行業私有雲之資訊安全治理。本研究之研究方法將採用基於ITIL (Information Technology Infrastructure Library)的事件管理規範、ISO 27001的控制項與ISO 27005的風險流程，以個案探討的方式根據策略、技術、組織、人員、環境構面推導出相關命題，接著用於對本研究的研究對象進行深度訪談。最後，本研究對銀行業的資訊安全治理策略提出建議，以讓銀行在雲端運算的資訊安全風險上有參考的依據。

關鍵詞 : 雲端運算、資訊安全、資訊安全治理、資訊技術基礎建設典範、國際資訊安全標準

目錄

參考文獻

一、中文部分: 古永嘉，楊雪蘭(譯)(2009)，企業研究方法 第十版。台北:華泰。(Donald R. Cooper, Pamela S. Schindler., 2008) 朱惠中，廖崇賢，陳惠娟(2006)，從管理層面探討當前的資訊安全問題，2006年資訊管理學術與實務研討會論文集，台北:私立景文技術學院。 行政院研究發展考核委員會(2009)，網路安全的挑戰與策略，來源: http://www.seminar2009.twnic.tw/download/d2s2c.pdf [2012, march 12] 沈柏村(2010)，ISO 27001資訊安全標準及驗證流程簡，金融聯合徵信雙月刊，20-22。 吳琮璠(1997)，資訊管理個案研究方法，資訊管理學報，4(1)，7-17。 林信亨(2009)，雲端運算應用趨勢與我國商機研究。台北:經濟部。 梁定澎(1997)，資訊管理研究方法總論，資訊管理學報，4(1)，1-6。 彭秀琴、張念慈(2010)，雲端運算下資訊安全之探討，經建會管制考核處，172-192。 陳萬淇(1995)，個案研究法。台北:萬泰。 黃小玲(2010)，如何整合ISMS與ITSMS，來源: http://www.icst.org.tw/docs/Fup/6月_如何整合ISMS與ITSMS.pdf [2010, june 21]。 許士軍(2011)，新時代環境下中小企業的蛻變，來源: http://www.cjcu.edu.tw/~wangspeech/bill/100-1/20110916.pdf [2012, may 29] 經濟部(2010)，99年中小企業家數－按行業別分(PDF檔)，來源: http://www.moeasmea.gov.tw/dl.asp?filename=192016395771.pdf [2012, may 10] 經濟部(2011)，2011中小企業白皮書(全).pdf，來源: http://book.moeasmea.gov.tw/book/doc_detail.jsp?pub_SerialNo=2011A01070&click=2011A01070# [2012, may 27] 傅雅萍，樊國楨，楊中皇(2009)，ISO/IEC 27005風險管理標準整合CORAS之可行性研究:以電力公司為例，資通安全專論T97022，財團法人國家實驗研究院科技政策研究與資訊中心。 劉永森（1991），層級分析法（AHP）中機率性判斷之研究，國立中山大學資訊管理研究所碩士論文。 劉興樺(2008)，資訊安全風險管理(ISO/IEC FDIS 27005)議題初探，聲威網際科技股份有限公司，來源:fsms.bsmi.gov.tw/cat/epaper/970331劉興樺.ppt [2012, march 12] 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，行

政院國家科學委員會科學技術資料中心。 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。 闕頌廉(1994)，應用模糊數學(3版)。台北:科技圖書。 IBM，資訊安全科技前瞻報告:新興安全科技趨勢展望，來源: http://www-935.ibm.com/services/tw/gts/pdf/outlook_emerging_security_technology_trends.pdf [2012, march 13] James Lyne(2012)，IT安全2011年度回顧與展望，來源: http://www.informationsecurity.com.tw/article/article_detail.aspx?tv=&aid=6555&pages=2 [2012, march 16]
二、英文部分: P. W. Andersen. (2001). Information Security Governance. Information Security Technical Report, 6(3), 60-70. S. H. Bakry. (2004). Development of e-Government: A STOPE view. International Journal of Network Management, 14(5), 339-350. K. Beckers, H. Schmidt, J.C. Kuster and S. Fassbender. (2011). Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. Proceedings of International Conference on Availability, Reliability and Security, 327-333. D. Bernstein, D. Vij and S. Diamond. (2011). An Intercloud Cloud Computing Economy - Technology, Governance, and Market Blueprints. Annual SRII Global Conference, 293-299. A. Bhardwaj and V. Kumar. (2011). Cloud Security Assessment and Identity Management. Proceedings of International Conference on Computer and Infonnation Technology, 387-392. J. S. Broderick. (2006). ISMS, Security Standards and Security Regulations. Information Security Technical Report, 11(1), 26-31. W. Bruijn, M. R. Spruit, M. Heuvel. (2010). Identifying the Cost of Security. Journal of Information Assurance and Security. 74-83. C. Chandersekaran, W. R. Simpson, R. R. Wagner. (2011). High Assurance Challenges for Cloud Based Computing. Proceedings of the World Congress on Engineering and Computer, (1), 1-6. CNS 27002: 2007 (2007). Information technology-Information technology-Security techniques-Code of practice for information security management, Chinese national standard. Taipei: Author. CSA. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing. Retrieved from Cloud Security Alliance, Institute for Learning Technologies Web site: http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf CSA. (2010). Top Threats to Cloud Computing. Retrieved from Cloud Security Alliance, Institute for Learning Technologies Web site: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf J. Esteves and R. C. Joseph. (2008). A Comprehensive Framework for the Assessment of eGovernment Projects. Government Information Quarterly, 25(1), 118-132. J. Fang and X. Meng. (2011). Application Investigation on Private Cloud in the Field of Group Company Financial Information Management. International Conference on Mechatronic Science, Electric Engineering and Computer, 1926-1929. I.M. Haw, S. S.M. Ho, B. Hu and D. Wu. (2010). Concentrated Control, Institutions, and Banking Sector: An International Study. Journal of Banking & Finance, 34(3), 485-497. S. Hosseinbeig, D. Karimzadgan-Moghadam, D. Vahdat and R. A. Moghadam. (2011). IT Strategic Alignment Maturity and IT Governance. International Conference on Interaction Sciences (ICIS), 67-72. ISO 27001: 2005. (2005). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization. N. Kim, R. J. Robles, S.E. Cho, Y.S. Lee and T. Kim. (2008). SOX Act and IT Security Governance. International Symposium on Ubiquitous Multimedia Computing, 218-221. M. Kretzschmar, M. Golling and S. Hanigk. (2011). Security Management Areas in the Inter-Cloud. IEEE International Conference on Cloud Computing, 762-763. P. Nastase, F. Nastase and C. Ionescu. (2009). Challenges Generated by the Implementation of the IT Standards COBIT 4.1, ITIL V3 and ISO/IEC 27002 in Enterprises. Economic Computation & Economic Cybernetics Studies & Research, (3), 1-16. NIST. (2011). The NIST Definition of Cloud Computing. Retrieved from National Institute of Standards and Technology, Institute for Learning Technologies Web site: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf M. C. Paulk, C. V. Weber, B. Curtis and M. B. Chrissis. (1995). The Capability Maturity Model: Guidelines for Improving the Software Process. U.S.A.: Big River Books N. Pham, L. Baud, P. Bellot and M. Riguidel. (2008). A Near Real-time System for Security Assurance Assessment. The Third International Conference on Internet Monitoring and Protection. 152-160. K. Popovic and Z. Hocenski. (2010). Cloud Computing Security Issues and Challenges. Proceedings of the 33rd International Convention, 344-349. S. Ramgovind, M. M. Eloff and E. Smith. (2010). The Management of Security in Cloud Computing. Information Security for South Africa (ISSA), 1-7. H. C. Relyea. (2008). Federal Government Information Policy and Public Policy Analysis: A Brief Overview. Library & Information Science Research, 30(1), 2-21. J. N. Rosenau. (1995). Governance in the Twenty-First Century. Global Governance 1,13-43. S. Sahibudin, M. Sharifi and M. Ayat. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. International Conference on Modeling & Simulation, 749-753. M. S. Saleh, A. Alrabiah and S. H. Bakry. (2007). Using ISO 17799: 2005 Information Security Management: A STOPE View with Six Sigma Approach. International Journal of Network Management, 7(1), 85-97. E. C. Schneider and G. W. Therkalsen. (1990). How Secure are your System?. Avenues to Automation, 68-72. F. B. Shaikh and S. Haider. (2011). Security Threats in Cloud Computing. International Conference on Internet Technology and Secured Transactions, 214-219. A. Shi, Y. Xia and H. Zhan. (2010). Applying Cloud Computing in Financial Service Industry. International Conference on Intelligent Control and Information Processing, 579-583. R. Solms and S.H. Solms. (2006). Information Security Governance: Direct-Control Cycle. Computers & Security, 25(6), 408-412. A. C. Strauss and J. M. Corbin. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. CA: Sage Publications. J. Yang and Z. Chen. (2010). Cloud Computing Research and Security Issues. International Conference onComputational Intelligence and Software Engineering (CiSE), 1-3. R. K. Yin. (1983). The case study method: An Annotated Bibliography. Washingtom, D.C.: COSMOS Corporation.