基於COBIT與ISO 27001建構資訊安全治理 : 以健保局為例

張淑清、曹偉駿

E-mail: 9707252@mail.dyu.edu.tw

摘 要

自1997年以來我國全面實施電子化政府，健保局為因應電子化政府的推動，因而建置健保IC卡及電子病歷交換等相關技術，雖然可省去換卡及資料交換的問題，但是健保資料其牽涉範圍極大且攸關全國人民隱私權，因此對於健保資料的保護，不僅是健保局的責任，國家也必須負起監督的義務。 因此，本研究針對隸屬於行政院衛生署之健保局為研究對象，藉由ISO 27001與COBIT之關聯性達成資訊安全治理。本研究透過個案研究的方式，第一階段主要是探討中央健康保險局之資訊安全概況；第二階段則是將ISO 27001納入COBIT中，且對該局之決策者以及資訊相關人員進行深度訪談，並以策略、技術、組織、人力及環境之主題推導出相關命題，且針對健保局提供資訊安全治理策略之建議，促使健保局達成營運永續之願景。

關鍵詞 : 資訊安全管理;資訊技術控制目標;國際資訊安全標準;資訊技術治理;資訊安全治理

目錄

參考文獻

一、中文部份 中央健康保險局(2008a)，中央健康保險局簡介[線上資料]，來源: http://www.nhi.gov.tw/webdata /webdata.asp?menu=1&menu_id=3&webdata_id=1159&WD_ID=16[2008, January 19]。 中央健康保險局(2008b)，中央健康保險局全球資訊網隱私保護及安全政策[線上資料]，來源: http://www.nhi.gov.tw/950322網站隱私權政策.htm[2008, January 2]。 中央健康保險局網站(2005)，全民健康保險統計動向[線上資料]，來源: http://www.nhi.gov.tw/webdata/webdata.asp?men u=1&menu_id=4&webdata_id=2063&WD_ID=[2008, Januar y 21]。 中華民國監察院(2004)，中央健康保險局之糾正案文[線上資料]，來源: http://www.cy.gov.tw/index.asp[2008, January 6]。 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，161-168。 行政院研究發展考核委員會(2008a)，行政院及所屬各機關資訊安全管理要點[線上資料]，來源: http://www.rdec.gov.tw/lp.asp?CtNode=3608&CtUnit=743&BasedSD=7&nowPage=2&pagesize=25[2008, January 20]。 行政院研究發展考核委員會(2008b)，行政院及所屬各機關資訊安全管理規範[線上資料]，來源: http://www.rdec.gov.tw/lp.asp?CtNode=3608&CtUnit=743&BasedSD=7&nowPage=2&pagesiz e=25[2008, December 20]。 李菱菱(2001)，國民健保IC卡之規劃與推動，研考雙月刊，25(1)， 50-57。 孫淑景(2003)，內控處理準則電腦資訊循環之個案研究-以BS7799資訊安全及COBIT控制目標為例，中原大學會計學系未出版之碩士論文，4-21。 曹子珊，曹偉駿(2004)，基於平衡計分卡架構設計適用於金融控股產業之資訊安全管理研究，電腦稽核，11，54-69。 葉俊榮(2005)，電子化政府資通安全發展策略與展望，研考雙月刊，29(1)，20-34。 劉見祥 (2006)，捍衛醫療資訊隱私權健保憑證邁入新紀元[線上資料]，來源: http://www.nhi.gov.tw/webdata /webdata.asp?menu=1&menu_id=&webdata_ID=1419[2008, January 10]。 樊國楨(2003)，資訊安全管理系統與稽核，行政院國家科學委員會科學技術資料中心，台北:行政院國家科學委員會。 謝安田(2006)，企業研究方法論(第三版)，彰化:著者發行。 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，資通安全分析專論T94003，1-33。 梁定澎(1997)，資訊管理研究方法總論，資訊管理學報，4(1)， 1-6。 李東峰(2001)，企業資訊安全控制制度之研究，第三屆全國資訊管理博士生聯合研討會論文集，1-22。 吳琮璠(1997)，資訊管理個案研究方法，資訊管理學報，4(1)，7-17。 二、英文部份 Andersen, K. V., & Henriksen, H. Z. (2006). E-Government maturity models: Extension of the Layne and Lee model. Government Information Quarterly, 23(2), 236-248. Andersen, W. P. (2001). Information security governance. Informati- on Security Technical Report, 6(3), 60-70. Elsevier Ltd. Bakry, S. H. (2004). Development of e-Government: A STOPE view. International Journal of Network Management, 14(5), 339-350. Bonoma, T. V. (1985). Case research in marketing: Opportunities, problems, and a process. Journal of Marketing Research, 22, 199-208. Broderick, J. S. (2006). ISMS, security standards and security regulations. Information Security Technical Report, 11(1), 26-31. Elsevier Ltd. 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. Churgin, P. G. (1995). Computerized patient records: The patients ’ response. Hmo Practice / Hmo Group, 9(4), 182-185. 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. Computer Security Institute. (2007). 2007 computer crime and security survey. Arlington, Virginia. Dyer, C. (1986). Disclosure of medical records in litigation. British Medical Journal, 293, 1298. Eloff, M. M. & Von Solms, B. (2000). Information security management: An approach to combine process certification and product evaluation. Computers & Security, 19(8), 698-709. Esteves, J., & Joseph, R. C. (2008). A comprehensive framework for the assessment of e-Government projects. Government Informa Forte, D. (2008). Selling security to top management. Network Security, 2008(3), 18-20. Gadd, C. S., & Penrod, L. E. (2000). Dichotomy between physicians ’ and patients ’ attitudes regarding EMR use during outpatient encounters. Proceedings/AMIA Annual Symposium, 275-279. Hall, M. A., & Rich, S. S. (2000). Genetic privacy laws and patients' fear of discrimination by health insurers: the view from genetic counselors. The Journal of law, medicine & Ethics: a journal of the American Society of Law, Medicine & Ethics, 28(3), 245-257. Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges, Information Security Technical Report, 11(1), 55-61. Elsevier Ltd. Hebert, M. A. (1998). Impact of IT on Health Care Professionals: Changes in work and the productivsity paradox. Health services management research: an official journal of the Association of University Programs in Health Administration / HSMC, AUPH, 11(2), 69-79. Information Systems Audit and Control Association. (2002). IS Standards, Guidelines and Procedures for Auditing and Control Professionals. Illinois: Author 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. IT Governance Institute. (2007). COBIT: Control Objectives Management Guidelines Maturity Models (4.1th ed.). United States of America: Author. Johnson, E. C. (2006). Security awareness: switch to a better programme. Network Security, 2006(2), 15-18. Moulton, R., & Coles, R. S. (2003). Applying information security governance. Computers & Security, 22(7), 580-584. National Institute of Standards and Technology. (2007). NIST Special Publication 800-100, Information security handbook, A guide for managers. Organization for Economic Co-Operation and Development. (1992). OECD Guidelines for the Security of Information Systems. Paris: Author. Organization for Economic Co-Operation and Development. (2001). Guidelines for the Security of Information System. (Rev. Ed.). Paris: Author. Organization for Economic Co-Operation and Development. (2002). Guidelines of the Security Information System and Networks - Towards a Culture of Security. Paris: Author. Ozier, W. (1997). Generally accepted system security principles, Computer Security Journal, 13(2), 69-75. Pasquinucci, A. (2007). Security, risk analysis and governance: a practical approach. Computer Fraud & Security, 2007(7), 12-14. Prakash, A., & Hart, J. A. (1999). Globalization and Governance: An Introduction. London: Routledge. Relyea, H. C. (2008). Federal government information policy and public policy analysis: A brief overview, Library & Information Science Research, 30(1), 2-21. Rusell, D. & Gangemi, G. T. (1992). Computer Security Basics. California : O ’ Reilly & Associates Inc. 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. Schneider, E. C., & Therkalsen, G. W. (1990). How secure are your system? Avenues to Automation, 68-72. 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. Schwarz, A., & Hirschheim, R. (2003). An extended platform logic perspective of IT governance: managing perceptions and activities of IT. Journal of Strategic Information Systems, 12(2), 129-166. tion Quarterly, 25(1), 118-132. Wilson, P. (2007). Governance and security: Side by side. Computer Fraud & Security, 2007(4), 15-16. Von Solms, B, & Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376. Von Solms, B. (2005). Information security governance: COBIT or ISO 1997 or both? Computers & Security, 24(2), 99-104. Von Solms, B. (2006). Information security - The fourth wave. Computers & Security, 25(3), 165-168. Von Solms, R. (1996). Information security management: The second generation. Computer & Security, 15(4), 281-288. Von Solms, R., & Von Solms, B. (2006). Information security governance: A model based on the direct - Control cycle, Computers & Security, 25(6), 408-412. Yin, R. K. (1989). Case study research: Design and methods. (Rev. ed.). Newburry Park, California: Sage Publications. Yin, R. K. (2001). Case study research: Deign and method. Sage Publications.