ITIL與ISO 27001建構大學校園資訊安全治理 : 以中部某大學為例

鄭植尹、曹偉駿

E-mail: 322065@mail.dyu.edu.tw

摘 要

隨著資訊技術的進步，校園資訊系統所提供的服務也越來多元化,享受便利的同時，個人的隱私資料、組織的機密文件也逐漸暴露在安全的漏洞之下。針對提升校園資訊服務的安全等級以及加強組織成員對於資訊安全的認知等目標，政府極力推動大學校園通過資訊安全管理系統稽核，目前ISO 27001當屬有效的稽核工具，但其中的控制措施項目相當繁雜。因此，如何簡化ISO 27001的控制措施以達到安全理論與實務上的最佳化已成為政府單位日益重視的議題，本研究將針對此議題提出基於ITIL與ISO27001之大學校園資訊安全治理模式，並以個案研究方法探討中部某大學之資訊安全治理概況。其研究流程首先針對研究對象之相關人員進行深度訪談。其次，再以策略、技術、組織、人力及環境等構面推導出相關命題，並針對大學校園環境的資訊安全治理策略提出建議，確保大學校園資訊安全治理的永續經營。 With the development of information technology, the service provided by the campus information system becomes increasingly diverse; at the same time of enjoying conveniences, the private information of individuals and the confidential documents of organizations are gradually exposed to the security vulnerability. To raise the security degree of campus information service and enhance the cognition of information security of the members in organizations, the government is actively promoting college campuses to pass the audit of the information security management system. At present, ISO 27001 is the effective audit tool, but its control measures are quite complex. Therefore, how to simplify the control measures of ISO 27001 to reach the optimization in security theory and practice has become the topic attracting increasing attention. Therefore, the research will propose the ITIL and ISO 27001-based campus information security governance model and discuss the situation of the information security governance of a university in middle Taiwan with the case study method. The research process is that we first conduct in-depth interview to the personnel related to the research subjects, then deduce related propositions in accordance with strategies, technologies, organizations, human resources and environments, and finally offer a proposal for the information security governance strategies of college campus to ensure the sustainable operation of college campus information security governance.

一、中文部份 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(pp. 161-168)，台北：私立景文技術學院。 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。 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]。 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。 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，收於中華資訊安全管理協會編，資通安全分析專論，來源：台北，中華資訊安全管理協會，編號T94003 [2005, September]。 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(pp. 1-22)，桃園縣。 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, 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(2), 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(2), 696-712. 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. 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 Information Quarterly, 25(1), 118-132. Fulford, H., & Doherty, N. F. (2003) , The application of information security policies in large UK-based organizations. Information Management and Computer Security, 11(3), 106 – 114. 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. 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. (2008). Aligning CobiT 4.1, ITILV3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute. 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. United states of America: Author. 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. 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. 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. (2006). Information security - The fourth wave. Computers & Security, 25(3), 165-168. Yin, R. K. (1989). Case study research: Design and methods. (Rev. ed.). Newburry Park, California: Sage Publications.

關鍵詞 : 資訊安全管理、資訊技術基礎建設典範、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 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(pp. 161-168)，台北:私立景文技術學院。 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。 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]。 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。 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，收於中華資訊安全管理協會編，資通安全分析專論，來源:台北，中華資訊安全管理協會，編號T94003 [2005, September]。 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(pp. 1-22)，桃園縣。 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, 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(2), 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(2), 696-712. 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. 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 Information Quarterly, 25(1), 118-132. Fulford, H., & Doherty, N. F. (2003) , The application of information security policies in large UK-based organizations. Information Management and Computer Security, 11(3), 106 – 114. 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. 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. (2008). Aligning CobiT 4.1, ITILV3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute. 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. United states of America: Author. 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. 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. 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. (2006). Information security - The fourth wave. Computers & Security, 25(3), 165-168. Yin, R. K. (1989). Case study research: Design and methods. (Rev. ed.). Newburry Park, California: Sage Publications.