

Information Security Governance for Campus Score Management Systems Based on ISO 27001 - A Case Study on Some Junior ...

徐敏凱、曹偉駿

E-mail: 386732@mail.dyu.edu.tw

ABSTRACT

From the 21 century, with information technology and the Internet developing rapidly, government and enterprises have started to import information systems in order to remain competitive and improve performance. With this trend and constant innovation of information network technologies, a variety of powerful and fast processing speed systems mushroomed. These systems not only bring equivalent benefits for the organization, but also make society organizations greatly rely on information systems. Since 1999, the government implemented comprehensive networks in education for promoting economy, and allowed the use of resources can be more smooth in campuses. But the information and communication face information security and confidentiality issues with comprehensive networks, including computer viruses, hackers, control negligence of internal staff and other related issues. The most required protection is privacy of teachers and achievements of students. Some campuses' programming is old, and therefore hackers can implant Trojanhorse to tamper files easily, even stealing users' passwords. The most worst situation always happen in primary schools and junior schools, even now having improved the security, but they is still at risk. Although the government greatly implemented campus information networks, it frequently ignored the problems of information security. For the issue of information security's governance, information technology and information security always play an important role in enterprises, and is less discussion and analyses for information security's governance of campus achievement systems. Therefore, through management processes of information security and improvement of related measures, this study tests the security of campus achievement management systems based on the ISO 27001 standard, and then gives some crucial suggestions.

Keywords : information security governance、 information security threats、 score management systems、 ISO 27001

Table of Contents

中文摘要	iii	英文摘要	iv
誌謝辭	vi	內容目錄	
vii 表目錄	ix	圖目錄	
x 第一章 緒論 第一節 研究背景與動機		1 第二節 研究目的	3
第三節 研究範圍與限制	4	第四節 研究流程	4
第一節 資訊安全與威脅	7	第二節 資訊安全治理	14
全標準之探討	21	第四節 校園成績管理系統	33
研究設計	36	第二節 研究方法	39
析 第一節 個案探討	52	第二節 命題推導	60
果	71	第五章 結論與建議 第一節 結論	73
	75	參考文獻	77

REFERENCES

一、中文部分 蔡憶懷(2000), 開放原始碼-Linux與自由軟體運動對抗軟體巨人的故事, 台北:商周出版。 陳萬淇(1995), 個案研究法, 台北:萬泰。 李順仁(2003), 資訊安全, 台北:文魁圖書出版社。 潘天佑(2011), 資訊安全概論與實務(二版), 台北:基豐資訊。 古永嘉, 楊雪蘭(譯)(2011), 企業研究方法, 台北:華泰。 樊國禎、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, 台北:行政院國家科學委員會科學技術資料中心。 樊國禎(2002), 資訊安全能力評鑑, 台北:行政院國家科學委員會科學技術資料中心。 行政院(1999), 行政院及所屬各機關資訊安全管理要點, 台北。 行政院教育部(2007), 教育體系資通安全規範, 台北。 行政院勞工委員會職業訓練局(2002), 資訊安全管理作業守則, 台北。 行政院研考會(2001), 台北電子化政府推動方案執行情形, 台北。 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。 劉文鈞(2006), 論資訊安全, 品質月刊, 42(10), 66-70。 吳琮璠(1997), 資訊管理個案研究方法, 資訊管理學報, 4(1), 7-17。 梁定澎(1997), 資訊管理研究方法總論, 資訊管理學報, 4(1), 1-6。 楊峻榮(2004), 以風險評估方式規畫校園資安機制, 台灣區域網路中心93年度研討會。 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。 陳耀民(2008), 應用自由軟體建構集中式學務管理系統-以嘉義縣國民小學為例, 南華大學資訊管理學

系碩士論文。鄭植尹(2010), 基於ITIL與ISO 27001建構大學校園資訊安全治理-以中部某大學為例, 大葉大學資訊管理學系碩士班碩士論文。胡雯婷(2011), 建置銀行業私有雲之資訊安全治理-以某銀行為例, 大葉大學資訊管理學系碩士論文。黃文谷(2011), 校園資訊系統安全關鍵評估機制之調查研究-以雲林縣國民小學SFS3學務系統為例, 雲林科技大學資訊管理系碩士論文。行政院研究發展考核委員會(2009), 網路安全的挑戰與策略[線上資料], 來源: <http://www.seminar2009.tw/wnic.tw/download/d2s2c.pdf> [May 23, 2013]。二、英文部分

A. E. Brown and G. G. Grant (2005). Framing the Framework: A Review of IT Governance Research. *Communications of the Association for Information Systems*, 15(2), 696-712. A. Calder (2006). Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide. J. Van Bon (Ed.). Van Haren Publishing. A. Calder (2009). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide. Van Haren Publishing. A. Cobit (2008). 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute (ITGI) and Office of Government Commerce (OGC). 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> [December 20, 2012]. D. B. Parker (1997). Information Security in a Nutshell. *Information System Security*, 6(1), 14-19. E. Maiwald (2004). *Network Security: A Beginner's Guide* (2nd ed.). New York: McGraw-Hill. H. C. Relyea (2008). Federal Government Information Policy and Public Policy Analysis: A Brief Overview. *Library & Information Science Research*, 30(1), 2-21. H. Susanto, F. Muhaya, M. N. Almunawar and Y. C. Tuan (2012). Refinement of Strategy and Technology Domains STOPE View on ISO 27001. arXiv preprint arXiv, 1204-1385. I. M. Haw, S. S. M. Ho, B. Hu and D. Wu (2010). Concentrated Control, Institutions, and Banking Sector: An International Study. *Banking & Finance*, 3(3), 485-497. J. Esteves and R. C. Joseph (2008). A Comprehensive Framework for the Assessment of Government Projects. *Government Information Quarterly*, 25(1), 118-132. J. N. Rosenau (1995). Governance in the Twenty-First Century. *Global Governance*, 1, 13-43. J. S. Broderick (2006). ISMS, Security Standards and Security Regulations. *Information Security Technical Report*, 11(1), 26-31. M. Raydel and F. Stefan (2011). Automation Possibilities in Information Security Management. *European Intelligence and Security Informatics Conference (EISIC)*, 259-262. M. Reiter and P. Rohatgi (2004). Homeland Security. *IEEE Internet Computing*, 8(6), 16-17. 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. M. E. M. Spruit and M. Looijen (1996). IT Security in Dutch Practice. *Computers & Security*, 15-2, 157. 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. 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. P. W. Andersen (2001). Information Security Governance. *Information Security Technical Report*, 6(3), 60-70. R. Richardson (2008). CSI Computer Crime and Security Survey. *Computer Security Institute*, 1, 1-30. R. Ahmad and L. Janczewski (2011). Governance Life Cycle Framework for Managing Security in Public Cloud: From User Perspective. *IEEE International Conference on Cloud Computing (CLOUD)*, 372-379. R. K. Yin (2003). Case study research: Design and methods (Rev. ed.). Newbury Park, California: Sage Publications. S. H. Bakry (2004). Development of e-Government: A STOPE View. *International Journal of Network Management*, 14(5), 339-350. S. H. Solms and R. V. Solms (2006). Information Security Governance: A Model based on the Direct-Control Cycle. *Computers & Security*, 25(6), 408-412. 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. S. J. Mousavian, Sh. Gilaninia, O. Taheri, H. Nikzad, H. Mousavi and F. Z. Seighalani (2012). Information Security Management on Performance of Information Systems Management. *Journal of Basic and Applied Scientific Research*, 2(3), 2582-2588. 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. T. Finne (2000). Information Systems Risk Management: Key Concepts and Business Processes. *Computer & Security*, 19(3), 39-50. T. V. Bonoma (1985). Case Research in Marketing: Opportunities, Problems and a Process. *Journal of Marketing Research*, 22(2), 199-208. W. D. Bruijn, M. R. Spruit and M. Heuvel (2010). Identifying the Cost of Security. *Journal of Information Assurance and Security*, 5, 74-83.