Information Security Governance for University Campus's Private Cloud　A Case Study on Some University in Middle Taiwan

E-mail: 389482@mail.dyu.edu.tw

ABSTRACT

The benefits of cloud computing services have been deeply rooted in our lives, and Business or personal use have been inseparable from cloud computing. But enjoying these convenient resources, the crisis of information leakage is also very great. Although cloud computing environments have high performance and flexibility and low costs, there are still many security issues to stop users to use cloud computing. Therefore, this thesis will explore information security issues in the university campus's private cloud, and propose information security governance based on Trusted Cloud Initiative. This research is based on ITIL (Information Technology Infrastructure Library) for incident management, based on ISO 27001 for the control items, and based on ISO 27005 for the risk procedure. In addition, using the way of case study this thesis derives several propositions in terms of five dimensions including strategies, technologies, organizations, people and environments. This research gives suggestions for the information security governance of university campus's strategies, and lets universities be able to handle the risk of information security for the cloud computing services.

Keywords : Information security management　ITIL　ISO 27001　ISO 27005　Information security governance

Table of Contents

REFERENCES

                        ( )(2009)   :   (Donald R. Cooper, Pamela S. Schindler., 2008)
             (2006)   2006   :
                  (2009)   : http://www.seminar2009.twnic.tw/download/d2s2c.pdf [2012, march 12]
     (1997)   4(1)　7-17   (2009)   :
     (1997)   4(1)　1-6   (2010)
172-192   (1995)   :   (2010)   ISMS　ITSMS   : http://www.icst.org.tw/docs/Fup/6
_   ISMS　ITSMS.pdf [2010, june 21]   (2010)　99   (PDF)   :
http://www.moeasmea.gov.tw/dl.asp?filename= 192016395771.pdf [2012, May 10]   (2011)　2011   ( ).pdf   :
http://book.moeasmea.gov.tw/book/doc_detail.jsp?pub_SerialNo= 2011A01070&click= 2011A01070# [2012, may 27]
     (2009)　ISO/IEC 27005   CORAS   :   T97022
                    1991   AHP

(2008)   (ISO/IEC FDIS 27005)   :fsms.bsmi.gov.tw/cat/epaper/970331

.ppt [2012, March 12]   (2005)   :   ISO/IEC 17799: 2005-06-15   12.6.1

(2010)   :

T 98002   :   IBM   :   :

http://www-935.ibm.com/services/tw/gts/pdf/outlook_emerging_security_technology_trends.pdf [2012, march 13]   James Lyne(2012)   IT

2011   : http://www.informationsecurity.com.tw/article/article_detail.aspx?tv= &aid= 6555&pages= 2 [2012, march 16]

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 and 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. 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(Jan.25,2013) CSA. (2009).Security Guidance for Critical Areas of Focus in Cloud Co-mputing.Retrieved from Cloud Security Alliance,Institute for Learning Technologies Web site: http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf (jan.8,2013)(Feb. 25, 2013) CNS 27002: 2007 (2007). Information technology-Information technology-Security techniques-Code of practice for information security management, Chinese national standard. Taipei: Author. Rusell, D. and Gangemi, G. T. (1992). Computer security basics. California : O'Reilly & Associates Inc. 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 ISO 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. Retrievedfrom National Institute of Standards and Technology, Instiute for Learning Technologies Web http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf(Jan.5,2013). 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 on Computational Intelligence and Software Engineering (CiSE), 1-3. R. K. Yin. (1983). The case study method: An Annotated Bibliography. Washingtom, D.C.: COSMOS Corporation.