A Study on ISMS Policy: Importing Personal Data Protection of ISMS

Chien-Cheng Huang[1, *], Kwo-Jean Farn[2], and Frank Yeong-Sung Lin[1]

[1] Department of Information Management,
National Taiwan University,
Taipei 106-17, Taiwan, ROC
d97725002@ntu.edu.tw, yslin@im.ntu.edu.tw

[2] Institute of Information Management,
National Chiao Tung University,
Hsinchu 300-10, Taiwan, ROC
kjf@iim.nctu.edu.tw

Received 15 August 2011; Revised 15 January 2012; Accepted 15 March 2012

Abstract. Once again, when entering the information age, digital space has aroused international competition in the fifth domain after land, navy, air force and aerospace. While enjoying the huge benefits provided by information and information systems, people also face severe challenges in terms of information security. The standard compliant information security management system (ISMS) has become a national information security policy, and risk management is already a consensus for the core task of establishing an ISMS. However, ISMS policy lacks a connection to the strategic risk management of organizations, which is normal for organizations which have passed ISMS certification. This study explores the nature of ISMS policy and describes the relationship of such a policy when establishing an ISMS by means of a case study. Besides, we also propose a method to integrate the ISMS with information security governance (ISG).

Keywords: ISMS, policy, ISG, personal data protection, information security management

Acknowledgment

The authors would like to express our appreciation to the anonymous reviewers for their precise suggestions, and the support from Local Tax Bureau, Hsinchu City, Taiwan, Republic of China.

References

[1] NICST (National Information and Communication Security Taskforce, Executive Yuan, Taiwan, R.O.C.), "*National Information and Communication Security Development Program (2009~2012)*," Information Security Dispatch Document No. 0980100055, February 5, 2009.

[2] ISO/IEC, "Information Technology – Security Techniques – Information Security Management Systems – Requirements," *ISO/IEC 27001:2005(E)*, October 15, 2005.

[3] C.C. Huang, K.J. Farn, F.Y.S. Lin, "A Study on Information Security Management with Personal Data Protection," in *Proceedings of 17th International Conference on Parallel and Distributed Systems*, Tainan, Taiwan, pp. 624-630, 2011.

[4] R. Ross et al., "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," *NIST Special Publication 800-37 Revision 1*, February 2010.

[*] Correspondence author

[5] MOJ (Ministry of Justice, Executive Yuan, Taiwan, R.O.C.), "*Personal Data Protection Act*," Presidential Decision Directive No. 09900125121, May 26, 2010.

[6] BSI (British Standards Institution), "Data Protection – Specification for a Personal Information Management System," *BS 10012:2009*, May 31, 2009.

[7] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C.D. Smith, D.I. Steinberg, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPPA) Security Rule," *NIST Special Publication 800-66 Revision 1*, October 2009.

[8] E. McCallister, T. Grance, K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," *NIST Special Publication 800-122*, April 2010.

[9] PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, Version 2.0, October 2010.

[10] ISO/IEC, "Information Technology – Security Techniques – Security Information Objects for Access Control," *ISO/IEC 15816:2002(E)*, February 1, 2002.

[11] ISO/IEC, "Information Technology – Security Techniques – Code of Practice for Information Security Management," *ISO/IEC 27002:2005(E)*, June 15, 2005.

[12] N. Madelung, O. Weissmann, "Marked-up Text of ISO/IEC 3rd WD 27002 (Revision) – Information Technology – Security Techniques – Code of Practice for Information Security Management," ISO/IEC JTC 1/SC 27 N9472, November 8, 2010.

[13] ISO/IEC, "Information Technology – Security Techniques – Code of Practice for Information Security Management," *ISO/IEC 1st CD 27002*, ISO/IEC JTC 1/SC 27 N10656, November 21, 2011.

[14] ISO/IEC, "Information Technology – Security Techniques – Privacy Reference Architecture," *ISO/IEC 1st CD 29101*, ISO/IEC JTC 1/SC 27 N8808, June 10, 2010.

[15] ISO/IEC, "Information Technology – Security Techniques – Privacy Framework," *ISO/IEC 29100*, December 15, 2011.

[16] ISO/IEC, "Corporate Governance of Information Technology," *ISO/IEC 38500:2008(E)*, June 1, 2008.

[17] J. Kim and K. Harada, "Text for ISO/IEC 1st CD 27014 – Information Technology – Security Techniques – Governance of Information Security," ISO/IEC JTC 1/SC 27 N9017, November 8, 2010.

[18] NICST (National Information and Communication Security Taskforce, Executive Yuan, Taiwan, R.O.C.), *Implementation Program on Information Security Responsibility Classification in Governmental Departments*, Information Security Dispatch Document No. 0980100328, June 1, 2009.

[19] RDEC (Research Development and Evaluation Commission, Executive Yuan, Taiwan, R.O.C.), *Guide for Web Application Security*, Version 2, March 2009.

[20] Taxation Agency (Taxation Agency, Ministry of Finance, Executive Yuan, Taiwan, R.O.C.), Dispatch Document No. 09822003350, November 4, 2009.

[21] ISO/IEC, "Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model," *ISO/IEC 15408-1:2009(E)*, 3rd Edition, December 15, 2009.

[22] ISO/IEC, "Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 2: Security Functional Components," *ISO/IEC 15408-2:2008(E)*, Third Edition; August 15, 2008.

[23] ISO/IEC, “Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Components,” *ISO/IEC 15408-3:2008(E)*, Third Edition; August 15, 2008.

[24] ICO (Information Commissioner's Office), *Privacy Impact Assessment Handbook*, Version 2, June 2009.