A Study on Information Security Management with Personal Data Protection

Chien-Cheng Huang
Department of Information Management
National Taiwan University
Taipei, Taiwan
d97725002@ntu.edu.tw

Kwo-Jean Farn
Institute of Information Management
National Chiao Tung University
Hsinchu, Taiwan
kjf@iim.nctu.edu.tw

Frank Yeong-Sung Lin
Department of Information Management
National Taiwan University
Taipei, Taiwan
yslin@im.ntu.edu.tw

***Abstract*—In the process of standardization, whether the announcement of a standard represents a cause or an outcome, it is opportunity of the trend of standardization or achievement. The process of standardization is to understand “why” and “how” to explore the detailed outline of a time flow. From a long-term perspective, a standard is the milestone of the standardization process. On May 26th 2010, with the announcement of the Personal Data Protection Act in Taiwan, information security management (ISM) of the Personal Data Protection Act has received much attention from the public. This study is centered on the working items of standards announced by the International Organization for Standardization (ISO) and the ongoing information security management system (ISMS) standards and standardization in order to propose standards which comply with the ISMS of the Personal Data Protection Act and methods which increase implementation control measures.**

Keywords: Information exchange, ISMS, information sharing, personally identifiable information, standardization.

I. Introduction

The Legislative Yuan in Taiwan issued an amendment of the “Computer-Processed Personal Data Protection Act” to the “Personal Data Protection Act” with the relevant revised text on April 27th 2010, and this was announced by the President on May 26th 2010 [1]. According to Article 18, which is related to the Personal Data Protection Act and information security management (ISM): “Those public sectors that conserve files with personal data shall assign specific persons to proceed security maintenance matters to prevent personal data from stealing, altering, damaging, reducing or disclosing.” and Article 27: “Those non-public sectors that conserve files with personal data shall adopt appropriate safety measures to prevent personal data from stealing, altering, damaging, reducing or disclosing. The Central Competent Authority for the Target Industry shall assign non-public sectors to draft plan for personal data file protection and maintenance or methods dealing with personal data after the termination of the business.”

Because of the financial risk involved in the announced rules and ongoing standards among the various target industries, the ISM of personal data has been a popular information security issue [2, 3, 4]. For example, according to one court decree in California, USA, concerning a collective litigation which violates privacy, seven plaintiffs accused Google Gmail’s embedded Buzz social networking service of privacy infringement. Google agreed to pay compensation of USD 8,500,000 in an out-of-court settlement, 30% of which goes to the lawyer, while USD 2,500 at most goes to each of the seven plaintiffs. The remainder will go to institutions dedicated to Internet privacy or education [5].

With the tremendous pace of development in electronics technology, the combination of computers and the Internet has dazzled people in the early twenty-first century. According to the “Guidelines Governing the Protection of Privacy and Transporter Flows of Personal Data” announced by the Organization for Economic Co-operation and Development (OECD) on September 23rd 1980, the security protection of personal data online will face various safety scenarios. On the other hand, besides the addition of “Notices and Damage Precaution Principles”, the privacy framework announced by the Asia-Pacific Economic Cooperation (APEC) reported the same principles as the guidelines announced by the OECD [6, 7, 8, 9].

On such a basis, in Section II, the framework of personal data protection standardization has been stated to explore ISMS implementation from a financial perspective. In Section III, the items of controls should be added when drafting the guidelines to personal data security protection standards. Finally, this research is discussed and concluded in Sections IV and V.

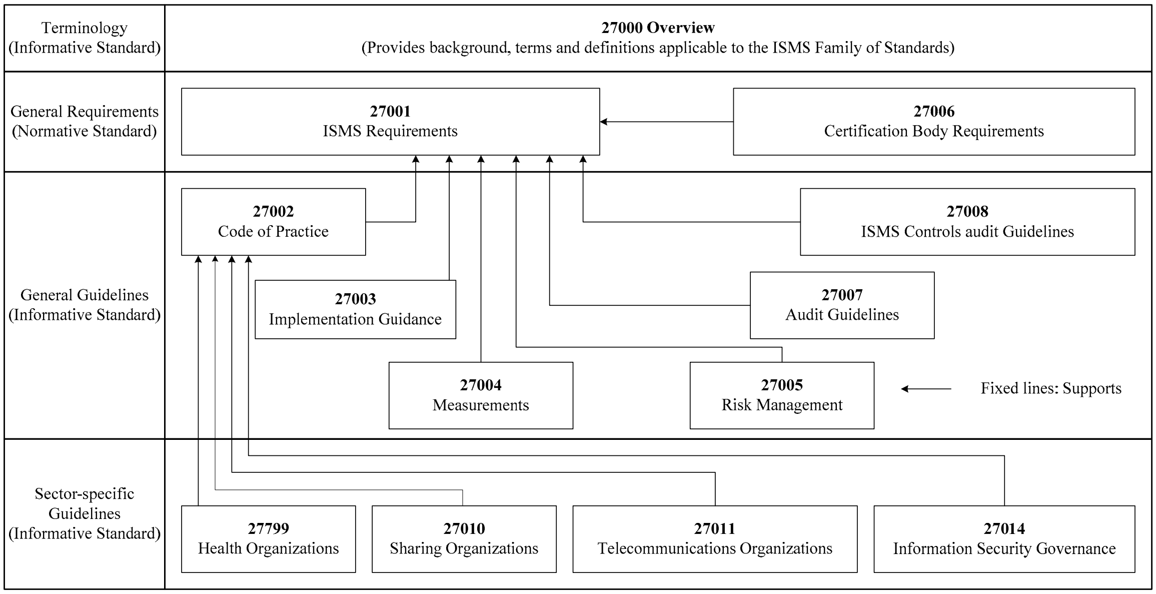
II. Personal data with ISM

Opportunities for future will be missed if the past is allowed to argue with today. Having been invited by the World Summit on Information Society (WSIS), Dr. Walter Fumy, Chairman of ISO/IEC JTC 1/SC 27, announced the ISM model of defense in depth (DiD) from the ISO viewpoint on September 24th 2004, which contained the ISO/IEC 27003 standards and was officially published on February 1st 2010 [10]. The first milestone for the work of ISMS standardization in stage one has been established, and this is shown in Fig. 1 [11, 12, 13].

The ISMS international standards provide a model to be followed when establishing and maintaining a management system. A consensus was reached by various experts on the characteristics when incorporating the ISMS model (ISMS family of standards) into the information security field, which was regarded as art internationally. The ISMS model is a reflection of the change which will proceed the implementation of various fields, which ISO 27799 and ISO/IEC 27011 have announced as being regulatory to the change of implementation for controls in the health and telecommunication fields, respectively [14, 15]. A correlation between ISO/IEC 29100 of the ISMS family of

1521-9097/11 $26.00 © 2011 IEEE
DOI 10.1109/ICPADS.2011.16

IEEE computer society



Note: ISO/IEC 27001 and ISO/IEC 27005 modified to refer ISO 31000 etc., which scheduled to be completed in May 2012.

Figure 1. ISMS family of standards relationships

standards and the ISMS will be an issue to be faced when establishing an ISMS audit in the implementation of personal data protection [16, 17].

Personally Identifiable Information (PII) is a request from the Federal Information Security Management Act (FISMA), which is a concept proposed to reinforce the index of the ISMS with regard to personal data security [18]. The personal data protection and related standards published by the ISM include the ISMS Family of Standards (ISO/IEC 27000 Family of Standards), BS 10012 [19], NIST SP 800-66 [20], NIST SP 800-122 [18], PCI DSS [21] etc. which can be provided as references for implementation. Due to operability, related standards were established from October 2003 to May 2006 when PII was incorporated into ISO/IEC JTC 1/SC 27/WG 5. The core components of the privacy standard framework are shown as ISO/IEC 29100 [22].

However, the regulation which decreed that “an aggregation effect should be considered” is listed in implementation section 10.7.2, “disposal of media” in ISO/IEC 27002 [23]. PII-related standards are being established, and these will comply with the data protection of personal information and ISMS regulations about privacy, as shown in Table I [23, 24]. Also, an ISMS with personal data protection will be established by referring to the added controls of ISO 27799 and ISO/IEC 27012 [14, 23, 24, 25, 26].

On the other hand, according to Article 2 of the Personal Data Protection Act, “disposal refers to records, input, storage, editing, alteration, change, search, delete, output, connection or internal transmission of personal data establishment and utilization.” The disposal of personal data covers storage, which is defined as below respectively by referring to related legislation [2, 7, 8]:

- **Information retention policy**: states that the duty of agencies in terms of the entity of personal data, classification and security level of electronic files, length of conservation, manner and custodian, laws, internal audit and request of information security governance (ISG) will be complied with.
- **Data retention and disposal policy**: states the implementation policy and the procedure of agencies to retain and dispose of data.

On such a basis, in order to protect the personal data of tax payers, a Local Tax Bureau has requested the House Tax, Levying Land Value Tax, Agricultural Land Tax, Vehicle Tax, Levying Land Increment Tax, Deed Tax, Stamp Tax, Levying Amusement Tax, Tax Unpaid, Export Tax Refund and various businesses to disclose their data retention and disposal policy. According to PCI DSS, requirements and testing procedure of ISMS controls are proposed for a personal data retention and disposal policy, and provided as a reference for each sales department [21].

In addition, according to Garfinkel and Shelat’s work [27], the overwritten disc can still be recovered as it is by referring to the security disposal or reused ISMS regulation of equipment, as shown in Table II [23, 24]. The operation flow for the sanitization of the magnetic data of discs and hard drives is shown as NIST SP 800-88 [18, 28, 29]. Then, the ISMS should introduce an appropriate standard regulation, as indicated in Table III [23]. This should proceed to the design of a personal data filing system and the implementation of working items, as shown in ISO/TR 15489-2:2001(E) [30].

A Local Tax Bureau can be taken as a case study to describe ISMS implementation, in which Article 18 of the Personal Data Protection Act has clearly specified the duty of public sectors in terms of ISM affairs of personal data [1]. This paper has established the principles by roles and responsibilities which correspond to the rights and duties of the Personal Data Protection Act, as listed below:

TABLE I. STANDARDS OF DATA PROTECTION AND PRIVACY OF PERSONAL INFORMATION IN ISO/IEC 27001 AND 27002

<table>
<tr><td>A.15.1.4</td><td>Data protection and privacy of personal information</td><td><u>Control</u>
Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.</td></tr>
<tr><td colspan="3"><u>Implementation guidance</u>
An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information.
Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who should provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personal information and ensuring awareness of the data protection principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personal information should be implemented.
<u>Other Information</u>
A number of countries have introduced legislation placing controls on the collection, processing, and transmission of personal data (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing, and disseminating personal information, and may restrict the ability to transfer that data to other countries.</td></tr>
</table>

- Civil Service Ethics Division: security and maintenance of personal data files.
- Legal Affairs Division: lawsuits involving damage/reimbursement and related penalties.
- MIS Division: the establishment and maintenance of related information technology (IT) will be released online or in other appropriate manners for public review, including the name of the personal data file, the agency name, contact, reasons and the purpose of conservation and type of personal data, etc.
- Administration Division: provides the person involved with an application and inquiry, reading and copying, etc.
- Audit Division: implements a personal data protection sales audit.
- ISMS-in-charge Division: Coordinates Personal Data Protection Act-related affairs.
- Various Divisions: each unit-in-charge will clearly notify and agree to the collection, disposal and use of personal data with written consent, and each unit-in-charge will notify the person involved in any stealing, disclosure, alteration or other damages of personal data caused by rule violation in an appropriate way after the case has been verified.

Information security management differs according to standards. The standard of information security differs according to implementation. Notwithstanding the foregoing, an appropriate guideline for the "methods dealing with personal data after the termination of personal data file security maintenance plan and affairs" will be established for implementation if various mandatory or referencing ISMS standards are followed in Taiwan.

TABLE II. STANDARDS OF SECURE DISPOSAL OR RE-USE OF EQUIPMENT IN ISO/IEC 27001 AND 27002

<table>
<tr><td>A.9.2.6</td><td>Secure disposal or re-use of equipment</td><td><u>Control</u>
All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.</td></tr>
<tr><td colspan="3"><u>Implementation guidance</u>
Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.
<u>Other information</u>
Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.
Information can be compromised through careless disposal or re-use of equipment. (Note: The vulnerabilities of inference control are made for personally identifiable information (PII).)</td></tr>
</table>

TABLE III. NORMATIVE REFERENCES OF CONTROLS IN ISO/IEC 27002

Controls	Normative references	Classes
Information security policy document (5.1.1)	ISO/IEC 13335-1:2004	Other information
Management commitment of information security (6.1.1)	ISO/IEC 13335-1:2004	Other information
Independent review of information security (6.1.8)	ISO/IEC 19011:2002	Other information
Inventory of assets (7.1.1)	ISO/IEC 27005:2008	Implementation guidance
Security of equipment off-premises (9.2.5)	ISO/IEC 18028	Implementation guidance
Network controls (10.6.1)	ISO/IEC 18028	Other information
Security requirements analysis and specification (12.1.1)	ISO/IEC 15408:1999 ISO/IEC 27005:2008	Other information
Policy on the use of cryptographic controls (12.3.1)	ISO/IEC 13888-1:2004 ISO/IEC 14516:2002 IEEE P1363:2000 OECD Guidelines for Cryptography Policy (1997)	Other information
Key management (12.3.2)	ISO/IEC 9796 ISO/IEC 14888 ISO/IEC 11770:1996	Other information
Access control to program source code (12.4.3)	ISO 10007 ISO/IEC 12207	Other information
Information leakage (12.5.4)	ISO/IEC 15408:1999	Implementation guidance
Reporting information security events (13.1.1)	ISO/IEC TR 18044:2004	Other information
Protection of organizational records (15.1.3)	ISO 15489-1:2001	Other information
Note: (*n*) is a session number of ISO/IEC 27002:2005(E).		

TABLE IV. REQUIREMENTS OF ISMS FOR INFORMATION SHARING (IS-ISMS) OF PERSONAL DATA

ISO/IEC 27001:2005(E)			
5. Security Policy [1,2,2,0,0]			
6. Organizing information security [2,11,2,0,0]			
7. Asset management [2,5,2,7,0] (Add one control objective)			
8. Human resources security [3,9,0,0,1]	9. Physical and environmental security [3,13,13,6,3]	10. Communications and operations management [10,32,24,3,11]	12. Information systems acquisition, development and maintenance [6,16,3,1,2]
11. Access control [7,25,10,2,6]			
13. Information security incident management [2,5,2,1,1] (Add one control objective)			
14. Business continuity management [1,5,2,0,0]			
15. Compliance [3,10,3,0,0]			
Note: [*m*, *n*, *o*, *p*, *q*]: [Number of Control Objectives for ISO/IEC 27001, Number of Controls for ISO/IEC 27001, Number of Added Controls for IS-ISMS, Number of New-added Controls for IS-ISMS, Number of Mandatory Controls for IS-ISMS]			

III. INFORMATION-SHARING OF PERSONAL DATA SHOULD BE AN ADDED REQUIREMENT OF ISMS

How the ISMS complies with the rules and makes adjustments according to the announcement of Personal Data Protection Act has become one of the focuses of ISM. A good ISMS policy can provide a successful full view when implementing the working items of ISMS, enabling graceful behavior and an unhurried attitude toward executors. On this basis, among the established ISMS standards, the requirements which should be added to ISO/IEC 27001, the regulation of the Personal Data Protection Act, are listed below [24]:

- **Section 4.2.1 b) 2):**
  Take business and legal or regulatory requirements, and contractual security obligations into account.
- **Section 4.2.1 c) 1):**
  Identify a risk assessment methodology suited to the ISMS, and the identified business information security, legal and regulatory requirements.
- **Section 5.2.1 c):**
  Identify and address legal and regulatory requirements and contractual security obligations.
- **Section 7.3 c):**
  Modification of procedures and controls which affect information security, as are necessary to respond to internal or external events which may impact the ISMS, including changes to:
  4) regulatory or legal requirements
- **Section A.15.1 (Compliance with legal requirements):**
  Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

Section 7.3 c) 4) will accommodate the legislative progress of the Personal Data Protection Act with revisions to be made within a certain time. Nevertheless, the controls of appendix A of ISO/IEC 27001 will refer to published and ongoing standards.

Information-sharing of personal data should refer to the requirements of the ISMS, as shown in Table IV. The interpretation of section 4 to section 8 of ISO/IEC 27001 in this text are all expanded, while control objectives were expanded in ISO/IEC 27010 [29]. Moreover, the new added control number is the unexpanded control which has been added.

In terms of the aspect of shared information of asset management, the existence of appropriate protection should be mandatorily verified during the exchange process, with a principle of minimum required privilege introduced for the information exchange policy. The user and operation procedure, and the IT operation procedure which represents users simply allow data access behavior to be authorized to complete the task assigned by information exchange working items. In order to control the information flow within the information system, between systems, within the internet and between internets, the authorization of mandatory checks is introduced for information systems and the internet so as to comply with related access policies and processes of information exchange for various operations [14, 15, 24, 29].

In the ISMS of information sharing (IS-ISMS), the mandatory controls described as “should” are shown in Table V [23, 26]. This study proposes four newly-added control measures: 1. the appropriate protection is verified during the operation of shared information exchange. 2. General requirements are made for access control. 3. The only identification of the theme of shared information. 4. The establishment of an early warning system which is provided as an information security alert for information-sharing.

As for the access control policy of information exchange between information systems, the data provided by the original information system should be placed in a temporary file format as per authorized search format requirements when the information system uses the data of other systems. Any direct access to data files or databases is prohibited. Only a minimum scope of data is allowed to be provided after files are converted through interface software, e.g. the data storage access control proposed by ISO/IEC 15816 [31]. On the other hand, this research proposes a framework of security for database systems (as indicated in Fig. 2) [32, 33], with the corresponding two aspects of DiD and defense in horizontal (DiH), respectively. In DiD, each data is processed by authentication, access control, certification of input data, and control of output data, to ensure the rationality of input data and the consistency of output data. In DiH, the application server executes a secret sharing approach to increase information confidentiality, improve robust database security, and enhance database survival. Moreover, a secret sharing approach is used for each data.

The purpose of information exchange protection is to ensure the existence of proper protection for the information exchange process between communities. A good index is provided in section 10.8 of ISO/IEC 27002 for the establishment of the regulation from an IT perspective [23]. The following controls, which should be added, are proposed by the paper for implementation purposes:

- **Level indication of shared information**: should divide the shared information into "person concerned only", "certain audience only", "information sharing communities only", and "open" levels, with clear indication.
- **Filtering of sensitive information**: sensitive data (e.g. facts of crime descriptions etc.) of one piece of information should be deleted or expressed separately when it reports different levels of information-sharing.
- **An information disclaimer of declined information-sharing should be established**: this should provide channels to the persons concerned, such as listening, understanding and clarifying suspicious points and difficulties with special requirements when they fail to acquire information.

On the basis of the above, reference should be made to the regulation of the ISMS family of standards and the creation of ISM controls which comply with the Personal Data Protection Act should be issues for implementation.

It seems that safety may be just like air; it is completely valueless, and can only be felt once it has been lost. It is time-consuming and difficult to identify verification when private information is disclosed externally, which is an unprecedented threat to e-Taiwan. There is a need to make the public fully aware that a successful, superior internet society is enabled, where convenience and safety to the lives of people are ensured only by having an ISMS implemented in daily life when faced with the rapid popularity of an internet-based lifestyle and incessant information security threats.

IV. Discussion

A standard is certified by a recognized organization with a consensus to provide documents for the related regulations, guidelines or characteristics of various activities or outcomes for normal or repeated use, to expect an optimal level of order under one circumstance. Standardization is an activity for the establishment of joint and frequently-used provisions upon real or potential problems within a certain scope to expect to achieve the optimal level of order. Such an activity of standardization particularly includes the establishment, issue and implementation processes of standards. In short, standards are the origin of standardization, while standardization is the practice of standards. The development of standards should be based on the summative outcomes of science, technology and practice, with the aim of facilitating optimal joint efficiency.

Table V. IS-ISMS shall do the mandatory controls in ISO/IEC 27002

Session Number	Session Name
N/A	Note: The appropriate protection is verified during the operation of shared information exchange.
8.3.3	Removal of access rights
9.2.5	Security of equipment off-premises
9.2.6	Secure disposal or re-use of equipment
9.2.7	Removal of property
10.1.2	Change management
10.1.4	Separation of development, test, and operational facilities
10.3.2	System acceptance
10.4.1	Controls against malicious code
10.5.1	Information back-up
10.7.2	Disposal of media
10.7.3	Information handling procedures
10.8.1	Information exchange policies and procedures
10.8.2	Exchange agreements
10.10.3	Protection of log information
10.10.6	Clock synchronization
N/A	Note: General requirements are made for access control.
11.1.1	Access control policy
11.2.1	User registration
11.2.2	Privilege management
11.6.1	Information access restriction
N/A	Note: The only identification of the theme of shared information.
12.2.4	Output data validation
N/A	Note: The establishment of an early warning system which is provided as an information security alert for information-sharing.

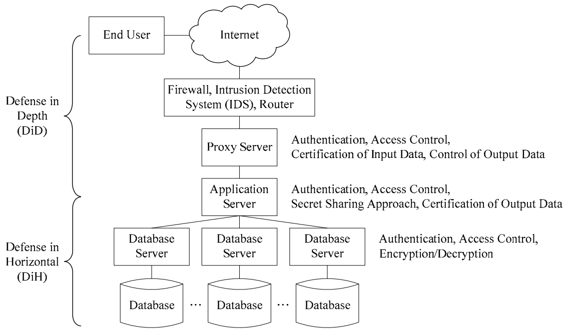

End User
Internet
Defense in Depth (DiD)
Firewall, Intrusion Detection System (IDS), Router
Proxy Server
Authentication, Access Control, Certification of Input Data, Control of Output Data
Application Server
Authentication, Access Control, Secret Sharing Approach, Certification of Output Data
Defense in Horizontal (DiH)
Database Server
Database Server
Database Server
Authentication, Access Control, Encryption/Decryption
Database
Database
Database

Figure 2. Database system security framework

The implementation of an ISMS is not an incident or a situation. It is a series of actions dispersed in the ISMS process. These actions can be seen everywhere, even in the operation at the top management level. The ISMS process is managed through planning, execution, supervision and improvement, as well as other fundamental management processes. For Personal Data Protection Act compliant implementation, please refer to the alignment methods for information security and businesses and the ISG framework announced in ISO/IEC 27014 [34, 35].

Consequently, this paper proposes an implementation framework which helps to correct business and ISMS of information security, followed by vision, strategy, planning, implementation and operation, as shown in Fig.

3. This Framework is a top-down approach. Firstly, to set up the objectives, strategies and a bundle portfolio including a master plan (program) and sub-plan (project) of implementation should be mapped out, all of which requires the use of appropriate assets to enable the operation. In an organization structure, categorization and classification are required for information and information systems at various stages, with ISMS running through the entire framework. ISMS is the integrity of both sides of information security. In fact, the promotion of the Personal Data Protection Act is the best example.

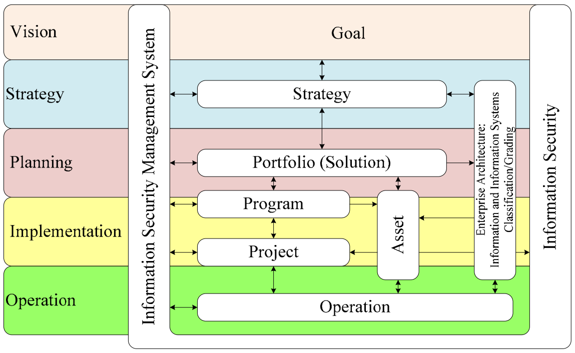


Figure 3. Information security implementation framework

V. Conclusion

In summary, a standard helps to accumulate knowledge and experience, while standardization expects to reinforce standard knowledge upon a systematic, consistent method for inheritance. This paper has referred to the development track of the ISMS family of standards to propose the Personal Data Protection Act compliant ISMS implementation method to progress the ISMS standardization and environment in Taiwan.

Acknowledgment

The authors would like to express our appreciation to the Local Tax Bureau, Hsinchu City, Taiwan, R.O.C., for their assistance in the material.

References

[1] MOJ (Ministry of Justice, Executive Yuan, Taiwan, R.O.C.), "*Personal data protection act*," Presidential decision directive No. 09900125121, May 26, 2010.

[2] 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.

[3] NICST (National Information and Communication Security Taskforce, Executive Yuan, Taiwan, R.O.C.), "*Reference manual for information systems classification/grading and authentication mechanism*," Information security dispatch document No. 0990100394, July 5, 2010.

[4] DGBAS (Directorate-General of Budget, Accounting and Statistics, Executive Yuan, Taiwan, R.O.C.), Information Management Center, Dispatch document No. 09990000855, July 28, 2010.

[5] R. McMillan, "Google settles privacy lawsuit over Buzz," *IDG News*, September 2010.

[6] APEC (Asia – Pacific Economic Cooperation), "*APEC privacy framework*," 2005.

[7] AustLII (Australasian Legal Information Institute), "*Privacy act*," 1988.

[8] M. Grall, and A. Plate, "4th working draft for ISO/IEC 27001 – Information technology – security techniques – information security management systems – requirements," ISO/IEC JTC 1/SC 27 N9001; November 15, 2010.

[9] Verizon Business, "*2010 Data breach investigations report*," 2010.

[10] ISO/IEC, "Information technology – security techniques – information security management system implementation guidance," *ISO/IEC 27003:2010(E)*, February 1, 2010.

[11] W. Fumy, "ISO/IEC JTC 1 Plenary Meeting," Presentation, Banff, Canada; November 2005.

[12] ISO/IEC, "Information technology – security techniques – information security management systems – overview and vocabulary," *ISO/IEC 27000:2009(E),* May 1, 2009.

[13] E. Andrukiewicz, and R. Kissel, "2nd working draft for ISO/IEC 27000 (revision) – information technology – security techniques – information security management systems – overview and vocabulary," ISO/IEC JTC 1/SC 27 N9027, November 23, 2010.

[14] ISO, "Health informatics – information security management in health using ISO/IEC 27002," *ISO 27799:2008(E)*, July 1, 2008.

[15] ISO/IEC, "Information technology – security techniques – information security management guidelines for telecommunications organizations based on ISO/IEC 27002," *ISO/IEC 27011:2008(E)*, December 15, 2008.

[16] ISO/IEC, "Information technology – security techniques – privacy reference architecture," *ISO/IEC 1st CD 29101*, ISO/IEC JTC 1/SC 27 N8808, June 10, 2010.

[17] ISO/IEC, "Information technology – security techniques – privacy framework," *ISO/IEC FCD 29100*, ISO/IEC JTC 1/SC 27 N9226, November 10, 2010.

[18] E. McCallister, T. Grance, and K. Scarfone, "Guide to protecting the confidentiality of personally identifiable information (PII)," *NIST special publication 800-122*, April 2010.

[19] BSI (British Standards Institution), "Data protection – specification for a personal information management system," *BS 10012:2009*, May 31, 2009.

[20] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C.D. Smith, and 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.

[21] PCI Security Standards Council, "*Payment card industry (PCI) data security standard: requirements and security assessment procedures*," Version 2.0, October 2010.

[22] K. Rannenberg, C. Sténuit, A. Yamada, and S. Weiss, "Working group 5 identity management and privacy technologies within ISO/IEC JTC 1/SC 27 – IT security techniques," Presentation, *Proceedings of the joint workshop of ISO/IEC JTC 1/SC 27/WG 5, ITU-T SG17/Q.6, and FIDIS on identity management standards*, Lucerne, Switzerland, September 30, 2007.

[23] ISO/IEC, "Information technology – security techniques – code of practice for information security management," *ISO/IEC 27002:2005(E)*, June 15, 2005.

[24] ISO/IEC, "Information technology – security techniques – information security management systems – requirements," *ISO/IEC 27001:2005(E)*, October 15, 2005.

[25] ISO/IEC, "Information technology – security techniques – ISM guidelines for e-government services," *ISO/IEC NP 27012*, November 8, 2008.

[26] 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.

[27] S.L. Garfinkel, and A. Shelat, "Remembrance of data passed: a study of disk sanitization," *IEEE Security & Privacy*, vol. 1, no. 1, 2003, pp. 17-27.

[28] R. Kissel, M. Scholl, S. Skolochenko, and X. Li, "Guidelines for media sanitization," *NIST special publication 800-88*, September 2006.

[29] M. Nash, "Text of ISO/IEC 1st CD 27010 – information technology – security techniques – information security management for inter-sector and inter-organizational communications," ISO/IEC JTC 1/SC 27 N9013, November 8, 2010.

[30] ISO, "Information and documentation – records management – part 2: guidelines," *ISO/TR 15489-2:2001(E)*, September 15, 2001.

[31] ISO/IEC, “Information technology – security techniques – security information objects for access control,” *ISO/IEC 15816:2002(E)*, February 1, 2002.

[32] J.J. Wylie, M.W. Bigrigg, J.D. Strunk, G.R. Ganger, H. Kiliççöte, and P.K. Khosla, “Survivable information storage systems,” *IEEE Computer*, vol. 33, no. 8, 2000, pp. 61-68.

[33] K.J. Farn, C.T. Chao, C.K. Hsu, and C.H. Song, “Key management method,” United States Patent, Patent No. US 6,658,114 B1, December 2003.

[34] ISO/IEC, “Corporate governance of information technology,” *ISO/IEC 38500:2008(E)*, June 1, 2008.

[35] 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.