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

1 Introduction

A first stage plan, the “National Information and Communication Infrastructure Security Mechanism Plan”, was passed by the Executive Yuan in January 2001, with the establishment of a National Information and Communication Security Taskforce (NICST) with a vision to “ensure that our country has a safe and reliable environment for information communications”. Ever since then, the plans of the government have enabled the development of a path of information and communication security (ICS).

After the outcome of the first stage plan, ICS development was continuously enabled to enhance the overall capability of the information security protection of our country. The Executive Yuan passed a second stage plan (2005~2008) in 2004, which had four major objectives, namely, to “enhance report effectiveness for an emergency”, “complete capability in information security protection”, “deepen information security cognition and education”, “facilitate international cooperation”; covering a Chief Information Security Officer (CISO) system, information security duty classification, and confidentiality protection, etc. This plan has had a certain level of impact on reinforcing the capability of information security of government agencies.

In 2008, the plan was renamed the “National Information and Communication Security Development Program (2009~2012)”, in order to achieve the four policy objectives listed in this program, i.e. “strengthening the overall response capacity”, “providing a reliable information service”, “Improving the competitiveness of enterprises” and “creating an enabling environment for a culture of information security” [1]. In order to make a smooth movement and fulfil various information security tasks, the labor in this project was divided according to the nature of various action plans, and was processed by the related departments and units of the Executive Yuan.

The contents of the information security management system (ISMS) policy and Personal Data Protection Act will be discussed in Section 2, while the relationship between ISMS policy and ISMS governance, and their relationship to the establishment of an ISMS, will be demonstrated in the case study in Section 3. Finally the research will be concluded in Section 4.

[*] Correspondence author

2 ISMS Policies with ISG

A basic requirement of ISO/IEC 27001 is that "the organization shall establish, implement, operate, monitor, review, maintain and improve documented ISMS within the context of the organization's overall business activities and the risks they face." Section 4.2.1 b of the ISO/IEC 27001 requests the organization "to define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology".

There must always be rules to follow when dealing with things, and the ISMS policy is a guideline for ISMS implementation. It provides a full view of the strategic risk management of calibration organizations. The created and completed ISMS policy provides rules for information security management (ISM), i.e. information security policy. On the other side, Section 5 of ISO/IEC 27001 clearly states that top management is liable for "management commitment" and "resource management" for ISMS implementation [2].

A good ISMS policy will be able to successfully provide the full view when implementing the working items of the ISMS, allowing the executors to adopt a smooth and unhurried attitude [3]. A smooth attitude would help to cultivate and fulfil the ISMS culture of an information security policy, while an unhurried attitude would encourage the trust of the personnel in the ISMS within the ISMS scope, and avoid any harm being done by over-enthusiasm. This would show that the plan executors of the ISMS were capable of grasping the direction of the business operation, and by drafting strategies and action plans, they could integrate resources, organize manpower, and swiftly arrange resources to resolve any pressing needs. In other words, a good ISMS policy has an extremely deep impact on the information security of an organization. When a cautious plan of ISMS has been established, it acts as a guideline to mid/long-term working items, and is associated with the rise/decline and success/failure of ISMS self-governance and self-guard.

Generally speaking, an ISMS policy mainly proposes general guidelines to the mid/long-term development of the ISMS plan of an entire organization, including the "information security policy", "information security issue policy" and "information security system policy" currently requested by the ISMS, with the corresponding three aspects of management, operation and technology, as shown in Fig. 1. The information security issue policy focuses on controversial issues in organizations, which they care about and deal with. The information system involves the interaction between people and information technology (IT), as well as the organization's IT capability in dealing with the security issue of "quality variation" caused by "quantity variation", which should focus on the ISMS control issue [2], [4]. The definition of an ISMS on a system is "a mechanism for the execution of the organization's function for the entire collection process, whether the data is collected manually or by computer or subsequent computer operation." The information system security policy of the ISMS is equipped with security targets and operational security regulations and elements, accompanied by guidelines to the steps normally used for policy implementation.

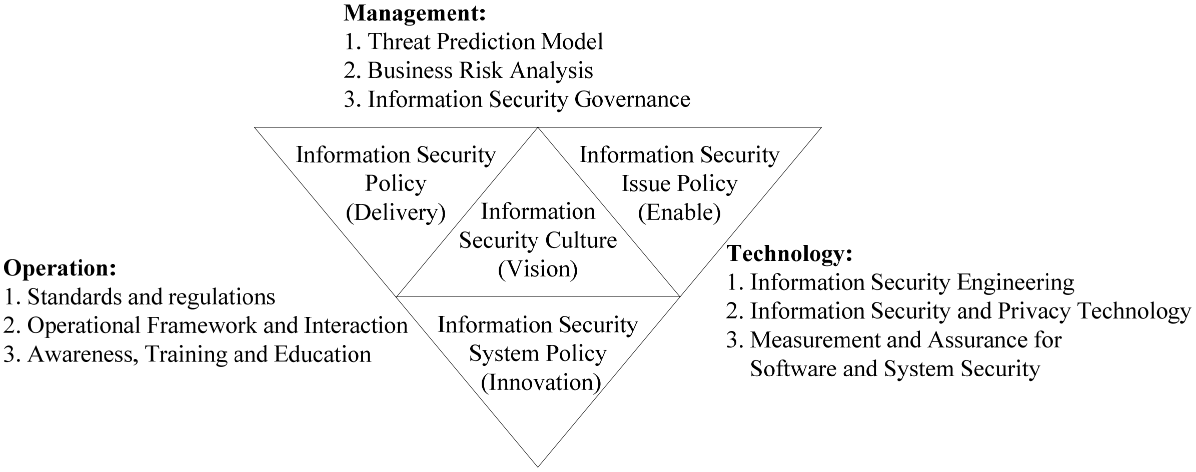
Management:
1. Threat Prediction Model
2. Business Risk Analysis
3. Information Security Governance
Information Security Policy (Delivery)
Information Security Issue Policy (Enable)
Information Security Culture (Vision)
Information Security System Policy (Innovation)
Operation:
1. Standards and regulations
2. Operational Framework and Interaction
3. Awareness, Training and Education
Technology:
1. Information Security Engineering
2. Information Security and Privacy Technology
3. Measurement and Assurance for Software and System Security

Fig. 1. Framework for information security management system policies

The Federal Government of the United States has been devoted to ISMS implementation since 1997, with the Federal Information Security Management Act (FISMA) being announced in 2002. As is clearly indicated in FISMA, the National Institute of Standards and Technology (NIST) is responsible for establishing guidelines, and the NIST has announced a tiered risk management approach to ISMS certification and accreditation (C&A) for risk management, involving tier 3 information system (environment of operation), tier 2 mission/business process (information and information flows) and tier 1 organization (governance) from down (tactical risk) to the top (strategic risk), respectively. In addition to a statement of strategic risk belonging to a scope of governance, it proposes an overall development blueprint and procedure [4].

On such a basis, the Personal Data Protection Act can be used as a case study in our country [5]. It is very important to establish a personal information management system (PIMS) independently. PIMS has become an issue to the ISMS. The objectives set in A.15.1 and the requirements of A.15.1.1 of ISO/IEC 27001 are shown in Table 1 [2]. The Personal Data Protection Act will be incorporated into the ISMS and defined as organization/governance policy in terms of the policy issue, with an appropriate information security policy relating to the job mission/business flow established according to ISO/IEC 27002, the ISMS Family of Standards (ISO/IEC 27000 Family of Standards), BS 10012 [6], NIST SP 800-66 [7], NIST SP 800-122 [8], PCI DSS [9] etc.

Table 1. Requirements of ISO/IEC 27001 for personal data protection act

A.15.1 Compliance with legal requirements Objective: To avoid breaches of any legal, statutory, regulatory or contractual obligations, and any security requirements.		
A.15.1.1	Identification of applicable legislation	Control. All relevant statutory, regulatory and contractual requirements, and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system in the organization.
A.15.1.4	Data protection and privacy of personal information	Control. Data protection and privacy will be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

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 is proposed by ISO/IEC 15816 [10]. In the ISMS of information sharing (IS-ISMS), the mandatory controls in ISO/IEC 27002 described as "should" are shown in Table 2 [3], [11]-[13]. Huang et al. proposed adding four new control measures [3].

Table 2. IS-ISMS shall do the mandatory controls in ISO/IEC 27002

ISO/IEC 27002 Session Number	**ISO/IEC 27002 Session Name**
N/A	Note: The appropriate protection is verified during the operation of shared information exchange [3].
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 [3].
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 [3].
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 [3].

The standardization work of ongoing personal information protection is involved in ISO/IEC 29100 and 29101 in terms of information system operation [14], [15]. How to observe and analyse the trend, forecast the change, and draft the appropriate ISMS policy information system policy from an operational perspective will be working items of risk management which should be accomplished by the implementation of the Personal Data Protection Act.

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 [16], [17]. Consequently, Huang et al. proposed 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. 2 [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. This framework is implemented in a Local Tax Bureau.

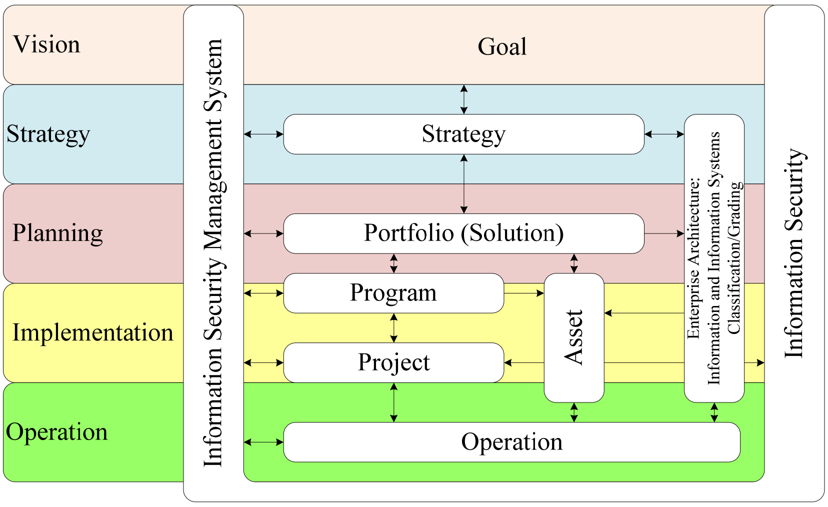

Fig. 2. Information security implementation framework [3]

3 ISMS Policy of Remote Backup for a Local Tax Bureau

The trend of information is prevailing right across the world, and the emergence of novel and advanced technologies has led human life into a digital society and a knowledge-based economy. The application of IT has been a huge catalyst for change in working styles, living environments and mindsets, which has largely enabled the social development of humans, and the advance of world civilizations, bringing humans into a new age. Nevertheless, people face severe tests of information security while enjoying the huge benefits of the digital age. The popularity of the internet and strong system program functions has brought users many benefits from time to time. However, attacks via the internet present challenges, with various methods of attack flooding the information society. These attacks can cause information security incidents or damage information systems, or even paralyze the entire internet. Therefore, an ISMS needs to be established in order to reduce the overall information security risk of our country and reinforce capability in information defence.

This is a good illustration of ISMS policies. The Tax Bureau is in charge of house tax returns and other local tax affairs, in order to expand tax applications over the internet, reinforce internet services, and offer greater convenience and a highly-efficient service concept to the people. The Bureau expects to see security and compliancy rules which protect the privacy of people’s taxation data and related important information [1], [18]. It has established its own ISMS to eliminate the possibility of anyone interfering with, destroying, or invading tax information, capable of reacting to operational risks, and enhanced to ensure the information security of people’s property, having implemented the ISMS standard administration.

From the beginning, the ISMS policy initiated by the Tax Bureau regarded “tax refund as a core business to be incorporated into the scope of certification and expanded accordingly”, “follows the original organization structure”, “drafts documents by self-learning through education training courses”, “incorporates a document drafting procedure into the Rule Inspection Team for review" and "self-audits information security with an established performance indicator", and proposed the following three constructive concepts and methods:

- **Incorporate an information security governance model and draft various information security management measures:**
  In order to relieve the impact of ISMS adoption in the original operational flow and resolve the worries of internal colleagues, the Tax Bureau has introduced an ISG model, with the Deputy Chief serving as CISO, combining the original various organizational structures, drafting policies and objectives to further drive various units to fulfil, execute, and regularly report their performance to the Chief.
- **Actively strive for a remote backup centre of the national finance system from Central Government:**
  After a risk assessment is done by the Risk Management Team of the Tax Bureau, a site backup (including a comprehensive service counter and backup of computer room) should be incorporated into the scope of risk management. However, the backup establishment of a computer room is costly and can cause financial difficulty. A simultaneous data remote backup system is drafted to continue the operation of the audit affairs. Due to nationwide consistency, centrally-orientated management is recommended, and this is listed as one of the ISMS policies after a calibration is made to the strategy.
- **Actively strive for opportunities for the occupational performance training of information security personnel:**
  In order to reinforce the operation of the information security protection of the Tax Bureau, it should actively strive for participation in the "maturity of government's information security assessment – web application software and e-mail security" accreditation plan [19].

Section 4.2.1 b of the ISO/IEC 27001 clearly states that the ISMS policy will be "aligned with the organization's strategic risk management context in which the establishment and maintenance of the ISMS will take place" [2]. During the information security management process, the "established full view" is divided into two parts, namely, external and internal, and then the feasibility analysis proceeds of the external factors "in consideration of operational and law/rule requirements". The high-scale risk management of preliminary risk assessment is undertaken by the management level, in which the remote backup for the computer room and occupational performance training for information security staff are the achieved outcomes.

ISG is incorporated into the ISMS during the process of the ISMS establishment. For example, in terms of remote backup, a business continuity plan of the ISMS was processed to request the information management centre of the Directorate-General of Budget, Accounting and Statistics (DGBAS) on February 16, 2009. Due to financial limitations, an operation is regularly processed to back up the data in separate Tax Bureaux. In practice, a large budget increase is required to establish hot spares if complying with the aforementioned administrative regulations.

Another plan is to follow the objective and principle of the legislative intention of Article 111 of the Constitution of our country. The Financial Data Center (FDC), Ministry of Finance, will be responsible for this, with an implementation model established and incorporated into the ISMS policy after a high-scale risk assessment has been done by the CISO of the Tax Bureau. The FDC will implement the working items of a remote backup for the implementation of an ISMS risk management plan according to the implementation items of ISG of ISO/IEC 27014. Among the "process/measurement" implementation items are striving for cost and efficiency synergistic analysis data of the remote backup working items of various Tax Bureaux coordinated by the FDC, while the CISO will take charge of the "organization/role and responsibility" aspect, and the Information Security Officer will be responsible for providing an analysis report, and reporting to the related units. In terms of the "security infrastructure" aspect, remote backup working items will be incorporated into the "Application Plan for Local Tax Information Platform Integration". According to the theory, more than 50% of the cost can be saved by simplifying the administrative process in terms of the "investment management" aspect. The Taxation Agency, the Ministry of Finance, officially classified remote backup as a duty of the FDC on November 4, 2009, which is expected to be completed by 2013 [20].

Table 3. ISMS with information security management processes

Management	Operation	Technology
Establish ISMS Policy	Monitor and Measure	
	Information Security Policy	Information Security System Policy
Establish Goals	Develop Information Security Management Profile	
Identify Targets	Compliance with Information Security Management Assessment	
Audit: 1. ISMS milestones and improved plans. 2. Effective implementation plans of ISMS. 3. Feedback mechanism of continuous improvement verification results for ISMS.		

On the basis of the above, the ISMS and ISM processes are effective implementations, as shown in Table 3 [2], [11]-[13], [21]-[23]. These can be divided into the three aspects of management, operation and technology. The ISMS policy is initiated from the management point of view, followed by objectives, and then by identifying the target. Operational and technological aspects belong to the information policy and information security system policy respectively, with implementation monitoring and measurement, followed by the development of an ISM profile and lastly, an assessment of the ISM regulation compliance.

Following the progress of the management system standards (MSS), the ISMS policy was renamed information security policy, and the information security policy was renamed information security-specific policy. The documentation of the information security risk management approach and information security rule is regulated in ISO/IEC Fourth WD 27001:2010-11-15. On the other hand, it is noteworthy about the privacy impact assessment (PIA) handbook was launched from Information Commissioner's Office (ICO) [24]. PIA is designed to regulate the personal data protection in risk management processes.

4 Conclusions

The ISMS policy is a summary of outcomes, accumulated experience and discipline, which are imperative resources for the reinforcement of information security and the promotion of ISMS implementation. Although there is no doubt that the ISMS policy can report stability, it is not invariable; it has to keep pace with the times and requires incessant improvement in terms of the new trend of information security technology and environmental change. The established ISMS policy has become the regulations for users of information systems, i.e. information security policy. It is the rule for the security of information systems and is even a guarantee, which is to be continuously advocated in operation and completed in advocacy, making it a foundation for the promotion of ISMS development and ISMS policy advance, and a guarantee of information security implementation. If there is no perception of ISM in mind and no ISG is embraced, there can be no recognition of information security technology, and a good master plan for ISMS can never be made. ISMS policies are the strategies and frameworks of the ISMS proposed after a comprehensive and complete review, in which the “remote backup” and “Information Personnel Occupational Training” of ISMS policy are clear outcomes after a full external view is established in the working items of risk management in the first stage of the ISMS.

5 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.

[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.