A Study on E-Taiwan Promotion Information Security Governance Programs with E-government Implementation of Information Security Management Standardization

Chien-Cheng Huang[1] and Kwo-Jean Farn[2]
(Corresponding author: Chien-Cheng Huang)

Department of Information Management, National Taiwan University[1]
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan, Republic of China
Taiwan Internet Protection Association[2]
3F.-6, No. 155, Sec. 1, Keelung Road, Taipei 11070, Taiwan, Republic of China
(Email: chienchenghuang@ntu.edu.tw)

(Received Aug. 16, 2014; revised and accepted Oct. 3 & Nov. 10, 2014)

Abstract

The promotion of Information Security Governance (ISG) has become an important factor in the implementation of e-government and information security management within the "National Information and Communications Technology Security Development Program (2009˜2012)" in continuing the "Plan for Establishment of Information and Communication Technology Infrastructure Security Mechanism (2001˜2008)" in Taiwan; in July 2013, the working outline of the project was adjusted. And, it was asked all departments of Executive Yuan and local government to process aggressively by regulation on December 25, 2013. This study examines information security development program, and strategies for meeting e-government and information security management requirements within the implementation of information security development programs through information security management systems (ISMS). Moreover, an action program for improved ISMS performance, using an approach combining ISG and ISMS, is proposed. Based on this, this research employs history analysis and in-depth interview methodologies to develop insights into e-Taiwan information security management. Furthermore, the research objective is to examine the relevance between the execution of e-government and information security management framework and ISMS implementation by using the ISG project approach.

Keywords: E-government, ISG, ISMS, standardization

1 Introduction

Information technology has taken the world by storm. Its emergence has given rise to a new level of digital knowledge systems. Its application has been catalytic to the rapid changes taking place in the way people work, live and think, and is facilitating the development of our society and civilization in a new era. However, along with the tremendous benefits and development of information technology comes the challenging problem of e-government and information security management [6, 8, 12, 25, 35, 36, 37, 44, 45].

The "Plan for Establishment of Information and Communication Technology Infrastructure Security Mechanism" in Taiwan was approved by the Executive Yuan on January 17, 2001. As a result, information security management system (ISMS) certifications have been the focus of the first two phases (2001˜2008). Third phase programs (2009˜2012) from the "National Information and Communications Technology Security Development Program" (simplified as "Information Security Development Programs") were renamed by dispatch document No. 0980080376 on January 20, 2009 [30]. Among the approved nine measures and thirty action programs mentioned earlier, the strengthening of information security audits and ISMS certification remained one of the nine key action programs in e-government and information security management implementation.

On Feb. 5, 2009, the National Information and Communications Technology Security Taskforce (NICST) formally notified various departments under the Executive Yuan that they were required to put the action programs into practice. The aim was to achieve the four policy objectives of "Strengthen the overall response capacity", "Provide reliable information services", "Improve the competitiveness of enterprises" and "Create an enabling environment for a culture of information security" listed in the information security development programs [30]. In the information security development programs, strengthening information security audits and ISMS certification were important actions in the implementation of e-government and information security management, where each governmental department had taken on these security responsibilities, as shown in Table 1. However, the ISMS effectiveness has often been questioned [17]. In addition, all elements of the action programs had been explicitly defined under the idea that "The scope of certification is limited to core businesses" in the important measures of "Strengthen Information Security Audits and ISMS Certification" for the information security development programs [30].

Although "information security management differs due to its standard, and information security standard may change due to implementation", it complies with ISO/IEC 27001:2005(E) requirements, and was implemented in terms of core businesses as listed in ISO/IEC 27001:2005(E) relevant clauses of limited core businesses for the ISMS certification scope, Section 1.1 and Section 4.2.1(a) [30]. Organizations should then be covered by the ISMS. However, a large number of organizations that have passed ISMS certification have still failed to provide the necessary ISMS policy documents requested in ISO/IEC 27001:2005(E), Section 3.1(a). Because of this failure, it must be acknowledged that such shortcomings within Taiwans ISMS authentication and certification system require urgent attention [9]. Furthermore, in view of the discussion on the ISMS certification effectiveness, relevant authorities expect that this issue will be dealt with through the information security governance (ISG) action programs, as listed in Table 1. Due to the change, we understand that the motive power which doesnt want to change, so we offer the promotive product of national vulnerability database (NVD) and security content automation protocol (SCAP) of security configuration management which are from National Institute of Standards and Technology (NIST) in the technology application category of ISMS standardization. However, in July 2013, the ISMS working outline mentioned above was modified; the detailed ongoing working process will be explained in this work through an in-depth interview (see Appendix A). After three years, it has become the policy of National Information and Communications Technology Security Development Program (2013˜2016) officially on December 25, 2013 [32].

This research employs history analysis and in-depth interview methodologies to develop insights into e-Taiwan information security management. In addition to the interviews, other documents and materials were obtained during the fieldwork period (see Appendix A). The remainder of this paper is arranged as follows. Section 2 examines information security development programs and ways of meeting of e-government and information security management requirements through ISMS. In Section 3, an action program using a combination of ISG and ISMS is proposed in order to improve ISMS performance. Discussion of the findings, conclusions and implications of this research, and the new requirement added in 2013, are given in Section 4.

2 Analysis of E-Taiwan Information Security Management

2.1 E-government Information Security Management and ISMS

"Regulatory or Legal requirements" are the key to the establishment of an ISMS, as prescribed under ISO/IEC 27001:2005(E) Sections 3.16, 4.2.1(b)(2), 4.2.1(g), 5.1(d), 5.2.1(c), 6(a) and 7.3(c)(4). It was ruled in Section 161 of the Administrative Procedure Act that "effective administrative regulations have to bind authority to the issuing department and its subordinate agencies". Moreover, information security development programs are classified as administrative regulations [10]. The governmental departments must comply with the nine action programs listed under the important measures of e-government and information security management, given in Table 1. In addition, the important action program measures and performance indicators of ISG promotion are listed in the information security development programs [30]. The important measures also explain that the ISG projects and ISMS are closely linked. In the practical guidelines of the ISMS control measures for the healthcare sector, it is clearly stated that ISG should be included in information governance or information assurance [15].

Lee and Kim [26] illustrated the scope of ISMS program integration for streamlining its effectiveness, as shown in Figure 1. However, whether or not the management structure of the organization area is applied depends on whether it is possible to establish legitimacy within the environment area. The question of whether it will continue to function in the governance area can be answered by checking the maintenance efficiency of the legitimacy. If the leading structure legitimacy is based on power, it will directly or indirectly influence the behavior of the individual and the group. On the other hand, if the system includes complete feedback and adjustment protocols, it can react accordingly to various situations, extending the system lifespan; otherwise, modification would be necessary. While the principles of a private department usually focus on achieving a set target, in a public department, the interests of the whole community are the main goal, not the organization itself. The influencing factors mentioned are complementary, or to be more precise, "the policy field" feature exceeds the importance of the "problem solving field" of a private unit, while the risk area includes managerial, social and information technology (IT)

Table 1: The important measures and action programs of the providing reliable information services in the information security development programs [30]

Goals	Important Measures	Action Programs
Provide reliable information services	E-government information security management implementation	The regulations and guidelines on development and maintenance of information security process in governmental departments.
		Promote ISG (information security governance).
		Promote information and information system classification/grading.
		Strengthen e-government information, communication security and implementation official data protection.
		Promote security certification of the information and communication devices for the agency.
		Enrich information security personnel.
		Enhance information security protection technique and quality of the services.
		Strengthen information security literacy and training ability.
		Strengthen information security audits and ISMS certification.
	Promote network security of the critical information infrastructures	The development of the critical information infrastructure protection strategy.

risk. Although Figure 1 is not accepted by ISO, its theory becomes the example in the launched project which is from Presidential Policy Directive (PPD)-21 and Executive Order (EO) 13636 of the United States. Therefore, it is still valuable.

The implementation of ISMS is more than an event or a condition, it is a series of activities scattered across the ISMS operation. These activities can even be found in the way management runs a business. The ISMS process is governed via the basic management process of "Plan", "Do", "Check" and "Act". On the other hand, on June 1, 2008, the International Organization for Standardization (ISO) published ISO/IEC 38500:2008(E), which consisted of six principles for information technology governance (ITG): responsibility, strategy, acquisition, performance, conformance and human behavior [18]. Table 2 shows the corresponding standard sessions offered by ISO/IEC 38500:2008(E) and ISO/IEC 27001:2005(E). On the other hand, the ISO/IEC 27001:2013(E), new version, has been launched on October 1, 2013 and ISG has been already in the requirement of ISMS [22].

In addition, ISO had already published a standard of the ISG for ISO/IEC 27014 [16, 20, 21]. Leaders must apply the principles of the ITG through the ISG framework (as indicated in ISO/IEC 27014:2013(E)) in ISMS. An ISG framework consists of objectives, focus areas and implementation models. The objectives of an ISG include business alignment, accountability and compliance. Business alignment focuses on enabling an alignment between business and information security objectives. Accountability aims to ensure that an entity takes responsibility for its actions and decisions. Compliance serves to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any information security requirements.

ISG needs to focus on five areas: strategic alignment, risk management, resource management, performance measurement and value delivery. In addition, when implementing ISG, the following four aspects must be considered: ISG processes, organization, architecture and investment management issues. Furthermore, ISG processes include the sub-categories: "Evaluate", "Direct", "Monitor", "Communicate" and "Assure" [21].

In Taiwan, the Information Management Center of the Directorate-General of Budget, Accounting and Statistics (DGBAS) was requested to handle the business continuity plan (BCP) of the ISMS by dispatch document No. 0980021063 on February 16, 2009, by the Executive Yuan. A Local Tax Bureau therefore performed an analysis of the ISG, as shown in ISO/IEC 27014. However, in terms of performance management, the Financial Data Center (FDC) of the Ministry of Finance (MOF) uses quality management systems for the procurement of software, and is more effective than Local Tax Bureaus, in addition to handling both the risk management and resource management as well. In terms of strategic alignment and value delivery, the MOF and various local governments must comply with the ISG for e-government services proposed by Lee and Kim [26], as shown in Figure 1, and stated in the e-government information transformation development plan by the Research, Development and Evaluation Commission (RDEC), and Article 111 of the Constitution as "Distribution of Competencies between Central and Local Governments". Finally, the chief information security officer (CISO) of a Local Tax Bureau establishes implementation models (as indicated in Table 3) and incorporates the ISMS policies [14].

Therefore, Local Tax Bureaus were requested by the central government to oversee the planning of offsite backups. After six months, the Taxation Agency then specified conditions within the "Integrated Local Tax Information Application Platform Program" promulgated by dispatch document No. 09822003350 on November 4, 2009, by the MOF. The FDC thus became the kernel responsible for the offsite backups. This is an instance of ISG application.

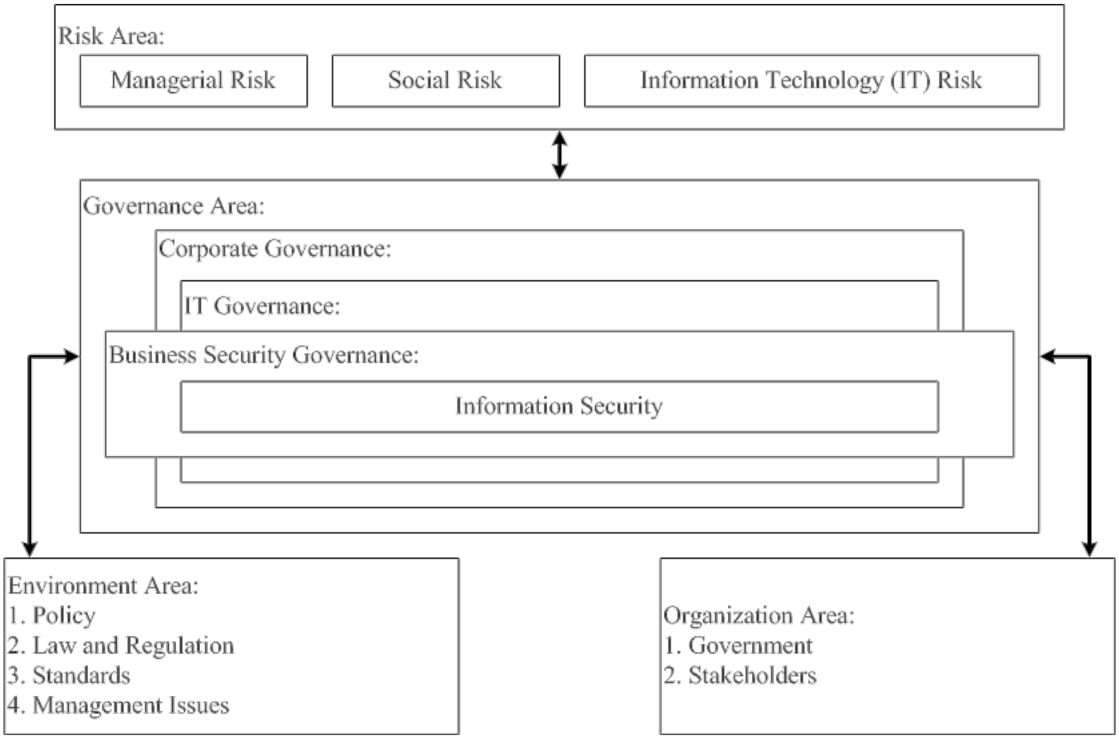


Figure 1: The scope of the ISG for e-government services

Table 2: A Comparison between ITG (ISO/IEC 38500:2008(E)) and ISMS Requirements (ISO/IEC 27001:2005(E))

Principles	ISO/IEC 38500:2008(E) Session Number	ISO/IEC 27001:2005(E) Session Number	ISO/IEC 27001:2013(E) Session Number
1. Responsibility	2.1.1, 3.2	4.2.1 (d), 4.2.3 (a)(3), 5.2.2	6.1.1, 6.1.2, 7.2 (a) , 7.2 (b) , 7.2 (c) , 7.2 (d), 7.3 (b), 7.3 (c), 9.1 (a)
2. Strategy	2.1.2, 3.3	4.2.1 (b)(3), 7	4.2 (b), 5.2 (a)
3. Acquisition	2.1.3, 3.4	5.2	4.2 (b), 7.1, 8.1, 9.3
4. Performance	2.1.4, 3.5	4.2.2 (b), 4.2.2 (h), 7	7.1, 8.1, 9.3
5. Conformance	2.1.5, 3.6	4.2.2 (e), 6	7.3 (b), 7.3 (c), 9.2
6. Human Behavior	2.1.6, 3.7	4.2.1 (b), 4.2.3 (a)(3)	5.1 (a), 9.1

Note: Descriptions of the six principles and guideline of ISG is in ISO/IEC 38500:2008(E).

Table 3: Illustration of the offsite backup implementation models of the ISMS risk treatment plan for a Local Tax Bureau

Implementation Models		**Description**
ISO/IEC 1st WD 27014 :2009-12-01	**ISO/IEC 27014 :2013-05-15**	
Process/Metrics	Communicate/Assure	Strive for the offsite backups to subsume efficient sharing work items of centralized management and response of the high quality network services of the e-government plan.
Organization/Role and Responsibilities	Direct/Evaluate	CISO is the kernel responsible. The information security officer is responsible to provide analysis reports.
Security Architecture	Proposals	Incorporate into "Integrated Local Tax Information Application Platform Program".
Investment Management	Communicate/Assure	Subsume "Local Tax Information Application Platform" and simplify administrative operations. Therefore, it shall be able to save the cost over 50%.

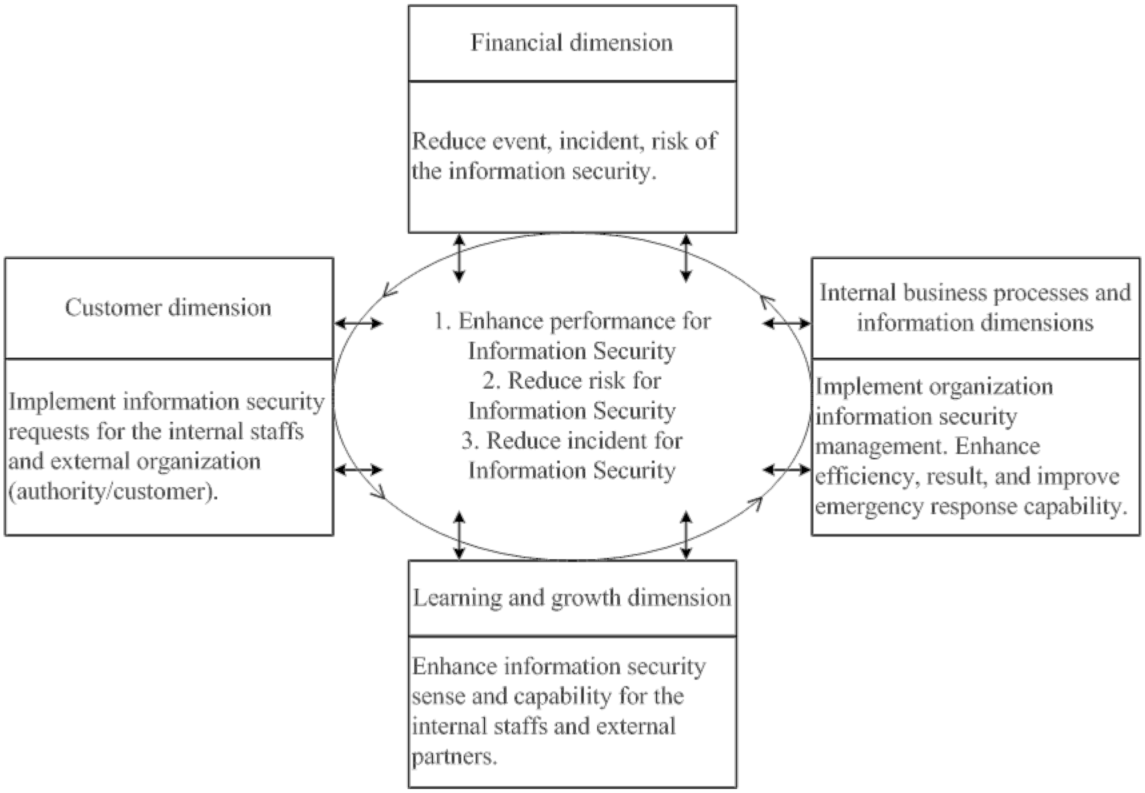

Financial dimension
Reduce event, incident, risk of the information security.
Customer dimension
Implement information security requests for the internal staffs and external organization (authority/customer).
1. Enhance performance for Information Security
2. Reduce risk for Information Security
3. Reduce incident for Information Security
Internal business processes and information dimensions
Implement organization information security management. Enhance efficiency, result, and improve emergency response capability.
Learning and growth dimension
Enhance information security sense and capability for the internal staffs and external partners.

Figure 2: Balanced scorecard and ISG maturity indicators

2.2 E-government ISG of ISMS

One of the United States Federal Governments ISMS regulations is that "ISG can be defined as to establish and maintain the framework, to support the management structure and procedure, and to provide the following certified processes: under risk management, to ensure that the objectives of information security strategy and business objectives are the same, to support business objectives through stringent policy and internal control to ensure they comply with relevant regulations, and to assign duties." [5]. Based on this, requirements for action programs for regulations and guidelines, in terms of the development and maintenance of information security processes in government departments, were included in the ISG programs. Therefore, ISG projects were included in the ISMS implementation, such as "ISMS policy and organizational strategic risk management context in which the establishment and maintenance of the ISMS will take place", along with "Internal ISMS audits", as described in ISO/IEC 27001:2005(E) Section 4.2.1(b)(3) and 6. In addition, the four dimensions of the maturity evaluation of the ISG were included in Section 7.2(f) (Results from effectiveness measurements) of Section 7 (Management review of the ISMS), as shown in Figure 2. They consist of "Financial", "Customer", "Learning and growth" and "Internal business processes and information". These were used as a basis to derive the various requirements listed in Section 7.3 (Review output). They shall be feasible and valid [9, 10, 15, 17, 18].

For example, Taiwans Personal Data Protection Act adopted principles such as the prevention of damage, inform, collection restrictions, the use of personal data, restriction of autonomy, protection of personal data integrity, security management, inspection and correction, and imputable [27]. Moreover, information security development programs were asked to work in conjunction with the legislative process of Personal Data Protection in setting/amending the management regulations for personal data protection, as shown in the "Strengthen e-Government Information, Communication Security and Implementation Official Data Protection", for the information security development programs [30].

However, it remains a challenge to establish relevant indicators in accordance with the requirements in ISO/IEC 27001:2005(E) Sections 4.2.2(d) and 4.2.3(c), while also meeting the requirements of Section 7.2 (f) (Results from effectiveness measurements) in the "Assessment of the ISMS management". Achieving this would not only enable management to evaluate whether Section A.15.1.4 (Data protection and privacy of personal information) of the "Compliance with legal controls" in the ISMS fulfills the decisions and measures of the Personal Data Protection Act, but it would also allow management to assess whether its protection requirements are in full compliance with the requirements of ISO/IEC 27001:2005(E) Section 4.2.1(c)(2) (Develop criteria for accepting risks and identify the acceptable levels of risk). Furthermore, it would allow management to determine whether the requirements to "Promote information and information system classification/grading" within the information security development programs are indeed being met [30].

Accordingly, after other e-government information security management action programs had been integrated with the ISG action programs, the relevant ISG projects were included in the implementation of the ISMS requirements, as described in Sections 4, 5, 6 and 7 of ISO/IEC 27001:2005(E), and shown in Table 2. It then became feasible to achieve improved results through the integration of the ISG with the ISMS implementation, as shown in Table 4 [19].

2.3 E-government Implementations of ISMS

Given the fact that there are still a large number of institutions that comply with ISMS certification as prescribed in ISO/IEC 27001:2005(E), but have failed the "business" requirements, NICST, in the "Implementation Program on Information Security Responsibility Classification in Governmental Departments" promulgated by information security dispatch document No. 0980100328 on June 1, 2009, by the Executive Yuan, specified that The scope of ISMS certification should initially cover organizational core business information systems, and gradually be expanded to cover the entire organization [29] (see Appendix B). On the other hand, ISO/IEC 27003:2010(E) was proposed to provide a checklist of the activities required to establish and implement an ISMS, and to support progress monitoring for ISMS implementation [19].

ISMS establishment is still one of the main factors in the above plans; however the deadline for obtaining three-party ISMS certifications for Level A and B institutions was postponed for two years. The institutions were required to complete these certifications by 2009 and 2011, respectively [29]. In addition, in order to better enforce ISMS, and to strengthen the action programs for information security quality and capability training, as shown in the "Implementation Program on Information Security Responsibility Classification in Governmental Departments", Note 3, NICST proposed a planning framework for civil servants information security awareness, and is currently preparing the training materials [34] (see Appendix B).

Therefore, the implementation effectiveness of e-government information security management measures can be improved with the establishment of an information technology security assessment framework (ITSAF), as shown in Figure 3. It is built into the action programs of the "Promote information and information system classification/grading". The relevant knowledge and skills are included in the aforementioned curriculum planning.

The cryptographic module validation program (CMVP), including the cryptographic algorithm validation program (CAVP) and common criteria evaluation and validation scheme (CCEVS), are shown in Figure 3. The main (assisting) organizers have already been established for action programs for information security development programs; however, this is not the case for the SCAP. Thus, this issue must be dealt with as soon as possible in order to fully construct a developmental environment for the implementation of e-government information security management. However, according to Figure 3, the work timetable for December 2012 remained incomplete except for CAVP, stopping the advance of the project. In other words, the root cause of this issue is the lack of ISMS design regarding technical rules in Table 4 [19]. However, Figure 3 is still the policy of security validation in the United States, but it is hard to use in the practical case. So far, it is asked to finish the assessment framework by the requirements from PPD-21 and EO 13636 by February 2016.

3 ISG Approach for E-government and Information Security Management

In the studies related to ISG, Abu-Musa [1] introduced an ISG framework that enables organizations to better understand, analyze, implement and evaluate ISG practices in order to achieve business success. The proposed ISG framework was developed based on the ISG conceptual framework proposed by the IT Governance Institute [23] and other ISG models and frameworks available in the literature [28, 33, 38, 39, 40, 41, 42, 43].

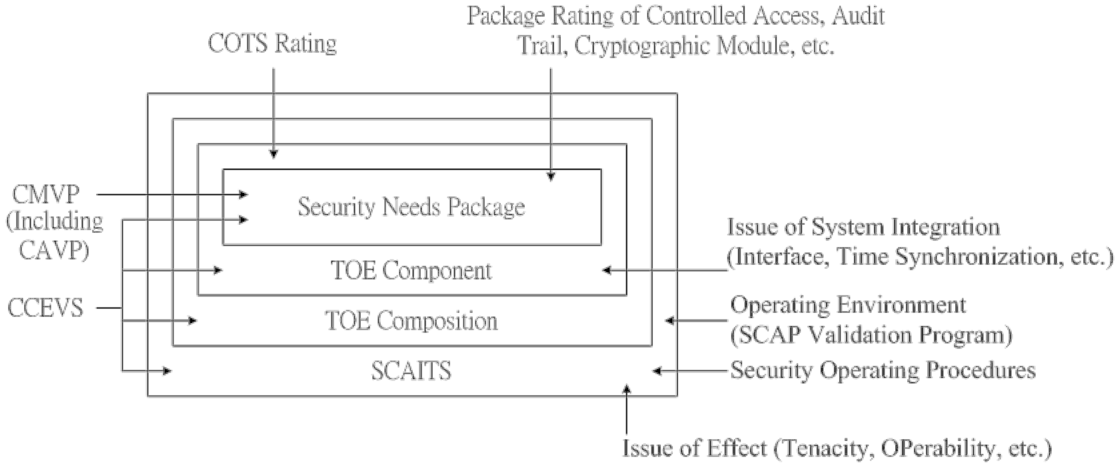
Based on the six aforementioned ITG principles and the four ISG dimensions described in Table 2 and Figure 2, as well as ISMS standards, this study proposes elements for evaluating the maturity of ISG. The specifications for policies, procedures, implementation, testing and integration in question are described as follows:

1) Policies:

- Provide all personnel with a set of formal and current policy guidelines that sets out ISMS directions.
- Establish a sustainable cycle framework and ISMS plan policy that are able to assess risks and implementation.
- Provide a policy document that covers the primary facilities and operations of regulated ISMS information assets.
- All policies must be approved in writing by management and relevant departments.
- The scope of the policy must include ISMS structure and clear division of responsibility, as well as its progress and adopted trustworthiness monitoring.
- The policy must clearly define disciplinary measures for any noncompliance.

Table 4: Description of the integration of the ISG planning sketch and phasing results in the ISMS [19]

Phase		**Obtaining management approval for initiating an ISMS project**	**Defining ISMS Scope and ISMS Policy**	**Conducting Information Security Requirements Analysis**	**Conducting Risk Assessment and Risk Treatment planning**	**Designing the ISMS**
Standard Compliance		1. ISO/IEC 27001 2. ISO/IEC 27000 3. ISO/IEC 9001, ISO/IEC 14001, and ISO/IEC 20000	1. ISO/IEC 27001 2. ISO/IEC 27005	1. ISO/IEC 27001 2. ISO/IEC 27002	1. ISO/IEC 27001 2. ISO/IEC 27002 3. ISO/IEC 27005	1. ISO/IEC 27001 2. ISO/IEC 27002 3. ISO/IEC 27004
Output	ISMS	1. Management approval for implementing the ISMS	1. The ISMS scope and boundaries 2. ISMS policy	1. Information security requirements 2. Information assets 3. The preliminary results from the information security risk assessment	1. Risk assessment reports 2. Risk treatment plan 3. Written notice of the management approval for implementing the ISMS 4. Management acceptance of residual risks 5. The Statement of the applicability	1. Information security policy 2. ISMS records and document control 3. The ISMS project implementation plan
	ISG		3. ISG principle	4. ISG assessment reports		4. ISG policy 5. The ISG project implementation plan 6. ISG records and document control


COTS Rating
Package Rating of Controlled Access, Audit Trail, Cryptographic Module, etc.
CMVP (Including CAVP)
CCEVS
Security Needs Package
TOE Component
TOE Composition
SCAITS
Issue of System Integration (Interface, Time Synchronization, etc.)
Operating Environment (SCAP Validation Program)
Security Operating Procedures
Issue of Effect (Tenacity, OPerability, etc.)

Notes:
1. CAVP: Cryptographic Algorithm Validation Program.
2. CMVP: Cryptographic Module Validation Program.
3. CCEVS: Common Criteria Evaluation and Validation Scheme.
4. COTS: Commercial Off-The-Shelf.
5. TOE: Target of Evaluation.
6. SCAITS: Security Certification and Accreditation of Information Technology Systems.
7. SCAP: Security Content Automation Protocol.,

Figure 3: United States Federal Government information technology security assessment framework

2) Procedures:
   - Be able to provide a formal and current program set on the ISMS implementation control measures of a ready-defined policy
   - Each program contained in the set must clearly define its applicable circumstance, method, time, object, and application details.
   - The programs contained in the set are designed for the asset owners and users, information resource management and data processing personnel, management and information security administrators. Information security responsibilities and expected behaviors must be clearly defined.
   - All program files must clarify the use of the ISMS control measures for action.
   - All program files must be approved in writing by management and relevant departments.

3) Implementation:
   - Every individual who is part of a program from the regulated program set must be fully aware of its program content.
   - Programs and control measure implementation from the ISMS program collection must be integrated with organizational daily operation, and must be consistent with program application. Regular training must be provided to strengthen this implementation.
   - There must be an established approach mechanism that ensures effective ISMS control measures geared toward operation efficiency.
   - ISMS policies and program sets must be incorporated into ISMS awareness and training programs.
   - Awareness of required knowledge and skills of ISMS personnel is required, and training and education mechanisms must be established.

4) Testing:
   - Build and run creditable routine evaluation and testing mechanisms on ISMS implementation effectiveness.
   - Establish ISMS control measures of appropriate information and information system level in line with policies and programs, and credible evaluation and testing capability.
   - Establish credible evaluation on continuous improvement and corrective action of the ISMS implementation, and testing capability on preventive measures.
   - Establish assessment and testing capability for the credibility of "Management and Respond" and "Response and Restore" of the ISMS security events and incidents.
   - As the implementation of the evaluation and testing depends on risks for the ISMS operation effectiveness, such plans must be approved in writing by management and relevant departments.

5) Integration:
   - The ISMS has become part of the organizational management system.
   - The ISMS is part of the capital planning and investment control (CPIC).
   - A review and improvement mechanism for the ISMS policies, procedures, implementation and testing has been established.
   - An appropriate organizational culture geared toward promoting ISMS has been established.
   - There is understanding and management of ISMS vulnerability.
   - Re-evaluate and appropriately adjust ISMS control measures according to changes in the information security environment.
   - Make decisions based on appropriate measured risks and costs, information security incidents and their results.

Based on Figure 4 and the ISMS standards [18, 20, 21], the subject and scope of the ISG, such as information, system and process that are necessary in the operating process must be verified. Once a consensus and conclusions are reached between the operator, personnel and relevant professionals on the standards, benchmarks and legislations to be used during the ISG process, the ISG process can be set in motion. Furthermore, the five vital components and their inter-relationships necessary for the launch of the ISG were listed in the IT assurance guide using COBIT [24].

The ISG process can be divided into three stages: planning, scoping and execution, as illustrated in the IT assurance guide using COBIT [24]. Planning is the first stage of the ISG process. In this stage, the ISG principles compatible with business and ISMS objectives are established. This indicates the link between enterprise information infrastructure and control objectives, conduct risk assessment, evaluation of threats, vulnerability, and possible impact on the business, and diagnoses risks associated with each related project. It also illustrates that it helps to think in terms of IT and ISMS resources in order to translate business goals into IT and ISMS goals, and in terms of infrastructure and human resources required to provide and support the services and information needed. Moreover, an ISG launch plan is based on risk. The identification of key business processes is based on value factors. It also assesses the degree of maturity of the ISMS process.

The second stage is scoping. It involves planning based on the area of the ISG launch, selecting control objectives

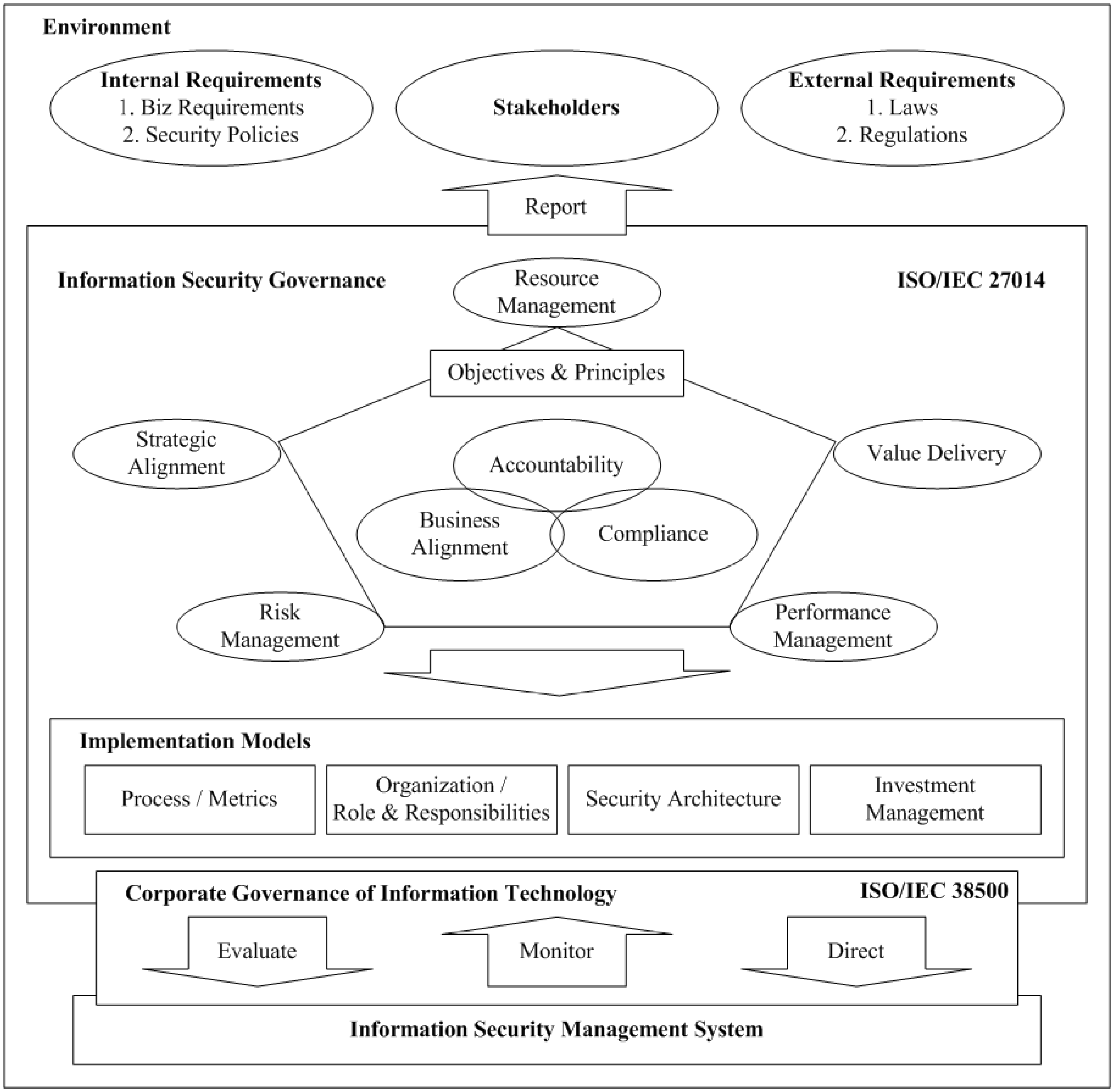


Figure 4: Elements of the ISG maturity evaluation

for key processes, and designing detailed plans according to these control objectives.

The third stage is execution. It subdivided into six steps:

Step 1. Identify or confirm key ISMS processes and self-assess the degree of maturity for the key ISMS processes.

Step 2. Update the choice of control objectives, customize the control objectives, and establish detailed audit programs.

Step 3. Test and evaluate control measures, update the level of maturity of the assessment process.

Step 4. Self-assess control measures, test and evaluate control measures.

Step 5. Diagnose residual risks in running a project; substantiate the fact that risks are under control.

Step 6. Report ISG conclusions.

From the above, it can be seen that, apart from its top-down direction, the ISG process has a great deal of overlap with the establishment of the ISMS. Therefore, it is appropriate to integrate these two processes. It is possible to achieve improved results by integrating the projects of the ISG with the ISMS implementation programs.

4 Discussion and Conclusion

A solid supply chain and functionality are crucial to the implementation of any management plans. Taking as an example the illustration of the important measures and performance indicators of “Promote Information and Information System Classification/Grading” for the information security development programs, the first point (1) “classification” is the standard of real initialization [31]. It was officially announced on July 5, 2010, during the testing period, that the investigation bureau of the ministry of justice had already confirmed the resource allocation for the financial dimension (as indicated in Figure 2), but in the working outline (2), “establish basic information security parameter criteria”, the classification was only finished in September 2013.

In July 2013, the minister without portfolio, Executive Yuan, of the information and communications technology security stated that the fourth period (2013˜2016) did not have a confirmed “development project”, and that this process would therefore be frozen, while the top priority work was actually the technical structure of the security operation center. On the other hand, the gradual promotion of information technology service management (ITSM) has already started, and the new policies incorporated into the security regulations have been officially adopted [31].

In order to avoid repeating the same error, these new policies should take “Backhouse et al.s circuits of power framework” into consideration. One of the main aims of this project is also to create a standard regulated environment for information security [4, 7, 13]. Scheduled in September 2013, the project already includes the IT risk cited in the technical checking section (as indicated in Figure 1), making it top priority as the first step of this long process.

The whole context of information security management is to address its diversity, mobility and complexity. The leader of different internal or external organizations will also be the main action initiator (see ISO/IEC 20000-1, Section 4.2). This section concretizes ISMS requirements through various levels or fields, using diverse equations and tools. These actions are connected in simultaneously building the ISG structure. In a four year plan, the vulnerability of standardization in ISG toward information security techniques has become an issue that ISMS must now face.

The process of ISMS standardization requires sympathy and reasoning. Sympathy refers to putting oneself in the shoes of standard creators, and seeing the standard in its entirety. A standard becomes alive when reasoning comes into play with sympathy. A standard is formed by an infinite number of chances, whether it is the cause or caused, an opportunity or the result of a trend, but it is never an accident. From a long-term perspective, one will begin to see that a standard is an unstoppable flow of trends. The reading and reasoning of ISMS standards requires the integration of both natural science and social science contexts to blend into a whole with culture and e-Taiwan.

More in-depth exploration into the establishment of top-down action programs on the ISG integrated with ISMS implementation in accordance with the framework of ISO/IEC 38500:2008(E) and ISO/IEC 27003:2009(E) is required. When the ISMS standardization process showed signs of “BananaVpeel words” and received no accusation, how to face the subject of ISMS standardization squarely became a natural phenomenon. Nevertheless, the deterioration of the ISMS quality culture will only lead to its loss of credibility in society. Confusion should be avoided on certification or the “Golden handcuffs syndrome”, as that would clearly disregard the requirements of the standard. What is more important is reestablishing the fundamental value of the ISMS standardization, and restoring public faith in ISMS credibility. This should be governments top priority in the development of information security standards.

Consequently, as part of the action programs of the ISG published in the third phase of the National Information and Communications Technology Security Development Program, mentioned earlier, and due to the fact that the players that shaped ISMS decisions and mechanisms were involved with complex, multi-level governance issues, the implication is that the ISMS standardization process had developed into the realm of information security management system knowledge [2, 3]. A method of capitalizing on this opportunity should become the next topic of key action programs in Taiwan ISMS standardization improvement [11].

Acknowledgments

The authors would like to express our appreciation to the anonymous reviewers for their useful suggestions. Besides, the authors would also like to thank the support from the Office of Information and Communication Security, Executive Yuan, Taiwan, Republic of China, and the Local Tax Bureau, Hsinchu City, Taiwan, Republic of China, for their assistance in the material.

References

[1] A. A.-Musa, "Information security governance in saudi organizations: an empirical study," *Information Management & Computer Security*, vol. 18, no. 4, pp. 226–276, 2010.

[2] I. Bache and M. Flinders, *Multi-level Governance*, Richmond, TX, USA: Oxford University Press, 2005.

[3] A. Back, G. V. Krogh, A. Seufert, and E. Enkel, *Putting Knowledge Networks into Action: Methodology, Development, Maintenance.* Berlin, Heidelberg, Germany: Springer-Verlag, 2005.

[4] J. Backhouse, C. Hsu, and L. Silva, "Circuits of power in creating de jure standards shaping the international information systems security standard," *MIS Quality*, vol. 30, pp. 413–438, 2006.

[5] P. Bowen, *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology (NIST) Special Publications 800-100, 2006.

[6] H. Chen, "Digital government: technologies and practices," *Decision Support Systems*, vol. 34, no. 3, pp. 223–227, 2003.

[7] S. R. Clegg, *Frameworks of Power*, London, UK: Sage Publications, 1989.

[8] E. Donna and D. C. Yen, "E-government: An analysis for implementation: framework for understanding cultural and social impact," *Government Information Quarterly*, vol. 22, no. 3, pp. 354–373, 2005.

[9] Executive Yuan, *Dispatch Document No. 096000567*, Taiwan, Republic of China, 2007.

[10] Executive Yuan Law and Regulation Commission, *Administrative Agency Legal Operation and Practice*, Taiwan, Republic of China, 2005.

[11] K. J. Farn, S. K. Lin, and C. C. Lo, "A study on e-taiwan information security classification and implementation," *Computer Standards & Interfaces*, vol. 30, no. 1-2, pp. 1–7, 2008.

[12] E. Gal-Or and A. Ghose, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005.

[13] C. Hsu, "Frame misalignment: interpreting the implementation of information security certification in an organization," *European Journal of Information Systems*, vol. 18, no. 2, pp. 140–150, 2009.

[14] C. C. Huang, K. J. Farn, and F. Y. S. Lin, "A study on ISMS policy: importing personal data protection of ISMS," *Journal of Computers*, vol. 23, no. 1, pp. 35–41, 2012.

[15] ISO, *Health Informatics - Information Security Management in Health Using ISO/IEC 27002*, ISO 27799, 2008.

[16] ISO, *Resolutions of the 38th SC27 WG1 Plenary Meeting Hold in Beijing, China*, ISO/IEC JTC 1/SC 27 WG1 N17800, 2009.

[17] ISO/IEC, *Information Technology - Security Techniques - Information Security Management Systems - Requirements*, ISO/IEC 27001, 2005.

[18] ISO/IEC, *Corporate Governance of Information Technology*, ISO/IEC 38500, 2008.

[19] ISO/IEC, *Information Technology - Security Techniques - Information Security Management System Implementation Guidance*, ISO/IEC 27003, 2010.

[20] ISO/IEC, *Text for ISO/IEC 3rd WD 27014: Information Security Governance Framework*, ISO/IEC/JTC1/SC27 N8712, 2010.

[21] ISO/IEC, *Information Tchnology - Security Techniques - Governance of Information Security*, ISO/IEC 27014, 2013.

[22] ISO/IEC, *Information Technology - Security Techniques - Information Security Management Systems - Requirements*, ISO/IEC 27001, 2013.

[23] IT Governance Institute, *Information Security Governance, Guidance for Boards of Directors and Executive Management (2nd edition)*, IL, USA: Rolling Meadows, 2006.

[24] IT Governance Institute, *IT Assurance Guide Using COBIT*, IL, USA: Rolling Meadows, 2007.

[25] B. Khoo, P. Harris, and S. Hartman, "Information security governance of enterprise information systems: an approach to legislative compliant," *International Journal of Management and Information Systems*, vol. 14, no. 3, pp. 49–55, 2010.

[26] S. Lee and J. D. Kim, "A framework of business security governance," in *Proceedings of the 3rd Joint Workshop on Information Security*, pp. 213–224, 2008.

[27] Ministry of Justice, "Personal information protection act," Taiwan, Republic of China, 2010.

[28] R. Moulton and R. S. Coles, "Applying information security governance," *Computers & Security*, vol. 22, no. 7, pp. 580–584, 2003.

[29] National Information and Communication Security Taskforce, *Implementation Program on Information Security Responsibility Classification in Governmental Departments*, Information Security Dispatch Document No. 0980100328, Taiwan, Republic of China, 2009.

[30] National Information and Communication Security Taskforce, *National Information and Communications Technology Security Development Program (2009~2012)*, Information Security Dispatch Document No. 0980100055, Taiwan, Republic of China, 2009.

[31] National Information and Communication Security Taskforce, *Reference Manual for Information Systems Classification/Grading and Authentication Mechanism*, Information Security Dispatch Document No. 0990100394, Taiwan, Republic of China, 2010.

[32] National Information and Communication Security Taskforce, *National Information and Communications Technology Security Development Program (2013˜2016)*, Information Security Dispatch Document No. 1020157911, Taiwan, Republic of China, 2013.

[33] S. Posthumus and R. von Solms, "A framework for the governance of information security," *Computers & Security*, vol. 23, no. 8, pp. 638–646, 2004.

[34] Research, Development and Evaluation Commission, *Planning Framework for Civil Servants Information Security Awareness*, Taiwan, Republic of China, 2009.

[35] S. Smith, D. Winchester, D. Bunker, and R. Jaimeson, "Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization," *MIS Quarterly*, vol. 34, no. 3, pp. 463–486, 2010.

[36] G. Strejcek and M. Theil, "Technology push, legislation pull? e-government in the European Union," *Decision Support Systems*, vol. 34, no. 3, pp. 305–313, 2003.

[37] C. W. Tan and S. L. Pan, "Managing e-transformation in the public sector: an e-government study of the Inland Revenue Authority of Singapore (IRAS)," *European Journal of Information Systems*, vol. 12, no. 4, pp. 269–281, 2003.

[38] A. Da Veiga and J. H. P. Eloff, "An information security governance framework," *Information Systems Management*, vol. 24, no. 4, pp. 361–372, 2007.

[39] B. von Solms, "Information security governance: COBIT or ISO 17799 or both?," *Computers & Security*, vol. 24, no. 2, pp. 99–104, 2005.

[40] R. von Solms and S. H. von Solms, "Information security governance: a model based on the direct-control cycle," *Computers & Security*, vol. 25, no. 6, pp. 408–412, 2006.

[41] R. von Solms and S. H. von Solms, "Information security governance: Due care," *Computers & Security*, vol. 25, no. 7, pp. 494–497, 2006.

[42] S. H. von Solms, "Information security governance - compliance management vs operational management," *Computers & Security*, vol. 24, no. 6, pp. 443–447, 2005.

[43] S. H. von Solms and R. von Solms, *Information Security Governance*, New York, USA: Springer, 2008.

[44] H. Xu, H. H. Teo, B. C. Y. Tan, and R. Agarwal, "Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services," *Information Systems Research*, vol. 23, no. 4, pp. 1342–1363, 2012.

[45] M. Yildiz, "E-government research: reviewing the literature, limitations, and ways forward," *Government Information Quarterly*, vol. 24, no. 4, pp. 646–665, 2007.

Chien-Cheng Huang received his M.S. degree in information management from the National Chiao Tung University in 2008, and his Ph.D. degree in information management from the National Taiwan University in 2014. He is an adjunct assistant professor with the National Taipei University of Nursing and Health Sciences. His current research interests include data mining, business intelligence, information security, and cyber/network forensics.

Kwo-Jean Farn is an adjunct associate professor with the National Chiao Tung University in Taiwan. He received his Ph.D. degree in 1982. He has had a 30-year career at Information Technology and about 20-year career at Information Security. He was the chair of the Implementation National Critical Information Infrastructure Protection Project at the Computer & Communications Research Laboratories/Industrial Technology Research Institute (CCL/ITRI) from 1999 to 2000. He had worked at the ITRI for more than 18 years until the summer of 2001. He has 9 patents in the information security area. He also received the National Standardization Award in 2009.

Appendix A: Interviewees and Documents

Position	Role	Interview method
Director, Office of Information and Communication Security, Executive Yuan	Decision Maker	Face-to-face interview
Director, Information & Communication Security Division, Investigation Bureau, Ministry of Justice	Manger	Face-to-face interview
Special Agent, Information & Communication Security Division, Investigation Bureau, Ministry of Justice	Executor	Face-to-face interview, e-mail, telephone follow-up
Associate Researcher, Office of Information and Communication Security, Executive Yuan	Original contributor to the document	Face-to-face interview, telephone follow-up
Assistant Researcher, Office of Information and Communication Security, Executive Yuan	Original contributor to the document	Face-to-face interview, telephone follow-up
Specialist, Office of Information and Communication Security, Executive Yuan	Original contributor to the document	Face-to-face interview, telephone follow-up
Senior Advisor, National Security Council	Advisor and decision	Face-to-face interview
Commissioner, National Communications Commission (NCC)	Decision maker	Telephone interview
Deputy Director, Technologies Administration Department, NCC	Manger	Face-to-face interview, telephone follow-up
Minister without Portfolio, Executive Yuan	Decision maker	E-mail
Deputy Director, Office of Information and Communication Security, Executive Yuan	Manger	Face-to-face interview, telephone follow-up
Project Consultant, Security Technology Center, Office of Information and Communication Security, Executive Yuan	Planner	Face-to-face interview
Technical Director, Security Technology Center, Office of Information and Communication Security, Executive Yuan	Executor	Telephone interview
Specialist, National Security Council	Executor	Face-to-face interview, telephone follow-up
Chief, System Design Section/Information Division, National Immigration Agency	Manger	Telephone interview
Documents	**Websites**	
IA (Information Assurance) Policy Chart	http://iac.dtic.mil/csiac/ia_policychart.html	
FISMA (Federal Information Security Management Act) Implement Project	http://csrc.nist.gov/groups/SMA/fisma/index.html	
CC (Common Criteria)	http://www.commoncriteriaportal.org/	
NVD (National Vulnerability Database)	http://nvd.nist.gov/	
ITIL (Information Technology Infrastructure Library)	http://www.itil-officialsite.com/	
IT (Information Technology) Security Evaluation Standards (in Chinese)	http://www.ncc.gov.tw/chinese/	
National information and communications technology security development program (2009˜2012) (in Chinese)		
Reference manual for information systems classification/grading and authentication mechanism (in Chinese)		
National information and communications technology security development program (2013˜2016) (in Chinese)		
Audit operational planning on information and communications technology security in governmental departments (2013) (in Chinese)		

Appendix B: Implement work requirements of "Implementation Programs on Information Security Responsibility Classification in Governmental Departments" [29]

Operating Name	Defense-in-Depth	ISMS Operating Promotion (Note 1)	Audit Modes	Educational Training of the Information Security	Professional Certificates (Note 4)	Detect Vulnerability in the Website of the Agencies
Class A	NSOC (Direct Protection) / SOC (Insourcing or Outsourcing), IDS, Firewall, Anti-Virus, E-mail Filter	Obtain third-party certification	Internal audit at least twice per year	① At least 3, 6, 18, 3 hours per year. (They fall into four categories in Note 2.); ② Obtain information security competence authentication, including information personnel and information security personnel (Note 3)	Maintain least two information security professional certificates	Twice per year
Class B	SOC (Option), IDS, Firewall, Anti-Virus, E-mail Filter	Obtain third-party certification	Internal audit at least once per year.	① At least 3, 6, 16, 3 hours per year. ② Obtain information security competence authentication, including information personnel and information security personnel (Note 3)	Maintain least one information security professional certificate	Once per year
Class C	Firewall, Anti-Virus, E-mail Filter	Self-establish the Team to Planning Operation	Self-review	At least 2, 6, 12, 3 hours per year.	Information security professional training	Once per year
Class D	Firewall, Anti-Virus, E-mail Filter	Advocacy to promote ISMS Concept	Self-review	At least 1, 4, 8, 2 hours per year.	Information security professional training	Once per year

Note 1 The scope of the ISMS certification shall cover information systems of the organizations core businesses, and be gradually expanded to cover the entire organization

Note 2 (1) General Chief: Relevant personnel takes charge of the chief position, e.g.: president, vice-president, department chair, chief information security officer, and etc.
(2) Information Personnel: Relevant personnel takes charge of the information operation, e.g.: system analysis and design personnel, system develop personnel, system management personnel, and system operation personnel, and etc.
(3) Information Security Personnel: Relevant personnel takes charge of the information and communication security, e.g.: information security management personnel, information security audit personnel, and etc.
(4) General User: Information system is used by the users, e.g.: administrator, accounting personnel, and etc.

Note 3 Information security competence authentication subject includes information & communication management system, information system risk assessment, information & communication audit, government information operation outsourcing security, information security incident operation, electronic document protection, e-mail security and web application security, and etc. The information and information security personnel of the class A and B agencies take trainings of the information security and obtain certifications from the planning and holding for Research, Development and Evaluation Commission, Executive Yuan.

Note 4 Information security professional certificates are published by the independent certification and authentication institution at home and abroad. The information security class includes ISO 27001 Lead Auditor (LA), Certified Information Security Manager (CISM), Systems Security Certified Practitioner (SSCP), Certification for Information System Security Professional (CISSP), Certified Ethical Hacker (CEH), Global Information Assurance Certification (GIAC), and etc.