

ABSTRACT

To assure the integrity and security of our information and communication infrastructure, a comprehensive national protection mechanism must be developed and a goal from national security perspective must be established. However, the development of this mechanism must adhere to certain national and international standards to assure its robustness. In this article, the current information technology (IT) security standardization activities in Chinese Taipei will be introduced, and the information and communication security decision and oversight system in our cabinet, which is the national information security protection mechanism, will also be described. Finally, the updated information on IT security projects in e-Taiwan will be provided.

1. Current Information Technology Security Standards Activities in Chinese Taipei

According to Article 2 of the Standards Act, the Ministry of Economic Affairs (MOEA) is stipulated as the standards authority. The Bureau of Standards, Metrology and Inspection under the MOEA is responsible for implementation matters of national standards. To develop national standards, BSMI establishes 26 National Standards Technical Committees (TCs), each of which consists of experts and scholars that are involved in standards-related businesses with a tenure of two years. Under these Committees, there are 169 sub-committees. Each sub-committee operates independently and is convened by the chairperson. TC 22 is responsible for information and communication standards, and it has the following sub-committees:

- SC1 Terminology and Basic Rule
- SC2 Code
- SC3 Software
- SC4 Hardware
- SC5 Chinese Information and Coding
- SC6 Communication Technology
- SC7 Data Processing
- SC8 Information and Communication Security

The major objectives of TC22/SC8 in 2005 are to develop standards for IT security certification/accreditation scheme and IT security assurance framework.

2. Standards in IT Security Certification and Accreditation Scheme

The IT security certification and accreditation scheme is shown in Figure 1 and major Chinese National Standards (CNS) developed by TC22/SC8 according to this scheme includes:

- CNS 14731: This standard is the guidelines for the accreditation bodies operating certification/registration of information security management systems and has been adopted by the Chinese National Accreditation Board (CNAB).
- CNS 12608: The standard is the assessment criteria for the laboratory accreditation and has been adopted by the Chinese National Laboratory Accreditation (CNLA).
- CNS 17799 and CNS 17800: The localized version of ISO/IEC 17799 and BS 7799 Part 2. The BSMI has adopted CNS 17800 to certify organizations that apply for ISMS certifications.
- CNS 15408: The localized version of ISO/IEC 15408.

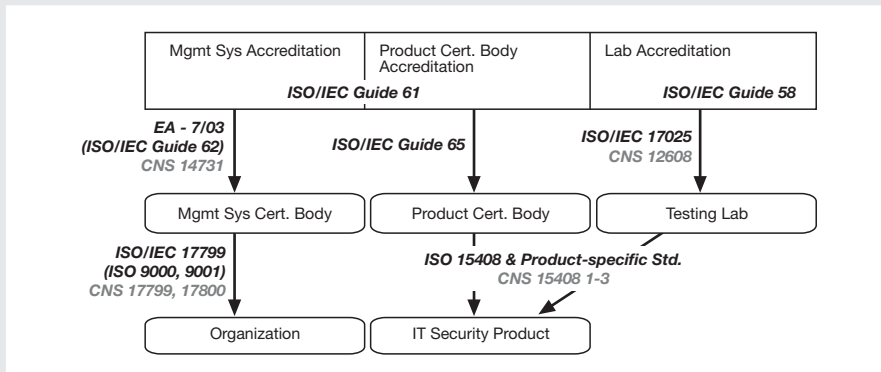


Figure 1: IT Security Certification and Accreditation Scheme of Chinese Taipei

3. Standards in IT Security Assurance Framework

IT systems are subject to failure and security violations due to errors and vulnerabilities. Therefore, an IT security assurance framework is required to manage errors, vulnerabilities

and risks in the life cycle of IT deliverables. TC22/SC8 references the IT security assurance framework in ISO/IEC TR 15443 to develop the required CNSs. Table 1 shows the list of these standards, their ISO counterparts and their current status:

ISO Number	CNS Number	Approval	Drafting	Planning
ISO/IEC 12207	CNS 14837	■		
ISO/IEC TR 13335-1	CNS 14929-1	■		
ISO/IEC TR 13335-2	CNS 14929-2	■		
ISO/IEC TR 13335-3	CNS 14929-3	■		
ISO/IEC TR 13335-4	CNS 14929-4	■		
ISO/IEC TR 13335-5				■
ISO/IEC 14598-1				■
ISO/IEC 14598-2				■
ISO/IEC 14598-3				■
ISO/IEC 14598-4				■
ISO/IEC 14598-5				■
ISO/IEC 14598-6				■
ISO/IEC 15408-1	CNS 15408-1	■		
ISO/IEC 15408-2	CNS 15408-2	■		
ISO/IEC 15408-3	CNS 15408-3	■		
ISO/IEC TR 15504-1	CNS 14785-1	■		
ISO/IEC TR 15504-2	CNS 14785-2	■		
ISO/IEC TR 15504-3	CNS 14785-3	■		
ISO/IEC TR 15504-4	CNS 14785-4	■		
ISO/IEC TR 15504-5	CNS 14785-5	■		
ISO/IEC TR 15504-6	CNS 14785-6	■		
ISO/IEC TR 15504-7	CNS 14785-7	■		
ISO/IEC TR 15504-8	CNS 14785-8	■		
ISO/IEC TR 15504-9	CNS 14785-9	■		
ISO/IEC 17799	CNS 17799	■		
ISO/IEC 21827				■

Table 1: List of CNS, their Status and the Corresponding ISO Standards

4. National Information and Communication Security Taskforce

In January 2001, the cabinet passed the National Information and Communication Infrastructure Security Mechanism Plan. According to this major plan, the National Information and

Communication Security Taskforce (NICST), i.e., an information and communication security decision and oversight system in our cabinet was established in March 2001.

The vision of the NICST is to assure information and communication network resources can be fully used in an obstacle-free and secure environment by year 2008. In order to meet this goal, six working groups (WGs) and one technical service center were formed. Each working group has a government agency as the convener. Figure 2 shows the organization structure of NICST.

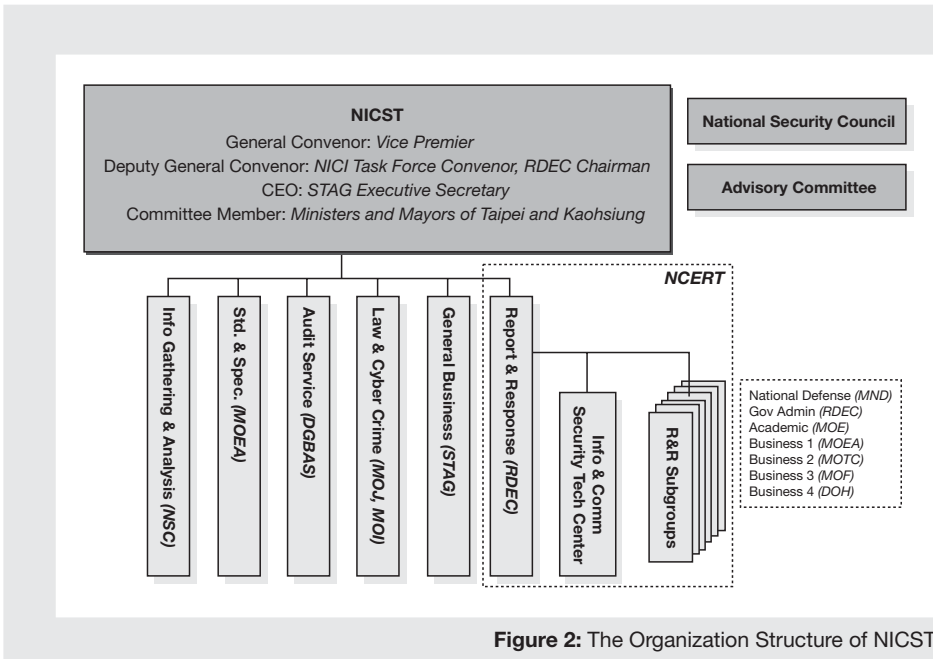


Figure 2: The Organization Structure of NICST

These six WGs include:

- Information Gathering and Analysis WG

This WG is led by the National Science Council (NSC). Its major function is to gather security related researches and practical data, provide timely, accurate and sufficient information, and effectively grasp the information and communication security development status in other countries.

- Standards and Specifications WG

This WG is led by the Ministry of Economic Affairs (MOEA). Its major function is to establish standards and actively participate in the regulation of international information and communication security standards.

- Audit Services WG

This WG is led by the Directorate General of Budget, Accounting & Statistics (DGBAS). The DGBAS organizes Security Audit Service Corps to provide effective assistance to agencies concerned in providing IT security audit service and undertaking security check.

- Law & Cyber Crime WG

Led by the Ministry of Justice (MOJ), its function is to promote the review, modification and legislation of information and communication security related regulations, strengthen horizontal communication among law enforcement agencies so as to integrate investigation resource, and actively participate in cross border and regional cooperation in reducing cyber crimes.

- General Business WG

Led by the Science and Technology Advisory Group of Executive Yuan (STAG), its function is to undertake national level information and communication security infrastructure, and coordinate cross-agency administrative efforts.

- Report and Response WG

This WG is led by the Research, Development and Evaluation Commissions (RDEC). Its major function is to establish government reporting and communication network, and feed related information into the network to minimize the impact of security incidents. This WG is also responsible to set up response team immediately and coordinate the efforts of Technology Service Center when emergencies happened.

5. Status Update on IT Security Projects in e-Taiwan

In the first RAISS Forum Proceedings, Chinese Taipei introduces the e-Security initiative of the e-Taiwan projects. After one year, much progress has been achieved in the various security projects. This includes the following major successes:

Natural Person Certificate (NPC) Project

- 868,415 certificates have been issued until 2005/06/20.
- More than 80,000 families have used NPC in declaring tax in May 2005 (approximately 1,100 last year).

Establish National Security Operation Center (NSOC)

- Started operation since February 2005.
- Formed Incident Data Exchange Common Format Taskforce, and testing IODEF-based data exchange with SOCs of Acer, e-Cop, TradeVan, and a number of other related security service providers.

Establish Certificate Interoperability Mechanism

- Bridge Certification Authority (CA) completed interoperability testing between the four CAs.
- Four more companies obtained funding to develop exemplary PKI applications.

Information Security Product Certification Scheme

- Smart Card evaluation laboratory has completely established.
- Firewall evaluation laboratory is now developing, and will be completely established before the end of 2005.

Dr Perry Liu

*Director, Information Security Service Center
Project Resource Division, Institute for Information Industry*



Dr Perry Liu is the Director of Information Security Service Center (ISSC) and Project Resource Division in the Institute for Information Industry (III). The major function of ISSC is to help government agencies in planning and constructing information and communication security infrastructure. In addition, ISSC provides technical and consulting services to government agencies in security protection and recovery assistance.

Dr Liu has been working for III in the past seven years, and had been involved in various systems development projects in the area of medical informatics, knowledge management, electronic commerce and information security.

Dr Liu received his Masters of Science in Electrical Engineering and PhD. from the National Cheng-Kung University in 1993 and 1997, respectively.

Introduction And Updates On Information Security Technologies Related Activities In Japan

Mr Koji Nakao

Co-Chair, RAISS Forum, Japan

*Director, Information Security Technology Department, IT Development Division, KDDI Corporation
Japan*

ABSTRACT

This paper highlights some of the key activities on Information Security Technologies in Japan. We focus on three major areas of interest. First, we discuss the Primary Recommendation on the preparations for a review of role and function of the Japanese government in addressing IT security issues, which is part of the security strategies provided by the Ministry of Economy, Trade, and Industry (METI). Next, we provide an update on the activities of Telecom-ISAC [Information Sharing, Analysis and Coordination] Japan, and finally, introduce the new security initiative, known as the Security Promotion Realizing Security Measures Distribution (SPREAD) Consortium. Telecom-ISAC Japan and SPREAD Consortium will both have a significant and positive impact on the Japanese Internet Service Providers (ISPs) and Internet end-users.

1. Overview of the Primary Recommendation on the Preparations for a Review of Role and Function of the Japanese Government in Addressing IT Security Issues

The following information is a result of the discussions by the Japanese security experts groups in the cabinet of Japan.

1.1 Orientation of the Primary Recommendation on Issues Related to IT Security

(1) Orientation of the Primary Recommendation

The Committee for Essential IT Security Issues has discussed two pressing issues pertaining to the "Government's Efforts in IT Security" and compiled "Primary Recommendation."

The two issues are:

1. The optimal comprehensive structure for implementing IT security measures.
2. Optimal measures by government to ensure information security internally.

A plan will be made to address each issue, targeted for realization within three years (by the end of 2007).

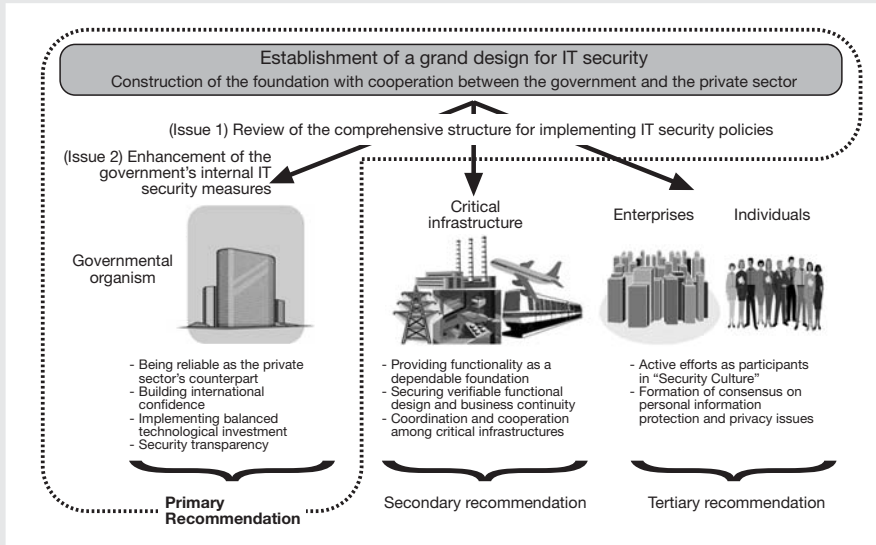


Figure 1: A Three-Tier Recommendations Encompassing Both Government and Private Sectors

(2) Basic Philosophy

Information technology (IT) has now taken root in the whole of society as a new social infrastructure actively utilized in industrial, economic and administrative activities, as well as the lives of the people. Building on the premise that failsafe information security is indispensable for the sound development of this social infrastructure, the government needs to examine the following nine common ideas as it tackles information security issues:

- (i) Protect all the components,
- (ii) Shift from "add-on type" to "built-in type",
- (iii) Ensure rationality and effective response to change,
- (iv) Adopt the "failsafe" concept,
- (v) Ensure legality, transparency, and the protection of human rights,
- (vi) Create a sustainable structure,
- (vii) Integrate and share expertise,
- (viii) Be aware of division of roles, and
- (ix) Set priority in accordance with the degree of impact.

Further, the government needs to embark on thorough, in-depth discussions on the relationship between security and crisis management.

1.2. Review of the Government's Functions and Roles in Addressing IT Security Issues

1.2.1. The optimal comprehensive structure for implementing IT security measures (Issue 1)

(1) Basic recognition - the need for "basic IT security strategies" at the national level

In conjunction with the increased need for efforts in IT security issues in various areas, the respective ministries and agencies that implement the policies should enhance the promotion of related measures from their own viewpoints.

For the overall coordination of these measures among the ministries and agencies, the government has established IT Security under the Cabinet Secretariat, the secretariat of the IT Security Promotion Committee, and the IT Security Expert Meeting (and the Committee for Essential IT Security Issues within it). Though these bodies continue to make good progress in their respective activities, the basic strategies at the national level beyond the ministry and agency borders do not yet seem to be sufficient.

The government will therefore need to further enhance measures in the responsible ministries and agencies, as well as to formulate basic IT security strategies at the national level.

In other words, the government must now take steps to build its own strategies independently after a focused and emphatic ascertainment of the "information security (securing the safety and reliability of an advanced information and telecommunications network)" under the e-Japan priority plans.

(2) Desirable specific measures

Once the government have ascertained and adjusted the measures of related ministries and agencies, it should be endowed with a system to allow the effective formulation and implementation of "basic information security strategies."

This should include the following:

- (i) Formulate basic strategies for IT security (mid-term, long-term, and annual plans).
- (ii) Enhance the functionality of information collection and analysis for formulating basic strategies.
- (iii) Implement ex-ante evaluations of related measures (including budgets) based on the basic strategies.
- (iv) Perform ex-post evaluations and publish the results.
- (v) Enhance the public relations function.

The system stated above must include a mechanism to evaluate the efficacy of investment in research and development pertaining to government-implemented IT security.

1.2.2. Optimal measures by government to ensure information security internally (Issue 2)

(1) Basic recognition - the need for strengthening "unified, cross-sectional, and comprehensive coordinating function" of the government in carrying out its measures

In view of the important information and national secrets in its possession, the government as a whole must develop a thorough set of high-level IT security measures capable of protecting the assets and rights of the nation and securing the reliability of Japan in international relations.

Therefore, in addition to the measures taken by individual ministries and agencies, a "unified, cross-sectional, and comprehensive coordinating function" will be crucial to promote and improve the level of the measures undertaken by the government as a whole.

Although the IT Security Office within the Cabinet Secretariat has been implementing activities to provide "unified, cross-sectional, and comprehensive coordinating function," its original purpose focused on providing protection from external attacks tampering government web pages. It has now come to realize its inability to respond to the rapidly-changing viewpoints as shown in the following page.

- (i) Coping with the possibility of leaks, tampering, or destruction of administratively important information from the inside.
- (ii) Coping with the possibility of failures in information systems due to shortcomings in system designs and erroneous settings or other types of errors in operation.
- (iii) Addressing the need to construct an information management structure within the government, to foster human resources specialized in IT security issues, to promote research and development, and to raise the levels of public awareness.

In view of the above, the government will need to undertake measures to enhance "unified, cross-sectional, and comprehensive coordinating function" in parallel with the efforts and measures undertaken by the ministries and agencies individually.

(2) Specific measures desired

The Cabinet Secretariat will need to take the following steps to enhance the "unified, cross-sectional, and comprehensive coordinating functionality" of the measures undertaken by individual ministries and agencies.

(i) Support for the promotion of comprehensive measures

- Formulate intra-government coordinated safety standards and evaluate the respective ministries and agencies based on the standards.
- Collect and analyze information as part of a regular review of the intra-government coordinated safety standards.
- Make provisions for budgets in conjunction with the recommendations made to the respective ministries and agencies to promote measures based on the evaluation results.
- Support the ministries and agencies with safe system designs on a request basis.

(ii) Support for measures addressing incidents related to IT security

- Enhance the timeliness and responsiveness of collection and analysis of information on vulnerability and signs of attacks.

- In so doing, regularly survey the status of operations/information systems of the respective ministries and agencies on a regular basis to obtain necessary information for routine risk analyses as to how the respective ministries and agencies would be affected if incidents occurred.
- Enhance the functionality of mechanisms to identify information on damages and analyze causes when incidents related to IT security occur within individual ministries and agencies.
- Enhance coordination among public and private organizations (such as Cyber Force of the National Police Agency, NICT, IPA, Telecom-ISAC, JPCERT/CC) and product developers in addressing incidents related to IT security.
- Support organizing IRTs (Incident Response Teams) in the respective ministries and agencies when formulating guidelines to respond to incidents related to IT security.

(iii) Support for fostering and securing human resources in government

- Support efforts to improve security competency of professional and personnel engage in IT security measures in government ministries and agencies. Support personnel policies in the ministries and agencies so as to enable long-term and systematical fostering of security-competent human resources.
- With respect to human resources with a high degree of technical knowledge on IT security in the government, their roles and responsibilities in their current appointment within the ministries and agencies need to be identified and clarified. The need for each role needs to be formalized to facilitate future recruitment and ensure adequate fosterage of each role, both externally and within the government.
- In conjunction with efforts to systematize the fosterage of human resources in universities and other educational establishments, open a career path for students who wish to become government employees.
- In conjunction with the implementation of continuous on-the-job-training (OJT) for government employees (i.e., end users), implement programs to improve the awareness among top officials.

2. Activities on Telecom-ISAC Japan

2.1 Overview

Security events such as scans and probes, computer intrusions, malicious software (viruses, worms, Trojans, etc), computer sabotage and denial of services (DoS Attacks, etc.) are well recognized in our IT environments today. One of the key solutions to protect against these security events and to minimize damages, such Internet risk should be closely observed by means of incident monitoring and analysis in conjunction with supports from ISPs (Internet Service Providers).

For this purpose, Telecom-ISAC [Information Sharing, Analysis and Coordination] Japan was founded in June 2002 with the aim to protect telecommunication infrastructure by working in concert with each ISAC Member, to cope with and take preventive measures against any incidents that may impede proper telecommunication services or endanger the information security of other important infrastructures.

To coordinate efforts to manage security incidents, Telecom-ISAC Japan is responsible for providing qualified Members with the opportunity for sharing proper information on security events and incidents and, as an independent and reliable association, also responsible for contacting and cooperating with other organizations that work on incidents.

As part of the missions, Telecom-ISAC Japan must be managed as an independent and reliable organization that collect, share, analyze, and provide information on security events and incidents through cooperation and coordination among Members.

Telecom-ISAC Japan takes immediate actions or preventive measures against incidents to minimize the effect on Members' telecommunication services and other important infrastructures as shown in Figure 2. Such contribution to the industry security provides the key motivation for the implementation and operation of Telecom-ISAC Japan.

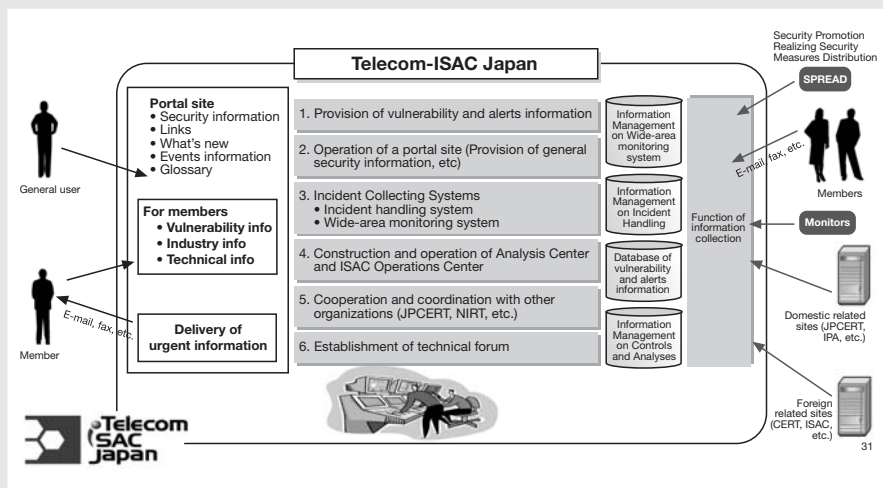


Figure 2: An Overview of Telecom-ISAC Japan

2.2 Specific Security Controls Discussed and Operated for Telecommunications Infrastructure

- 1) Incident responses
 - Large-Scale Worms, such as Blaster, Sobig.F, Netsky, etc
 - Against Antinny, Constant DDoS attacks to ACCS

- 2) Research and investigation of Botnets which are increasingly active in our IT environments
 Since Botnets are proliferating actively in the Internet, the current activities of Botnets are observed and reported by the ISAC member for the purpose of information sharing.

- 3) Development of Wide-Area Monitoring System
 Telecom-ISAC is now planning to install probe devices (traffic monitors, IDS, virus detection systems etc.) for the purpose of collecting security information from networks, mainly ISPs such as:
 - a) the traffic flow data on a real time basis; and
 - b) the various security logs from Fire-Wall, IDS, and Virus-Detector.

Information on traffic flow data and security logs are collected swiftly at the ISAC Center and analyzed in an integrated manner. One critical goal of the Wide-Area Monitoring System is to ensure that incidents that emerged in our environments can be identified timely and responded promptly to the ISAC members.

4) Research activities on Trace-Back

As a new technology to support Telecom-ISAC activities, trace-back technology is also identified to detect malicious spoofed source addresses. This research is an on-going process to study application level trace-back together with network level trace-back. The output of this will enable ISAC to share information relating to spoofed malicious attackers and enable such malicious activities to be curtailed efficiently and effectively.

2.3 Collaborations with Related Organizations

A common theme defined in Telecom-ISAC Japan is "Sound competition among ISPs starts with harmonized collaboration". In general, many security activities are currently required in the Internet environment and most of them need close collaboration among ISPs.

It is also important for the ISAC to collaborate and coordinate with other security organizations such as JPCERT/CC, IPA, NICT and NISC. Further collaboration is also necessary with related international organizations and/or groups.

Activities on ISAC will be indispensable for the establishment of secure telecommunication infrastructure such as secure services provision and secure ISP operations. Security controls discussed and implemented in the ISAC will also be applicable for any other information relying environments or society based on IT.

3. Security Promotion Realizing Security Measures Distribution (SPREAD) Consortium

3.1 Overview

In recent years, increased damage caused by problems such as computer viruses and worms together with incidents involving information security have caused increased concerns with the effect they might have on the information exchange infrastructure. There is a strong

desire for a precise yet speedy response, involving close cooperation between IT groups, to tackle these information security issues.

A preparatory committee was hence established in early 2004 to discuss a suitable action policy to ensure and maintain security for all Internet users. As a result, and with the support of IT companies and organizations in Japan, the Security Promotion Realizing Security Measures Distribution (SPREAD) Consortium was established on 30 June 2004.

The SPREAD Consortium is a non-profit organization made up of representative companies from diverse industries associated with computers and the Internet, and includes Japan Network Security Association and Telecom-ISAC Japan (as described earlier), a number of hardware and software makers, ISPs, system integrators, mass merchandisers and media, user community and government organizations. Close cooperation between these groups will promote simple, speedy and reliable delivery of security information including published vulnerabilities and measures to Internet users.

3.2 Activities of the SPREAD Consortium

The following are initial activities of the SPREAD Consortium, undertaken since its formation in June 2004:

- Delivery of easy-to-understand security information to general Internet users.
- Formation and management of a community for speedy and reliable communication of security information to Internet users.
- Staging of security awareness events with wide access to Internet users, and promotion of security awareness amongst Internet users.

A national security awareness event targeting at general Internet users was also planned for and conducted in June 2005. The event was known as the Information Security Month.

SPREAD Consortium's supporting companies will continue to grow as the group continues to improve user awareness of security issues. The cross platform, cross system nature of the collaboration will help to spread and maintain a safe, secure and enjoyable environment for Internet users, with ongoing promotion being carried out through mutual cooperation between participating companies. In order to create a more secure and enjoyable Internet environment, as well as to ensure and maintain the security of the user environment, the SPREAD Consortium is now in an important position to promote Internet security in Japan.

Mr Koji Nakao

Co-Chair, RAISS Forum, Japan

Chair, ISO/IEC JTC 1/SC 27/WG 1, Japan

*Director, Information Security Technology Department,
IT Development Division, KDDI Corporation*



Koji Nakao is the Director of Information Security in KDDI, Japan. Since joining KDDI in 1979, Koji has been engaged in the research on multimedia communications, communication protocol, secure communicating system and information security technology for the telecommunications network.

In the IT standards arena, Koji has been involved in ISO and ITU-T activities for many years as for telematic services protocol and information security technology. He is currently the chairman of SC 27/WG 1 in Japan, focusing mainly on information security management standards development and implementation.

Koji is also an active member of Japan ISMS user group, which was established in the first Quarter of 2004. He is a board member of Japan Information Security Audit Association, and concurrently, a Technical Group Chairs (ISEC: information security) of The Institute of Electronics, Information and Communication Engineers.

Koji received the B.E. degree of Mathematics from Waseda University, in Japan, in 1979. He received the IPSJ Research Award in 1992. He is a member of IPJS and IEICE. Koji has also been a part-time instructor in Waseda University and the University of Electro-Communications since 2002.

ABSTRACT

This paper introduces Korea's Information Security Management System (ISMS) Certification Scheme, focusing on the current review of the scheme and its related activities. In addition, it provides a view on the trend of ISMS in Korea, and future direction and improvement planned in the certification scheme and related operational processes.

1. Introduction

The increasing use of information and communications technologies in both business and the public sector has significantly raised more concerns over cyber security threats and vulnerabilities - and, therefore, risks - against which both businesses and public institutions need to take action. Along with the growth in the use of information and communications technologies, Korea has found herself particularly vulnerable to security-related problems due to a lack of countermeasures in many existing information security systems and organizations. In order to ensure the safety and reliability of information assets, it has become important for organizations to take competent information security countermeasures and provide the confidence that sensitive information is securely protected and maintained. Against this backdrop, an efficient approach to achieve an information security management system (ISMS) has become a vital issue, and one which is equally important to all nations around the world.

The purpose of this paper is to introduce Korea's ISMS Certification Scheme, focusing especially on the current review of the scheme and the concurrent legal activities in relation thereto. Korea's ISMS certification scheme is based on the Information and Communications Network Utilization and Information Protection, Etc, Act (enacted in May 2002). The Act recommends but not mandate the implementation of ISMS. There is no punitive measures against non-compliance. Organizations are encouraged to implement ISMS voluntarily. The ISMS scheme is a comprehensive system implementing technological, managerial, and physical countermeasures that are necessary to provide stability of telecommunications networks, and protection of an organization's information assets.

The ISMS scheme is certifiable to provide assurance of proper implementation and practice of ISMS in organizations. The certification scheme in Korea is managed and promoted by the Korea Information Security Agency (KISA).

2. ISMS Certification System in Korea

2.1 Overview

Korea ISMS is a comprehensive system that ensures the consistent management and operation of information security. It works on the principle of putting in place appropriate technologies, management procedures, and information protection measures with the purpose of protecting the major information assets of an organization. The ISMS certification system refers to the system in which KISA conducts an objective evaluation and certifies ISMS status of an individual organization, such as information and communication service providers, private entrepreneurs, or those who provide physical facilities for an information and communication service, for examples, Internet Service Providers (ISPs) and Internet Data Centers (IDCs). The assessment aims to determine whether or not the organization in question has met minimum criteria in terms of technical, physical, and managerial measures, in accordance with the ISMS standard.

The system is based on, and finds its validity in, Section 47 of the Act on the Promotion of Information and Communications Network Utilization and Information Protection.

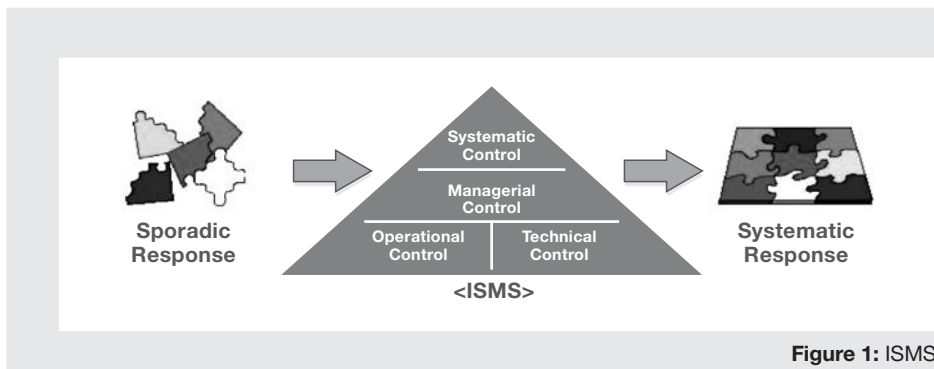


Figure 1: ISMS

2.2 Certification System

The certification system, as shown in Figure 2, is supported by the Ministry of Information and Communication (MIC), the certification body (KISA), a certification committee, and an assessment team. The MIC team establishes policies, upgrades ISMS, and provides financial support in its implementation and execution. KISA carries out the certification assessment and issues certificates to certified organizations when the conditions are met within the criteria. The certification committee under KISA consists of ten experts selected from academies, research centers, and other related organizations. The tenure of each member is two years. The assessment committee comprises 29 assessors in the ISMS team of KISA and external experts. In 2005, an additional seventy nine assessors has been recruited and trained in Korea.

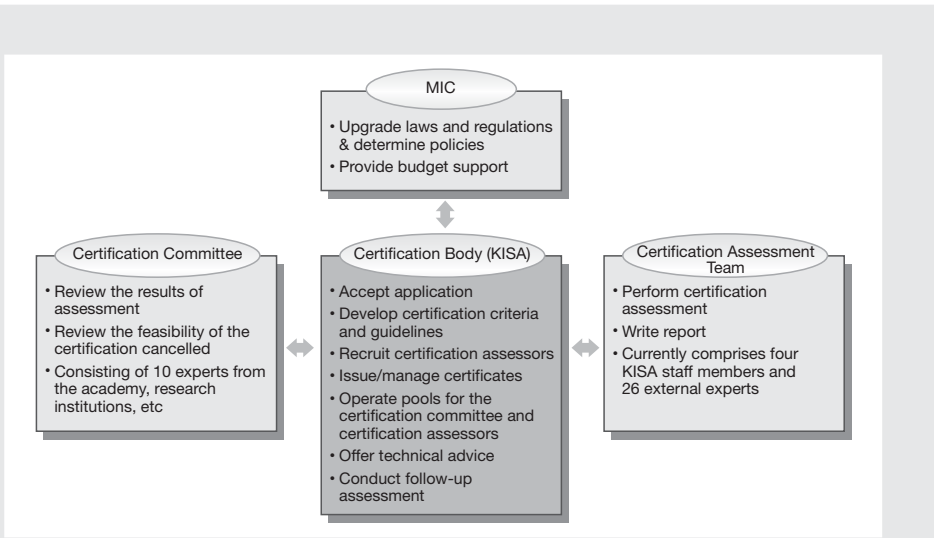


Figure 2: ISMS Certification System

2.3 Candidate Organization for Certification

Based on Section 47 of the Act on the Promotion of Information and Communications Network Utilization and Information Protection, candidates for certification include ISPs, telecommunication organizations that provide physical facilities for communications services, and other communications carriers determined by the Presidential decree. Under the

enforcement ordinance of the Act which also acts as a Presidential decree, those companies have to be registered as communications carriers, other organizations that manage networks, servers, or other communications facilities, such as IDCs, and private businesses that operate information and communications networks connected with ISPs on a national scale, may all be classified as candidate organization for certification. In short, those which operate information and communication networks, linked with the Internet, may apply for ISMS certification.

2.4 ISMS Certification Criteria

ISMS Certification Criteria, as illustrated in Figure 3, was promulgated by an announcement made by the MIC (No. #2002-22). The Criteria consists of 14 requirements for five information security management processes, three control points for documentation, and 120 control points for 15 areas of countermeasures, totaling 137 items. All the requirements listed above should be met in order to gain ISMS certification.

Firstly, ISMS should be established and operated in line with the five information security management processes. Secondly, all the details of ISMS establishment and operation should be documented to ease comprehension of the system by other interested parties. Thirdly, the control points should be identified through a thorough risk analysis. Countermeasures need to be put in place based on the results of the risk analysis.

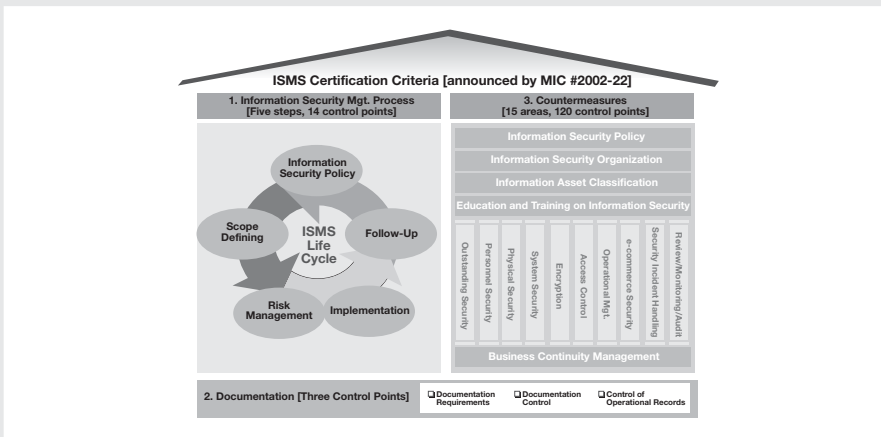


Figure 3: ISMS Certification Criteria

2.4.1 Information Security Management Process Requirements

ISMS is developed and operated on the basis of the establishment of information protection policy, a definition of the ISMS scope, risk management, implementation, and follow-up management.

This process is not simply a series of procedures, but a cyclical process of multiple steps, as depicted in Figure 4.

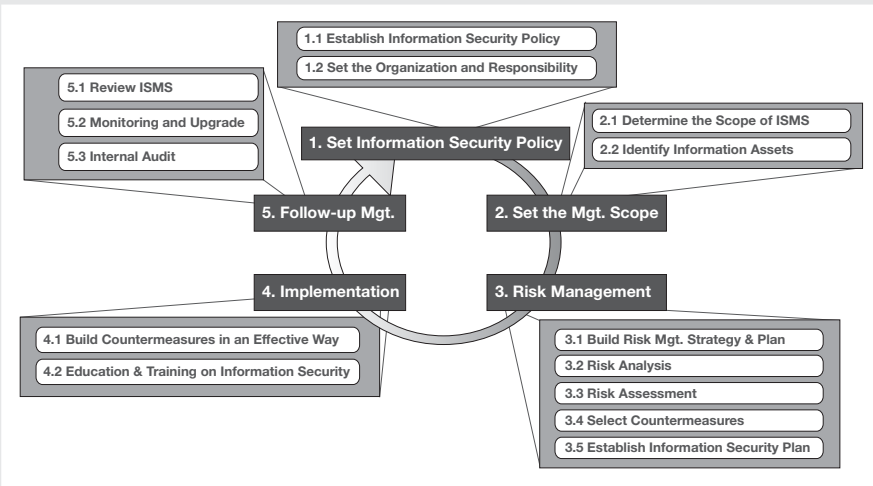


Figure 4: Information Security Management Process Requirements

2.4.2 Documentation Requirements

As previously mentioned, the basis of the establishment and operation of ISMS must always be documented in such a way that people find it easy to understand, search, and enquire. The documentation includes the requirements specification, control of the documents, and control of the records.

2.4.3 Countermeasures for Information Protection Requirements

ISMS is a system that aims to establish countermeasures to control the security risks relating to information systems. The ISMS certification assessment criteria suggest 120 controls points for 15 areas, as depicted in Table 1.

Area of Control	Detailed Control Points	No. of items
1. Information Security Policy	Approve & release the policy, maintain the policy and its systems	5
2. Information Protection Organization	System, responsibility, and role of the organization	4
3. Outsider Security	Negotiate the contract and service level, ensuring outsider security	4
4. Information Asset Classification	Conduct an investigation into the information assets, classify, and handle those assets	4
5. Education and Training on Information Security	Establish, operate, and assess the education and training program	4
6. HR Security	Assign and define responsibilities, assess staff qualifications, manage the staff in charge of major tasks, ensure confidentiality management	5
7. Physical Security	Physical protection district, physical access control, data center security, equipment protection, and office protection	12
8. System Security	Analyze, design, build, and implement the system and manage change	13
9. Encryption	Encryption policy, use of encryption, and key management	3
10. Access Control	Access control policy, user access management, and scope of access control	14
11. Operational Management	Operational procedures, responsibility, system operation, network operation, documentation management, malignant software control, remote computer issues, and work undertaken on a remote basis	22
12. e-commerce Security	Manage the security of the exchange agreement, e-commerce, open servers, and user notification	5
13. Security Incident Handling	Response planning and systems, response & recovery, follow-up assessment	7
14. Review, Monitoring & Audit	Review legal requirements compliance, review information security policy and measures, monitoring and security audit	11
15. Business Continuity Management	Build business continuity management system, plan and build business continuity management, test and maintain business continuity management plan	7

Table 1: Countermeasures

While the specification is comprehensive, it does not mean that all the 120 control points in the 15 areas must be put in place in order to implement ISMS. Once a decision is made after risk analysis, specific control points from the 120 in the 15 areas should be selected in order to reduce any risks identified as significant to the organization. In the event that a required control point is not found in the 120 points, specific reasons for selecting outside the 120 points should be clearly indicated as it will be reviewed at the time of assessment for certification.

2.5 Types of Certification Assessment

The certification process includes certification assessment, re-approval assessment, reassessment, and follow-up assessment. For Korea ISMS implementation, each certification is valid for three years. Recipients of the certification are subject to follow-up assessment at least once a year. Table 2 describes the four types of certificate assessment.

Classification	Details
Certification Assessment	Initial certification assessment
Re-approval Assessment	Assessment conducted in order to extend the validity of the certificate prior to its expiration (within three years of certification)
Reassessment	Assessment conducted in the event of large-scale changes to the ISMS
Follow-up Assessment	Assess the ISMS system in order to confirm that organizations holding certification appropriately maintain their management systems

Table 2: Types of Certification Assessment

2.6 Certification Assessment Fee

As the assessment process is resource intensive, a fee is chargeable by the authority involved. The assessment fee depends on the number of employees in the applicant's company, the size of the facilities related to information and communications, etc.

<p>Certificate Assessment Fee = Application Fee + Direct Labor Cost + Direct Expenses</p> <p>No. of days required to conduct assessment = No. of days determined depending on the number of employees + No. of days determined depending on the information and communications facilities</p> <p>Direct Labor Cost = Unit price of technicians by level * No. of days spent conducting assessment</p>

Table 3: Certificate Assessment Fee

The unit price of technicians by level is determined by unit labor cost and the software technician's competency level. Application costs may vary slightly depending on the assessment type.

2.7 Procedures of the Certification Assessment

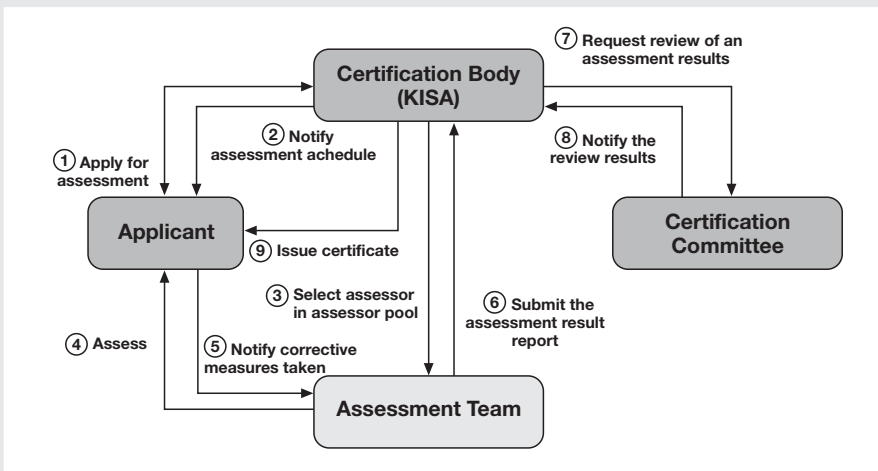


Figure 5: Basic Certification Procedure Flow

The certification process takes approximately three months after an application is submitted for a certificate to be granted. The certificate assessment consists of an assessment of the

technology and the documentation. It requires roughly four assessors to conduct the assessment per day. For any defects discovered during the assessment process, the applicant is afforded one month to take supplementary measures. Once such measures are

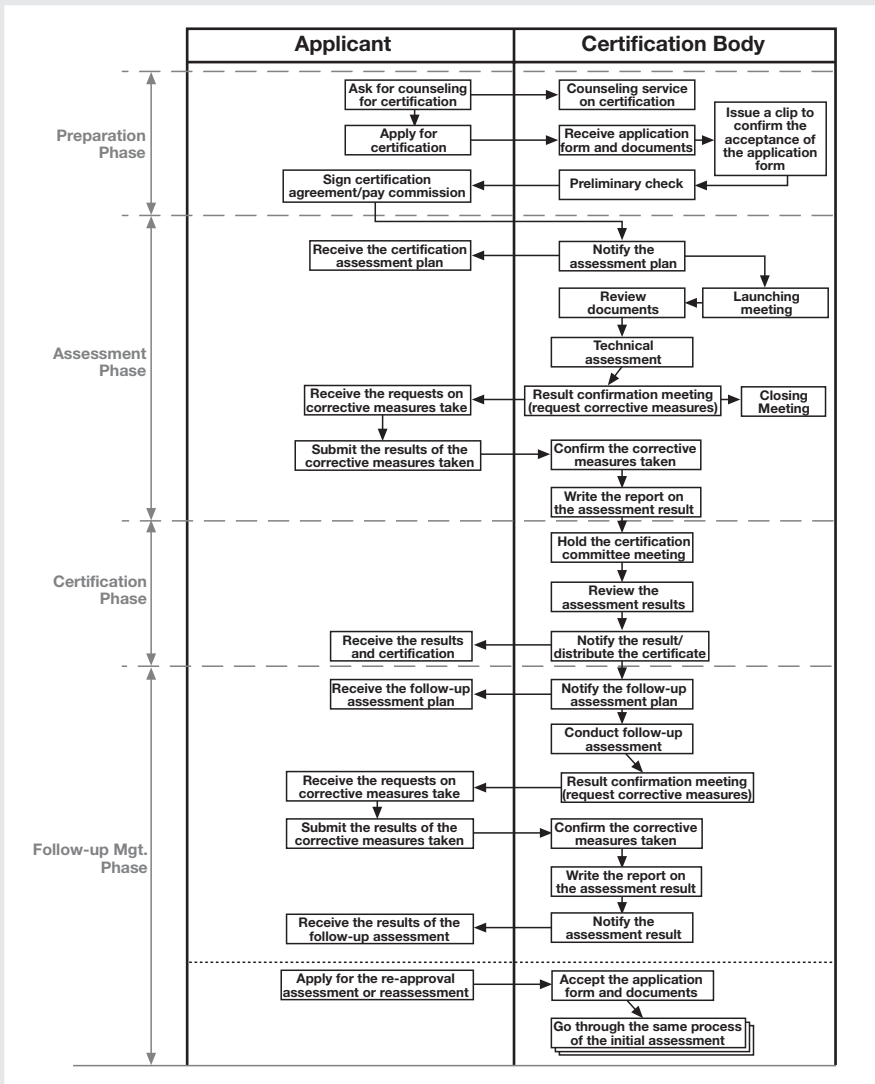


Figure 6: ISMS Certification Procedures

taken, the assessment committee will review and approve the results of the assessment and determine whether or not to grant a certificate. Figure 6 describes the entire certification process.

The assessment procedures may be divided into the four phases, namely, preparation, assessment, certification, and follow-up assessment. Details of each phase are summarized in Table 4.

Phase	Action	Details
Preparation	Apply and File	- File the application documents and request additional documentation
	Assessment Agreement	- Discuss and notify of the certification assessment plan
Assessment	Documentation Assessment	- Review and confirm submitted documents
	Technical Assessment	- Assess the detailed review methodology and procedures - Conduct a penetration test of the network and systems - Conduct an assessment based on the assessment criteria (checklist) - Analyze, evaluate vulnerability, and assess the results of the risk analysis - Assess related recordings and documentation - Establish and implement protection measures, assessing whether or not they have been implemented - Conduct on-site inspection and hold a meeting with those in charge - Confirm assessment results
	Write Assessment Report	- Write and submit the assessment results report
Certification	Review & Decide (Certification Committee)	- Review and discuss the assessment results at the Certification Committee meeting
	Notification of the Assessment Results	- Notify of the assessment results
	Issue Certificate	- Validity period for certification: three years
Follow-up Management	Follow-up Assessment	- Frequent check-ups of certificate maintenance: once a year
	Reassessment & Re-approval Assessment	In the event of any changes, such as changes to the scope of certification after the initial assessment has been conducted - Certification assessment conducted in order to extend the validity of the certificate prior to expiration (three years)

Table 4: Details of Certification Assessment in Each Phase

2.8 Documentation System of ISMS Certification

The documentation system of ISMS Certification is described in Figure 7. The ISMS policy development guide and ISMS control point guide are currently under development.

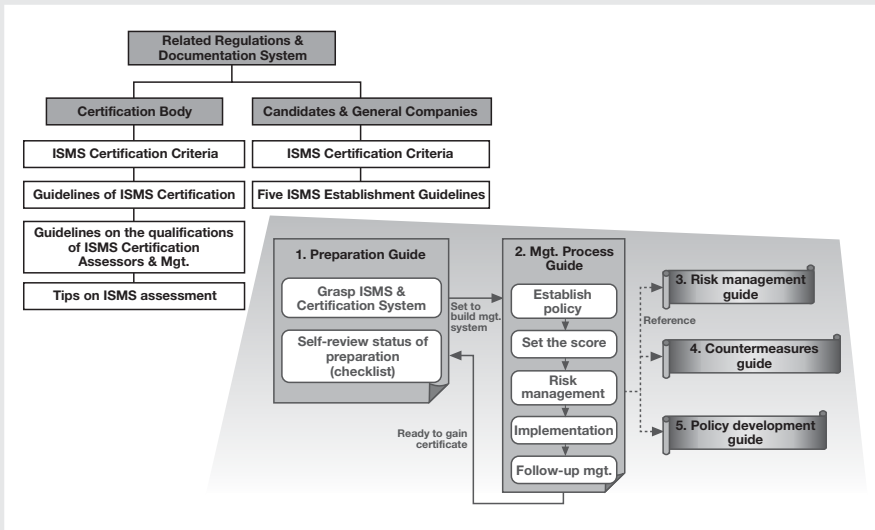


Figure 7: ISMS-Related Guidelines & Documentation System

2.9 Current Status on Certified Organizations

Since the ISMS certification assessment system was first launched in 2002, a total of 28 certificates have been issued. Five additional organizations are currently undergoing the assessment review process. In 2005, 14 organizations are expected to obtain certification. After 2005, the number of KISA-ISMS certificates issued is projected to be higher than the BS 7799-2 certification.

	'01	'02	'03	'04	'05	Total
KISA-ISMS		1	6	18	4(5)	29
BS7799	2	5	11	13	2	33

- Figures in parenthesis () represent the number of companies which are currently under assessment

Table 5: Current Status of Certificates Issued by Year

2.10 Expected Benefits of the ISMS Certification System

In terms of the practical benefits of the ISMS certification scheme, we examine a sample of the companies that have obtained certification since 2002. While each company is different, most of them enjoy the benefits of the ever growing recognition of the importance of information protection and security. Table 6 summarizes the typical benefits that certified companies can expect to enjoy.

Company	Benefits
N(Bank)	Spurred by ISMS Certification, they laid the foundations of an organization dedicated to information security
K(Internet Data Center)	Directors and employees have more positive attitudes towards information security, and the capabilities of the unfolding activities to secure them the information protection they have acquired
K(Telecommunications)	Environment created to enhance the information protection levels and imbed information security procedures in the company
Information Security Consulting Service Provider	Customer confidence in ISMS consulting services improved
H Group (Airline, Transportation)	All steps, from the beginning of ISMS planning, to its completion, have been conducted by its own security provider, resulting in increasing knowledge and expertise in ISMS certification processes and requirements.

Table 6: Benefits of ISMS Certification System Based on Case Studies

3. Trends in ISMS

3.1 Background and Necessity for Building an ISMS

As the security risk in the use of information systems has increased significantly since the 1990s, companies have started paying attention to the methods used to reduce risk by ensuring the continued management of information. More and more organizations have realized that using a technical approach alone cannot ensure information security. This realization has eventually led to the formation of ISMS.

Today, a number of companies are greatly interested in, and pay close attention to the establishment of an information protection and management system. However, simply possessing an information protection and management system does not guarantee that a company ceases to have concerns over the protection of its information security. Without the active participation of the employees and continued maintenance provided by the companies, ISMS is, in effect, nothing more than a set of documents. In addition, even among companies that operate the ISMS effectively, tasks related to risk management, information asset identification, documentation management and change, and history management have actually caused great burden on the staff in charge of ISMS operation. This is why an increasing number of companies are expressing interest in building up and operating an ISMS to overcome the difficulties related to security risk, implementation, and update management of the increasing amount of documented information.

By storing details of all information security protection activities on databases (DBs) and securing automated processes, the staff in charge of information security protection can support the information security activities of those in charge of security and management, guarantee the continuity of the security work undertaken, and maintain the level of security services required. In order to introduce and operate such a system, companies should consider a number of aspects, such as environment, budget, and the impact of introducing such a system, among others. Table 7 illustrates the changes that might be expected as companies introduce an information security protection system.

An installed ISMS based on the ISMS certification framework allows an organization to minimize the efforts required to perform maintenance while maximizing the benefits.

Before ISMS	After ISMS
Difficulty in conducting risk management, e.g. risk analysis and evaluation undertaken using sheets	Consistent risk analysis and evaluation achieved easily, including risk management procedures of the information security protection system
Difficulty conducting continuous maintenance and change management over extended periods of time	Maintenance and change management conducted easily in batches based on DB
Requests for too much documentation creates difficulties in guaranteeing consistent implementation	Due to the system's history management function, documentation required on history (trace) greatly reduced
Difficulty in measuring risk management activities on a regular basis	Real-time measurements easily taken using the monitoring function

Table 7: Benefits of Introducing an ISMS

3.2 Major Functions of ISMS

The main functions of ISMS are the management of risk, change, implementation, and documentation. The risk management function allows a company to choose an appropriate risk management method and build a system to consistently perform all the varying tasks relating to the identification and evaluation of assets, the evaluation of threats and weaknesses, risk evaluation, the assessment of DoA (Degree of Acceptance), the establishment of information protection measures, and plans. The change management function has various documented change management procedures built in so that staff in charge of each function can easily perform and approve the tasks of requesting, handling, and confirming changes. This approach does not generate an omission in the history of changes made and substantially reduces the burden of documentation. The implementation management function streamlines the work process by allowing staff in charge of information protection at each division to check the protection activities and manage the update history of the documentation. The document management function clearly illustrates the policies, guidelines, and procedures that spread across an organization in order to grant those in charge easy access to the information they need. It also enhances the recognition among employees on the importance of information security protection.

3.3 Perspectives

In the future, companies will develop a variety of policies, guidelines, and procedures, as they reinforce their internal controls in an attempt to protect their assets from threats imposed on their information security. For the systematic management of all the activities involved in information security protection, companies should not only implement ISMS, but also endeavor to automate the system. In future, companies will continue to find out the best ways to successfully protect their information, and ISMS will be critical in the process.

4. Future of Korea's ISMS Certification System

4.1 Continuous Upgrade of ISMS Certification Assessment Criteria

IT and infrastructure technology have developed at great speed, one which is beyond our expectation. These features of the rapidly-changing IT industry and its environment in Korea need to be reflected in the ISMS certification assessment criteria. Such a reflection will enable Korean firms to have all the information security protection measures they need. With the development of Internet and e-commerce, the protection of personal information has emerged as a hot issue in today's privacy-conscious society. A number of companies are currently grappling with an increasing amount of Spam email. Therefore, an analysis on whether the ISMS currently in place is capable of effectively handling the issue of Spam email will be carried out. Any shortages found from the analysis will be overcome by the continual revision of the criteria of the ISMS certification assessment.

4.2 Customer-Oriented Support Service for ISMS

Those companies that are exposed to ISMS for the first time often find it difficult to establish and operate the system on their own. There are some companies who have installed and operated ISMS on their own, but the vast majorities seek specialized consultancy services to help them operate ISMS. Those firms that are willing to establish ISMS but find the cost of the consulting services prohibitive may opt to have the system installed on a step-by-step basis, following an on-site technical advice service provided by KISA. In this case, it is the responsibility of the company to initiate the installation of ISMS. The technical advice

given by KISA is very helpful for them to establish the system more effectively. A series of steps will assist companies in installing ISMS to protect their information assets. This, in turn, will enable them to achieve their management goals.

4.3 Ensuring Transparency and Simplifying Certification Procedures

Upon conducting an assessment, the assessors may be able to access to sensitive corporate information. All assessors must sign and submit a confidentiality agreement and code of ethics before their assessment work. This ensures a fair and transparent assessment. On the other hand, the assessors also do their utmost to enhance work efficiency by simplifying the documentation to be submitted for an assessment, and by meeting customer requests, such as deletion of personal information (for example, residential ID number, etc). It is the primary task of the assessment body to assist their customers in establishing the ISMS and acquiring certification.

4.4 Joint Assessment with BSI Korea

Depending on the purpose of the application for a certificate, some companies may try to obtain the British Standards Institute (BSI) BS 7799 certificate and the certificate of KISA ISMS all at once. In this case, the applicant must undergo the processes defined by the two organizations separately that can be quite cumbersome. In order to develop a solution to this issue, KISA has been investigating cooperative avenues with BSI. At this stage, mutual BSI and KISA certification recognition has proven difficult to establish. KISA remains in the process of trying to establish ways to conduct a joint assessment for companies applying for both certificates. Although the details of any joint assessment methodology and approach are yet to be determined, it seems to be emerging as a good opportunity to lay the foundation on which BSI Korea and KISA might build confidence in each other and develop a cooperative approach.

4.5 Training of ISMS Certification Assessors and Improvement of the Certification System

As the ISMS certification system becomes more widely used, the necessity to cultivate more and more specialist assessors is growing. In May 2005, individuals with professional expertise in a variety of areas were recruited by KISA and scheduled to receive education and training. For those eventually chosen as assessors upon completion of the training courses, an appointment letter will be granted and opportunities will be given for them to participate not only in the assessment field, but also in a variety of areas to encourage them to contribute to the further development of the ISMS certification system. Once the certification system is widely adopted by a number of Korean firms, it might become desirable to hand over certifying authority to a private organization. There are, however, a growing number of hurdles to negotiate before such a step is realized: firstly, the ISMS market needs to expand and the fee should be raised to realistic levels. Further study into the certification system needs to be continued in earnest.

Prof Heung-Youl Youm

*Professor, Department of Information Security
Soonchunhyang University, Korea*

Rapporteur, Q.9/SG17, ITU-T

Vice-Chairman, TC1, TTA



Prof Heung-Youl Youm has been working for Soonchunhyang University as a Professor since 1990. Since joining Soonchunhyang University, he has taught thousands of students or technical experts on how the information or network security works, and has published more than 60 technical papers in information security journals or conferences. He is the author or co-author of ten books on information security, including Internet Security Technology, published in 2003 by Sangreung Publishing Company, Korea.

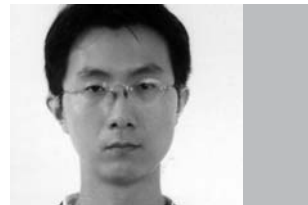
He had worked for ETRI as a senior member of technical staff and had been involved in research and development on various types of transmission systems, including NAS-CEPT conversion system, for telecommunication network, for more than 8 years since 1982.

He has been involved in ITU-T and TTA activities for many years. He is currently a vice-chairman of TC1 of Telecommunication Technology Association, Korea. He also serves as a Rapporteur for Question 9 of SG17, ITU-T.

He has served as a board member or chairman for a number of government-related committees, from the Ministry of Information and Communication, Korea Information Security Agency, and National Information Service. He received his PhD degree of information security from Hanyang university in Korea in 1990.

Mr Kyu-Man, Ko

*Assessor, Information Infrastructure Protection Division
Critical Infrastructure Security Management Team
Korea Information Security Agency, Korea*



Kyu-Man, Ko has been working for the Korea Information Security Agency as a Korea-ISMS Assessor since 2002. He is a Certified Information Systems Auditor (CISA).

He has been involved in research and development on security vulnerability analysis and Public Key Infrastructure (PKI) for three years since 1999. He graduated from Yonsei University with a Masters degree in Computer Science.