



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



CHINESE TAIPEI

ABSTRACT

This paper provides an update on the information security standards development and usage in Chinese Taipei, and also the observations made in recent trend relating to the Cybersecurity threat.

1. Introduction

The development of security related standards is an on-going task in Chinese Taipei to support the validation mechanism of information and communication security, and to satisfy the requirements of interested parties that were established recently based on the framework of national information and communication security standards. In 2005, the Information and Communication Security Technology Center (ICST) drew a roadmap to develop 37 IT security directives and guidelines for government agencies. Currently, 16 guidelines are in the drafting stage. In 2006, ICST plans to publish 12 information and communication security related guidelines.

2. The Development Framework for Information Security Standard

The Bureau of Standards, Metrology, and Inspection (BSMI) has adopted a framework for developing the information and communication security standards. The framework was proposed during the end of 2005 [1], as shown in Figure 1. The framework serves as the development guidance for information security standards up to 2008.

The fundamental standards comprise of three categories:

- Requirements, Security Services and Guidelines;
- Security Technology and Mechanism; and
- Security Evaluation Criteria.

Standards for information system security technology and mechanisms are intended to be used as the basis for evaluation of the security properties of IT products and information systems. Standards for ISMS certification mechanisms are the foundation for auditing and certification. These standards support the full range of business applications, such as Finance and Medicare. In addition, there are other security standards that should be considered for the individual application within the respective knowledge domain.

Application : Finance (CNS 14644, ISO 13491, ...), Medicare (ISO 17090, ...), ...		
ISMS Certification Mechanisms (CNS 27001 ...)		
Requirements, Security Services & Guidelines	Security Technology & Mechanism	Security Evaluation Criteria
1. IT Security Mgmt	1. Identification & Authentication	1. IT Sec Evaluation Criteria
2. IS Mgmt Practices	2. Confidentiality	2. IT Sec Evaluation Method
3. NW Sec Management	3. Integrity	3. IT Sec Assurance Framework
4. Sec. Mgmt Metrics	4. Non-repudiation	4. Operating System Security Assessment
5. IDS	5. Crypto Algorithms	5. Cryptography Module Security Requirements
6. IS Incident Mgmt	6. Auditing & Alarm	6. Bio-Tech Security Evaluation
7. TTP Service Mgmt	7. Public Key Management	7. Sys Sec Engineering
8. IS Object Access Control	8. Biometrics	...
...
IS Technology Certification Mechanisms (eg. CNS 15408, ISO/IEC 19791, ...)		

Figure 1: BSMI Development Framework for Information Security Standards

3. Publication Plan of Standards in 2006

In 2006, Chinese Taipei plans to publish 12 information and communication security related standards supporting the framework as shown in Figure 1. Among them, two most popular and demanded standards are CNS 17799 and CNS 27001, the localized version of ISO/IEC 17799 and ISO/IEC 27001, respectively, which were approved in April 2006. The 12 new standards are as follows:

(A) Requirements, Security Services and Guidelines

- ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management (Completed).
- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems - Requirements (Completed).
- ISO/IEC TR 18044:2004 Information technology -- Security techniques -- Information security incident management.
- ISO/IEC 21827:2002 Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM®).

(B) Security Techniques and Mechanism Related Standards

- ISO/IEC 10118-3:2004 Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions ISO/IEC 10118-3:2004/Amd 1:2006.
- ISO/IEC 11770-1:1996 Information technology -- Security techniques -- Key management -- Part 1: Framework.
- ISO/IEC 13888-1:2004 IT security techniques -- Non-repudiation -- Part 1: General.

(C) Security Evaluation Criteria Related Standards

- ISO/IEC TR 15446:2004 Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets.

4. Standards Drafts in 2006

In 2006, Chinese Taipei plans to also begin drafting 14 information and communication security related standards based on the recently updated ISO/IEC standards in the respective areas of information security. They are:

(A) Requirements, Security Services & Guidelines

- ISO/IEC TR 14516:2002 Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services.
- ISO/IEC 15945:2002 Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures.
- ISO/IEC 15816:2002 Information technology -- Security techniques -- Security information objects for access control.
- ISO/IEC 18028-3:2005 Information technology -- Security techniques -- IT network security -- Part 3: Securing communications between networks using security gateways.
- ISO/IEC 18028-4:2005 Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access.

(B) Security Evaluation Criteria

- ISO/IEC TR 15443-1:2005, Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework.
- ISO/IEC TR 15443-2:2005 Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods.
- ISO/IEC 19790:2006 Information technology - Security techniques - Security requirements for cryptographic modules.

(C) Miscellaneous (Software and System Engineering and Application)

- ISO/IEC 15504-1:2004 Information technology -- Process assessment -- Part 1: Concepts and vocabulary.
- ISO/IEC 15504-2:2003 Information technology -- Process assessment -- Part 2: Performing an assessment (include Cor 1:2004).
- ISO/IEC 15504-3:2004 Information technology -- Process assessment -- Part 3: Guidance on performing an assessment.
- ISO/IEC 15504-4:2004 Information technology -- Process assessment -- Part 4: Guidance on use for process improvement and process capability determination.
- ISO/IEC 15504-5:2004 Information technology -- Process assessment -- Part 5: An exemplar Process Assessment Model.
- ISO 13491-2:2005 Banking -- Secure cryptographic devices (retail) -- Part 2: Security compliance checklists for devices used in financial transactions.

5. IT Security Directives & Guidelines for Government Agencies

The implementation of security standards in government agencies in Chinese Taipei is guided by recent IT Security Directives and Guidelines. The Directive categorizes the different government agencies, based on their criticality [2], into four classes, from A to D. Each category has a minimum level of requirements that is mandated, and additional guidelines that are recommended. Besides requiring the agencies to comply with the related national standards, and considering common security requirements of the government agencies, ICST has also developed a roadmap for the implementation of the 37 IT security directives and guidelines for the government agencies [3]. As shown in Table 1, the roadmap includes a timeline for their implementation. The required security standards are further grouped into five categories, namely: (1) Incident Report and Response; (2) Classification; (3) Evaluation and Implementation; (4) Security Control; and (5) Testing and Certification.

Name of Document		Year to Develop			
		2005	2006	2007	2008
Category: Incident Report & Response					
1	Incident Report & Response Directives	X			
2	Contingency Guidelines		X		
3	System Continuity Guidelines			X	
4	Computer Forensics Guidelines			X	
Category: Classification					
5	Code of Security Responsibility Classification	X			
6	Data & System Classification Guidelines			X	
7	Security Impact Classification Guidelines			X	
Category: Evaluation & Implementation					
8	Information Security Management Audit Directives			X	
9	ISMS Implementation Guidelines			X	

Table 1: IT Security Directives & Guidelines for Government Agencies

Name of Document		Year to Develop			
		2005	2006	2007	2008
Category: Evaluation & Implementation (cont'd)					
10	System Risk Assessment Guidelines		X		
11	IS Audit Evaluation Guidelines				X
12	IS SDLC Security Guidelines			X	
13	Computer Audit Guidelines				X
14	E-Data Protection Guidelines	X			
15	System Interconnect Security Guidelines				X
16	System Outsourcing Guidelines	X			
17	IS Product Selection Guidelines	X			
18	IS Education/Training Guidelines				X
Category: Security Control					
19	Wireless Network Security Guidelines		X		
20	Portable Media Security Guidelines			X	
21	VoIP System Guidelines				X
22	Physical Isolation Guidelines		X		
23	Web Service Security Guidelines			X	
24	E-mail Security Guidelines		X		
25	Firewall Guidelines		X		
26	VPN Guidelines		X		
27	IDS/IPS Guidelines		X		
28	Malicious Code Protection Guidelines			X	
29	Operating System Security Guidelines		X		
30	System Patch Guidelines			X	

Table 1: IT Security Directives & Guidelines for Government Agencies (cont'd from page 17)

Name of Document		Year to Develop			
		2005	2006	2007	2008
Category: Security Control (cont'd)					
31	E-ID Authentication Guidelines		X		
32	PKI Guidelines				X
33	PK Management Guidelines				X
34	Web Application Security Guidelines		X		
Category: Testing & Certification					
35	System Certification & Accreditation Authority Process Guidelines				X
36	Network Security Testing Guidelines				X
37	System Security Testing Guidelines				X
Total number of documents		5	11	11	10

Table 1: IT Security Directives & Guidelines for Government Agencies (cont'd from page 18)

In 2005, the following five documents were approved and published:

- Incident Report & Response Directives.
- Code of Security Responsibility Classification.
- E-Data Protection Guidelines.
- System Outsourcing Guidelines.
- Information Security Product Selection Guidelines.

In 2006, 11 new documents were drafted on schedule, namely:

- Contingency Guidelines.
- System Risk Assessment Guidelines.
- Wireless Network Security Guidelines.
- Physical Isolation Guidelines.
- E-mail Security Guidelines.
- Firewall Guidelines.
- VPN Guidelines.
- IDS/IPS Guidelines.
- Operating System Security Guidelines.
- E-ID Authentication Guidelines.
- Web Application Security Guidelines.

6. Trends Observed in Hacker Intrusion Incidents

Cybersecurity is expanding its substance within the cyber and real economy. Cyber threats escalate its significance in terms of variations and frequency. Efforts to combat cyber threats have been extended with variation in terms of participants involved and activities programmed. In Chinese Taipei, ICST had recently brought together a network of more than 13,000 government officials involved in research, development, evaluation, and commissioning (RDEC) activities in the economy to share and distribute computer emergency alerts and advisory information. ICST had also established a National Security Operation Center (NSOC) and this serves as a key platform in Security Incident Data Exchange (SIDEx) among government Security Operation Centers (SOCs) and commercial managed security services providers.

In the past three years, the operation experience of NSOC, ICST has found that social engineering attack using email combined with Zero-day vulnerability exploit code are most prevalent. This poses a serious threat to the Chinese Taipei government agencies [4] [5] [6]. In general, two major trends have been observed in hacker intrusion incidents:

- 1) More application-level vulnerabilities in particular email, browser, office software, and utility programs such as file compression application (viz., WinRAR), have been exploited by crackers. This trend means that the critical defense line has been pushed backward to end-user (client) machine.
- 2) Targeted social engineering, e.g., forged or counterfeit email account with malicious attachments or hyperlinks, combined with Zero-day attacks have become a serious threat to data protection and privacy. Since social engineering techniques are based on flaws in human logic, known as cognitive biases, and there is no patch or anti-virus signatures for Zero-day attacks, protecting end users from such targeted attacks have become a major challenge for our ubiquitous network society.

7. References

- [1] Kwo-Jean Farn, 'A Study of Development Framework of Information and Communication Security Standards', A Project Acceptance Report, BSMI, October 2005.
- [2] 'Implementation Plan of Practice for Classification of Information Security Responsibility for Government Agency', National Information and Communication Security Task Force (NICST), Taiwan, 20 July 2005.
- [3] 'Roadmap of Information and Communication Security Guidelines', Management Plan of Information and Communication Security Services and Protection, NICST, 2005.
- [4] Microsoft Security Bulletin MS05-036, Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214), 12 July 2005.
- [5] Microsoft Security Bulletin MS06-027, Vulnerability in Microsoft Word Could Allow Remote Code Execution (917336), 13 June 2006.
- [6] Microsoft Security Bulletin MS06-048, Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (922968), 8 August 2006.

Dr Perry Liu

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



Dr Perry Liu is the Director of Information Security Service Center (ISSC) and Project Resource Division in 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 Institute for Information Industry (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.



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



JAPAN

ABSTRACT

This paper presents an update of Information Security Management Systems (ISMS) activities in Japan. Most of the contents are based on inputs from the Japan Information Processing Development Corporation (JIPDEC). The ISMS user's guide for medical organizations is also highlighted.

1. Japan's ISMS Conformity Assessment Scheme

The Conformity Assessment Scheme for Information Security Management Systems (ISMS) in Japan is based on an internationally consistent third party conformity assessment scheme for information security management. This scheme is intended to raise the overall level of information security in Japan and to provide confidence in the level of information security to other countries.

2. International Standardization on ISMS (for information)

International standards for information security management are developed by the Joint Technical Committee ISO/IEC JTC 1 (Information technology) /SC 27 (IT Security techniques). ISO/IEC 17799:2000 - "Code of Practice for Information Security Management" was prepared by the committee and published in year 2000. Soon after its publication, a revision process started and the revised version, ISO/IEC 17799:2005¹, was issued in 2005. To align with the 27000 series of standards, this standard is scheduled to be renumbered as ISO/IEC 27002 in 2007. ISO/IEC 17799:2000 was translated and published as a Japanese national standard, JIS X 5080:2002 in 2002. In May 2006, the revised version, ISO/IEC 17799:2005, was also published as JIS Q 27002:2006. Another international standard, ISO/IEC 27001:2005², was developed based on the British Standard BS 7799-2:2002³ by the same committee

¹ ISO/IEC 17799:2005 - Information technology - Code of practice for information security management is an international standard that provides the code/best practice for implementing an effective ISMS to those responsible for an organization's information security.

² ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements is an international standard that provides requirements for an organization to establish an ISMS.

³ BS 7799-2:2002 - Information security management systems - Specification with Guidance for Use is a British Standard used as the basis for BS 7799 certification.

and issued in October 2005. This standard was also published as a Japanese national standard, JIS Q 27001:2006 in May 2006.

3. ISMS Certification Criteria in Japan (ISO/IEC 27001)

Criteria for certification under the ISMS scheme (hereinafter referred to as ISMS certification criteria) provides a basis for use by third party certification bodies in assessing the conformity of organizations' ISMS that seek to achieve certification under the ISMS scheme. In the ISMS scheme, ISMS certification criteria (Version 0.8) were firstly developed based on both international standards: ISO/IEC 17799 and BS 7799-2. The certification criteria (Version 0.8) were issued in April 2002 for a pilot project of the ISMS scheme. After the pilot project, ISMS certification criteria (Version 1.0) were issued in April 2002 along with the launch of the full-scale operation of the ISMS scheme. The ISMS certification criteria (Version 1.0) were then revised in line with the revision of BS 7799-2 and replaced by ISMS certification criteria (Version 2.0) in April 2003. The criteria (Version 2.0) have subsequently been used as the basis for ISMS certification under the scheme. In October 2005, an international standard that specifies requirements for ISMS, ISO/IEC 27001:2005, was published. This standard was translated and published as a national standard JIS Q 27001:2006. The ISMS certification criteria (Version 2.0) were also replaced with JIS Q 27001 for subsequent certification. Under the transition schedule for ISMS certification, the transition is to be completed by October 2007 (18 months from the publication of JIS Q 27001:2006). Upon which, the existing ISMS certification criteria (Version 2.0) will be retired.

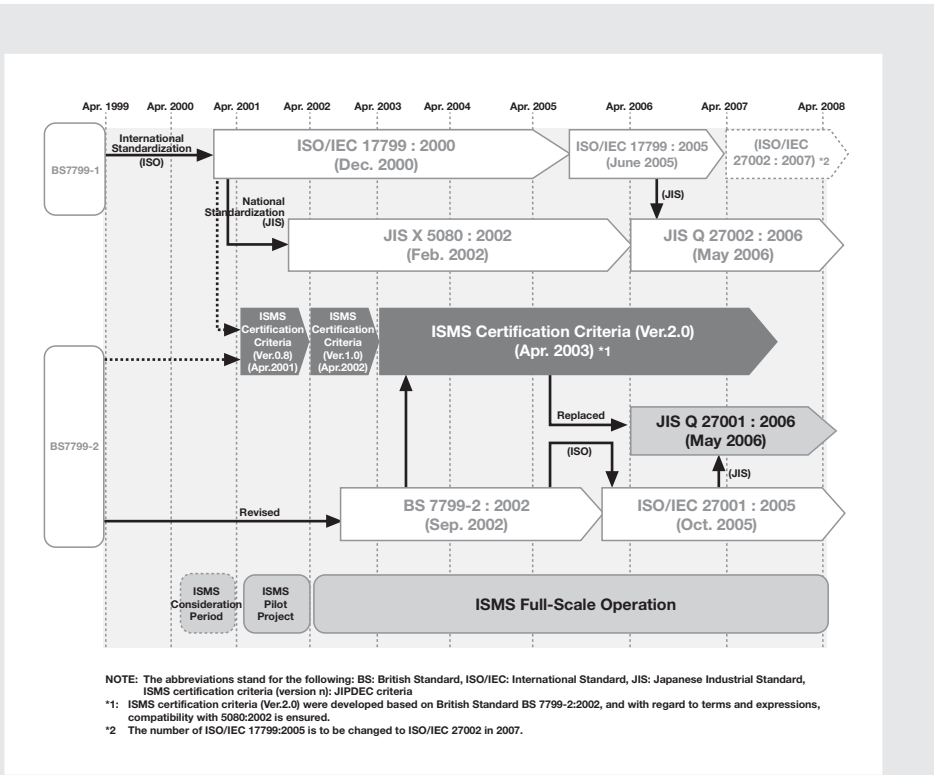
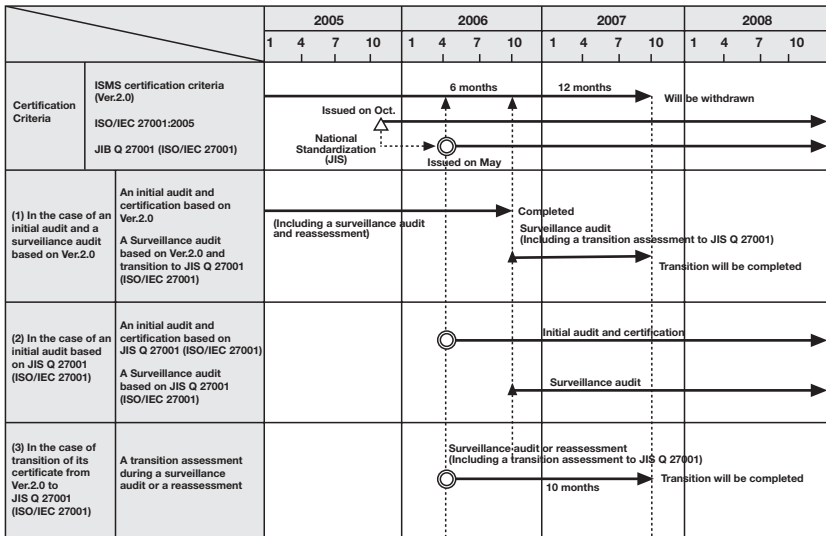


Figure 1: Development of ISO and JIS Standards on ISMS

4. Transition Schedule for JIS Q 27001 Implementation

The transition schedule for ISMS certification was initiated on 20 May 2006, on the publication of JIS Q 27001 (ISO/IEC 27001) for a period of 18 months. Under this schedule, there are three ways for organizations to transit its existing certification, or alternatively, obtain a new certificate based on the new scheme. The transition scheme are: (1) conduct an initial and surveillance audit based on Version 2.0; (2) conduct an initial audit based on JIS Q 27001 (ISO/IEC 27001); and (3) transition of certification based on Version 2.0 to JIS Q 27001 (ISO/IEC 27001).



NOTE: 'Ver.2.0' represents ISMS certification criteria (ver.2.0).

Figure 2: Transition of Certification for Version 2.0 to Certification for ISO/IEC 27001

5. Operation of the ISMS Conformity Assessment Scheme

The ISMS conformity assessment scheme has a comprehensive structure composed of “certification bodies” that assess, certify and register an applicant organization’s ISMS based on ISO/IEC 27001, “auditor training bodies” that conduct training necessary for ISMS auditors, an “auditor certification body” that certifies and registers ISMS auditors, and an “accreditation body” that assesses the competence of those bodies in implementing such tasks. This structure of the ISMS scheme will be changed to ensure conformity with the new standards for the accreditation systems, i.e., ISO/IEC 17011:2004 and ISO/IEC 17024:2003, with, for example, the operation of auditor certification services and the accreditation of auditor training bodies scheduled for transfer to a separate organization/ organizations outside JIPDEC.

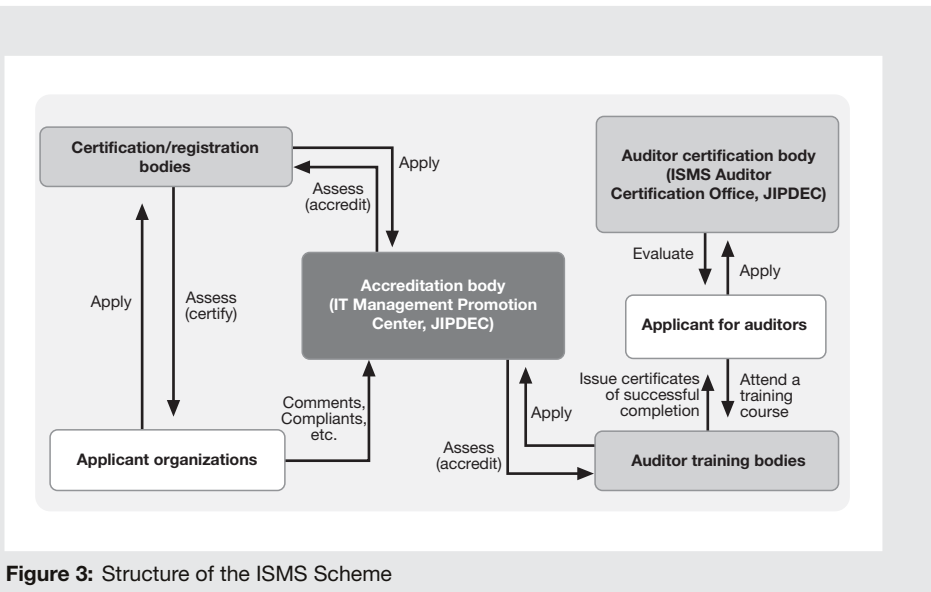


Figure 3: Structure of the ISMS Scheme

The following outlines the functions of each component that comprises the ISMS Conformity Assessment Scheme:

(a) Accreditation body: IT Management Center, Japan Information Processing Development Corporation (JIPDEC)

- Operates, maintains and manages the overall ISMS Conformity Assessment Scheme;
- Accredits certification bodies and conducts periodical surveillances and 3- or 4-year re-assessment;
- Accredits auditor training bodies and conducts periodical surveillances and 3-year re-assessment;

- Provides information on the ISMS Conformity Assessment Scheme; and
- Receives comments and complaints about the ISMS Conformity Assessment Scheme.

(b) Certification bodies

- Achieve accreditation based on Accreditation Criteria for ISMS Certification bodies;
- Carry out assessment and registration of applicant organizations according to the Criteria for the Certification of ISMS; and
- Conduct periodical surveillances and 3-year re-assessment of registered organizations.

(c) Applicant organizations: Organizations seeking ISMS certification under the scheme

- Establish the scope and policy of the ISMS;
- Choose a certification body and make an application to the body;
- Undergo the assessment (Stage 1 and Stage 2) based on ISMS certification criteria and are certified and registered based on the result of the assessment; and
- When registered, are able to use the accreditation symbol on commercial documents.

(d) Auditor training bodies

- Achieve accreditation based on Accreditation Criteria for ISMS Auditor Training Bodies and Criteria for the ISMS Auditor Training Course;
- Carry out training for ISMS auditors; and
- Determine whether a student should be deemed qualified or not based on the student's continual evaluation and the result of a final examination in a comprehensive manner.

(e) Auditor certification body: ISMS Auditor Certification Office, Japan Information Processing Development Corporation (JIPDEC)

- Evaluates and certifies ISMS auditors (provisional auditors, auditors and lead auditors) according to the Qualification Criteria for ISMS Auditors; and
- Conducts re-evaluation of ISMS auditors every three years for their 3-year renewal of ISMS auditor certification.

6. Development of ISMS Guides for the ISMS Scheme

To support the implementation of ISMS, three ISMS User's Guides have been developed by JIPDEC for organizations and specific sectors. They are:

(a) ISMS User Guide (general guide)

This guide provides explanations about requirements of the ISMS certification criteria (Version 2.0) and was produced to help organizations establish their ISMS. It is now being revised based on the latest publication of ISO/IEC 27001.

(b) ISMS User Guide for Medical Organizations

This guide was produced to provide medical organizations with guidance on the establishment of an ISMS in accordance with ISMS certification criteria Version 2.0

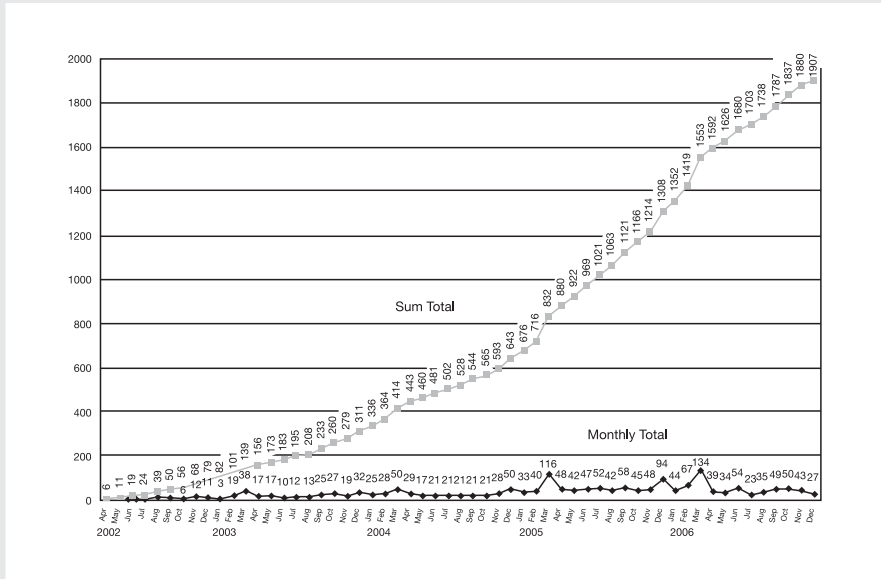


Figure 4: The Number of Certified ISMS Organizations (as of 27 December 2006)

(published in November 2004) and is referred to the “Japanese Industrial Standards (JIS) Information Technology - Code of practice for information security management” JIS X 5080:2002 (ISO/IEC 17799) as best practices.

This guide is based on the Plan-Do-Check-Act (PDCA) model to ensure that there is a continuous improvement process and therefore, a system for managing information security has been established and is being maintained. This further describes the relationships between risk assessment processes, selected controls, and a Statement of Applicability (SoA). This also contains a reference document in ISO 27799 (Health informatics -- Security management in health using ISO/IEC 17799).

An English version of this guide is available for reference at <http://www.isms.jipdec.jp/doc/JIP-ISMS114-10E.pdf>

(c) ISMS User Guides for the Credit Industry

This guide is currently under development with the support of the government and leading credit card companies. It is aimed to be compatible with both ISO/IEC 27001 and some industry standards developed by international payment brands. The publication of this guide is to encourage adoption of ISMS standards in the Credit Industry.

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 WG 1/SC 27 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 1st 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.