



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CAMBODIA CHINESE TAIPEI JAPAN MALAYSIA SINGAPORE SOUTH KOREA THAILAND



AUSTRALIA

ABSTRACT

This paper describes the standardization priorities in Australia concerning information security in 2005. The main focus of Australian committee is the ISO/IEC 27000 series of standards concerning information security management. Standards Australia's management mechanisms ensure liaison between this and the related work on sector-specific information security standards and risk management standards. An early priority for 2006 will be the revision of the Australian Handbook 171 concerning IT evidence collection and converting it to the status of a standard.

1. Introduction

Australian information security standardization¹ continues to be managed in three parts:

- generally applicable information and IT security standards;
- application-specific IT security standards; and
- risk management standards.

2. Application Specific IT Security Standards

Generally applicable information security standards are the main topic of this paper. However, there is important work done on sector-specific security standards in the areas of banking, telecommunications, health and transport ticketing and tolling. These standards, where possible, use security mechanisms based on the work of ISO/IEC JTC 1/SC 27.

3. Risk Management Standards

Australia has a very active committee developing standards and guidelines for risk management. The Information Standardization Committee liaises closely with the Risk Management Committee to ensure that the risk management concepts used within SC 27's information security risk management projects align with risk management concepts used in other domains. As a result of this work, Standards Australia has developed and published an Information Security Risk Management Guideline (HB 231). It is expected that

¹ Australia does have separate standards work in the area of physical security and crowd control, but these are outside the scope of this paper.

ISO/IEC 27005 (Information Security Risk Management) will supersede this guideline when that project is completed. Standards Australia is actively working on the ISO/IEC 27005 project so that this transition can take place as soon as possible.

4. Generally Applicable Information and IT Security Standards

Standards Australia's Sub-committee IT/12/4 is the mirror committee that tracks and contributes to the projects of ISO/IEC SC 27. Most effort is devoted to working on ISO/IEC projects because most information security problems are essentially the same world-wide, and there is little point in developing specific national standards to respond to them.

4.1 Information Security Management Standards (ISMS)

The most active work area is the standards concerning the management of information security and the ISO/IEC 2700x series of standards. The most widely used information security standards are ISO/IEC 27001 and ISO/IEC 17799 ISMS standards. Considerable effort continues to be devoted to informing the public, through presentations in industry seminars, of the best ways to use these standards. This is essential because there is a risk that some organizations will focus on compliance at the expense of ensuring the use of these standards demonstrably supports the key business objectives of organizations. The Australian Standard on Information Security Management System Requirements, AS/NZS 7799-2, is also being progressively withdrawn and replaced by ISO/IEC 27001. AS/NZS 7799-2 will be changed to 'withdrawn but available' status so that it remains available for organizations pending transition of their ISMS to the ISO/IEC 27001 standard.

Related to ISMS, considerable standardization committee's time has been devoted to information security measurements and contributions to the ISO/IEC 27004 (Information security management metrics and measurement) project. The committee is most concerned that any metrics standard does not drive inappropriate management behavior by focusing on measurement values for their own stake. The measurement standard must encourage the use of measurements to provide an objective indication of how effective an information security programme supports an organization's business.

4.2 Mutual Recognition of ISO/IEC 27001 Certification

The Australian industry reports that their use of the national ISMS standard (AS/NZS 7799-2) is limited because they need international recognition of their information security programmes. The publication of ISO/IEC 27001 to replace AS/NZS 7799-2 was a major step in meeting this need. A second requirement is for mutual recognition of the ISMS certifications performed by different certification bodies internationally. Standards Australia is therefore participating in international initiatives lead by ISO Committee on Conformity Assessment (CASCO) and the International Accreditation Forum (IAF) to develop an internationally recognised protocol for accredited certification. There may be benefits if mutual certificate recognition in the updated certification regime is staged and initially implemented at a regional level.

4.3 Security Standards Toolkit

Australian industry users of ISO/IEC information security standards are confused about which of the myriad of ISO/IEC information security standards are relevant in particular circumstances. Standards Australia would be interested in working with other RAISS Forum members to develop a toolkit that could help users find the right standard or set of standards to meet their needs. As a starting point, the structure in the SC 27/WG 1 roadmap could be used, but this would need to be extended to cover the standards developed by SC 27/WG2 and WG 3. The initial focus could be information security management for all types of organization taking the following as the standards core.

- ISO/IEC 13335 - Risk management
- ISO/IEC 17799 - Code of practice
- ISO/IEC 27001 - Management system
- ISO/IEC 18028 - Network security
- ISO/IEC 18043 - Intrusion detection
- ISO/IEC 18044 - Incident management

Later mechanism standards and assurance standards could be added, along with industry sector-specific standards.

5. Biometrics Based Identity Management

Similar to many other economies, Australia has a high interest in biometric standards that can be used as part of identity management solutions for high criticality government applications, passports, and the protection of critical infrastructure. Accordingly, Australia is very interested in the work of the proposed new biometrics and identity management working group in SC 27 as well as the work of ISO/IEC JTC 1/SC 37.

Initially, the Australian government is taking the lead to identify national and regional initiatives requiring biometric authentication. Although there are currently no identified requirements for regional standards to support Asian identity management initiatives, Standards Australia is interested to work in this area when such needs arise, and has experts available to do the necessary work.

6. IT Evidence Collection

In 2003, Standards Australia developed HB 171 which contains guidelines for the collection of IT evidence. This was developed to support enforcement of Australian civil and criminal laws by helping IT personnel ensure that the evidence they collect is suitable for use in Australian courts and has the maximum possible 'weight' or credibility.

Based on experience with the use of these guidelines, a revision is currently in preparation that will update requirements and elevate this document to the status of a national standard. Standards Australia is able to share its experiences in the use of HB 171 with other Asian standards bodies, and if there is interest, to cooperate to develop an ISO/IEC standard based on Australian experience.

7. The Business Case for Industry Funding of Standards Development

Although there is wide use of Australian, ISO and IEC standards in Australia, and associated recognition of the benefits of their use brings to the government and business, it is sometimes difficult to find experts who are available to work on new standardization projects. This problem is especially acute in standardization areas like information security, where the standards are important across the economy as a whole, but are not associated with the

core business of most of the users of the standards. We expect that this will be a problem elsewhere in Asia. Whilst it is common for national standardization programmes to be initiated and initially funded by the governments, as the discipline matures, an industry funding model is often necessary. This is the case in Australia.

Standards Australia and its committee members are continually challenged by a need to develop a business case for industry funding of the experts that need to be involved in standards setting. It is our experience that a good basis for the business case for involvement in information security standardization is based on the observation that is rare for companies to compete on the basis of the information security levels they achieve. That being the case, everyone wins if many organizations contribute a little so that all can benefit from the aggregate outcome of these contributions. This business benefit can be magnified when it is acknowledged that participation with expert peer professionals in the standards development process can be a low cost and high value part of the professional development and skill maintenance of the people involved.

This business value may be similar in other Asian economies. It is recommended that a business case for participation in standards development based on these principles be used where necessary in both developed and developing economies.

8. Conclusion

Australia has a long established standardization regime. However, as the nature of the economy is changing, there is a need to change the approach and priorities associated with setting standards.

In the area of information security, current high priorities are

- 1) the management of information security;
- 2) biometrics; and
- 3) IT evidence collection.

Standards Australia has recently completed a major organisational overhaul and review of its processes and priorities. This experience can be shared with other RAISS Forum members wishing to set up or review their national standardisation programme.

Mr John Snare

*Senior Consultant
Fujitsu Australia*

*Chairman, Committee IT/12/4 - Information Security Techniques
Standards Australia*



Mr John Snare is a Senior Consultant with Fujitsu Consulting and has worked in the area of information security risk management for 18 years. He has held senior executive positions with accountabilities for information security management and has extensive experience in the development and implementation of business-aligned strategies for the management of information security risks.

John's professional focus is on the effective management of information security and information security management systems. John has been Chairman of the Committee IT/12/4 - Information Security Techniques of Standards Australia, responsible for information security standards for the last 15 years. He was the Co-Editor of ISO/IEC 27001 for information security management systems. John has been closely involved in both the development and application of the ISO/IEC 17799 and AS/NZS (BS) 7799.2 standards concerning the management of information security since their inception. In the past, he has led research teams on projects concerning encryption algorithms and key management, and was a member of the team that developed the original ITU X.509 standard. More recently, his interests have been focused on broader security management issues.

Prior to joining Fujitsu, John has worked for Telstra and Adacel Technologies, managing and leading teams of developers and integrators of directory and security products, establishing information security policies and standards, and managing implementation of security and identity management infrastructure.



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CAMBODIA CHINESE TAIPEI JAPAN MALAYSIA SINGAPORE SOUTH KOREA THAILAND



JAPAN

ABSTRACT

This paper presents an update on the progress of various key activities on Information Security and related Technologies implementation in Japan. We discuss three major topics:

- 1) Current Status of Information Security Management System (ISMS) in Japan;
- 2) Botnets Research in Telecom-Information Sharing and Analysis Centre (Telecom-ISAC) Japan; and
- 3) Information Security Policy in the Government of Japan.

1. Current Status of ISMS in Japan

In the inaugural RAISS Forum meeting [1], we presented the Japan's Comprehensive Strategy for Information Security, and the Information Security Management System (ISMS) that was introduced as part of the Conformity Assessment Scheme to improve IT Security Governance in organizations. Since then, as shown in Figure 1, the number of certified organizations has increased (from 625 in January 2005) to 1,141 on 4 November 2005. (Afternoon: As of 6 February 2006, this has further escalated to 1,321.)

The Conformity Assessment Scheme is continuing through 2006, and additional activities are now being developed to further improve and facilitate the implementation of ISMS in Japan. This includes developing methodologies for the measurement of ISMS effectiveness, and a guideline on information security management for telecommunications. More details pertaining to these activities will be reported in the next meeting.

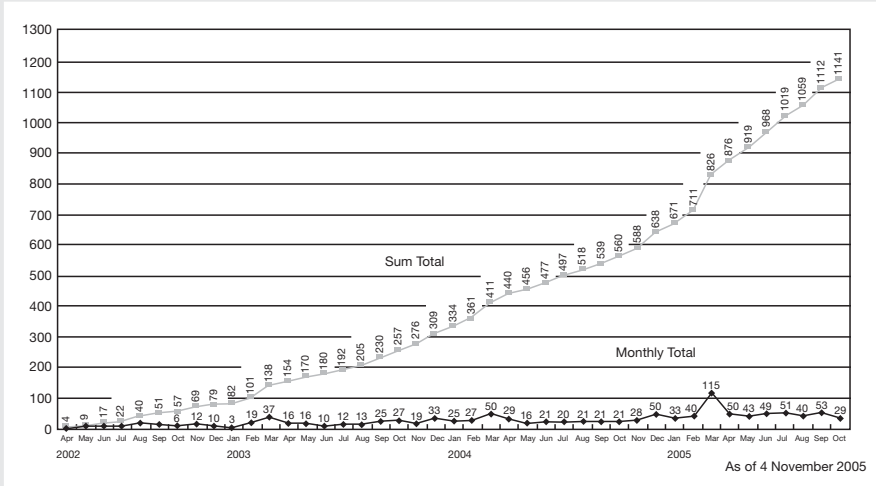


Figure 1: Updated Number of ISMS Certified Organizations in Japan

2. Botnets Research in Telecom-ISAC Japan

In the 2nd RAISS Forum meeting [2], we also discussed about information sharing and analysis for telecommunications (Telecom-ISAC), in particular, for Internet Service Providers (ISPs), that was operational in Japan since 2002. One of its current activities involves the observation and investigation of Botnets¹ activities in Japan. Telecom-Information Sharing and Analysis Centre (Telecom-ISAC) Japan has implemented the following three actions as shown in Figure 2 to deal with the Botnet challenges in Japan:

- Monitoring and observing for Botnets;
- Research Bots behaviors using Honey Pot systems; and
- Conduct analysis of ISPs traffics.

First, ISAC monitors the network to observe for Bots behavior from infected PC as indicated in A in Figure 2. Such Bots behaviors were recorded by the PCs located at network edges.

¹ Botnets refer to networks of Bots (short for Robots, also known as Zombies), which are Trojan programs that can be controlled remotely by the Bot Controller (usually an Internet Chat Relay (IRC) server), to conduct fraudulent or cyber-criminal activities on the Internet, including, but not limited to, software piracy, distributed denial of service attack for extortion, spamming, and identity theft.

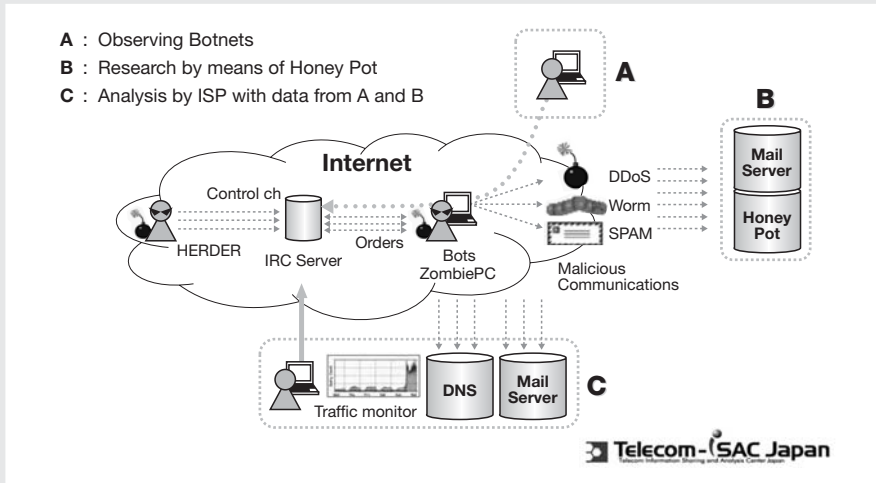


Figure 2: Botnets Research in Telecom-ISAC Japan

The second activity was to capture the Bots behaviors at the Mail Servers and Honey Pots systems. These systems were also located at the network edges. The third was to monitor the traffic exchanged on the Internet focusing on DNS and IRC traffics. These activities were carried out in collaboration with major ISPs in Japan.

A detailed record of the activities and findings of the analysis would not be appropriate for this report. The following provides a summary of the results obtained:

- 1) Rate of infection by the Bots is estimated at between 2 and 2.5 percents in Japan;
- 2) According to our experiments, it took about four minutes for an unprotected PC to be attacked and infected by the Bots; and
- 3) More than 7,000 Bots objects were captured and analyzed, which identified about 80 unique types of Bots.

The results showed that the perpetuation of cyber-criminal activities using Bots and Botnets are increasing, and the importance of ensuring all computer systems are adequately updated and protected to prevent being attacked and infected by Bots and other malicious software on the Internet.

These analysis activities are continuously being carried out by Telecom-ISAC Japan to keep up to date with the latest Bots behavior on the Internet.

3. Information Security Policy in the Government of Japan

3.1 Overview of the National Information Security Center (NISC)

As part of Japan's National Strategy for Information Security, the National Information Security Center (NISC) was established on 25 April 2005 by the IT Strategy Headquarters. Together with this development, the Information Security Policy Council (ISPC) has also become part of the IT Strategy Headquarters since 30 May 2005 .

One of the NISC's objectives is to be the central entity in Japan specializing in research and developing policies, strategy, and measures to address information security issues. The NISC currently consists of both government officials from related ministries and agencies, and experts from the private sectors. The structure of government organizations in relation to information security policy is illustrated in Figure 3.

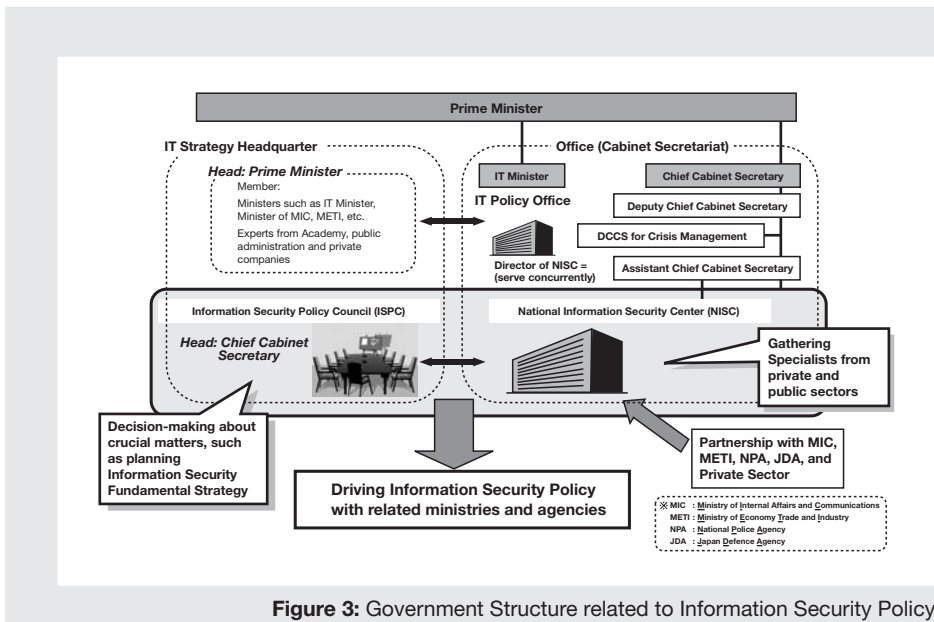


Figure 3: Government Structure related to Information Security Policy

The following five crucial functions were assigned to NISC:

- 1) Development of Fundamental Strategy
Establishment of a 3-year plan (middle-long term plan). The plan shall be comprehensive and include R&D and technical strategy. Moreover, the key issues and challenges relating to information security should be identified in each ministry, and addressed in the formulation of the strategy.
- 2) Comprehensive Measures for Government Bodies
A government-wide framework for information security measures shall be specified and the framework should be appropriately evaluated.
- 3) Development of Response Capability
Functions of information collection relating to security incidents shall be strengthened in cooperation with the related organizations such as Incident Response Team (IRT) and ISAC.
- 4) Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP)
In case of cyber-terrorism aimed at critical infrastructures, potential impact analysis among critical infrastructures shall be investigated. In addition, security counter-measures applicable to any critical infrastructures shall be identified and specified.
- 5) International Strategy
International strategy of Japan for information security shall be planned to strengthen the relationship with foreign organizations.

The next sub-section elaborates the five functions of NISC.

3.2 Information Security Policy in Japan

(a) Development of Fundamental Strategy

The first Information Security Fundamental Plan shall be tentatively provided by the end of 2005. In the course of its provision, the following three special committees have been established to pursue the issues to be addressed.

- Security Culture Special Committee (for fostering a culture of security)
- R&D Special Committee (for investigating R&D technical measures in information security)
- CIIP Special Committee (for studying specific security measures to protect critical infrastructures)

Figure 4 depicts the roles of the above three special committees.

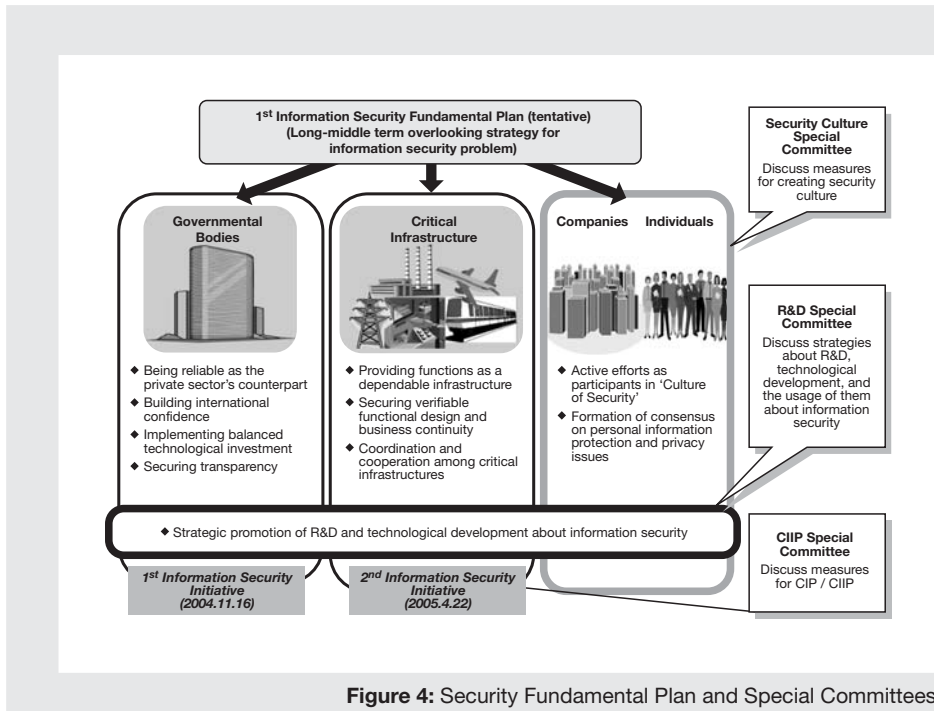


Figure 4: Security Fundamental Plan and Special Committees

(b) Comprehensive Measures for Governmental Bodies

The following new documents have been issued in September 2005 to provide comprehensive measures especially for Japanese governmental bodies.

- i) **Governmental Information Security Principles** to strengthen information security measures.
- ii) **Framework for operating Government-wide Information Security Measures (GISM)**, to guide the planning and implementation of information security measures for governmental purposes, based on the management process of the ISMS Plan-Do-Check-Act (PDCA) cycle of continuous improvements.
- iii) **Government-wide Information Security Measures (GISM)**, specifying government-wide standard for information security measures.

(c) Development of Response Capability

In order to provide incident response capability, National Incident Response Team (NIRT) was established in April 2002. The members of NIRT have expanded to include many network security experts from both public and private sectors. Responsibility of NIRT is to respond to incidents occurred at e-Government networks and Critical Infrastructures. The action flows between Cabinet Secretariat including NIRT and Liaison Officers (Ministries, etc) is shown in Figure 5.

(d) Critical Infrastructure Protection (CIP)/ Critical Information Infrastructure Protection (CIIP)

In October 2001, a “Government-Private Sector Partnership” plan was established in a governmental IT security experts meeting for the purpose of protecting Critical Infrastructures. In order to improve this partnership, as a framework, three new sectors are now added to the list of Critical Infrastructures. They are, freight, water work, and medical services. Specific issues to be addressed are discussed at the CIIP special committee. The relationship between critical infrastructures in the public sectors and the government are illustrated in Figure 6.

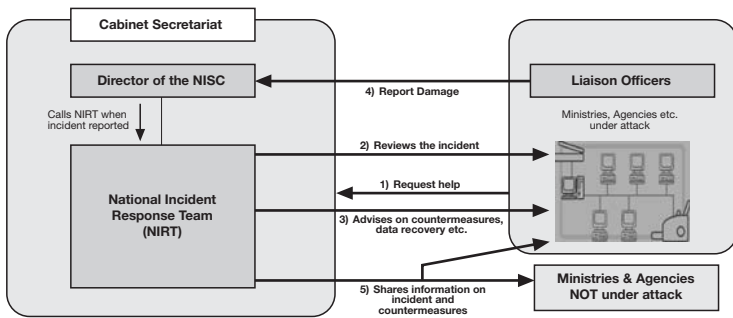


Figure 5: Response Capability

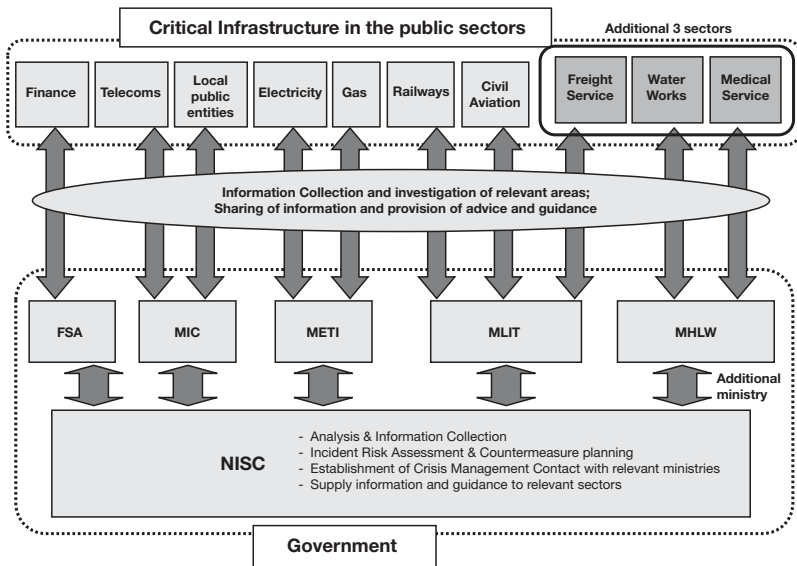


Figure 6: CIP/CIIP

(e) International Strategy

The government of Japan is communicating with other countries and economies to promote fruitful relationship with information security agencies located abroad. For this purpose, the point of contact shall be identified for each country/economy.

4. Next Step - Future Challenges

Looking forward, NISC has identified the following directions and plans as the next stage of development to enhance Japan's information security readiness.

- 1) Encourage information security literacy and enhance security level in every organization and at grassroots level;
- 2) Promote international cooperation and collaboration for information security; and
- 3) Develop human and technological resources to support information security needs.

The above Information Security Policy will be updated half annually.

5. References

- [1] Nakao, K., Information Security Technologies in Japan, in Inaugural Regional Asia Information Security Standards (RAISS) Forum Meeting, (Tokyo, Japan, 2004), 44-53.
- [2] Nakao, K., Introduction and Updates on Information Security Technologies Related Activities in Japan, in 2nd Regional Asia Information Security Standards (RAISS) Forum Meeting, (Singapore, 2005), 17-27.

Mr Koji Nakao

Co-Chair, RAISS Forum, Japan

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

*Director, Department of Information Security Technology,
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 Chair (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.



Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CAMBODIA CHINESE TAIPEI JAPAN MALAYSIA SINGAPORE SOUTH KOREA THAILAND



MALAYSIA

ABSTRACT

This paper is an extension of the paper “Updates on Information Security Standards Activities in Malaysia” published in Volume 2 of the RAISS Forum Proceedings [1]. This paper provides further updates and highlights of the information security standards development in Malaysia, including Malaysia's participations in the 31st ISO/IEC JTC 1/SC 27 Working Groups meetings and 3rd RAISS Forum meeting that was hosted in Malaysia and also the information security standards activities planned for 2006.

1. Objectives

The objective of this paper is to highlight Malaysia's activities in information security standards development since the last update published in Volume 2 of the RAISS Forum Proceedings.

2. Activities Update on Standards Development

Due to resource limitation and constraint, Malaysia is not able to develop a full suite of information security standards to meet its local need. Hence, Malaysia participates actively in international standardization activities with special focus on the work and projects of ISO/IEC JTC 1/SC 27 Working Group 1 (WG 1). The focus of local standard development is currently on Business Continuity Management, and constant reviews on international standards are carried out to determine its relevance for adoption. Presently, some of the standards that have been distributed for public comment prior to the adoption process are:

- a) ISO/IEC 27001 on Information technology -- Security techniques -- Information security management systems -- Requirements
- b) ISO/IEC 18028 on Information technology -- Security techniques -- IT network security

3. Malaysia's Participation in 31st ISO/IEC JTC 1/SC 27 Working Group Meeting on Information Security and the 3rd RAISS Forum Meeting

Malaysia continues to be a participant in international standards development activities through participation in ISO/IEC meeting and the RAISS Forum meeting. Malaysia hosted

the 31st ISO/IEC JTC 1/SC 27 Working Groups meeting on Information Security that was held at the Regent Hotel, Kuala Lumpur from 7 through 11 November 2005. Malaysia sent the largest delegation to the meeting with over 30 delegates and observers, comprising representatives from members of TC5, WG 1, WG 2 and WG 3. The majority of delegates participated in WG 1 meetings. The rationale in allowing such a large delegation to participate in the meetings is to create interest and encourage larger and more consistent participation of future TC 5 and WGs meetings.

Two events were also held in conjunction with the meeting namely, the hosting of the RAISS Forum Meeting and organizing the Awareness Seminar on Information Security Standards.

A half day 3rd RAISS Forum Meeting was held on 12 November 2005. It had good participation from regional economies including Australia, Cambodia, Japan, Malaysia, New Zealand (observer), Singapore and South Korea, and representatives from SC 27 WG 1 to address regional interests. Discussions were held on the proposed projects which were brought up during the 2nd RAISS Forum Meeting. Even though it was only a half day meeting, many agenda objectives were achieved.

The Information Security Standard Awareness Seminar was organized in the morning, of 12 November 2005, and it was well attended by local and international participants from the government agencies, local authorities, financial institutions, telecommunication companies, application service providers, academic sectors and other ICT service providers. The objectives of the seminar were:

- To get latest updates from international experts regarding standards development activities on Information Security.
- To disseminate information on information security standards development in Malaysia.
- To create awareness on the importance of international standards development, particularly in information security.
- To promote and encourage active participation from private and public sectors in information security standards development activities.
- To share the experience of other countries on Information System Management System (ISMS) implementation.

ISO/IEC JTC 1/SC 27 Chairman and Conveners from WG 1, WG 2 and WG 3 delivered talks on their respective areas during the Awareness Seminar.

All events were funded by the Department of Standards Malaysia (DSM) and organized by SIRIM Berhad with TC5 as the advisor. All the events went well and the large presence of Malaysian delegates to the 31st ISO/IEC JTC 1/SC 27 WGs Meetings and the RAISS Forum Meeting indicated keen interest from the industry and provided an opportunity for the delegates to participate actively in the information security standards activities.

4. Activities Planned for 2006

Information security standards development activities are continuously evolving in Malaysia. There are some activities planned for year 2006 that includes reviews of international standards and organizing an awareness seminar on information security standards for the general public. A few public workshops are also planned to be organized to attract the industry players for recruitment as new experts to participate in the technical WGs.

There are a number of standards that Malaysia is interested to participate but have to prioritize its limited resources. Focus is therefore on ISO/IEC 27000 series of standards especially ISMS Implementation Guidance, Information Security Management Measurement, ICT Disaster Recovery Services, and ICT Security Evaluation.

5. Conclusion

Malaysia is very keen to continue its involvement in information security standards development both locally and internationally. Participation in the international standards meetings and forums are benefiting the development activities tremendously.

6. References

- [1] Abdul Jalil, S., Updates on Information Security Standards Activities in Malaysia, in 2nd Regional Asia Information Security Standards (RAISS) Forum Meeting, (Singapore, 2005), 46-49.

Ms Rafidah Abdul Hamid

Policy Analyst
National ICT Security and Emergency Response Centre (NISER)



Rafidah Abdul Hamid is a Policy Analyst with the National ICT Security and Emergency Response Centre (NISER). In her appointment, Rafidah has been actively involved in various information security projects including training, auditing and consultancy. Her domain of expertise includes Information Security Management System (ISMS), Information Security Standards and Security Policies. Prior to joining NISER, Rafidah was a Lecturer and an Analyst Programmer.

Rafidah holds a BIT (Hons.) and MSc (IT) degree from Universiti Utara Malaysia. She is a certified BS 7799 Lead Auditor and also holds GIAC Security Essential Certification (GSEC) from the SANS Institute.