



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA   CAMBODIA   CHINESE TAIPEI   JAPAN   MALAYSIA   SINGAPORE   SOUTH KOREA   THAILAND



# SINGAPORE

## ABSTRACT

This paper presents updates on the development of a new standard “Guidelines for Information and Communications Technology (ICT) Disaster Recovery (DR) Services”, under the ISO/IEC Joint Technical Committee 1 (JTC 1) Sub-Committee 27 (SC 27) Working Group 1 (WG 1). This new standard was originally proposed by Singapore to WG 1 in April 2005 and is based on a published Singapore Standard.

## 1. Introduction

In 2004, Singapore developed and published Singapore Standard SS507 - “Singapore Standard for Business Continuity/Disaster Recovery (BC/DR) Service Providers”<sup>1</sup>. It has since been adopted widely within the country as a specification for the certification of business continuity/disaster recovery (BC/DR) service providers.

In order to benefit service providers offering similar services in other countries, the Singapore standard must be further developed into an international standard. To this end, at the 30th ISO/IEC JTC 1/SC 27/WG 1 Meeting held in April 2005 in Vienna, Austria, Singapore presented the standard as a new work item, proposing it to be used as a base document for further development into an international standard under ISO.

With the official ballot approved in August 2005, it marked the birth of the project ISO/IEC 24762 “Guidelines for Information and Communications Technology (ICT) Disaster Recovery (DR) Services” to be developed in WG 1. Mr Philip Sy of Singapore, was subsequently appointed as the Project Editor for this project. Mr Sy is also concurrently the Co-Chair of the Information Security Management (ISM) Working Group under the Security and Privacy Standards Technical Committee (SPSTC) in Singapore.

<sup>1</sup> Singapore Standard SS507 was described in Volume 2 of the RAISS Forum Proceedings.

In the course of the ballot, a number of comments were received from the National Bodies<sup>2</sup> (NBs), while one National Body contributed a reference document for consideration. These comments and contribution were discussed amongst representatives from the NBs at the 31st ISO/IEC JTC 1/SC 27/WG 1 Meeting in Kuala Lumpur, Malaysia, in November 2005. A summary of the discussion is presented in this document.

## **2. Updates from WG 1 Meeting**

### **2.1 Meeting with Subject Matter Experts**

The JTC 1/SC 27 Working Groups meetings were held at the Regent Hotel in Kuala Lumpur, Malaysia from 7 to 11 November 2005. The discussion session for project ISO/IEC 24762 was held on the third day of the meetings, i.e. 10 November 2005. The discussion was attended by a total of 22 subject matter experts from Canada, Japan, Malaysia, Poland, Singapore, South Korea, Spain and Switzerland.

The discussion group deliberated the following agenda:

- ISMS family standards - Can the ICT DR standard fit into and therefore benefit from being a member of the ISMS series of standards?
- Standard scope - Besides DR services, what other aspects of business continuity management should the new standard cover?
- Review of comments on draft as well as one contribution from the NBs.

### **2.2 ISMS Family Standards**

The ISO/IEC 27000 series of standards refers to the ten consecutive ISO numbers 27000 to 27009. These numbers have been explicitly reserved for the Information Security Management System (ISMS) standards. A number of these standards are already well-known with some on the way to being published, while the rest will only have their numbers finalized later.

<sup>2</sup> National Bodies refer to the member countries participating in ISO.

To date, only ISO/IEC 27001 Specification for ISMS - Requirements (this standard was previously known as the BS 7799 Part 2 standard under the British Standard Institute) has been published, while 27002 has been reserved for the renumbering of the existing ISO/IEC 17799 Code of practice for information security standard after April 2007. Several other ISMS standards have also been identified<sup>3</sup>.

In order to address concerns over how standards would be selected to be part of the ISMS series, WG 1 developed and published a set of criteria for assessing which types of standards and guidelines qualify to be included in the ISMS series. Each standard within the ISMS series must meet all the following criteria:

- Provide direct support and give detailed guidance for the implementation of the Plan-Do-Check-Act (PDCA) processes defined in ISO/IEC 27001, e.g.
  - Defining ISMS scope
  - Risk assessment
  - Identification of assets
  - Effectiveness of information security;
- Contribute and add value to ISO/IEC 27001 PDCA processes; and
- Specify its relationship to ISO/IEC 27001 and what guidance support it provides.

This set of criteria also excludes standards that only address the implementation of security controls. Based on the above guidelines, the ICT DR standard would not qualify as an ISMS standard because it only addresses the implementation aspects of the business continuity management process and does not provide direct guidance support for the implementation of the ISO/IEC 27001 PDCA processes.

This was a sentiment echoed by the discussion group who unanimously agreed to keep it outside the ISMS numbering scheme. However, there was consensus that there were still

<sup>3</sup> For more information on the other ISO/IEC 27000 series of standards, please refer to Mr Ted Humphreys' paper on page 66 in the Proceedings.

advantages to keep the DR standard number close to the 27000 series, e.g. 2701x if the number is still unallocated. This recommendation was presented to WG 1 where it was clarified that, except for the reserved 27000-27009 ISMS standards, the allocation of ISO numbering to ISO documents was purely a random process, so the number once allocated would not be changed.

### **2.3 Standard Scope**

In the course of the new work item ballot, there were several comments from various NBs on whether the standard needs to be more broad-based to include, in addition to disaster recovery services, all elements of business continuity management, such as business continuity planning and services.

There is a distinction between disaster recovery and business continuity. In general, disaster recovery is concerned about the capability for technology recovery during a crisis, while business continuity is concerned about sustaining the business and its operations during a crisis.

As such, the discussion group took the opportunity to review the scope of the ICT DR standard. The following conclusions were drawn at the end of the session:

- The standard would retain its focus on technology disaster recovery and would not include other areas of the business continuity management. These areas would be addressed by other existing standards and best practices. Nonetheless, in order to maintain its relevance to ISO/IEC 27001 and ISO/IEC 17799 (in time to come to be ISO/IEC 27002), the standard would still mention how disaster recovery fits into the overall business continuity management.
- In general, the standard would apply to the provision of both in-house as well as outsourced ICT DR services. This is to ensure that the standard is applicable to organizations that wish to develop, establish and maintain their own ICT DR capability. If there were any areas in the standard which would apply differently, clear distinction would be made in the document to indicate and distinguish between the two.

## 2.4 NB Comments and Contributions

The discussion group further reviewed all the comments from the NBs that were received at the end of the August 2005 new work item ballot. 26 comments were consolidated during the ballot and they came from Brazil, Japan, Netherlands and UK. The feedback also included comments on the scope of the standard as discussed in the previous section.

Although it was a laborious and time-consuming exercise, the review process had to be carried out in order to address all the concerns from the NBs. In cases where the comments were not clear enough and representatives from the concerned NBs were not present to elaborate, the Project Editor would seek clarification from the NBs separately after the meeting.

The discussion group also accepted a contribution from the US to consider as a reference document - the US National Institute of Standards and Technology (NIST) publication SP 800-34 Contingency planning guide for information technology systems.

## 2.5 Next Steps

Based on the WG discussion, the Project Editor for ISO/IEC 24762 would revise the base document and produce the first working draft for circulation to the NBs by January 2006. This would be in time for discussion and review again at the next SC 27/WG 1 meeting scheduled to take place in May in Madrid, Spain.

## 3. References

- [1] "SS 507:2004: Singapore Standard for Business Continuity/Disaster Recovery Service Providers", SPRING Singapore, 2 Bukit Merah Central, Singapore 159835, URL: <http://www.standards.org.sg>, 2004.
- [2] "ISO/IEC JTC 1/SC 27 N4479: Proposal for a New Work Item on Guidelines for Information and Communications Technology Disaster Recovery Services", ISO/IEC JTC 1/SC 27, 2005.

## Mr Kin-Chong Chan

*Deputy Chair, Security & Privacy Standards Technical Committee  
IT Standards Committee, Singapore*

*Vice President  
Special Interest Group in Security & Information InteGriTy (SIG^2)*

*Information Risk Manager, Asia  
JPMorgan Chase Bank, N.A.*



Mr Kin-Chong Chan is currently an Information Risk Manager with JPMorgan Chase Bank for the Asia Pacific region, a regional risk management role that covers the diverse areas of risk assessment, system security design, third-party service provider IT audit, regulatory compliance, security process engineering, and user security awareness.

Before joining JPMorgan Chase, Kin-Chong was with Singapore-listed company Stratech Systems, where he held the concurrent portfolio of Head, e-Business R&D labs, as well as Senior Security Consultant, and was the principal behind the security design of e-Government and e-Business applications. Prior to that, he served as Assistant Director in the Infocomm Development Authority of Singapore (IDA), where he championed the adoption of standards and technologies such as public key infrastructure, smart cards and biometrics in both the public and private sectors, and was also chief editor of the government's Security Technology Roadmap in the year 2000.

Kin-Chong has been actively involved in the related fields of technology and information security for more than eight years. He has diverse experience in planning, designing, implementing and managing IT security initiatives. As Deputy Chair of the Singapore Security and Privacy Standards Technical Committee (SPSTC), he continues to be an active player in the development, adoption and promotion of information security standards in Asia. Recently, he has also assumed the position of Vice President for SIG^2, a regional not-for-profit Special Interest Group in Security and Information inteGriTy (<http://www.security.org.sg>). He is a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA).

Awarded the prestigious Singapore National Computer Board scholarship in 1992, Kin-Chong studied at the Carnegie Mellon University in Pittsburgh, USA where he graduated with Honors in 1996 with double bachelor degrees in Mathematics and Computer Science.



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CAMBODIA CHINESE TAIPEI JAPAN MALAYSIA SINGAPORE SOUTH KOREA THAILAND



# SOUTH KOREA

## ABSTRACT

This paper introduces South Korea's new national identification (ID) infrastructure on the Internet, focusing on the framework of the alternative method of protecting its existing resident registration ID against misuse and theft. In addition, it presents the guidelines and typical application areas of the alternative method, and a future roadmap for the alternative methods in Korea.

## 1. Introduction

When an Internet website needs to identify the user who is subscribing or registering for an account, the Internet site would prompt the user to submit his resident registration ID, which is a permanent national ID issued by the Korean Government when he was born. The Internet website checks if the resident registration ID matches the real name provided by the user using a background protocol, known as the real name matching service. If they match, the Internet site allows the user to subscribe to it. In this scenario, the user must submit his resident registration ID to the Internet site. This system has a few anticipated problems:

- The submitted resident registration ID may contain a number of privacy-related information such as the birth date, birth month, birth year, birth place, and sex;
- There is a possibility for someone to use other resident registration ID to subscribe to the Internet site, which is known as identity theft; and
- The user loses protection right of privacy information like resident registration ID by using it when he subscribes to the Internet site.

A new solution to the above-mentioned problems is proposed, such that:

- The user must use a new random ID issued by a Third Trusted Party (TTP) instead of the resident registration ID, when subscribing or registering for an account to access an Internet site;
- The new national ID should have no privacy-related information so that no one can associate the new random national ID with the privacy-related information of the user; and
- The new random national ID should be issued to the user.

This alternative method, now known as the South Korea's new national ID infrastructure, is currently being developed by the Ministry of Information and Communication (MIC). It aims to protect its existing resident registration ID against misuse and ID theft. It is still subject to changes.

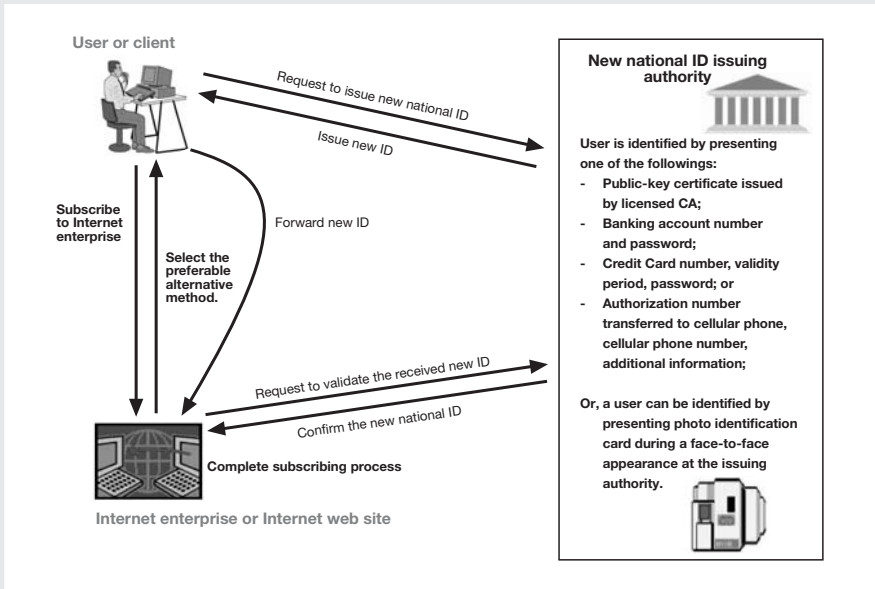
## **2. National Identification Infrastructure in South Korea**

### **2.1 Overview**

The resident registration ID has been used in very large area, especially, where the user wants to subscribe to the Internet site. The resident registration ID is a permanent ID issued by the Korean government. It is very difficult to change the resident registration ID as it includes much privacy-related information of the user, and it is valid for the lifetime of the user. However, it poses the three problems as highlighted in Section 1.

To avoid those problems, the alternative method, which uses the new pre-issued random ID to subscribe to the Internet site, is proposed. The random ID is issued by a new ID issuing authority to identify the user on the Internet. It does not include any privacy-related information and it is easily revoked, updated, or renewed by the user any time, and it is valid only for a specific period of time. The alternative method is a new kind of authentication scheme and uses the techniques and the protocols that are approved by Korea Information Security Agency (KISA) or the Korean government.

The conceptual framework of the alternative method is shown in Figure 1. There are three parties involved in the alternative method; (1) a new ID issuing authority; (2) an Internet site, and (3) the user. The new ID issuing authority issues the new national ID to the user, the Internet site provides the internet services to the user, and the user requests the Internet provider to validate and use the new national ID and enjoy the Internet services provided by the Internet site.



**Figure 1:** The Conceptual Framework of the Alternative Method

The operational procedure of the alternative method is as follows:

- The user visits the Internet site and wants to subscribe to it.
- The Internet site prompts the user for the new national ID. In the case where the user has no new national ID, the user will be redirected to the new national ID issuing authority in order to receive the new national ID from it. In the case where the user has obtained the new national ID, the user is identified by presenting the new national ID to the Internet site.
- The new national ID issuing authority identifies the user using the authentication token generated by one of the four identification methods: a method based on the public-key certificate issued by the licensed CA, a method based on banking account number with its password, a method based on the credit card number with its password and validity period, and a method based on a cellular phone number with its authorization code and some additional information.
- After the new national ID issuing authority proves the identity of the user, it issues the new national ID to the user which will be forwarded to the Internet site.

- The Internet site sends the received national ID to the issuing authority to validate it.
- The issuing authority returns the validity result to the Internet site.
- If the return is positive, the Internet site allows the user to subscribe to it. This completes the subscription procedure.

There are four major components in the alternative method: the identification method of the user, new ID issuing authority, technologies approved by KISA, and new national ID.

The user is authenticated by the new ID issuing authority by presenting the authentication token generated by one of the four identification methods. For example, in the case where the user has a public-key certificate, the user generates the signature value generated by the private key corresponding to the public key in the certificate and sends it to the new ID issuing authority. The new ID issuing authority checks the validity of the received signature by using the public key certificate. If the signature is valid, the identity of the user has been identified. In the case where the user has the cellular phone and chooses the identification method using the cellular phone, the ID issuing authority sends the authorization code to the user's cellular phone. The user recognizes the authorization code and sends it back to the ID issuing authority via the web transaction. Then, the ID issuing authority identified the user by comparing the transmitted authorization code with the received authorization code.

The new ID issuing authority provides the new random national ID to the user. The security technologies for the alternative method including the protocol and security mechanisms will be evaluated with regard to the security and availability and approved by KISA.

The new ID is more than 13 digits in length considering the compatibility with the resident registration ID.

## **2.2 Guidelines for the Alternative Method**

The guidelines for the alternative method have been defined by the Korean government. It takes into consideration the requirements of each component of the alternative method.

First of all, there are requirements for the capabilities of the new ID issuing authority: the operational capability, financial capability, and capability of minimum required facility and equipment. The new ID issuing authority must have at least eight staffs for administering the equipments and facilities, with at least USD 5 million of business funds set aside as a form of financial assurance for the system. Moreover, it should be equipped with equipment to maintain registration information, equipment to generate the new ID, and protection equipment such as the firewall, IDS, and IPS.

Secondly, the new national ID issuing authority should be a Trusted Third Party (TTP), that is, an authority trusted by all participating entities in the system.

Finally, the new national ID issuing authority should provide a fair ID offering service to any Internet service provider.

There are two types of assessments to evaluate the conformance of the requirements: the conformance assessment and privacy influence assessment. KISA carries out the conformance evaluation of new ID issuing authority to determine if all the requirements of the new ID issuing authority are satisfied, where the requirements of the new ID issuing authority is published by KISA. In addition, KISA performs the influence assessment of privacy information to determine if the new ID issuing authority takes appropriate measures to protect all privacy-related information against any kinds of threats in the large scale database.

If the new ID issuing authority passes these tests performed by KISA , a certification mark indicating that the new ID issuing authority is certified conformance to the security and operating standards by KISA will be accredited by the Korean government. This means that the Korean government endorses the new ID issuing authority.

### **2.3 Application Area**

There are five alternative methods that have been approved by KISA as of December 2005. These alternative methods can be grouped into two classes: the alternative method based on public key certificate, the alternative method based on the shared secret. The Internet site chooses a specific alternative method among five alternative methods according to the required security level, level of ease use, and legal requirement of each Internet site.

	Alternative method based on certificate	Alternative method based on the shared secret	Name and resident registration ID matching service
Security level	High	Medium	Low
Ease of use	Low	Medium	High
Reparation of damage	By Digital Signature act	By civil law	By civil law

**Table 1:** Comparison of the Alternative Methods

There are two major additional services: the age and gender confirmation service. In the case where a specific service can be provided according to the age of the user, an Internet site requests the new ID issuing authority to inform the age of the user. Then, it provides information about age range such as under age 12, under age 18, or over age 19. In the case where a specific service can be provided based on the gender of the user, an Internet site requests the new ID issuing authority to send the information about the gender of the user. Then it provides the Internet site with the necessary information.

## 2.4 Future Roadmap

Currently, adoption of the alternative method by Internet sites is not compulsory. There are two possible options for adopting the method: the mandatory enforcement by law or the recommended best practice by using the current guideline. The government has not decided which of these two options will be adopted. In the case where adoption is mandatory, the future roadmap would be as follows:

- A trial service would be started from the end of year 2005;
- A review team will be formed to determine the scope of applicability of the alternative method;
- A law will be made by end of year 2006; and
- The scope of alternative service will be extended from the beginning of year 2007 under the new law.

In the case where a recommended best practice is being adopted, the roadmap would be as follows:

- Trial service will be provided from the end of year 2005; and
- The scope of alternative method will be extended from the 3rd quarter of year 2006.

To determine the concrete option, the Advisory Committee has been organized under MIC since January 2006. This advisory committee comprises four subcommittees namely: Usage Improvement Subcommittee, Smooth System Transition Subcommittee, Legislation Subcommittee, and Promotion Subcommittee. The activities will be completed in 2nd quarter of 2006 and thereafter, it will determine the way forward for the adoption of the alternative method.

### **3. Conclusion**

The Internet services have been developed at great speed, one which is beyond our expectation. However, the resident registration ID is used when subscribing to the Internet site. To protect user's personal data in this resident registration ID, the new ID infrastructure is constructed by the Korean government. This is currently not compulsory. However, it should be made mandatory to gain more effective result. In the case where social consensus is focused on the mandatory enforcement, the relevant law will be made by the end of year 2006. Regardless of which enforcement is chosen, the new ID infrastructure will be extended the scope of application area very quickly in order to protect user's personal data in the resident registration ID.

Acknowledgement: This paper was supported by ITRC project, MIC, Korea.

### **4. References**

- [1] MIC, Guideline for the Alternative Method, Ministry of Information and Communications, Korea, October 2005.
- [2] H.Y. Youm and S.R. Lee, The Trend of the Alternative Method and Its Future Direction, Korea IEE journal, November 2005.

## Prof Heung-Youl Youm

*Professor, Department of Information Security  
Soonchunhyang University, South 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 eight 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, South 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 Ministry of Information and Communication, Korea Information Security Agency, and National Information Service. He received his PhD degree from Hanyang University in South Korea in 1990.



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CAMBODIA CHINESE TAIPEI JAPAN MALAYSIA SINGAPORE SOUTH KOREA THAILAND



# THAILAND

# Information Risk Management Course For Technical Personnel, Based On BS 7799 / ISO/IEC 17799 Standard

Dr Komain Pibulyarajana, Dr Banchong Harangsri  
Ms Siriwan Apisiridej, Ms Doungkamol Suppitayakorn, Mr Puth Nateesuwan  
*Thailand*

## ABSTRACT

This paper proposes a course outline for information risk management for Technical Personnel based on the BS 7799 / ISO/IEC 17799 standard. The paper discusses the methodology for the course to let the participants have a drill for risk assessment on a prepared and practical IT environment.

## 1. Introduction

In the previous work [1], we proposed to modify the original Information Security Management Systems (ISMS) courses to make them more appropriate to Technical Personnel such as System Administrators and Network Administrators. The two courses are:

- ISMS Auditor/Lead Auditor [2]; and
- Practical Information Risk Management with ISO/IEC 17799.

The main problem of the two courses is that they are not guiding Technical Personnel in making an effective risks assessment of their environment. Therefore, our focus in this paper is to modify just the risk assessment part in the original work to suit the Technical Personnel's perspective.

Table 1 shows the proposed course outline that we plan to conduct in Thailand. The course could be described as follows:

**Presentation 1:** Provide the course overview and objectives.

**Presentation 2:** Provide the concept of information security and background to two parts of the ISMS standard: ISO/IEC 17799:2000 and BS 7799-2:2002.

**Presentation 3:** Provide the security standard framework. The framework introduces an IT Security life cycle known as the Plan-Do-Check-Act (PDCA) process.

**Presentation 4:** Provide the management issues for this standard that management has to take into account such as establishment of this standard, management responsibility, management review and improvement.

**Presentation 5:** Introduce ten security domains in the standard.

**Workshop 1:** With the understanding of ten domains, this workshop is required for the participants to present their understanding in the domains in detail.

**Presentation 6:** This is the presentation that was modified from the original one [ref. to RWTUV] to make it more applicable to Technical Personnel. This presentation provides the modified risk assessment for them.

**Workshop 2:** This workshop was also modified from the original one [ref. to RWTUV]. With the background of risk assessment from presentation 6, this workshop requires the participants to study/investigate and analyze risks in an IT environment equipped with the necessary equipments and servers as follows:

- A router;
- A firewall;
- A database server; and
- A web server.

The detail of this workshop which is our major contribution is in the next section.

<b>Day 1</b>	
<b>Time Description/Objectives</b>	
08:30	Coffee/Registration/Welcome
09:00	<b>Presentation 1:</b> Introduction <ol style="list-style-type: none"> <li>1. Introduction/Delegates</li> <li>2. Course Overview</li> <li>3. Course Learning Objectives and Continuous Assessment Process</li> <li>4. Course Methodology</li> </ol>
09:45	<b>Presentation 2:</b> An Overview of Information Security Management System <ol style="list-style-type: none"> <li>1. Information Security</li> <li>2. Background to ISO/IEC 17799:2000 &amp; BS7799-2:2002</li> </ol>
10:45	Break
11:00	<b>Presentation 3:</b> Using BS7799-2:2002 as a Model for ISMS <ol style="list-style-type: none"> <li>1. Structure, Purpose</li> <li>2. PDCA Model</li> <li>3. Interrelationship between ISO/IEC 17799:2000 and BS7799-2:2002</li> </ol>
12:00	Lunch
13:00	<b>Presentation 4:</b> BS7799-2:2002 Management Issues <ol style="list-style-type: none"> <li>1. Information Security Management System               <ul style="list-style-type: none"> <li>• Establishing and Managing ISMS</li> <li>• Documentation Requirements</li> </ul> </li> <li>2. Management Responsibility</li> <li>3. Management Review of the ISMS</li> <li>4. ISMS Improvement</li> </ol>
15:00	Break
15:15	<b>Presentation 5:</b> ISMS Controls
16:15	<b>Workshop 1:</b> BS7799-2:2002 Controls (10 Domains)
18:00	End of Day 1
<b>Day 2</b>	
<b>Time Description/Objectives</b>	
08:30	<b>Presentation 6:</b> Techniques for Risk Management <ol style="list-style-type: none"> <li>1. Systematic Approach to Risk Assessment</li> <li>2. Risk Management Process               <ul style="list-style-type: none"> <li>• Risk Assessment</li> <li>• Risk Treatment</li> </ul> </li> </ol>
10:45	Break
11:00	<b>Workshop 2:</b> Risk Assessment and Treatment
12:00	Lunch
15:00	End of Day 2

**Table 1:** Proposed Course Outline

## 2. Risk Assessment and Treatment (Workshop 2)

The purpose of this workshop is to let the participants practice or sharpen their skills on risk assessment in a prepared IT environment that is applicable to their office environment. The scenario prepared consists of a router, a firewall, a database server and a web server. The scenario combined the risks of the four equipment into one list of risks. Some of the risks belong to the router, some to the firewall, and some to the database server and the rest to the web server. Figure 2 shows the list of risks from Question 1 to Question 31.

Some of the statements in the list are at risk and the rest are not. For example the following statement is at risk:

In-band management sessions are not allowed from authorized IP addresses from the internal network, whereas this statement is OK (not at risk):

Job/Batch queues are reviewed regularly to detect unauthorized job submissions.

<b>Step 1</b>	<b>Select 2 systems that most meet your experience.</b>
	E1. Router (RO)
	E2. Firewall (FW)
	E3. Database Server (DS)
	E4. Web Server (WS)
<b>Step 2</b>	<ul style="list-style-type: none"> <li>- Put system codes (E1-E4) in front of each statement below that belong to the system(s)</li> <li>- Select the appropriate security risk area(s) for the statement and justify why the statement is related to the area(s)</li> <li>- Select the appropriate controls from BS 7799-2:2002 Standard and justify why the statement is related to the controls</li> <li>- Justify why the statement is at risk or not</li> <li>- If at risk, modify the statement to make it less risk</li> </ul>
	Q1. The connections are not restricted to known IP addresses of neighbor routers from a trusted Autonomous System (AS).
	Q2. All traffic is not denied by default.
	Q3. The number of concurrent user access is not set to an appropriate number.
	Q4. Documented procedures for reviewing content prior to posting to a production web server are not present.

**Table 2:** Workshop 2 on Risk Assessment and Treatment

Q5.	Service ports are not blocked from untrusted sites.
Q6.	The account policy (access control policy) is not configured to restrict unauthorized logon attempts.
Q7.	The unused ports are configured to deny access to them.
Q8.	Auditing is not turned on.
Q9.	Job/Batch queues are reviewed regularly to detect unauthorized job submissions.
Q10.	Interfaces that are not in use are disabled.
Q11.	Default administrator accounts are enabled.
Q12.	Directory browsing is disabled.
Q13.	Only an administrative account is used when doing administrative jobs.
Q14.	A procedure is not in place to remove the sample files, scripts, help and development files from the system.
Q15.	Web pages stating "Under Construction" or equivalent wording or graphics were found on a production server.
Q16.	The system is set to reject access to remotely administer it.
Q17.	Traffic to a sensitive system is not encrypted.
Q18.	Stored procedures are not restricted access by authorized personnel.
Q19.	In-band management sessions are only allowed from authorized IP addresses from the internal network.
Q20.	Common vulnerable ports based upon the SANS Top 20 Vulnerabilities are not filtered.
Q21.	The system does not accept traceroute.
Q22.	The security rule set is consistent with the organization's written information security policy.
Q23.	Accounts used to support replication are not restricted to authorized personnel.
Q24.	Production and development systems on a shared host are clearly separated and identified.
Q25.	Administrative accounts are not renamed.
Q26.	Installations of firmware updates are not periodically scheduled.
Q27.	Administrator/root accounts do not have strong passwords.
Q28.	Simple Network Management Protocol (SNMP) passwords/community strings are set as default.
Q29.	The latest security patch has been installed.
Q30.	A screened subnet architecture is used.
Q31.	Audit trail data is not maintained for a certain period of time.

**Table 2:** Workshop 2 on Risk Assessment and Treatment (cont'd from page 59)

From the combined list of risks, the participants have to:

- put an appropriate system code (E1-E4) in front of each statement;
- select appropriate security risk areas (see the areas in Figure 1) for the statement and justify why the statement is related to the areas;

- select appropriated controls from the standard and justify why the statement is related to the controls;
- justify whether the item is at risk; and
- if at risk, modify it to make it less risky.

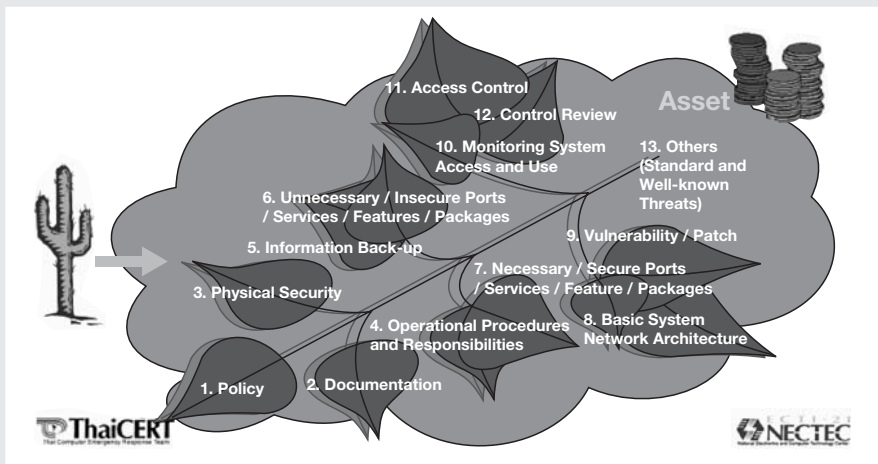


Figure 1: Security Risk Areas

### 3. Conclusion

This modified course aims to help Technical Personnel with technical background in learning about this management security standard and being able to apply the knowledge gained to their IT environment. The proposed approach will also help narrow the gap of the applicability of the security management standard to the daily jobs of Technical Personnel.

### 4. References

- [1] Banchong, H., Komain, P., Doungkamol, P. and Siriwan, A., Modified Risk Assessment using a New Logical Way of Thinking - Project Proposal and Discussion, in 2nd Regional Asia Information Security Standards (RAISS) Forum Meeting, (Singapore, 2005), 61-67.
- [2] ISMS Auditor/Lead Auditor, RWTÜV, 23 February 2004.

## **Dr Komain Pibulyarojana**

*Head of National Security Section  
National Electronics and Computer Technology Center (NECTEC)  
Ministry of Science and Technology, Thailand*

*Director  
Thai Computer Emergency Response Team (ThaiCERT)*



Dr Komain Pibulyarojana is the Head of the National Security Section, National Electronics and Computer Technology Center (NECTEC), Ministry of Science and Technology, Thailand. He is concurrently the Director of Thailand's Computer Emergency Response Team (ThaiCERT). Dr Komain is also the Secretary of Security Committee, part of Thailand's Electronic Transactions Commission responsible for reviewing and advising the security requirements for the Commission.

His area of interest and specialization includes Computer Network; Network Security; Information Security Standards, Information Security Management; Risk Assessment and Management and Security Policies.

## **Dr Banchong Harangsri**

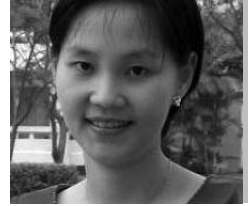
*Head  
Security Standard Research and Development (SSRD) Division  
Thai Computer Emergency Response Team (ThaiCERT)  
National Electronics and Computer Technology Center (NECTEC)  
Ministry of Science and Technology, Thailand*



Dr. Banchong Harangsri is the Head of Security Standard Research and Development (SSRD) Division of ThaiCERT, NECTEC. He is also the Secretary of the Security Committee. His area of interest and specialization includes Information Security, Network Security, Security Standard, and IT Security Audit.

## Ms Siriwan Apisiridej

*Assistant Researcher  
National Electronics and Computer Technology Center (NECTEC)  
Ministry of Science and Technology, Thailand  
Thai Computer Emergency Response Team (ThaiCERT)*



Siriwan Apisiridej is a staff of the SSRD of ThaiCERT and an assistant researcher at NECTEC. She is also the Secretary of the Security Committee. She specializes in the Information Security Standard and Security Audit.

## Ms Doungkamol Suppitayakorn

*Project Analyst  
Security Standard Research and Development (SSRD) Division  
Thai Computer Emergency Response Team (ThaiCERT)  
National Electronics and Computer Technology Center (NECTEC)  
Ministry of Science and Technology, Thailand*



Doungkamol Suppitayakorn is the project analyst of SSRD of ThaiCERT, in charge of translating, arranging, developing, and conducting security policies framework for Thai users.

## Mr Puth Nateesuwan

*Assistant Researcher  
Security Standard Research and Development (SSRD) Division  
Thai Computer Emergency Response Team (ThaiCERT)  
National Electronics and Computer Technology Center (NECTEC)  
Ministry of Science and Technology, Thailand*



Puth Nateesuwan is an Assistant Researcher of the SSRD of ThaiCERT. His area of interest and specialization includes Information Security Standard and Security Audit, Computer Network and Network Security.



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CAMBODIA CHINESE TAIPEI JAPAN MALAYSIA SINGAPORE SOUTH KOREA THAILAND



# SC 27 REPORT

## ABSTRACT

In today's diverse business environments, and markets being globally inter-connected across mobile, wireless and broadband networks, information security is playing an ever more important role than before. To benefit from the new dynamics of the connected world and market opportunities, it is critical for businesses to deal with the risks and protect the organizational information asset.

International information and IT security standards provide a means for developing solutions and a basis for doing business securely. ISO/IEC JTC 1/SC 27 is an international centre of expertise in the field of information and IT security standards and has been at the forefront of this work for over a decade. This paper provides an overview of the SC 27 work, as well as looking at the future programme of work in the specific area of information security management.

## 1. The ISO 27000 Family of Standards

Working Group 1 (WG 1) in SC 27 has embarked on a programme of work relating to the development of a family of information security management system (ISMS) standards referred to as the 27000 series of standards.

- ISO/IEC 27000 ISMS Fundamentals and Vocabulary
- ISO/IEC 27001 ISMS-Requirements
- ISO/IEC 27002 (ISO/IEC 17799 after 2007)
- ISO/IEC 27003 ISMS Implementation Guidance
- ISO/IEC 27004 Information Security Management Measurements
- ISO/IEC 27005 Information Security Risk Management

Work on ISMS standards is being carried out in close collaboration with ITU-T and will result in joint publication of these standards. ITU-T has already embarked on an 'ISMS telecoms requirements' document (X.1051) based on BS 7799 Part 2:2002 and this is expected to be further developed in alignment with the ISO/IEC 27001 development. In addition ITU-T is collaborating on ISO/IEC 27002 and is considering collaboration of the other ISMS developments - ISO/IEC 27003-27004.

## 2. ISO/IEC 27001 ISMS - Requirements

The first of these standards, ISO/IEC 27001, was published on 15 October 2005. This standard is based on and replaces the standard BS 7799 Part 2 which has been used world-wide for third party management system audits and certification and is now withdrawn. Both ISO/IEC 27001 (ISMS) and BS 7799 Part 2:2002 (ISMS) use the Plan-Do-Check-Act (PDCA) process model as adopted in ISO 9001 (Quality Management System or QMS) and ISO 14001 (Environmental Management Systems or EMS). This PDCA process defines a cycle of activities that defines the establishment of an ISMS, the implementation and operational use of the ISMS, regular monitoring and review of the ISMS, and improving and updating the ISMS to take account any changes necessary. This process cycle is designed to ensure that effective information security is implemented and it remains effective through a process of continual improvement.

The PDCA process model in ISO/IEC 27001 has a set of risk management processes for identifying and assessing the risks and impacts, for treating these risks with various management options, one of which is to reduce the risks by the appropriate selection of controls. Annex A of this standard contains the set of controls from ISO/IEC 17799:2005, which can be selected for implementation according to which risks need to be reduced.

## 3. ISMS Certification

It is important to note that ISO/IEC 17799:2005 is a Code of Practice for Information Security Management and is not applicable for accredited certification - it was neither designed nor suitable for certification purpose. Whereas, the specification standard, ISO/IEC 27001 Information Security Management System (ISMS) - Requirements, has been designed to be applicable for accreditation certification. ISO/IEC 27001 is a revised version of BS 7799 Part 2:2002, a standard that has been used for accreditation certification for the past seven years. The certification process used for this is exactly the same as that used for ISO 9001 for QMS assessments and ISO 14001 for EMS assessments. Now ISO/IEC 27001 has been published and BS 7799 Part 2:2002 has been withdrawn and future certification can be transferred over to using the ISO standard. National Accreditation Bodies that are involved in the process will be issuing a Certification Transition Statement which will give details of the time period during which organisations, working together with their Certification Body, will need to make the transition from BS 7799 Part 2:2002 to ISO/IEC 27001.

The International Register for ISMS Accredited Certificates is now published at the new Web site [www.ISO27001certificates.com](http://www.ISO27001certificates.com) (and also at [www.xisec.com](http://www.xisec.com)). This Register will function as an International Register for the purpose of registering an organisation's ISMS certificate. Certification Bodies throughout the world should continue to provide the Registrar with the details of all new certificates as well as any updates to existing certificates using the same notification process in operation today.

#### **4. ISO/IEC 27002 (ISO/IEC 17799:2005) - Code of Practice for Information Security Management**

The revised version of ISO/IEC 17799 was published on 15 June 2005. This new edition provides many new features and improvements in order to keep best practice for information security up-to-date with progress and trends and to include changes in ways of doing business. These new features include additional best practice:

- To cover the increase in the use of external services and outsourcing and how to manage the use of these services securely;
- To extend the controls and guidance on asset management and to cover issues such as 'acceptable use' and 'ownership';
- The introduction of new technologies and how these technologies are being used, such as the growing use of mobile and wireless networks;
- To address the problem of 'mobile code';
- The growing number of new threats and risks confronting business and extensions to incident management controls and guidance;
- To provide a comprehensive approach to human resource security; and
- To address the growing problem of vulnerability management, including patch management.

Improvements have been made to the 'user friendliness' of the standard, to make it easier for readers to distinguish what the control is in contrast to what the implementation guidance for the control is. The revised version provides business with an important tool for managing its information security risks and to enhance its ability at managing its incidents and to support its business continuity capability whilst maximising its investments and opportunities in the marketplace. The key objective of this code of practice is to enable business to protect the confidentiality, integrity and availability of its sensitive and critical information.

ISO/IEC 17799:2005 Code of Practice for Information Security Management is clearly related to the ISMS family of standards. However ISO/IEC 17799 will not change its number in the short term, but in April 2007, the proposal is to allocate the number ISO/IEC 27002 to the ISO/IEC 17799 standard. Given the existing success, uptake and market penetration of ISO/IEC 17799, this will enable the market to become familiar with this new series of numbers.

#### **5. ISO/IEC 27003 ISMS Implementation Guidance**

SC 27 is undergoing the development of 'ISMS Implementation Guidance' standard with the intention of providing more help and guidance on implementing the different elements of the PDCA process in ISO/IEC 27001. This will make use of Annex B of BS 7799 Part 2:2002 with considerable extensions.

#### **6. ISO/IEC 27004 - Information Security Management Measurements**

As well as the standard ISO/IEC 27003, there is also a standard ISO/IEC 27004 'Information Security Management Measurements' being developed. This development is aimed at addressing how to measure the effectiveness of ISMS implementations (processes and controls) and will specify metrics and provide guidance concerning measurement techniques applicable for determining and describing the efficiency and effectiveness of information security management systems in support of ISO/IEC 27001 (see above). It includes resources (information security controls), and activities (information security processes and procedures). The metrics are used mainly for the measurement of the "Do" components of an ISMS (Implement and operate the ISMS) as input to the "Check" (monitor and review) components of an ISMS, with the goal of providing a means for taking decisions at the "ACT" (maintain and improve the ISMS) stage, leading to continuous improvement of the ISMS cycle. This standard will provide a valuable tool for business generating a range of effectiveness indicators for benchmarking and setting performance targets.

## **7. ISO/IEC 27005 Information Security Risk Management**

This standard is to help with implementing the risk processes in ISO/IEC 27001 - this work will make use of and incorporate the developments that have been made for MICTS Part 2 which is on information security risks.

## **8. ISO/IEC 27000 ISMS Fundamentals and Vocabulary**

This standard will explain the basic principles and vocabulary for ISMS standards. It will also serve as a reference model to explain the relationships between these standards. MICTS Part 1<sup>1</sup> will be used for some of this 27000 development.

## **9. Other Developments**

SC 27 has also embarked on other important areas of standardization such as the recent project on Disaster Recovery Services which is based on the Singapore standard SS507. This project will develop a much needed standard in this area.

## **10. Summary**

In conclusion, SC 27 is at the leading edge of standardization work for both information and ICT systems. It has published many standards that are in use today around the world providing secure applications, services and networks to businesses and governments. These standards cover both management and technical aspects addressing a range of business and technological risks. It also liaises with other standards groups and user organisations to collaborate on joint work such as with ISO/TC 68 in the area of banking, ITU-T on telecoms standards, and JTC 1/SC 37 on biometrics. SC 27 continues to work with experts and business around to ensure work is up to date, appropriate and driven by market needs.

<sup>1</sup> MICTS refers to Management of Information and Communications Technology Security (MICTIS) and the Part 1 standard is on concepts and models for information and communications technology security management.

### Mr Ted Humphreys

*Chartered Fellow of BCS CITP, CISM  
Convenor of ISO/IEC JTC 1/SC 27/WG 1*

*Director  
XiSEC Consultants Ltd, UK*



Mr Ted Humphreys (Chartered Fellow of the BCS - FBCS CITP, CISM) is the Director of XiSEC Consultants Ltd, a UK company providing Information Security Management consultancy services around the world. He has been an expert in the field of information security and risk management for more than 27 years. During this time, he has worked for major international companies (in Europe, North America and Asia), as well organizations such as the European Commission and the OECD.

Mr Ted Humphreys, the internationally acknowledged father and management guru (and some say spiritual leader) of the ISO/IEC 17799 and ISMS (BS 7799) standards and the global BS 7799 certification movement, has been: the editor of BS 7799 Part 1:1999, ISO/IEC 17799:2000, the 1999 and 2002 editions of BS 7799 Part 2 the ISMS standard and the EA 7/03 the ISMS accreditation guidelines. He is the Founder and Director of the ISMS International User Group and is responsible for the International Register of BS 7799/ISMS Certificates. In 2002 he was honoured with the Secure Computing Lifetime Achievement Award. This international award recognizes his noteworthy achievements in shaping and promoting the development and standardization of information security management BS 7799 best practice standards.