

ABSTRACT

This article is an extension of the paper published in the inaugural issue of the RAISS Forum Proceedings, which provides further updates and highlights of the information security standards development and other related activities in Malaysia.

1. Objectives

The objective of this paper is to highlight Malaysia's activities in information security standards development since the last update at the first RAISS Forum meeting in Tokyo, Japan on 19 November 2004.

2. Activities Update on Standards Developments

Reviews are being done continuously of the relevant international standards which may be suitable for adoption. Currently, some of the standards that are sent for public comment prior to the adoption process are:

1. **ISO/IEC 17799:2005**
 - Code of Practice for Information Security Management

2. **ISO/IEC 18033-1:2005**
 - Information technology - Security techniques - Encryption algorithms - Part 1: General

3. **ISO/IEC 18033-3:2005**
 - Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers

4. **ISO/IEC 18033-4:2005**
 - Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers

5. **ISO/IEC 13888-1:2004**
 - IT security techniques - Non-repudiation - Part 1: General

6. **ISO/IEC 13888-2:1998**
 - Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques

7. **ISO/IEC 13888-3:1997**
 - Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques

With regards to the progress on the establishment of a national Business Continuity Management (BCM) standard, the first draft of the first part of the standard is currently being circulated for internal review

Malaysia continues to be a participant in international standards development activities mainly through ISO/IEC and RAISS Forum meetings. Malaysia is keenly preparing for the hosting of the ISO/IEC JTC 1/SC 27 Working Groups (WGs) Meetings to be held in November 2005 at Kuala Lumpur.

3. Activity Updates - Other Developments

The Malaysian Technical Standards Forum Berhad (MTFSB) was established in early 2005. It is an entity consisting of local telecom industry players that are involved in the development of best practices and guidelines for communications industry.

Awareness programmes on security standards are being continued and an Information Security Management Systems (ISMS) seminar for financial institutions was held in April 2005. So far, one financial institution in Malaysia has been certified under BS 7799-2:2002.

4. Conclusion

Information security standards development activities are continuously evolving in Malaysia and the country is very keen and committed for organizations in the country to practice and adopt security standards in their business operations. Malaysia is keen to continue her involvement and participation in the international standards meetings and forums for the benefit of the country and so far, much has been gained through those involvements.

Mr Shamsuddin Bin Abdul Jalil

*Policy Analyst
National ICT Security & Emergency Response Centre (NISER)
MIMOS Berhad*



Shamsuddin Bin Abdul Jalil is a Policy Analyst with the National Information, Communications, and Technology (ICT) Security & Emergency Response Centre (NISER), MIMOS Berhad. In his appointment, Shamsuddin has been actively involved in various Information Security Management projects including trainings, consultancy and audits. Shamsuddin has extensive involvement in the development of various security courses conducted by NISER, including general security awareness training, ISO/IEC 17799 and BS 7799-2:2002 Awareness and Implementation Trainings, and Business Continuity Planning courses. Prior to joining NISER, Shamsuddin was a systems developer and lecturer.

Shamsuddin obtained his Masters and Bachelor's Degrees in Computer Science from Universiti Putra Malaysia, Selangor. He is a GIAC Security Essentials Certification (GSEC) holder, a certified BS 7799 Lead Auditor and is also an Associate Business Continuity Professional (ABCP). His domain of expertise includes Information Security Management Systems (ISMS); BCP; Information Security Standards; Risk Assessment and Management and Security Policies.

Standards Updates From Singapore Including Development Of A New Business Continuity And Disaster Recovery Standard

Mr Kin-Chong Chan

*Deputy Chair, Security & Privacy Standards Technical Committee
IT Standards Committee, Singapore
Information Risk Manager, Asia, JPMorgan Chase Bank, N.A.
Singapore*

ABSTRACT

IT security plays a vital role in securing the information assets of organizations and businesses, especially in today's global war against terrorism. Standardization of IT security is the work of international standards bodies, such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This paper presents timely updates of the IT security standards organization and development programme in Singapore, under the Security and Privacy Standards Technical Committee (SPSTC) that is responsible for the promotion, development and adoption of IT security standards in Singapore. The paper also introduces and describes the development of a new standard for business continuity and disaster recovery service providers. The standard was developed, published and adopted in Singapore in 2004. It has now been accepted as a base document for further development into an international standard called "Guidelines for information and communications technology disaster recovery services" under the ISO/IEC Joint Technical Committee 1 (JTC 1) Sub-Committee 27 (SC 27) Working Group 1.

1. Introduction

In Singapore, the Security and Privacy Standards Technical Committee, or SPSTC, undertakes the responsibility of promoting, developing, and adopting technical standards in IT security and privacy. Updates to its organization and focus, and the development of a new standard for business continuity and disaster recovery are described in the following sections of this paper.

2. The Security & Privacy Standards Technical Committee

2.1 Organizational Structure

The SPSTC is one of several Technical Committees under the Information Technology Standards Committee, or ITSC. The ITSC is an industry-led effort made up of volunteer members from the industry, supported by the Standards, Productivity and Innovation Board (SPRING Singapore) and the Infocomm Development Authority of Singapore (IDA Singapore).

The ITSC promotes and facilitates national infocomm standardization programs and the participation of Singapore in the international standardization activities. Under its purview, there are nine Technical Committees and one Special Interest Group, as shown in Figure 1.

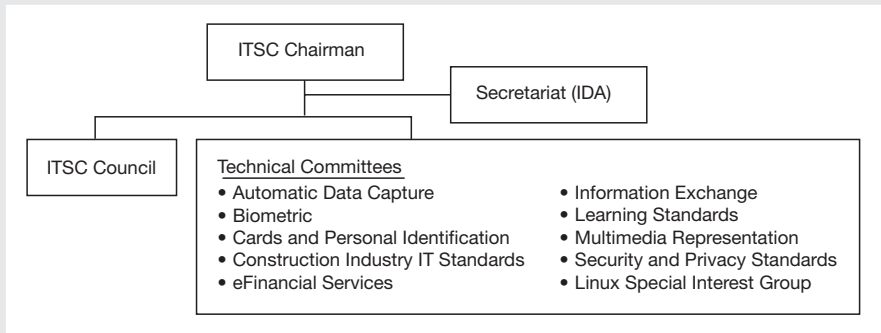


Figure 1: ITSC Organization

The SPSTC is one of the Technical Committees under the ITSC. The committee is made up of volunteers from local and foreign financial institutions, security technology vendors and practitioners, telecommunication and network providers, research and development community, end-user groups and government agencies. It is led by chair Mr Meng-Chow Kang, Microsoft, and deputy chair Mr Kin-Chong Chan, JPMorgan Chase.

2.2 Working Groups and Changes

There are currently five active working groups (WGs) under the SPSTC. There have been a number of changes to the WG structure in 2005 and this section describes the primary changes.

The first major change is the merger of the ISMS WG and the Network Security WG into the new Information Security Management WG, making it one of the largest, if not the single largest, WG under the committee. The merger re-aligns the work undertaken previously by the two separate teams in order to more efficiently manage the combined resources as well as to mirror SC 27/WG 1 more effectively. The latter is especially important in anticipation of the development of the new ISO/IEC 2700x series management standards. The new

working group is co-chaired by Mr Philip Sy, PSB Certification, and Mr Tim-Meng Ching, Lucent Technologies.

The second major change is the formation of a new working group on Privacy Technology. This new working group is chaired by Mr Lawrence Tan from IDA Singapore. An introduction and overview of this WG is presented in the next section.

Lastly, the Public Key Infrastructure (PKI) WG is re-organized and transformed into a new working group on Cryptography. With a renewed and broadened agenda and focus on cryptographic techniques, this working group will be better positioned to more effectively mirror SC 27/WG 2. It is jointly led by Dr Bao Feng of the Institute for Infocomm Research (I²R), and Mr Juay-Guan Hee of the DSO National Laboratories.

The remaining two existing working groups remain unchanged. With the above changes, the five WGs are now:

- Business Continuity & Disaster Recovery (BC/DR)
- Cryptography
- Information Security Management (ISM)
- Privacy Technology
- Security Assurance

The organization of the SPSTC and its WGs is presented in Figure 2.

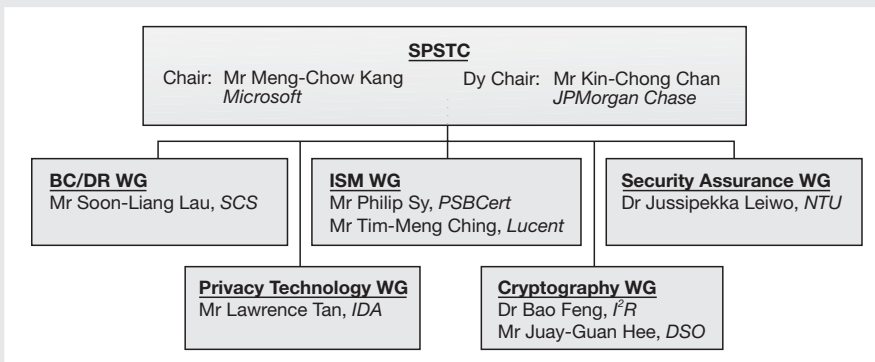


Figure 2: SPSTC and Its Working Groups

2.3 Privacy Technology Working Group

The recent spate of the widely publicized loss, theft and unauthorized sale of confidential personal information has sent a timely reminder to the world of the importance of continuing the effort to protect consumer or personal privacy.

In modern business practices, most information for which there is a privacy concern is associated with technology. In reality, technology is now used extensively by every organization to collect, store, process, distribute and share private personal data.

In contrast, standards related to the control and management of privacy data and the awareness of the privacy requirements for the acceptable use of such technology are still severely lacking or inadequate. Moreover, while technology can provide new opportunities for the infringement of privacy, it can also provide the best safeguards against privacy incursions. This is therefore the first motivation for the need of privacy standardization related to technology.

Privacy standardization would promote greater awareness and adoption of best practices as well as the use of privacy enhancing technologies. It would also play an important role in helping organizations meet national and international legal and regulatory requirements on personal data protection.

It was against this backdrop that the new working group for Privacy Technology was established under the SPSTC. Today, the working group is led by Mr Lawrence Tan of IDA Singapore, with keen participation by key representatives from both the infocomm industry and government bodies. It has a charter to develop and promote infocomm privacy standards, and monitor and create opportunities to collaborate with international efforts in the same area. One of its first deliverables is a management or operational framework standard for managing technology privacy.

3. Business Continuity and Disaster Recovery Standard

3.1 Background

The awareness of business continuity and disaster recovery, or BC/DR, services has grown significantly due to the threats of global terrorism, outbreak of contagious disease, natural

Standards Updates From Singapore Including Development Of A New Business Continuity And Disaster Recovery Standard

disaster, and geopolitical tension. These factors threaten the resiliency of information technology and telecommunications infrastructure worldwide. Consequently, organizations both within and outside Asia are evaluating alternative locations for recovery in the event of disruptions.

Today's BC/DR service providers face challenges such as a need to differentiate themselves in order to retain competitive advantage as well as the need to maintain and constantly improve service levels. In addition, there is a general lack of awareness and clarity amongst the end-user community over the different types of service providers and the risks involved in outsourcing arrangements for BC/DR functions.

For end-user organizations, a BC/DR standard would provide clarity over the different types of BC/DR service providers, help them in selecting the best-fit BC/DR service providers, ensure that the service providers offer high service quality, and help mitigate the risk of outsourcing through the adoption of industry best practices. And for BC/DR service providers, the standard would provide a basis to differentiate service providers and serve as a benchmarking guideline to help ensure their services are able to meet the organization's business continuity requirements.

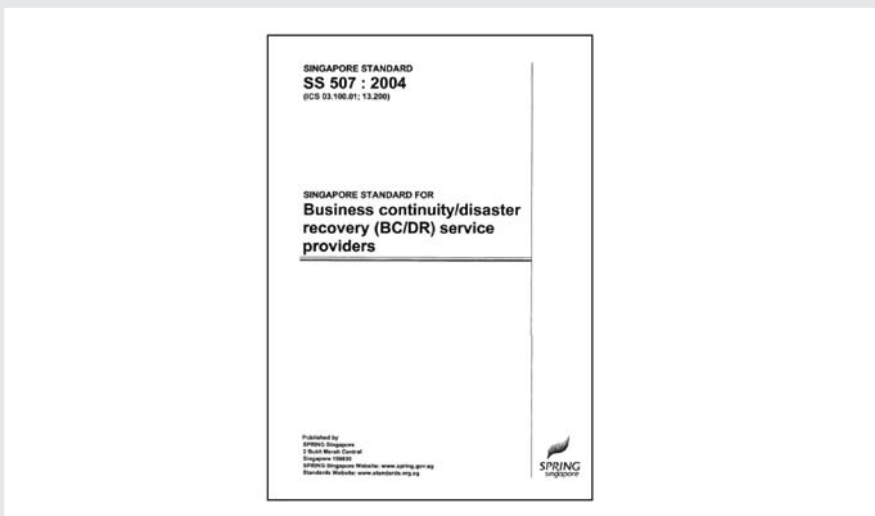


Figure 3: Singapore Standard for Business Continuity/Disaster Recovery Service Providers

3.2 Development Framework

The BC/DR Standard was developed by key players in the BC/DR industry based on a multi-tier framework. The development framework is presented in Figure 4.

The foundation layer of the development framework consists of Policies, Processes, Programme, Performance Measurement, People and Products.

- **Policies.** Key industry players and the government are instrumental in establishing the policies and associated regulations, and setting the overall direction for the BC/DR industry.
- **Processes.** The processes involved in deriving the requirements of the standard ensure that the requirements can be implemented and enforced.
- **Programme.** A formal programme needs to be established to enforce the requirements of the standard and neutral audit by external parties would be a key component of the programme.
- **Performance measurement.** In conjunction with audit assessment, key performance measures would need to be identified.
- **People.** A pool of skilled and knowledgeable workers would help to operate, uphold and maintain the relevance of the BC/DR requirements. Awareness and training courses in the BC/DR arena would help keep professionals in the industry abreast of the latest trends and developments.
- **Products.** The products and services offered by BC/DR service providers would help to shape the landscape of the BC/DR industry. Service providers should continue to upgrade their assets and resources to further enhance their products and services to pre-empt and respond to changing customer needs.

The foundation layer helps to define the supporting infrastructure from which services are derived. The international best practices highlight widely adopted practices that help to improve BC/DR activities in specific areas and present an added level of provision above the services provided.

The overall BC/DR standard requirements are drawn up from a composite view of these layers and with a balance between cost effectiveness and standard rigor considerations.

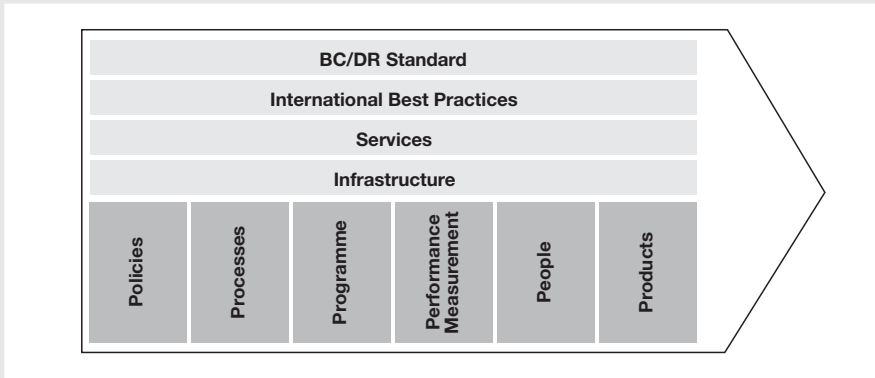


Figure 4: BC/DR Standard Development Framework

3.3 Standard Scope and Structure

The BC/DR standard specifies the stringent requirements that BC/DR service providers must possess so that they can provide a trusted operating environment and help companies secure and recover critical data in a crisis. These requirements include stipulations for operating, monitoring, maintaining and up-keeping BC/DR services offered to clients.

The standard consists of five key components:

- **General requirements.** These requirements must be met by both BC/DR service providers of physical facility and services. They provide assurance to clients and potential customers that they have deliberated on unforeseen events which may affect their ability to fulfill their service obligations to clients. Such considerations include risk mitigation via prior arrangements with other service providers in the industry.
- **Disaster recovery facility qualification.** These requirements must be met by BC/DR service providers providing a secure physical operating environment to facilitate clients' recovery efforts. Besides the basic physical facility, they also include

environmental controls, telecommunications requirements, continuous power supply and non-recovery amenities such as parking and accessibility to food and water.

- **Service provider capability qualification.** These requirements specify the service capabilities of the BC/DR service providers to clients besides the physical recovery facilities. In addition to qualified staffing, other minimum capabilities include capacity to support simultaneous invocation of disasters by clients.
- **Guidelines for selection of recovery sites.** These guidelines serve as guidance for potential clients who are in the process of selecting a recovery site as part of their BC/DR requirements and BC/DR service providers who are in the process of building additional recovery sites to expand their global operations.
- **Recommended industry best practices.** While individual practice may not be unanimously accepted and adopted, collectively they represent a set of practices that are considered prevalent among BC/DR service providers. Moreover, industry best practices promote professionalism and growth of the BC/DR industry. While these practices are not currently mandatory, they may eventually evolve into compulsory requirements as the industry matures.

The above structure is illustrated in Figure 5. Note that the first three components (colored in darker shade of gray in the diagram) lend themselves to being specifications for certification, while the last two components (colored in lighter shade of gray in the diagram) serve more effectively as guidelines.

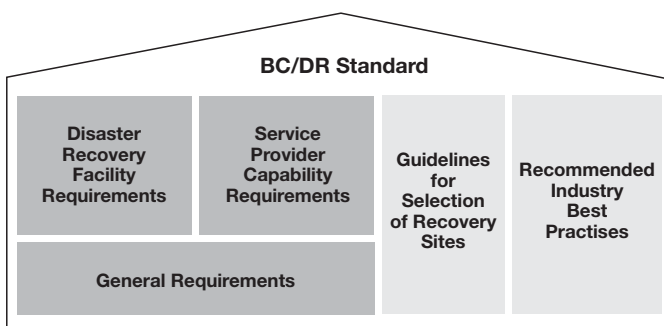


Figure 5: BC/DR Standard Structure

3.4 Complementing WG 1 Roadmap

The ISO/IEC 17799:2005 Code of practice for information security management is highlighted as a major standard in the roadmap of SC 27/WG 1. The BC/DR standard supports the implementation of several controls in ISO/IEC 17799. In particular, the standard supports the Business Continuity Management requirement (clause 14), while also contributing to requirements on third-party access (clause 6) and service delivery (clause 10) in the case where the organization's DR services are outsourced. The standard therefore provides a perfect guideline to the Business Continuity Management requirement in ISO/IEC 17799. Refer to Figure 6 for the relevant references to ISO/IEC 17799.

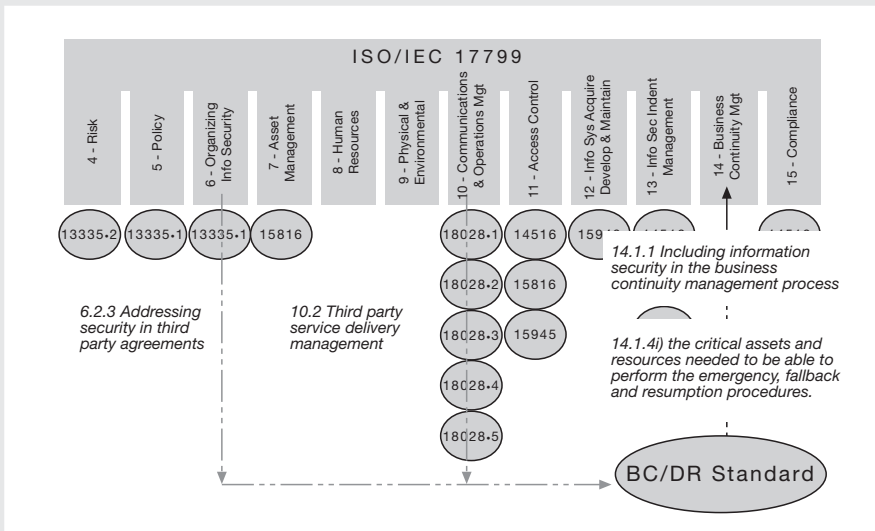


Figure 6: How the BC/DR Standard fits into ISO/IEC 17799

3.5 Current Status and Future Work

The BC/DR Standard was published in 2004 as Singapore Standard SS 507 - "Singapore Standard for Business Continuity/Disaster Recovery (BC/DR) Service Providers". Since then, the standard has been used as a specification for the certification of BC/DR service providers in Singapore under PSB Certification.

At the launch of the certification scheme in December 2004, seven companies were awarded the certification. The companies were: Hewlett-Packard, IBM, National Computer Systems and Singapore Computer Systems in the BC/DR service provider category; and Equinox, SingTel Expan and StarHub in the DR facility category. Several more organizations have applied to be certified under this scheme.

In April 2005, at the 30th ISO/IEC JTC 1/SC 27/WG 1 Meeting 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. With the official ballot approved in August 2005, Singapore will appoint the Project Editor in the project discussion group in WG 1 to develop the "Guidelines for Information and Communications Technology Disaster Recovery Services".

4. References

- [1] "SS 507:2004: Singapore Standard for Business Continuity/Disaster Recovery Service Providers", SPRING Singapore, 2 Bukit Merah Central, Singapore 159835
<http://www.standards.org.sg>, 2004

Mr Kin-Chong Chan

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

*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 SIG², 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.

ABSTRACT

This paper informs on how Thailand implements IT security standards and its progress, based on BS 7799-2:2002. It first mentions about a 4-phase plan to strategically move the country to a better and more secure environment, which then discusses about the progress of security standards activities in Thailand.

1. IT Security Strategic Plan

In 2003, the Thai government established the Information Technology Security Committee mainly to set the strategic direction of IT security for our Internet society. As reported in the paper "Security Standard Experience and Roadmap in Thailand" published in the inaugural RAISS Forum Proceedings[1], this Committee was established to remedy the risks resulting from the need to do electronic transactions in a secure and reliable manner over the Internet. In early 2004, the Committee determined an IT security strategic plan with four phases as shown in Figure 1.

The four phases of the IT Security Strategic plan comprises:

- a. Phase 1** (3-month period): Study e-commerce categories in Thailand to see how the business and government sectors conduct e-commerce, such as the type of e-commerce involved; Business to Government (B-G); Business to Customer (B-C); and Business to Business (B-B).
- b. Phase 2** (6-month period): Study the underlying technologies that e-commerce applications are using, such as VPN, XML, and PKI.
- c. Phase 3** (3-year period): Provide security standards and guidelines as well as personnel development. The first two phases have been completed and we are now in this phase which began in 2004.

In the area of IT security standards, Thailand published her first IT Security Standard based on the BS 7799-2:2002 standard [2], with addition of local requirements. So far, we have distributed around 3,000 copies of the standard to the public.

As part of the implementation plan, we are also developing a series of guidelines, to assist businesses in understanding the base standard. The guidelines that we plan to develop include system security, e-transaction security, and network security guides.

For general users' security awareness development, we plan to increase public awareness in IT security, such as Safety Net e-learning videos. Two video scripts have already been made available on the Internet, one is on how to do e-transaction in a secure manner and the other is on how to protect against Internet Phishing attacks. A few more of such scripts are planned to be completed this year.

To improve the security knowledge and competency of IT security personnel, we are developing a series of IT security auditing courses in 2005, also based on BS 7799-2:2002 to train security auditors, IT managers, as well as other IT personnel. This is to build up more IT security personnel on auditing.

d. Phase 4 (1-year period): To establish a comprehensive national security policy, inclusive of policy for electronic transactions. This phase is target to begin development in 2007. With sufficient ground work for IT security done in the earlier phases, we will then be ready to establish the national policy to set direction for IT security in Thailand.

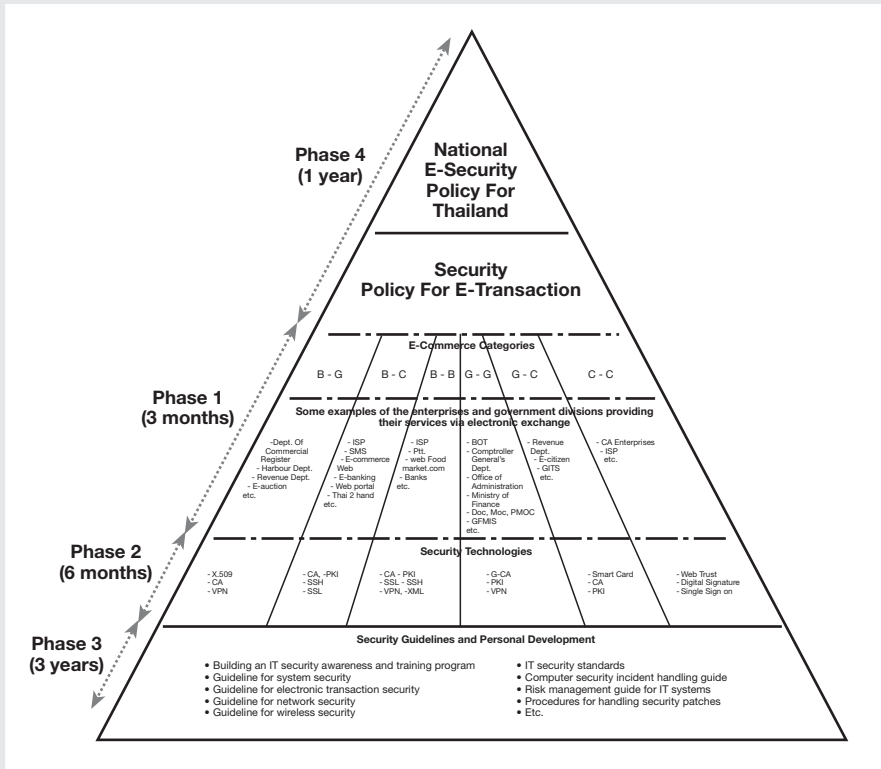


Figure 1: Thailand IT Security Strategic Plan

2. The Progress of Security Standard Activities in Thailand

Figure 2 and 3 show the updated timeline from [1] and our strategies to get the security standards implementation process completed in a few years to come.

In 2005, we aimed to conduct a series of public outreach activities to increase the level of awareness of security standards in the country, such as distributing the standards publications to the government agencies/departments (see also Figure 3). To date, the distribution is on going and progressing as per earlier plan. Between 2005 to 2007, organizations will be

encouraged to implement security standards through activities such as the provision of the public awareness building and training course. From 2007 onwards, activities will be organized to follow up and evaluate what we have done in the last few years. Examples of follow up activities are provision of security audit, security standard status evaluation, upgrade support to move up to level 2 and 3 respectively of Security Maturity Model as proposed in [1].



Figure 2: Security Standards Implementation Timeline

Year 2005	Year 2005-2007	From year 2007
<ul style="list-style-type: none"> • Distribute Thailand security standard (3,000 books) to the government sector • Arrange the security standard review meeting by IT specialists • Categorize the organizations according to the security level required 	<ul style="list-style-type: none"> • Make the National Security Policy • Make CEOs & CIOs aware of the importance of the security standard • Provide a training course on how to implement the standard (for CEOs, CIOs & IT managers) • Provide another one on how to secure all security processes (for system administrators & IT managers) • Create public awareness (E-learning, on T.V., etc) 	<ul style="list-style-type: none"> • Provide IT security audit • Survey and evaluate the status of the standard in the government sector and award to organizations with level 1 passed • Push to upgrade security level to a higher level, 2 and 3, respectively • Publicize a book about the successful organizations and their success factors as showcases for others to follow

Figure 3: Detailed Implementation Strategies

On August 4, 2005, a security standard review workshop was conducted to evaluate how the IT specialists respond to the standard book released. Around 300 participants from the

government sector attended the workshop. The standard was generally well-received and acknowledged by the public.

Many important issues were also discussed, with questions raised for further deliberation and resolution. The participants were concerned with the timeline of implementation, as well as the details of some of the controls involved. The following questions were sampled from the workshop:

- Is it likely to mandate implementation of the security standard in Thailand?
- What are the potential problems/issues relating to its implementation?
- What are the necessary criteria to classify organizations?
- How would business be affected or benefit from the implementation?
- Is it appropriate to apply the three-level standard implementation in Thailand?

3. Conclusion

The focal point in security standard implementation is to have a clearly defined strategic direction. By carrying out the activities as planned to encourage the adoption and implementation of security standards, it is hoped that many organizations in Thailand will be able to improve the level of their IT security readiness and prevent themselves from many various threats on the Internet, with a sufficient pool of security experts to help the country strengthen its current position.

4. References

[1] "Security Standard Experience and Roadmap in Thailand", Inaugural RAISS Forum Proceedings, 19 November 2004, p.78-82.

[2] BS 7799-2: 2002, Specification for Information security management systems.

Dr Komain Pibulyarojana

*Head of National Security Section
National Electronics and Computer Technology Centre (NECTEC)
Ministry of Science and Technology*

*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). 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

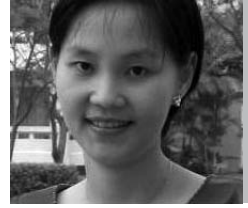
*Head
Security Standard Research and Development (SSRD) Division
Thai Computer Emergency Response Team (ThaiCERT)
National Electronics and Computer Technology Centre (NECTEC)
Ministry of Science and Technology*



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 Centre (NECTEC)
Ministry of Science and Technology
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 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 Centre (NECTEC)
Ministry of Science and Technology*



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