



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



# PROJECT DISCUSSION

# Discussion On The Way Forward For Projects And Future Of The RAISS Forum

This discussion session intended to re-look into every project that were initiated during the previous two meetings. The project status and how it should progress were being discussed.

Those present in this discussion were:

1. Mr Meng-Chow Kang, Co-Chair, Singapore
2. Mr Koji Nakao, Co-Chair, Japan
3. Ms Yean-Lan Thay, Secretariat, Singapore
4. Dr Perry Liu, Chinese Taipei
5. Mr Hiroshi Takechi, Japan
6. Ms Miho Naganuma, Japan
7. Prof Heung-Youl Youm, South Korea
8. Mr Dae-Yong Byun, South Korea
9. Mr Sung-Yong Lee, South Korea
10. Prof Pauline C. Reich, invited guest from Waseda University, Japan

## (A) Project Discussion

### 1) Security Standards Toolkit

The aim of this project is to address the issue of information sharing and dissemination especially to the Asian economies with neither formal organizations nor special interest groups to keep tap of security standards developments and adoption. Inputs were gathered from Chinese Taipei, Malaysia, South Korea, Thailand and Singapore. Further inputs would be needed from the rest of the participating economies to make it complete.

Mr Kang informed the meeting that inputs were gathered from Australia and New Zealand, awaiting inputs from Japan before this toolkit could be published as a document under the RAISS Forum.

### 2) Business Continuity Management

During the previous meeting, Malaysia had volunteered to lead in the discussion and development of guidance document in this area but no draft was submitted. Hence, no discussion on this project was able to be done at the meeting. Members felt that this topic is an important topic and would be a good discussion item in ISO/IEC JTC 1/SC 27/WG 4, the new working group focusing on Security Controls and Services. It was highlighted that under ITU-T study group 16 (SG16) Question 25 (Q 25), similar work which is known as

disaster recovery/emergency response was started to identify incidents in the telecommunication sector. The meeting then agreed to rename this project to Information and Communications Technology (ICT) Business Continuity/Disaster Recovery (BC/DR) & Emergency Readiness to look into ICT readiness for BC/DR emergency response.

### 3) Application Security Standard

Mr Kang updated that Singapore is pursuing this standard as one of the priority work item, and will try to get the standards available in the area of a) process and b) tools and techniques such as threat modeling tool and techniques. An improved version has been circulated with an important addition of a policy framework. This work item could potentially become one of the work item in SC 27/WG 4, and the inputs were sought from the member economies. It was suggested to indicate the target users for different sections within this document, and it would be established as a guidance document in the RAISS Forum for contribution towards the work in SC 27/WG 4.

Prof Youm highlighted the importance of input validation and data protection for developers, and informed that ITU-T has a guide on security development. Dr Liu felt that this document is unique because it is meant for software developers, and is in line with the software development life cycle (SDLC). He suggested including information on secure engineering.

Mr Nakao opined that the term application security is broad and felt that the current draft tries to put in all the content. He suggested having part 1 of the standard focusing on architecture/framework/model on application security, and the subsequent parts each conceiving more details catered to the different users, such as the developers, management, end-users, etc.

The meeting agreed to structure the standards as follows:

- Part 1** Overview, concept, principles, general categorization, and a brief overview of the remaining parts of the standards
- Part 2** Secure development process
- Part 3** Secure application architecture
- Part 4** Protocols and layer structure related to data/processes and output
- Part 5** Specific environment like web-application, also applying part 1 to 4
- Part 6** Client-Server platform/bulky application coded on platform
- Part 7** Assurance

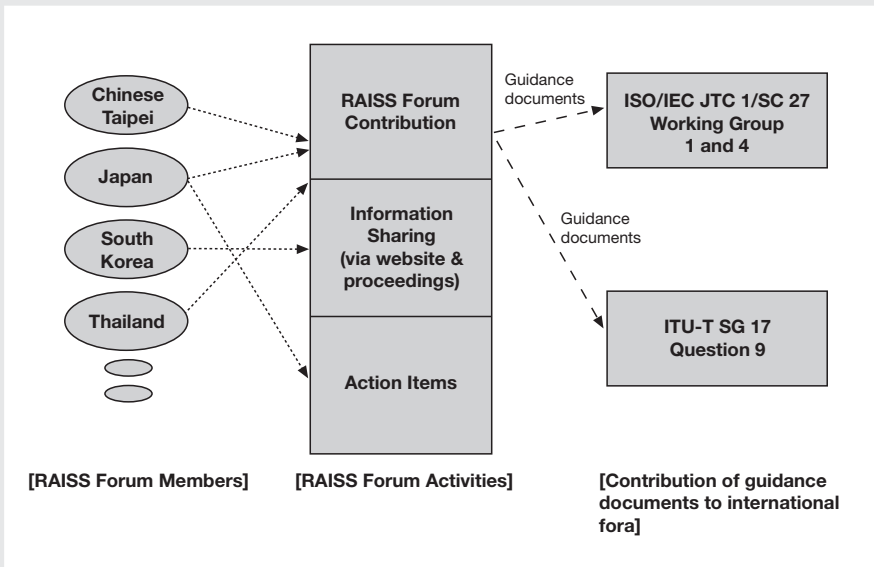
**(B) Future of the RAISS Forum**

**1) Publications**

For the publication of the RAISS Forum proceedings and guidance document, future copies will be produced in softcopy format, allowing interested parties to download from the websites.

**2) Alignment of RAISS Forum Work with Other International Fora**

The topic of aligning RAISS Forum work with other international fora such as JTC 1/SC 27 and ITU-T was discussed. In general, the meeting felt that it would be good to contribute guidance documents delivered at the Forum to SC 27.



**Figure 1:** Overview of aligning RAISS Forum with International Fora

Figure 1 shows an overview of how the RAISS Forum could contribute to the international fora such as SC 27 and ITU-T. With participating economies sharing ideas, knowledge and contributions at the RAISS Forum, guidance documents produced could contribute to SC 27/WG 4 or ITU-T to bridge their gaps and use as base documents to initiate new work items. Members felt that the Forum could generate a toolbox of technology and/or standards

where we could contribute mature content to international platform as they have already been supported by the Asia Pacific countries. Where possible, it would be good to have common standards for the Asia Pacific region for mutual recognition.

In general, members felt and concurred that this Forum is a good platform to:

- Bridge the gap between ITU-T and JTC 1/SC 27;
- Explore possibility of helping out security related experiments and project implementation, and develop deployment guidelines and standards;
- Share best practices and guidance amongst the economies; and
- Meetings will proceed if there are at least four participating economies attending the meeting.

### **3) Reaching Out to Developing Economies**

Dr Liu suggested perhaps the Forum should consider how to reach out to the developing economies such as Indonesia and Vietnam. Mr Kang updated that he has been sharing the Forum proceedings and progress of IT security standardization with the government officials of emerging economies like Cambodia, Vietnam and Indonesia but the challenges for these economies are the lack of budget for traveling to attend meetings. Collaboration opportunity has also been explored with another association but the association has its own agenda to drive and hence, organizing RAISS Forum meeting with their activities might give the audience the wrong impression that the RAISS Forum subsumes under that association. The collaboration was henceforth not possible.

### **4) Technology Sharing**

Mr Nakao informed that Japan would like to share the incident monitoring system to collect more information and report from the region, such as how each economy implement the sensor network and monitor the security attacks. Mr Kang added that this would be good for collaboration to derive some guidance document on the deployment of sensors and collection of data, and it is also beneficial for the Computer Emergency Response Team (CERT) community. This work will be discussed in detail during the next meeting.



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



# APPENDIX

### **Meng-Chow Kang**

#### **1. Introduction**

Although ISO/IEC, ITU, and other international standards bodies have been in operation for many years, regional economies in Asia, except for a few developed nations like Australia, Japan, and Korea, have mainly been the adopters of international security standards. As many regional economies are also new in the security standards arena, and not in the main or core participants or contributors to the development of existing international security standards, they all face unique challenges in various aspects of adoption and deployment.

Regional economies also face challenges in establishing security standards bodies, cultivating industry involvement and participation, and promulgating knowledge and use of international security standards within their economy, especially when there is limited local security expertise that is familiar with security standards, as well as standards development and deployment.

There are potential benefits or values that we could develop and share across the region, if regional economies begin to share their knowledge, expertise, and more importantly experiences in the area of international security standards adoption and deployment. Emerging economies and new security standards bodies could immediately benefit from the experiences, and eliminate wastages in terms of repeating mistakes and errors that other more matured bodies have gone through previously. Similarly, from a regional perspective, the aggregated learning and experiences could potentially be useful for identifying new directions and needs in security standards development in the international standards communities.

#### **2. Objectives**

The Regional Asia Information Security Standards (RAISS) Forum is therefore proposed to reap the potential benefits and values through regional security standards bodies' participation and collaborations.

The Forum is to act as an overall focal point for the Asian standardization community on information security issues by:

- providing a platform for sharing of knowledge, exchange of ideas and dialogues on standards related issues, challenges, and directions, in particular, relating to the adoption, deployment, and implementation of ICT related standards in the region;
- ensuring that the security-related standardization activities in Asia adequately reflect the requirements of the market constituents at a strategic level;
- providing a mechanism that could be used to follow-up on Asia policy requirements on Information Security standards issues;
- providing effective co-ordination between organizations of relevant standardization work programmes and their execution;
- ensuring Asia requirements for standards and standards work in this area are correctly interfaced with international standards activity, and standards activity in other regions, to avoid conflict or duplication of effort; and
- acting as a strategic communication interface between relevant standards authorities and agencies on international standardization related topics.

### **3. Initial Tasks**

Initially, the RAISS Forum shall:

- Organize workshops & seminars for knowledge sharing and exchange of experiences and information relating to the adoption, deployment, and implementation of standards and promulgation of standards activities in the region;
- Establish liaison with the appropriate standards bodies or authorities/agencies interested in promoting or adopting international standards;

- Consider the implementation aspects of Information Security standards to Asia countries and other relevant Asia policy institutions;
- Consider appropriate proposals to improve Asia countries usage of international information security standards;
- Provide a common view where possible related to information security international standards;
- Create a mailing list for the members to share experience and knowledge in information security standards; and
- Establish a homepage/website for the forum where reports and recommendations are published.

#### **4. Membership**

The RAISS Forum shall be open to any Asian National Standards bodies/committees/ organizations and their relevant technical groups, and to additional interested parties as specified below.

The Forum shall invite participation of stakeholder interests, including individuals representing:

- Hardware and software manufacturers/vendors;
- Information society service providers;
- Telecommunication service providers;
- Regulatory authorities in Asia;
- Research centres; and
- Academia.

## 5. Liaison Activities

The Forum may appoint electronic or physical liaisons.

## 6. Working Methods

- The initial Chair and possibly a Co-Chair will be nominated by the founding members of the Forum. Further refinement of this Terms of Reference shall consider the period of service for the various appointments in the Forum, and future method of nomination. The current Co-Chairs for the RAISS Forum are Mr Meng-Chow Kang of Singapore, and Mr Koji Nakao of Japan.
- The Secretariat shall be provided by voluntary members of the RAISS Forum, either as a permanent appointment, or follows the terms of appointment of the Chair of the Forum. The current Secretariat is Ms Yean-Lan Thay of IT Standards Committee, Singapore.
- The Forum will work on a voluntary basis.
- Physical meetings may be held as required, but full electronic working facilities shall also be arranged.
- The Forum shall work by consensus; its approved outputs should document any minority views.
- The Forum should focus on adoption of existing international standards.
- The Forum may organize open meetings or seminars on specific topics.
- The Forum role is advisory; its recommendations shall not be binding on the participating organizations.
- The Forum members are encouraged to participate in relevant international and global standardization efforts.
- The Forum shall provide a report on its activities.

## 7. Conclusion

The terms of reference detailed in this paper are essentially a framework to guide the collaboration, coordination, and execution of activities to bring the RAISS Forum forward, and ensure that the underlying objectives of the Forum could be successfully achieved. It is important that participants and members of RAISS Forum continue to maintain and update this guide to ensure its relevance and adequacy to meet the changing demands of IT security standardization, as well as the evolving needs of the Forum as it matures. It would be a failure of the Forum if these terms become the showstoppers to execution and running of the Forum. Ultimately, the knowledge and experiences shared, and open dialogues in the Forum meetings are the key deliverables that would benefit contributing and participating members.

Participation by the various economies in Asia in the initial meeting held on 22 April 2004 in Singapore and the inauguration meeting held on 19 November 2004 in Tokyo have both shown the region's recognition of the needs for such a Forum. These needs have been further confirmed at the Panel Discussion session held in Tokyo, which identified future works required for moving forward with the objectives of the RAISS Forum.

## 8. Acknowledgement

This paper was developed in conjunction with the contributions provided by Mr Ariffuddin Aizuddin of National ICT Security and Emergency Response (NISER), Malaysia. I would like to express my deepest appreciation to Mr Aizuddin for his support and contributions to make the RAISS Forum possible. Also thanks to the online members of RAISS Forum Online<sup>1</sup> who have also previously provided feedback to the earlier draft of the terms of reference, in particular, Mr John Snare of Australia, and Prof Jussipekka Leiwo of Singapore.

<sup>1</sup> The online discussion group was set up in MSN Group web site (<http://groups.msn.com/RAISSForum>) as an online forum for ongoing dialogues for coordination of RAISS related activities, as well as continuous discussion on topics relating to security standardization in the region. At the moment, membership to this online group is on invitation only.