

**RAISS Forum Proceedings (Volume 2)**

Meng-Chow Kang (Ed.)

27 - 28 June 2005

■  
SINGAPORE

## **Editor**

### **Meng-Chow Kang, CISSP, CISA**

Co-Chair, RAISS Forum

Chair, Security & Privacy Standards Technical Committee  
of the Information Technology Standards Committee, Singapore

Chief Security & Privacy Advisor, Asia Pacific Region, Microsoft

1 Marina Boulevard  
#22-01 One Marina Boulevard  
Singapore 018989

## **Contact**

### **RAISS Forum Secretariat**

c/o ITSC Secretariat  
Infocomm Development Authority of Singapore (IDA)

8 Temasek Boulevard  
#14-00 Suntec Tower Three  
Singapore 038988

Email: [nitsc@ida.gov.sg](mailto:nitsc@ida.gov.sg)

**ISBN 981-05-4022-1**

Copyright © 2005  
Printed in Singapore

### **Mr Meng-Chow Kang, CISSP, CISA Co-Chair, RAISS Forum**

**Chair, Security & Privacy Standards Technical Committee  
ITSC, Singapore**

**Chief Security & Privacy Advisor  
Asia Pacific Region, Microsoft**

Security is only as strong as the weakest link. This is one of the few security principles that many of us have learnt and used in our practices. Security weaknesses can result from many inadequacies, not just technology, but more commonly in people practices and processes. When security weaknesses are identified and left unmanaged, they become information risk. Security standards provide a means for us to close or avoid many of those known security weaknesses. They also provide a common language for improving information security communications, promoting better interoperability, and raising the bar for the perpetrators.

In a region like Asia, whereby a great diversity of culture prevails, we also see a great diversity in the area of standards development, adoption and practices. This presents many challenges as well as opportunities for us when we are addressing the issues and requirements and security standards development, adoption, and implementation relating to information security in Asia.

The RAISS Forum is a regional gathering of information security standards experts, contributors, and organizations from around the Asia Pacific region aiming at these opportunities to deal with those challenges in the region. The Forum was conceptualized in late 2003, and officially inaugurated on 19 November 2004. The Forum aims to provide a platform for standard bodies in Asia to discuss and share knowledge and experiences on issues relating to information security standards adoptions, developments, and other related activities. The Forum also provides a platform for identifying and developing security standards and other supporting activities at a regional level to fulfill the needs of Asia.

Since the first meeting that was held in Tokyo in November 2004, members of the RAISS Forum have continued to meet informally and separately in different occasions, and discussed over emails and the online forum the issues that were shared at the meeting, and follow-up actions and projects that are meaningful to the Forum members and participants. The second RAISS Forum meeting was the outcome of those ongoing dialogues.

One of the key developments in the area of information security over the past few years was the revision of the ISO/IEC 17799:2000<sup>1</sup> security standards in ISO/IEC JTC 1/SC 27 Working Group 1. In June 2005, the revision was finalized and published by ISO. This development marks a major milestone in the development of standards relating to information security management, and the revised standard offer many improvements and new opportunities to the industry and organizations in the region. The Forum members recognized the importance of this development, and with the generous sponsorship and support of Microsoft, PSB Certification<sup>2</sup>, the Singapore infocomm Technology Federation (SITF)<sup>3</sup>, and the IT Standards Committee (ITSC), Singapore<sup>4</sup>, Mr Ted Humphreys, Convenor of ISO/IEC JTC 1/SC 27/WG 1, and Dr Angelika Plate, Co-Editor of ISO/IEC 17799 Revision, we were able to organize a one-day tutorial workshop on this new revision as part of the second RAISS Forum meeting in Singapore. The workshop had more than 60 participants (from both domestic and overseas) and the feedbacks received were very positive and encouraging.

The second meeting brought together the original members of the RAISS Forum, except for Australia, which could not send a representative this time, and with the addition of South Korea, represented by Prof Heung-Youl Youm of Soonchunhyang University, and Mr Kyu-Man Ko of Korea Information Security Agency (KISA).

The meeting was opened with a keynote by Mr Humphreys and Dr Plate, which provided an update on the SC 27 activities and standards development status, and more importantly, clarity on the roadmap of

<sup>1</sup> ISO/IEC 17799:2000 - "Code of Practice for Information Security Management"

<sup>2</sup> PSB Certification - <http://www.psbcert.com/>

<sup>3</sup> Singapore infocomm Technology Federation (SITF) - <http://www.sitf.org.sg/>

<sup>4</sup> IT Standards Committee (ITSC), Singapore - <http://www.itsc.org.sg/>

SC 27/WG 1, the future development of ISO/IEC 17799:2005 and the new family of information security standards, to be numbered as part of the ISO/IEC 27000 series.

In addition to the economy updates on the respective security standards related strategies, activities, progresses, and challenges, which are reported in this proceedings, the meeting also received and discussed several project proposals from Thailand and Singapore. This includes a proposal to adapt the BS 7799 Lead Auditors training program for Network and Systems Security Administrators, a security standards toolkit to share best practices in security standards related organizations and activities, and an application security assurance framework. The Singapore Standard on business continuity and disaster recovery for service providers (SS 507) was also presented and discussed. SS 507 has been proposed as a contribution for a new work item in SC 27/WG 1, which was accepted through the formal balloting process during mid August 2005.

As in the previous proceedings, all the papers that were presented in the meeting (except for the tutorial) have been included in this publication in order to document the knowledge and information shared and extending them to other economies that could not be present at the meeting. A summary of the consensus reached and key action items identified are also included to capture the main outcome of the meeting, and serves as a basis for follow-up in subsequent meetings.

While this proceedings is being published, the third meeting is also being planned, which is scheduled to be held on 12 November 2005, in Kuala Lumpur, Malaysia. Regional security standards bodies or groups interested in joining the meeting should contact the Secretariat of the RAISS Forum via email at [nistc@ida.gov.sg](mailto:nistc@ida.gov.sg).

In a technology prevalent society that we are in today, security standards are recognized globally by both businesses and governments as a key ingredient to protect information assets and enable new business opportunities. There are, however, many challenges relating to the development and adoption of security standards due to the complexity involved in deciding standards elements and interfaces, as well as

implementing standards across the diversity of platforms and products. The lack of expertise and knowledge in the wide variety of security standards available and in development raises further challenges to governments and businesses attempting to realize the potentials of security standards. The RAISS Forum is a small but important step forward that will help to reduce the challenges through the sharing of knowledge, experiences, and resources in standards development and adoption.

The second meeting in June 2005 has achieved another important milestone in the objectives that we have set forward in the inauguration of the RAISS Forum. To realize and reap the benefits of security standards, continued supports, participations, and contributions from regional economies in Asia Pacific are critical. This includes the continued supports from the local national body and government such as ITSC, the Standards, Productivity and Innovation Board (SPRING Singapore), Infocomm Development Authority of Singapore (IDA), and the industry, that provided much of the expertise and sponsorship needed to make ongoing progress possible.

### **Acknowledgement**

As in any forums and knowledge sharing events and meetings, the desired outcome would not be achieved if not for the contribution and active participation of the members, speakers, and participants involved. I am grateful to have the generous supports of all the members, speakers, and participants who have in one way or another contributed to the success of the second meeting, as well as the speakers' follow-on work to have their presentation written for this proceedings, which would not otherwise materialize. I would also like to thank Microsoft (Asia Pacific), PSB Certification, SITF, ITSC, SPRING Singapore, and IDA for the financial and management supports rendered for organizing the Forum and publishing this proceedings. And finally, special thanks to Mr Koji Nakao (Co-Chair of RAISS Forum), and Ms Yean-Lan Thay (Secretariat of RAISS Forum), for all the efforts and hard work put into the realization of the Forum and this meeting.

## Mr Meng-Chow Kang

*CISSP, CISA  
Co-Chair, RAISS Forum, Singapore*

*Chair, Security & Privacy Standards Technical Committee  
ITSC, Singapore*

*Chief Security & Privacy Advisor, Asia Pacific Region, Microsoft*



Based in Singapore, Meng-Chow is the regional Chief Security & Privacy Advisor for Microsoft Asia Pacific region. His current responsibilities include developing and implementing Microsoft's trustworthy computing strategy in the region, and providing advice and guidance to customers and IT professionals on security best practices and solutions for implementing and managing information security in their organizations.

Meng-Chow has been a practicing information security professional for more than 18 years, with experiences spanning from technical to management in the various security and risk management roles that he has held in the Singapore government, major financial institutions, and security technology provider. His last position prior to Microsoft was Vice President and Regional Information Risk Officer of JPMorganChase.

Since 1998, Meng-Chow has also been concurrently chairing the Singapore's IT Security and Privacy Standards Technical Committee (SPSTC), representing Singapore in the ISO/IEC JTC 1/SC 27 Security Techniques Sub committee. In 2004, Meng-Chow initiated and begun co-chairing the Regional Asia Information Security Standards (RAISS) Forum. In November 2004, Meng-Chow was also appointed Associate Rapporteur of Study Group 17 (Security and Language), ITU-T focusing on addressing the Study Question relating to Cybersecurity. Meng-Chow is also a board member of the Asia Advisory Board for the International Information Systems Security Certification Consortium (ISC<sup>2</sup>).

In August 2005, Meng-Chow was presented with the accolade "IT Evangelist of the Year 2005" by the Singapore National Infocomm Competency Centre (NICC) in recognition of his work and contribution to the IT security community and standards arena. Meng-Chow was also presented the "Distinguish Award" from the Standards, Productivity and Innovation Board (SPRING Singapore) in September 2005 for his effort and leadership in shaping the IT security standardization landscape in Singapore.

Meng-Chow received his MSc degree in Information Security from the Royal Holloway and Bedford New College, University of London. He has been a Certified Information Systems Auditor (CISA) since 1997, and a Certified Information Systems Security Professional (CISSP) since 1998.

# Contents

|    |  |     |
|----|--|-----|
| 01 | <b>Program Of The RAISS Forum Workshop On ISO/IEC 17799:2005 (E)</b>   | 07  |
| 02 | <b>Agenda Of The 2nd RAISS Forum Meeting</b>   | 08  |
|    | <i>Status Update From Each Economy</i>   |     |
| 03 | <b>Chinese Taipei</b><br>IT Security Activities In Chinese Taipei<br>Perry Liu   | 10  |
| 04 | <b>Japan</b><br>Introduction And Updates On Information Security<br>Technologies Related Activities In Japan<br>Koji Nakao   | 17  |
| 05 | <b>Korea</b><br>ISMS Certification Scheme In Korea<br>Heung-Youl Youm, Kyu-Man Ko  | 28  |
| 06 | <b>Malaysia</b><br>Updates On Information Security Standards Activities In Malaysia<br>Shamsuddin Bin Abdul Jalil  | 46  |
| 07 | <b>Singapore</b><br>Standards Updates From Singapore Including Development<br>Of A New Business Continuity And Disaster Recovery Standard<br>Kin-Chong Chan                        | 50  |
| 08 | <b>Thailand</b><br>Thailand Status Update On IT Security Standards And Implementation<br>Komain Pibulyarajana, Banchong Harangsri, Siriwan Apisiridej,<br>Doungkamol Suppitayakorn | 61  |
|    | <i>Other Contribution</i>  |     |
| 09 | <b>Security Standardization In ITU-T</b><br>Koji Nakao, Meng-Chow Kang   | 68  |
| 10 | <b>An International Common Language For Information Security</b><br>Ted Humphreys, Angelika Plate  | 76  |
|    | <i>Proposals</i>   |     |
| 11 | <b>Building Synergy And Collaborating Towards Improving Security<br/>Standardization in Asia Pacific Region - Project Proposal And Discussion</b><br>Meng-Chow Kang                | 86  |
| 12 | <b>Modified Risk Assessment Using A New Logical Way Of Thinking</b><br>Komain Pibulyarajana, Banchong Harangsri, Siriwan Apisiridej,<br>Doungkamol Suppitayakorn                   | 96  |
|    | <i>Appendix</i>  |     |
| 13 | <b>Appendix A: 2nd RAISS Forum Meeting - Summary Notes</b>   | 110 |
| 14 | <b>Appendix B: Terms Of Reference</b>  | 113 |

# 01

## Program Of The RAISS Forum Workshop On ISO/IEC 17799:2005 (E)

**27 June 2005, Monday, Orchard Hotel, Singapore**

This workshop is jointly organized by the Regional Asia Information Security Standards (RAISS) Forum, IT Standards Committee (ITSC) and the Security Chapter of the Singapore infocomm Technology Federation (SiTF). It aims to inform about the changes between ISO/IEC 17799:2000 and the new ISO/IEC 17799:2005 (E) published during mid June 2005, the drivers behind this new standard, certification aspects and future trends in ISMS standardization.

### Instructors

- Mr Ted Humphreys  
Chartered Fellow of BCS CITP, CISM  
Chair of ISO/IEC JTC 1/SC 27 WG 1
  
- Dr Angelika Plate  
Co-Editor of ISO/IEC 17799:2005 and Editor of ISO/IEC 27003

### Program

| Time               | Topic   |
|--------------------|---|
| 0830hrs to 0900hrs | Registration  |
| 0900hrs to 0930hrs | Introduction <ul style="list-style-type: none"><li>- History</li><li>- Background and drivers for the revision</li><li>- Overview: Content and Structure</li></ul>  |
| 0930hrs to 1030hrs | 17799 GAP ANALYSIS - OLD versus NEW<br>The Changes - Clauses 5 to 7   |
| 1030hrs to 1100hrs | Tea-Break   |
| 1100hrs to 1230hrs | 17799 GAP ANALYSIS - OLD versus NEW<br>The Changes - Clauses 8 to 10  |
| 1230hrs to 1330hrs | Lunch   |
| 1330hrs to 1500hrs | 17799 GAP ANALYSIS - OLD versus NEW<br>The Changes - Clauses 11 to 15   |
| 1500hrs to 1530hrs | Tea-Break   |
| 1530hrs to 1700hrs | FUTURE ISMS WORLD <ul style="list-style-type: none"><li>- ISO/IEC 27001 (ISO version of BS 7799 Part 2)</li><li>- Certification Transition Statements</li><li>- ISO 27000 series of standards</li><li>- EA 7/03 and other certification aspects</li></ul> |

# Agenda Of The 2nd RAISS Forum Meeting

**28 June 2005, Tuesday, Orchard Hotel, Singapore**

**Morning: 0900hrs to 1200hrs**

**Session Chair:**

**Mr Meng-Chow Kang, Singapore**

**Co-Chair of RAISS Forum**

- Welcome and opening followed by review of minutes, action items, and proceedings of first meeting
  - by Mr Koji Nakao and Mr Meng-Chow Kang, Co-Chairs of RAISS Forum
  
- Keynotes address
  - by Mr Ted Humphreys, Convenor, ISO/IEC JTC 1/SC 27/WG 1
  - and Dr Angelika Plate, Co-Editor, ISO/IEC 17799:2005 (E)
  
- Outcome and action items from ISO/IEC JTC 1/SC 27 Plenary and Working Groups meetings held in Vienna, Austria, 11 to 19 April 2005
  - by Mr Ted Humphreys
  
- Updates from participating member economies [Part I]
  - Chinese Taipei
  - Japan
  - Korea

**Afternoon: 1300hrs to 1800hrs**

**Session Chair:**

**Mr Meng-Chow Kang, Singapore**

**Co-Chair of RAISS Forum**

- Updates from participating member economies [Part II]
  - Malaysia
  - Thailand
  - Singapore

- New project discussion [Part I]
  - Update on Singapore's BC/DR new work proposal in SC 27
    - by Mr Kin-Chong Chan
  - Outcome and action items from ITU-T SG 17 Security Study Groups meetings held in Moscow in April 2005 - Solicitation of papers/contributions to ITU-T Security Symposium to be held in Geneva in Q4/2005
    - by Koji Nakao
  - Collaboration with ThaiCERT - A proposed co-research project together with ThaiCERT to produce training course materials for technical and management personnel in Thailand to improve their security level based on the security standards, by Dr Banchong, ThaiCERT, National Electronics and Computer Technology Center (NECTEC)
  
- New project discussion [Part II]
  - New project proposal on "Security Standards Toolkit"
    - by Meng-Chow Kang
  - Any Others
  
- Review of the RAISS Forum Terms of Reference
  - By Meng-Chow Kang
  
- Tentative schedule and draft agenda for next meeting
  - Date: 12 November, Saturday
  - Venue: Kuala Lumpur, Malaysia, in conjunction with SC 27 working groups meetings
    - All participating members
  
- Any other business