

JOINT SPSTC-RAISE FORUM SEMINAR

10 March 2010

Singapore Security Standards Projects

RAISE
Regional Asia Information
Security Exchange **FORUM**

Chan Kin Chong

Chair, Security & Privacy Standards
Technical Committee, Singapore

RAISE
Regional Asia Information
Security Exchange **FORUM**

Security & Privacy Standards Technical Committee (SPSTC)

Background

Established in 1999 as one of the Technical Committees under the Singapore IT Standards Committee (ITSC).

Objective

To promulgate the development and adoption of information security and privacy standards in Singapore, by evaluating the relevant ISO and other international or national standards for adoption and use in Singapore, and support the development of new standards where necessary or applicable to the advancement of the information security and privacy domains in Singapore.

Strategic Thrusts

- Active Participation
 - Develop or participate in the development of new standards in the relevant areas of information security and privacy technology, at both the national level as well as the international level by active participation in international forums including SC 27 and RAISE Forum.
- Awareness
 - Promote the adoption of standards, by organising activities and events and publishing articles on information security and privacy standards.

Security & Privacy Standards Technical Committee (SPSTC)

Organisation

- Chair: CHAN Kin Chong (JPMorgan Chase Bank, N.A.)
- Secretary: HO Kee-Vin (Protiviti)
- Members: Subject matter experts and representatives from the industry, government bodies, academia and research institutes

Working Groups

- WG4 ▪ Business Continuity/Disaster Recovery (BC/DR) WG – led by LAU Soon Liang (NETS)
- WG4 ▪ ICT Readiness on Business Continuity Management JWG – led by LAU Soon Liang (NETS), ONG Liong Chuan (SP Powergrid)
- WG1 ▪ Information Security Management Standards (ISMS) WG – led by Philip SY (e-Cop)
- WG4 ▪ Security Controls & Services (SCSS) WG – led by HOO Chuan Wei (BT Singapore)

Specialists

- WG2 ▪ Cryptography – Dr BAO Feng (I2R), HEE Juay Guan (DSTA), LIN Yih (DART)
- WG5 ▪ Privacy Technology – Lawrence TAN (IDA)
- WG3 ▪ Security Assurance – Albert PICHLMAIER (IDA)

International Standards Development

ISO/IEC JTC 1/SC 27 Activities

Working Group 4

- **ISO/IEC 27031: Guidelines for ICT Readiness for Business Continuity**
 - Based on SS 540: Singapore Standard for Business Continuity Management (BCM)
 - Project Overview:
 - Provide a framework on the impact of ICT in ensuring business continuity for any organisation – private, governmental, and non-governmental.
 - Identify and specify all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organisation's ISMS, helping to ensure business continuity.
 - Enable an organisation to measure its continuity, security and hence readiness to survive a disaster in a consistent and recognised manner.
 - Project Co-Editors: Ron Miller (GB), ONG Liong Chuan & Philip SY (SG)
 - Status: Final committee draft (FCD), aiming to be published as International Standard in 2010

International Standards Development

ISO/IEC JTC 1/SC 27 Activities

Working Group 4

■ **ISO/IEC 27032: Guidelines for Cybersecurity**

■ Project Overview:

- Define Cybersecurity, or security of the Cyberspace, viz-a-viz Internet security, network security, critical information infrastructure protection, etc. which are already addressed in other standards and initiatives.
- Provide guidance to address issues arising from the gaps between the different security domains in the Cyberspace environment.
- Provide an infrastructure for collaboration between security stakeholders in the Cyberspace – both consumers and providers.
- Identify common Cybersecurity issues/risks and provide guidance on the controls to address these issues/risks.
- Provide a framework for information sharing, coordination and incident handling.

■ Project Co-Editors: Aloysius CHEANG (SG), Koji NAKAO (JP)

■ Status: First committee draft (CD)

International Standards Development

ISO/IEC JTC 1/SC 27 Activities

Working Group 2

■ **ISO/IEC 29192: Lightweight Cryptography**

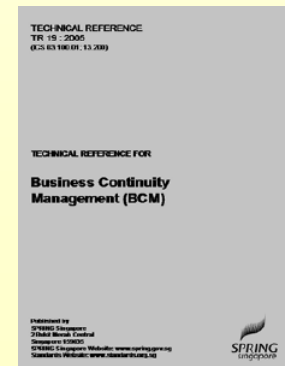
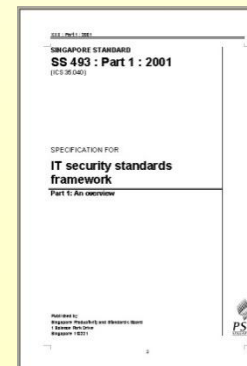
- At the Nov 2009 SC 27/WG 2 meeting in Redmond, resolution to develop ISO/IEC WD 29192 (working draft) into multi-part standard and call for contributions (CFC):
 - Part 1: General
 - Part 2: Block ciphers
 - Part 3: Stream ciphers
 - Part 4: Mechanisms using asymmetric techniques

- In response to the CFC, researchers at the Singapore *Institute for Infocomm Research (I2R)*, Dr Zhou Jianying, Dr Joseph Liu, et. al. submitted a proposal for ISO/IEC 29192 Part 4:
 - Address the need for extreme efficiency in situations where power, computational and memory/storage resources are severely limited (e.g. wireless sensor network).
 - Provide an identity-based signature (IBS) scheme using lightweight and power-saving cryptographic algorithms without the need for full Public Key Infrastructure (PKI) implementation delivering improved security on top of symmetric key cryptography.
 - Allow multi-time re-use of offline storage of pre-computed information.

Singapore Standards Development

Published Singapore Security Standards

- SS 493 : 2001: IT Security Standards Framework
- SS 501 : 2003: PKI Security Standards – Framework Overview
- SS 507 : 2008: Standard for Business Continuity/Disaster Recovery Service Providers



Standards Events

Seminars and Workshops

- Oct 27, 2009: *International Standards for Information Security Seminar*
 - Track 1: Standards for Information Security Management
 - Track 2: Standards for Information Security Management
 - Track 3: Applied Common Criteria - Evaluation Aspects
 - Workshop on Common Criteria

- Oct 28, 2009: *Writing a Security Target (ST) - The first step towards successful Common Criteria certification Workshop*

| Time | Title | | |
|----------------------|--|---|---|
| Day 1: 27/10/2009 | | | |
| 08:30 - 09:00 | Registration | | |
| 09:00 - 09:15 | Welcome Message by Mr Ho Kee-Vin, Secretary, Security & Privacy Standards Technical Committee (SPSTC) and Manager, Protiviti | | |
| 09:15 - 09:30 | Keynote Address: IT Standardisation in Singapore by Mr Robert Chew, Chairman, IT Standards Committee (ITSC) | | |
| 09:30 - 10:15 | International Security Standards Development by Mr Chan Kin Chong, Chair, SPSTC and Information Risk Manager, JP Morgan Chase Bank, N.A. | | |
| 10:15 - 10:45 | Morning Refreshments | | |
| 10:45 - 11:15 | Japanese Activities for Standardisation by Mr Sakuma Yasuhiro, Japanese Industrial Standards Committee (JISC) and Assistant Director, Ministry of Economy, Trade and Industry (METI) | | |
| 11:15 - 12:00 | Revision of ISMS Standards ISO/IEC 27001 & 27002 by Mr Philip Sy, Chair, ISMS Working Group, SPSTC and Principal Consultant, e-Cop.net | | |
| 12:00 - 13:15 | Lunch-break | | |
| 13:15 - 16:00 | Track 1 | Track 2 | Track 3 |
| | 13:15 - 13:30 Track One Introduction by Mr Philip Sy, Chair, ISMS Working Group, SPSTC and Principal Consultant, e-Cop.net | 13:15 - 13:30 Track Two Introduction by Mr Hoo Chuan Wei, Chair, SCSS Working Group, SPSTC and Security Information Officer, Business Continuity, Security & Governance Practice, BT Singapore | 13:15 - 13:30 Track Three Introduction by Mr Albert Pichlmaier, Member, SPSTC and Technical Manager, IDA Certification Body (SCCS) |
| | 13:30 - 14:15 ISMS Working Group Updates by Mr Philip Sy, Chair, ISMS Working Group, SPSTC and Principal Consultant, e-Cop.net | 13:30 - 14:15 International Disaster Recovery Standard (ISO/IEC 24762) by Mr Ahmad Nizari, Member, BC/DR Working Group, SPSTC and Vice President, Citi Business Continuity Services | 13:30 - 14:15 Principles of Common Criteria (ISO/IEC 15408) & CCRA by Mr Albert Pichlmaier, Member, SPSTC and Technical Manager, IDA Certification Body (SCCS) |
| | 14:15 - 15:00 Measuring Information Security Performance (ISO/IEC 27004) by Mr Philip Sy, Chair, ISMS Working Group, SPSTC and Principal Consultant, e-Cop.net | 14:15 - 15:00 Towards an International Standard for Cybersecurity (ISO/IEC 27032) by Mr Aloysius Cheang, Project Co-Editor, ISO/IEC 27032 Guidelines for Cybersecurity and Member, SPSTC | 14:15 - 15:00 Security Target - The Key Requirements Document Part 1 by Mr Albert Pichlmaier, Member, SPSTC and Technical Manager, IDA Certification Body (SCCS) |
| | 15:00 - 15:15 Afternoon Refreshments | 15:00 - 15:15 Afternoon Refreshments | 15:00 - 15:15 Afternoon Refreshments |
| | 15:15 - 16:00 Challenges in Information Security Risk Management (ISO/IEC 27005) by Mr You Cheng Hwee, Member, ISMS Working Group, SPSTC and Director of Consulting | 15:00 - 15:15 Afternoon Refreshments | 15:15 - 16:00 Common Criteria Evaluation |

Standards Events

Seminars and Workshops

- March 10, 2010: *8th RAISE Forum Joint Seminar on Regional Information Security Development*
- Monthly Information Security Talks
 - Joint collaboration with Association of Information Security Professionals (AISP)
 - Starting from April 2010, launch first series of monthly ISO/IEC 27001 talks that combine practical business examples and case studies to provide participants with practical insights on how to plan, design, implement and audit an ISMS
- Host for JTC 1/SC 27 Plenary and WG meetings in Spring 2011, Singapore



Thank You!

Kin-Chong Chan, CISSP, CISA, MAISP

- Chair, Security & Privacy Standards Technical Committee (SPSTC), Singapore – <http://www.itsc.org.sg>
- Executive Council Member, Association of Information Security Professionals (AISP) – <http://www.aisp.sg>
- Vice President, Information Risk Management, JPMorgan Chase Bank, N.A.

Email: kin.chong.chan@jpmorgan.com
chan.kin.chong@aisp.sg

