

ISMS Working Group Updates

Presented by: Philip Sy



.....
An industry partnership supported by IDA Singapore and SPRING Singapore

Topics

- ICT Security Standardization
- Active projects in SC27 WG1



Security & Privacy Standards Technical Committee

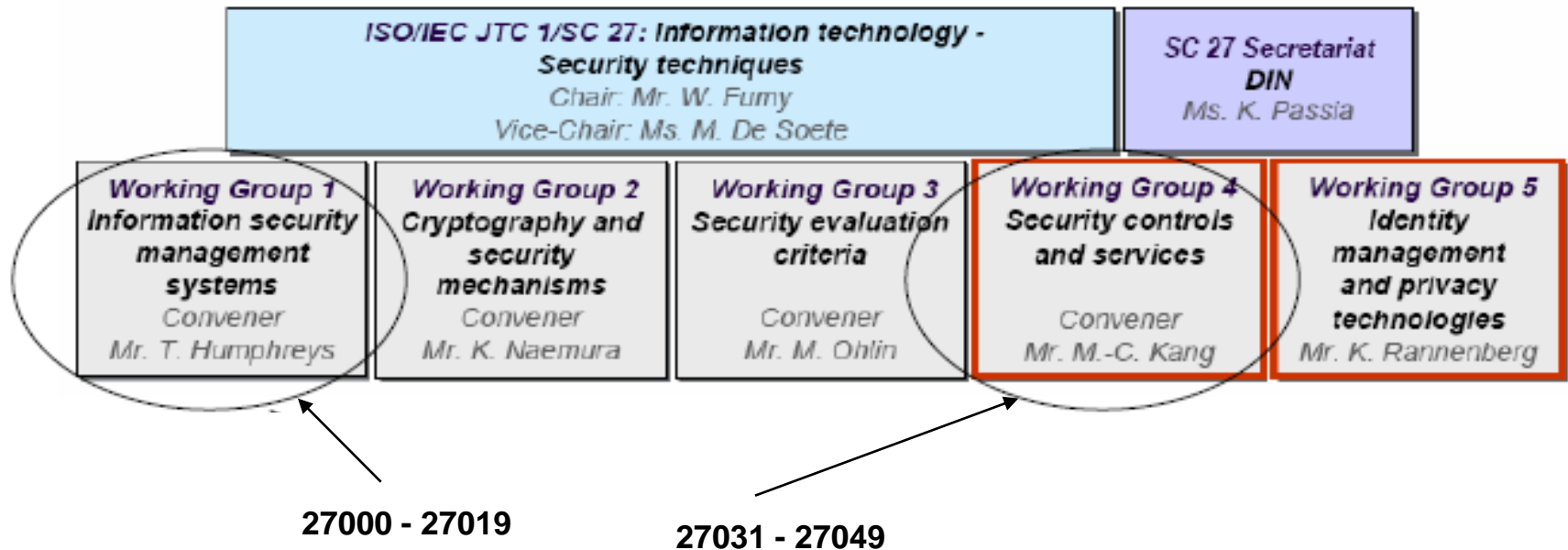
- one of TC under ITSC
- security and privacy standardization
- promote the awareness, development and adoption of security and privacy technology standards
- represent Singapore on SC27 participation



.....
An industry partnership supported by IDA Singapore and SPRING Singapore

ISO/IEC JTC1 SC27

- primary resource for international standards on IT security techniques



Security & Privacy Standards Technical Committee

- ISMS (Information Security Management Standards) WG mirroring SC27 WG1
- Cryptography WG mirroring SC27 WG2
- Security Assurance WG mirroring SC27 WG3
- SCSS (Security Controls & Services) WG mirroring SC27 WG4
- Privacy Technology WG mirroring SC27 WG5



Topics

- ICT Security Standardization
- Active projects in SC27 WG1



WG1 Scope

- Development and maintenance of the ISO/IEC 27000 ISMS standards family
- Identification of requirements for future ISMS standards and guidelines
- On-going maintenance of WG1 standing document SD WG 1/1 (WG 1 Roadmap)
- Collaboration with other Working Groups in SC 27, in particular with WG 4 on standards addressing the implementation of control objectives and controls as defined in ISO/IEC 27001



Type of Standards

Type A – Vocabulary Standard

Type B – Requirements Standard

Type C – Guidelines Standard

Type D – Related Standard



ISO/IEC 27000 Vocabulary Standard – Information security management system – Overview and vocabulary (Type A)

- overall framework of a systematic vocabulary and a set of the fundamentals, with the terms and definitions to be commonly used in WG 1 related standards .



ISO/IEC 27001 – Information security management systems – Requirements (Type B-1)

- requirements standard
- core of the ISMS related standards family
- certifiable standard
- provides a means for organizations to provide assurance to relevant stakeholders on their information security management
- First published in 2005
- Currently under revision



ITSC Seminar 2009 – ISMS track – Measuring Information Security Performance
**ISO/IEC 27006 – Requirements for bodies providing audit and
certification of information security management systems
(Type B-1)**

- specifies requirements and provides guidance for bodies providing audit and certification of an Information Security Management system (ISMS)
- in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001.
- for accreditation of certification bodies providing ISMS certification scheme.
- first published in 2007



ISO/IEC 27002 – Code of practice for information security management (Type C-1)

- previous ISO/IEC 17799 renumbered
- overall guidelines standard on the implementation of information security controls
- directly supports ISO/IEC 27001



ISO/IEC 27003 – Information security management systems implementation guidance - under development (Type C-1)

- guideline standard supporting ISO/IEC 27001
- providing guidance material pertaining to the Plan-Do-Check-Act (PDCA) model
- providing independent guidance as to how organizations should select information security controls from “Controls” listed in ISO/IEC 27002
- how an organization can improve implemented controls with consideration of changing circumstances.
- FDIS stage



ISO/IEC 27004 – Information security management measurements - under development (Type C-1)

- guideline standard
- provides the ability to effectively measure, through metrics, of the level of success of the implemented controls and processes from the ISO/IEC 27001
- FDIS stage



ISO/IEC 27005 – Information security risk management - under development (Type C-1)

- gives guidelines for information security risk management
- addresses principles of information security risk management, and methods for risk assessment, risk treatment and acceptance, risk communication, and risk monitoring and review
- giving further information on how to address the requirements ISO/IEC 27001.
- Published in 2008



ISO/IEC 27007 – ISMS Auditor Guidelines – (Type C-

1)

- giving guidance on ISMS audits
- support ISO/IEC 27006 and the generic auditor guidance provided in ISO/IEC 19011



Sector specific standard (Type C-3)

- **ISO TR 13569 – Banking and related financial services – Information security guidelines - Published**
 - giving guidance on ISMS audits
 - support ISO/IEC 27006 and the generic auditor guidance provided in ISO/IEC 19011
- **ISO/IEC 27799 – Health informatics -- Security management in health using ISO/IEC 17799 - under development**
- **Information security management guidelines for telecommunications**
- **ISMS Standards for the World Lottery Association**
- **ISMS Standards for the Automotive Industry**



Task of ISMS WG

- Ballot, comment and contribute for WG1 standards
- Promote the adoption of ISMS standards
- Identify and develop any relevant SS standards



Thanks

(for more information, you can contact Philip Sy at spstc_psy@yahoo.com)



.....
An industry partnership supported by IDA Singapore and SPRING Singapore