

International ICT Security Standards — ISMS and Security Controls and Services Standards

Walter Fumy

Chair, ISO/IEC JTC 1/SC 27 – Security techniques

Meng-Chow Kang

Convener, Security Controls and Services Working Group, ISO/IEC JTC 1/SC 27

Chief Security Advisor, Microsoft Greater China Region

Introduction

Security standards, while not a panacea, play a crucial role in helping practitioners and managers to work with the complexity of today's technology and business environment and manage the competing challenges involved in managing information and related risks. They provide the baseline for managing known security issues and risks, and are essential as a common language for people, organization, and systems to communicate and interoperate, and come to a common understanding of the requirements and agreement for suitable solutions and actions. In addition, studies have established positive economic contribution of standardization to national gross domestic product (GDP) [1].

However, not all questions relating to information security have an answer in security standards today as well. This therefore presents many opportunities for new knowledge to be developed and contributed to the information security and related standards arena.

There are a number of organizations developing and promoting the use of standards worldwide. ISO is a federation of national standards bodies from 157 countries and economies, one from each country or economy. It has 3,093 technical bodies, including 201 technical committees, 542 subcommittees, and 2,287 working groups. ISO's works result in international agreements that are published as International Standards (IS). As of 2007, there are 17,041 standards and standard-type documents published, including 1,105 (57,477 pages) published in 2007.

This article introduces the standards activities of ISO/IEC JTC 1/SC 27¹, and provides an overview of the standards projects in development, focusing on the work of WG 1 on information security

¹ The International Organization of Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly setup the Joint Technical Committee 1 (JTC1) to look into Information and Communication Technology (ICT) standardization. Subcommittee 27, or in short, SC 27, focuses on ICT Security Techniques.

management system (ISMS) standards, and WG 4 on information security controls and services standards.

ISO/IEC JTC 1/SC 27

In early 1990, ISO/IEC JTC 1 formed Sub-committee 27 (SC 27) with 18 national bodies as founding members to focus on the development of standards for the protection of information and ICT. Since then, SC 27 has been a center of security expertise and developed numerous standards that have been widely used in the industry. SC 27 membership has also grown to 51 national bodies (37 “Participating” (P) and 14 “Observing” (O) members).² The scope of SC 27’s development covers a wide range of standards including generic methods, techniques, and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security, in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms;
- Security management support documentation including terminology and guidelines;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security; and
- Security evaluation criteria and methodology.

From 1990 to 2005, SC 27 was organized with three working groups, focusing on information security management, cryptographic and security mechanisms, and security evaluation and assurance related standards, respectively. In April 2006, at the 17th Plenary meeting in Madrid, SC 27 finalized its re-organization with the addition of two new working groups, namely, security controls and services, and identity management and privacy technology, including the security of biometrics. The addition of the new working groups are to ensure adequate coverage of standards needs by the industry to address new requirements resulting from the proliferation of new ICT systems, and the Internet.

Figure 1 depicts the organization of SC 27, and the officers who are currently appointed in the sub-committee and the respective working groups.

² “P” members have voting rights, whereas “O” members may contribute and comments but have no voting rights. As of April 2008, the Participating members are: Australia, Austria, Brazil, Belgium, Canada, China, Costa Rica, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Italy, India, Japan, Kazakhstan, Kenya, Korea, Luxemburg, Malaysia, Netherland, New Zealand, Norway, Poland, Russian Federation, South Africa, Singapore, Spain, Sri Lanka, Sweden, Switzerland, UK, Ukraine, Uruguay, US, and Venezuela; Observing members are: Argentina, Belarus, Estonia, Hong Kong, Hungary, Indonesia, Ireland, Israel, Lithuania, Romania, Serbia, Slovakia, Thailand, and Turkey.

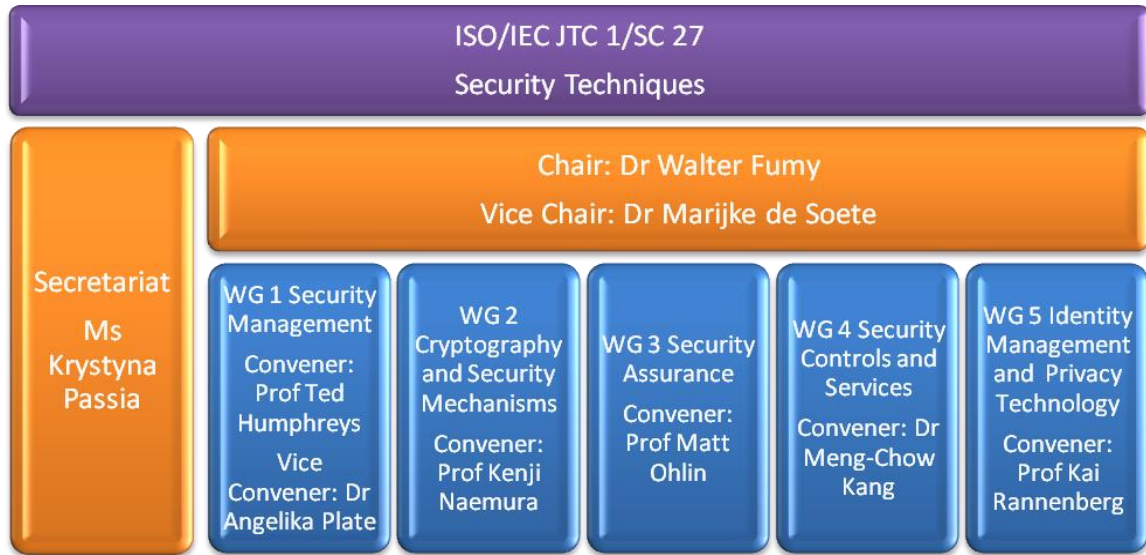


Figure 1: SC 27 Organization and Officers

Current Activities

The SC 27 working groups meet for one week once in every six months, in one of the 51 member country whereby national bodies' comments and input to standards projects are deliberated and resolved, and new proposals are studied. Between these meetings, project editors (appointed through the former process of national bodies' contribution and balloting) work on respective drafts of the standards within specific timeline for national bodies' comments and input before each meeting.

The sub-committee holds its two-day plenary meeting annually, in conjunction with the working group meetings in spring each year to review the project status, approve or disapprove the elevation of project status (from initial study proposal to final draft international standard), and deliberate on other related administrative and technical issues as they arise. Between these meetings, working groups and project editors may also hold ad-hoc workshop and meetings to deliberate specific topic of interest or work on specific standard project amongst members and/or other organizations (for example, ITU-T).

The sub-committee and each working group within SC 27 further establish formal liaison with other standards-related organizations and associations worldwide, as a form of collaborative partnership. The goals of these liaisons are (1) to ensure maximum participation and collaboration among all relevant parties to achieve broad consensus and globally applicable standards; (2) to optimize the use of limited resources so as to ensure cost effectiveness, maximize use of available standards, and improve ability to support the ever growing demand for standardization; and (3) to improve the outreach of deliverables, extending their use in additional context and at the same time improving overall recognition of specific standards.

Information Security Management Standards

The scope of work involved in information security management related standards span across both WG 1 and WG 4. WG 4 was in fact created in order to reduce the work load of the previous WG 1, and undertake new projects on areas that could be developed in parallel with the projects in WG 1 in order to accelerate the development process involved and better manage the limited resource available.

The scope of WG 1 covers the development and maintenance of the ISO/IEC 27000 family of Information Security Management System (ISMS) standards and guidelines; identification of requirements for future ISMS standards and guidelines; and liaison and collaboration with organizations and committees dealing with sector-specific requirements and guidelines for ISMS, for examples, ITU-T (Telecommunications), ISO TC 215 (Healthcare), ISO TC 68 (Financial Services), ISO TC 204 (Transportation), and World Lottery Association (Gambling).

The ISO/IEC 27000 family of ISMS standards and guidelines include the following, addressing a wide spectrum of ISMS, from basic definitions to implementation and its auditing³:

- ISO/IEC 27000 – Overview and vocabulary ;
- ISO/IEC 27001:2006 – ISMS requirements;
- ISO/IEC 27002:2007 – Code of practice;
- ISO/IEC 27003 – ISMS implementation guidance;
- ISO/IEC 27004 – Information security management measurements;
- ISO/IEC 27005:2008 – Information security risk management;
- ISO/IEC 27006:2007 – Accreditation requirements;
- ISO/IEC 27007 – ISMS auditing guidance; and
- ISO/IEC 27011:2008 (ITU-T X.1051)⁴ – Information security management guidelines for telecommunications organizations.

With the wide adoption of the ISMS standards since their publication in 2005,⁵ and to meet industry- and sector-specific requirements, members of WG 1 have also initiated a number of new studies and project proposals along this line of development, such as:

- Information security governance (Study Period);
- Sector-Specific ISMS Standards for the World Lottery Association (Study Period);

³ Except for ISO/IEC 27007, which is currently in the working draft status, and ISO/IEC 27000, and 27004, which have attained Final Committee Draft (FCD) status, the rest of the family has either been published as International Standards, or attained Final Draft International Standard (FDIS) status, which will be published within the next few months.

⁴ Note the corresponding ITU-T Recommendation, which has the same contents and the IS, in which the standard was developed collaboratively between the two organizations. Note also that this standard is the first sector-specific version of ISMS that is based on ISO/IEC 27001 requirements catered for the telecommunications industry.

⁵ See ISO/IEC 27001 Certification Register at <http://www.iso27001certificates.com/>. As of May 2008, 4,139 organizations have been certified compliance with the ISO/IEC 27001 standard for ISMS.

- Information security for Critical Infrastructure – Sector-specific guidance (Study Period);
- ISM guidelines for e-government services (New work item proposal);
- Information security management: sector to sector interworking and communications for industry and government (New work item proposal); and
- Guidance for Auditors on ISMS Controls (New work item proposal).

Information Security Controls and Services Standards

In support of and extending the scope of work of WG 1, WG 4 focuses on identifying and developing requirements and standards in the areas of information security controls and services, including addressing emerging needs such as standards relating to Cybersecurity, ICT for disaster recovery services and outsourcing. The scope of work for WG 4 is structured into three areas of requirements, namely:

1. Standards for addressing the needs of new and emerging—previously **unknown**—security issues, for preparing organizations to respond to those issues, through the use of a combination of risk reduction and readiness controls and services. This includes,
 - a. ISO/IEC 27031 – ICT Readiness for Business Continuity (Working Draft);
 - b. ISO/IEC 24762:2008 – Guidelines for ICT disaster recovery services;
 - c. ISO/IEC 18043:2006 – Selection, deployment and operations of intrusion detection systems (IDS);
 - d. ISO/IEC TR 18044:2002 – Information security incident management. In the April 2008 meeting, the working group has further proposed that this technical report be revised and elevated to become an IS; and
 - e. ISO/IEC 27032 – Guidelines for Cybersecurity (Working Draft).

To support the implementation of TR 18044 and ISO/IEC 27031 in incident readiness and response, China National Bodies have also proposed a new study period on “Categorization and classification of information security incidents”. This was also identified and suggested as a new item for development by the European Network Information Security Agency (ENISA) in a liaison request.

2. Standards for addressing **known** risk issues that have been identified, in particular, specified in the ISMS code of practice standard (ISO/IEC 27002), but require further elaboration of requirements and provision of implementation guidance, such as:
 - a. ISO/IEC 18028:2005/6 – Network Security (parts 1 to 5), which is currently undergoing revision, and will be published in the near future as ISO/IEC 27033 (parts 1 to 7) standard
 - b. ISO/IEC 27034 – Application security, which is another multi-parts standard for addressing the management needs for ensuring the security of applications from an organization user perspective

- c. ISO/IEC TR 14516 (ITU-T X.842) – Guidelines on use and management of Trusted Third Party services (TTP)
- d. ISO/IEC 15945 (ITU-T X.843) – Specification of TTP services to support the application of digital signatures
- e. ISO/IEC 15816 (ITU-T X.841) – Security information objects for access control
- f. ISO/IEC TR29149 – Best practice on the provision of time-stamping services⁶ (new project starting in Oct 2008)

In addition to the above, a study period on the security of outsourcing has also been proposed in Oct 2007, and further extended in April 2007 for members' contributions.

3. Standards for addressing the **aftermath** of information security incidents. Currently, there is no specific standard addressing this area of requirements. However, a six months study period has been initiated in April 2008 by the Malaysian National Body on the subject "Evidence acquisition procedures for digital forensic".

As security controls and services are also required for supporting the implementation of cryptographic mechanisms, and other technical security capabilities, WG 4 scope of work is therefore not limited to those as defined in ISO/IEC 27002, but also WG 2, and potentially WG 3 and WG 5 in the near future. The structure, based on unknown, known and aftermath of risk issues, that is adopted in WG 4 for categorization of the various standards therefore provide a more comprehensive perspective on its scope of work, as well as a basic structure for identifying standards requirements going forward.

Concluding Remarks

Managing information security is an ongoing undertaking in organizations, in view of the changing nature of information security risks. SC 27 promotes a management systems approach, through the use of ISO/IEC 27001 ISMS incorporating a cyclical systems process of Plan-Do-Check-Act (PDCA) to ensure new risks are identified while known risks are managed in a continuous improvement manner. The approach is supported by additional standards addressing the controls requirements and services needs, in all the three stages of information security risks development, from preparing for the unknown, addressing the known, to investigating the occurrence of information security incidents. This article focuses on these two aspects of the management systems approach, which are aligned with the scope of work of WG 1 and WG 4 in SC 27. Supporting, implementing, and operating these security controls and services require cryptographic and security mechanisms, including identity, privacy, and biometric related mechanisms, protocols and systems, and the needs for their security evaluation and assurances, which are areas of focus by WG 2, WG 5, and WG 3, respectively.

⁶ This project was transferred from WG 2 in April 2008 with the approval of SC 27 Plenary, in view of the nature of the technical report, which is on the security management and services aspects of time-stamping.

Developing standards are not without challenges. With numerous standards organizations undertaking this major endeavor in parallel, much coordination, information sharing, and collaboration are necessary to minimize duplication of efforts and maximize the use of limited resources. Liaison therefore plays a critical role in addressing this concern. Furthermore, while many countries/economies have representation in SC 27 (and other standards organizations), the systems of standards development are based around members' contributions of resources and contents, and majority vote of consensus to ensure fairness in the process. As such, this may not necessarily meet all the requirements of the stakeholders or align with their respective views of approach desired. Participation and communications by and amongst members, coupled with the use of the PDCA systems of continuous improvements are therefore key success factors to ensure continue usability of security standards to the members.

References

1. Fumy, W.: International Standardization of IT Security. RSA Conference Japan, Tokyo, Japan (2008)