



Getting Ready to the Changing Risk Situation

- An Overview of the Security Controls and Services Working Group (WG 4)

“Security standards can play an active role in helping organisations to prepare and be ready for new and emerging information security risk issues. This article focuses on the work of the international standards group SC 27/WG 4 which develops standards on information security controls and services standards to help organisations improve their ICT security readiness.”

Kang Meng-Chow, PhD, CISSP, CISA
 Chief Security Advisor, Microsoft Greater China Region
 Convenor, Security Controls and Services Working Group (WG 4)
 ISO/IEC JTC 1/SC 27

1 INTRODUCTION

“Change is the only constant”, someone once said. This applies to every facet of life, and is equally true in the ICT and information security risk arena today. While standards have often served as a means to bring order to things, to provide for consistency and predictability so as to establish common baselines and improve interoperability, in view of the changing nature of the risk environment, today’s security standards should serve beyond those fundamental needs. As a lever to change the nature of the risk environment in favour of the defender and users of information and ICT, security standards can play an active role in helping organisations get prepared and be ready for new and emerging risk issues. Getting ICT security ready is key to being able to deal with change effectively and efficiently. Such is a perspective adopted in the new “Security Controls and Services” standards working group, also known as WG 4, in ISO/IEC JTC 1/SC 27¹.

WG 4 was formally established in September 2006. Its primary aim is to provide standards to help organisations in ICT security readiness. There are three important areas in security readiness, as we will discuss in this paper. To be ready, existing or known risk issues should be managed. This involves the implementation of the ISO/IEC 2700x series of Information Security Management Systems (ISMS) standards. Next is to be ready to deal with new and emerging ICT security issues and other security needs that resulted from the proliferation and use of ICT and Internet related technology in organisations. Finally, when a security breach or an incident happens, organisations should be prepared to handle and manage it, to recover from the impact, and also being able to investigate and learn from the mishap.

¹ The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly setup the Joint Technical Committee 1 (JTC 1) to look into Information and Communication Technology (ICT) standardisation. Subcommittee 27, or in short, SC 27, which was formed in early 1990, focuses on ICT Security Techniques.

This article introduces the standards activities of ISO/IEC JTC 1/SC 27 WG 4, providing an overview of the standards projects in development in relation to the area of information security controls and services standards for improving organisation's ICT security readiness.

2 INTRODUCING 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 centre of security expertise and developed numerous standards that have been widely used in the industry. SC 27 membership has 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:

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

From 1990 to 2005, SC 27 was organised 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 finalised its re-organisation 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.

² "P" members have voting rights, whereas "O" members may contribute and provide 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, Luxembourg, 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 depicts the current organisation of SC 27, and the officers who are presently appointed in the sub-committee and the respective working groups.

The SC 27 working groups meet for one week once in every six months, in one of the 51 member countries 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 workshops and meetings to deliberate specific topic of interest or work on specific standard project amongst members or with other organisations (for example, ITU-T).

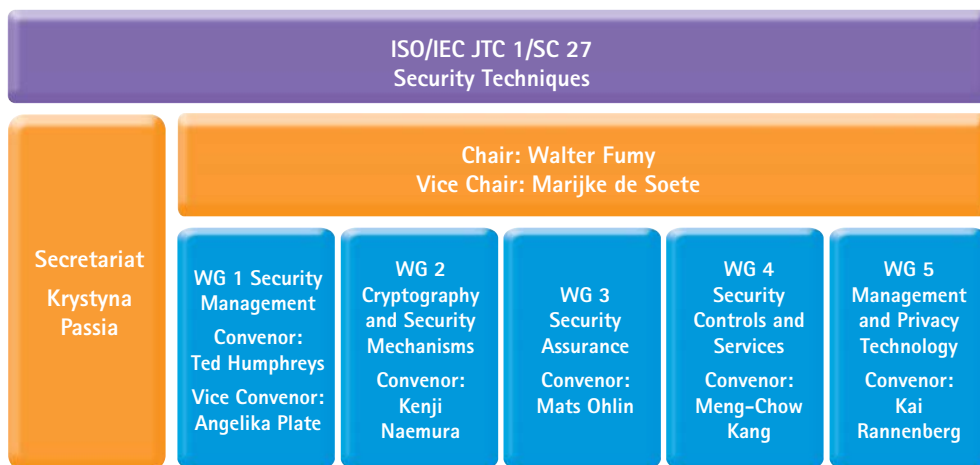


Figure 1: SC 27 Organisation and Officers

The sub-committee and working groups within SC 27 further establish formal liaison with other standards-related organisations and associations worldwide. 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 optimise the use of limited resources so as to ensure cost effectiveness, maximise use of available standards, and improve ability to support the ever growing demand for standardisation; 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.

Projects undertaken in WG 4 include those inherited from WG 1's previous scope of work (prior to September 2006), and newly studied and approved through JTC 1. These projects are designed and structured based on a defence-in-depth framework as shown in Figure 2. The framework covers three distinct areas of requirements, namely: (1) the need to prepare and respond to unknown and emerging security issues; (2) the need to manage and prevent the occurrence of known security issues; and (3) the need to manage, including investigate information security issues or incidents that have occurred, due to failure of the information security system or a natural disaster.

3 WG 4 RELATED STANDARDS FRAMEWORK

While WG 4's standards supports the implementation of the ISO/IEC 2700x series of standards developed and standardised in WG 1, its scope of work is not confined to those scoped within the ISO/IEC 2700x series of standards. For example, Cybersecurity issues involves more than establishing ISMS in organisations, as it also relates to the secure provisioning of Internet/Cyberspace related applications and services, and individual secure and safe use of the Cyberspace (as drafted in WD ISO/IEC 27032).

As noted earlier, the mission of WG 4 is more objectively aligned to the needs of ICT security readiness. Figure 2 was therefore developed as a structured framework to present a more comprehensive depiction of WG 4's scope, covering the three aspects of information and ICT security, i.e., managing the known security issues, preparing for the unknown and emerging security issues, and preparing for security breaches and incidents handling, including investigating into possible causes to learn from the mishaps.

Within each area of the framework, there are a number of security requirements and related standards, including existing and new projects/topics. Current projects that were previously handled in WG 1 and WG 2, as well as new projects, proposals and studies were identified when WG 4 was established. The list of work items are then aligned to the structure of the framework. Figure 3 depicts the alignment of those existing and future topics to the three categories of security controls and services requirements shown in Figure 2.

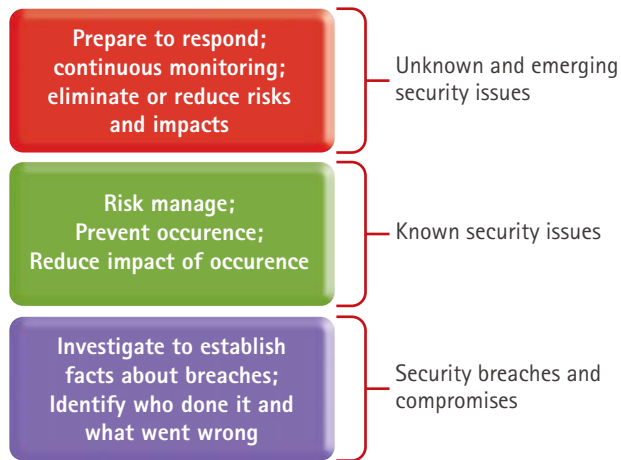


Figure 2: Three main areas of needs for security controls and services in a defence-in-depth framework

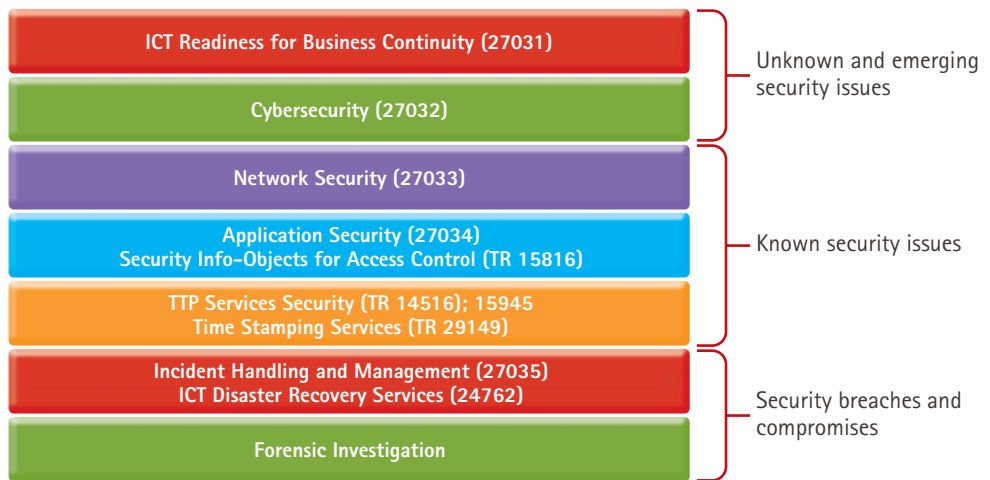


Figure 3: Mapping of existing and new projects/proposals to the three areas of needs

4 WG 4 STANDARDS DEVELOPMENT

In the area of new and emerging security issues, WG 4 developmental activities focus on preparing organisations to respond to new and emerging security issues, through the use of a combination of risk reduction and readiness controls and services. They include:

- 1) ISO/IEC 27031 – Guidelines for ICT readiness for Business Continuity (Working Draft);
- 2) ISO/IEC 24762:2008 – Guidelines for ICT disaster recovery services;
- 3) ISO/IEC 18043:2006 – Selection, deployment and operations of intrusion detection systems (IDS); and
- 4) ISO/IEC 27032 – Guidelines for Cybersecurity (Working Draft).

To support the implementation of ISO/IEC TR 18044 and ISO/IEC 27031 in incident readiness and response, the China National Body has proposed a new study period on "Categorisation 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. In addition, new standards in the area of vulnerability and updates management, threat monitoring, and guidelines for defining and detecting triggering events, should also emerge to support the readiness needs.

Another important aspect of improving ICT security readiness in organisations is to address 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. By managing and addressing these known issues, organisations could then focus its resources in identifying changes in the risk environment, and make necessary preparation for those changes. In this area, WG 4 activities focus in standards such as the following:

- 1) 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;
- 2) ISO/IEC 27034 – Application security, which is another multi-parts standard for addressing the management needs for ensuring the security of applications from an organisation user perspective;
- 3) ISO/IEC TR 14516 (ITU-T X.842) – Guidelines on use and management of Trusted Third Party services (TTP);
- 4) ISO/IEC 15945 (ITU-T X.843) – Specification of TTP services to support the application of digital signatures;
- 5) ISO/IEC 15816 (ITU-T X.841) – Security information objects for access control; and
- 6) ISO/IEC TR 29149 – Best practice on the provision of time-stamping services³ (new project starting in October 2008).

³ 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.

In addition to the above, a study period on the security of outsourcing has also been proposed in October 2007 which was extended in April 2008 for members' contributions.

Finally, having ISMS and the necessary security controls against new and emerging risks do not guarantee that the organisation is completely safe and secure against security attacks and breaches. In this regard, it is necessary for organisations to also get ready for potential mishaps so that they may be handled and managed in the most effective and efficient manner possible. Such preparation should include measures to facilitate after-the-fact collection of residual data to support the forensic investigation process and facilitate learning and improvement. A standard for addressing the aftermath of information security incidents and breaches is ISO/IEC TR 18044:2002 – Information security incident management which has been in place since 2002. In the April 2008 meeting, the working group proposed that this technical report be revised and elevated to become an International Standard (IS), which will take on a new standard number, i.e., ISO/IEC 27035, upon formal approval.

Currently, there is no specific standard addressing the area of forensic investigation requirements. However, a six months study period has been initiated by the Malaysian National Body on the subject "Evidence acquisition procedures for digital forensics" in the April 2008 meeting in Kyoto. We are looking forward to the National Bodies' support for this work to move to a developmental stage by October 2008 in the meeting in Cyprus.

As security controls and services are also required for supporting the implementation of cryptographic mechanisms, and other technical security capabilities, WG 4's scope of work in the area of managing known risks 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 categorisation 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.

5 CONCLUDING REMARKS

Managing information security is an ongoing undertaking in organisations, in view of the changing nature of information security risks. SC 27 promotes a management system 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 the scope of work of WG 4 in SC 27. Supporting, implementing, and operating the 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. The scope of work of WG 4, while comprehensive, is therefore not an end by itself.

Developing standards are not without challenges. With numerous standards organisations undertaking this major endeavour in parallel, much coordination, information sharing, and collaboration are necessary to minimise duplication of efforts and maximise 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 organisations), the systems of standards development are based on members' contributions of resources and contents, and majority vote or 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 or desired approach. Participation and communications by and amongst members, coupled with the use of the PDCA systems of continuous improvements are key success factors to ensure continue usability of security standards to the members.