

# 4 section four

## Development of International Standards on Information Security Management



Since the publication of ISO/IEC 17799 in year 2000, the ISO/IEC JTC 1 WG 1 (and the recently established WG 4) has been busy in the standardisation of the information security management practices and requirements. The publication of ISO/IEC 27001 on Information Security Management System (ISMS) requirements and the revision of ISO/IEC 17799 in year 2005 have marked another milestone on information security management standardisation respectively. This article intends to update readers on the recent development of the ISO/IEC 27000 standard series, and other supporting standards focused on individual control and service.

Philip Sy  
Principal Consultant, e-Cop  
Convenor, ISMS Working Group, SPSTC

### 1 Introduction

The world is becoming smaller, thanks to the advancement of information and communications technology (ICT) and the globalisation trend. However, it is also becoming a more risky place for business. The openness of Internet, the complex business model enabled by ICT implementation, the heavy-dependency on ICT system and infrastructure, and the rising trend of computer fraud together present to us a business world where any business may become the victim of the next major security incident or scandal. The problem is that, until recently, the awareness of such risks is comparatively low as business decision makers tend to leave the technical issues to their Information Technology people. However, due to the complexity of today's business and the rising importance of information to a business's success, information security is no longer just a technical issue but needs to be driven by top management using an overall organisational approach.

In view of this rising need, ISO/IEC JTC 1 / SC 27 has established itself as one of the major platforms for international standardisation for IT security techniques. Two of its most important achievements are the publication of ISO/IEC 27001 and ISO/IEC 17799 respectively in year 2005. The former standard specifies a management system that can be used to ensure that information security risks are well managed by organisations, while the latter standard is a code of practice for information security management, in the form of information security control implementation.

Since the publication of ISO/IEC 27001, businesses have responded positively to the standard and a rising number of certificates are being issued with reference to the standard. As of end of August 2007, 2,323 ISO/IEC 27001 certificates [1], have been issued worldwide to various organisations, while 1,556 to-be-obsolete BS 7799 (or equivalent) certificates [1], are in the process of upgrading to ISO/IEC 27001 certificates within the year. This is

encouraging as it demonstrates that the business world (and non-business organisations as well) welcomes information security standardisation and certification and there is strong market need worldwide in the adoption and application of the standard.

## 2 International, Regional and Singapore Platform for Information Security Standardisation

### 2.1 JTC 1 / SC 27

ISO/IEC JTC 1 / SC 27 have been described as an "international center of security expertise" [2]. It has been a primary resource for international standards on IT security techniques. Currently it has 5 working groups focusing on five different areas of security standardisation. They include: WG 1 on Information Security Management System (ISMS) standards and guidelines; WG 2 on security techniques in cryptography; WG 3 on security evaluation of IT systems and products; WG 4 on information security controls and services; and WG 5 on identity management and privacy technologies.

SC 27 also partners with other committees and organisations to harmonise and synergise the international standardisation effort. Some of major partners include ISO TC 68 for banking standards and ITU-T for telecommunications standards.

Singapore, represented by the Security & Privacy Standards Technical Committee (SPSTC) under ITSC, is one of the active members in SC 27 and, has in the past years, been contributing through the following activities:

- a) Nominated and contributed experts to take up positions in SC 27, e.g. WG convenor, project editor, and co-rapporteur;
- b) Submitted working drafts and new work item proposals based on relevant Singapore standards; and
- c) Voted, contributed and commented on various standards at different stages.

### 2.2 RAISS (Regional Asia Information Security Standards) Forum

The Regional Asia Information Security Standards Forum (RAISS) is formed to provide a platform for sharing of knowledge and learning experiences in regional economies on information security standards development, their adoption and deployment; and at the same time enables the regional bodies to identify opportunities for regional collaborations to further the course of international information security standards development and to promulgate them more effectively in the Asia region. It is currently Co-Chaired by Singapore and Japan, with members from Australia, Japan, Korea, Malaysia, and Singapore.

The Forum has been holding meetings in the region regularly, the latest being the 6th RAISS Forum Meeting hosted by Singapore on 22 and 23 August 2007. The topics that were discussed ranged from Business Continuity and Disaster Recovery to Application Security. The discussion and sharing in the Forum, has led to some new work item proposals being formulated and submitted to ISO/IEC SC 27/WG 4, such as the proposals on ICT Readiness for Business Continuity Management and Application Security.

## 2.3 SPSTC (Security & Privacy Standards Technical Committee)

IT Standardisation in Singapore is driven by the ITSC (Information Technology Standards Committee) under the standardisation framework provided by SPRING Singapore. Out of the various technical committees under ITSC, SPSTC is tasked specifically to look at information security and privacy standardisation. The mission of SPSTC is to promote the awareness, development and adoption of information security and privacy technology standards. Industry experts in these areas are actively involved in the activities, either at the technical committee level, or as members of one of the working groups.

The SPSTC has 6 working groups and 1 joint working group (JWG) in collaboration with the BCMTC (Business Continuity Management Technical Committee) under SPRING Singapore. The working groups mirror the SC 27 structure as follows:

- 1) ISMS (Information Security Management Standards) WG mirroring SC 27/WG 1;
- 2) Cryptography WG mirroring SC 27/WG 2;
- 3) Security Assurance WG mirroring SC 27/WG 3;
- 4) SCSS (Security Controls & Services) WG mirroring SC 27/WG 4; and
- 5) Privacy Technology WG mirroring SC 27/WG 5.

The BC/DR WG and ICT Readiness JWG focus on the standardisation activities relevant to disaster recovery service and infocomm technology readiness for business continuity management respectively. Both of these topics are under development or newly proposed working items in SC 27/WG 4.

## 3 International Development of Information Security Management Standards

### 3.1 ISO/IEC 27000 Family

Within SC 27, ISMS (Information Security Management System) standards and guidelines fall under the scope of WG 1, which includes:

- 1) Development and maintenance of the ISO/IEC 27000 ISMS standards family;
- 2) Identification of requirements for future ISMS standards and guidelines;
- 3) On-going maintenance of WG 1 standing document SD WG 1/1 (WG 1 Roadmap); and
- 4) 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.

WG 1 has planned and is developing a family of ISO 27000 standards in support of the ISMS implementation. The ISO 27000 family, and the other supporting standards, are further categorised to facilitate the user to understand the purpose of individual documents and how to use particular standards in relation to other relevant standards.

### 3.2 Types of Standard [3]

WG 1 has adopted a four layer model to develop relevant Information Security standards:

(a) Type A - Vocabulary Standard

This type of standard provides fundamental information including common terminology.

(b) Type B - Requirements Standard

This type of standard provides relevant specification for organisations to achieve compliance and/or certification through demonstration of their abilities to meet information security requirements specified in the standards. They include the following sub-types:

B-1: Addresses the requirements for Information Security Management Systems (ISMS); and

B-2: Addresses sector-specific ISMS requirements standards and standards containing requirements for ISMS auditing.

(c) Type C - Guidelines Standard

This type of standard provides guidance to organisations to implement the type B standards at either overall aspects or specific areas, or provides guidance in applying the information security management processes in specific industry. They include the following sub-types:

C-1: Addresses overall aspects of information security management systems/management processes/controls/techniques;

C-2: Addresses specific parts of information security systems/management processes/controls/techniques; and

C-3: Addresses sector-specific information security systems/management processes/controls.

(d) Type D - Related Standard

This type of standard provides further guidance on specific relevant information security areas or related techniques, not necessary explicitly and directly related to the Type B and Type C standards.

### 3.3 WG 1 Information Security Road Map [3]

WG 1 also has ongoing work on outlining the road map for information security standards. In its latest version published in June 2007, the road map describes the relevant information security standards that are currently planned, under development, or newly published.

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

To facilitate the harmonisation of WG 1 related standards and to provide a common and clear understanding, WG 1 is developing ISO/IEC 27000 as an 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 27000 standard will make use of the material from ISO/IEC 13335-1, but will be further enhanced based on subsequent WG 1 development. It is currently at Committee Draft (CD) stage.

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

ISO/IEC 27001 is a requirements standard and forms the core of the ISMS related family of standards. It is a certifiable standard and provides a means for organisations to provide assurance to relevant stakeholders of their information security management through certification process, which has been well established and recognised.

Since ISO/IEC 27001 was published on 15 October 2005, 2,323 organisations worldwide have been certified using the standard (as of end of August 2007) [1], with part of them newly certified using the standard while the others upgraded from BS7799 or other similar certifications.

### 3.3.3 ISO/IEC 27006 - Requirements for bodies providing audit and certification of information security management systems (Type B-1)

The ISO/IEC 27006 standard specifies requirements and provides guidance for organizations providing audit and certification services on Information Security Management System (ISMS), in addition to the requirements contained in ISO/IEC 17021 and ISO/IEC 27001. This standard is particularly useful for the accreditation of certification bodies providing ISMS certification scheme.

ISO/IEC 27006 was published in February 2007.

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

WG 1 reached a resolution in 2007 to transition the numbering of previous ISO/IEC 17799:2005 to the 27000 series of documents. The well-known Code of Practice has been re-numbered to 27002, without any change to the technical content.

ISO/IEC 27002 is an overall guideline standard on the implementation of information security controls and directly supports ISO/IEC 27001 Information security management system - Requirements standard.

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

ISO/IEC 27003 is a guideline standard supporting ISO/IEC 27001 by providing guidance material pertaining to the Plan- Do-Check-Act (PDCA) model. This standard may draw text from Annex B of BS7799-2, "PD 3004:2002 - Guide to the implementation and auditing of BS 7799 controls", and "PD 3005:2002 - Guide on the selection of BS 7799 Part 2 controls" as appropriate, except those part related to risk management issues in order to avoid duplication with ISO/IEC 27005.

This standard is also expected to extract concepts, models and guidance material for information security to provide independent guidance as to how organisations should select information security controls from "Controls" listed in ISO/IEC 27002 and how an organisation can improve implemented controls with consideration of changing circumstances.

ISO/IEC 27003 is currently at Working Draft (WD) stage.

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

ISO/IEC 27004 is a guideline standard that provides the ability to effectively measure, through metrics, the level of success of the implemented controls and processes from the ISO/IEC 27001.

ISO/IEC 27004 will consider a number of measurements, including appropriateness in the context, cost effectiveness, efficiency and control level implementation and provide a means to evaluate the output of the ISMS processes. This allows an effective measurement of the information security activities used to protect an organisation's information assets.

ISO/IEC 27004 will also look into the evaluation of whether the specific application of ISO/IEC 27001 has adequately met the needs of the organisation and would contribute towards the continuous improvement for an organisation.

ISO/IEC 27004 is currently at Committee Draft (CD) stage.

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

ISO/IEC 27005 is based on the developments that were made for the standard on "IT Security techniques - Management of information and communications technology security (MICTS) - Part 2: Information security risk management". It provides guidelines on information security risk management, and 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 of ISO/IEC 27001.

ISO/IEC 27005 and is currently at Final Committee Draft (FCD) stage.

### 3.3.7 ISO/IEC 27007 - ISMS Auditor Guidelines - New Work Item Proposal (Type C-1)

At the meeting in South Africa in November 2006, SC 27/WG 1 initiated a Study Period to identify the need for a standard giving guidance on ISMS audits. With the completion of the Study Period, WG 1 has decided to propose this standard as a new work item intended to support ISO/IEC 27006 and the generic auditor guidance provided in ISO/IEC 19011.

This standard will not repeat the information in ISO/IEC 19011 and will elaborate on the requirements of ISO/IEC 27001 and ISO/IEC 27006. In addition, this standard will not add any new requirements beyond what is contained in these documents.

### 3.3.8 ISO PDTR 13569 - Banking and related financial services - Information security guidelines - Published (Type C-3)

ISO 13569 is intended for use by financial organisations, and providers of services to financial organisations, that wish to employ a prudent and commercially reasonable information security programme.

### 3.3.9 ISO CD 27799 – Health informatics – Security management in health using ISO/IEC 17799 – under development (Type C-3)

ISO 27799 is currently under development by ISO/TC215/WG 4 and is intended to become an international standard designed to provide useful guidance on the application of ISO/IEC 27002 control statements in the health care environment in addition to the identification of key provisions as "normative" or mandatory in health care sector.

### 3.3.10 Information security management guidelines for telecommunications (X.1051/27031) – New Work Item Proposal (Type C-3)

This "Information security management guidelines for telecommunications" document was originally developed by ITU-T and was accepted as a sector-specific ISMS standard to be included in the SC 27 programme. SC 27 intends to adopt this standard as one of their sector-specific ISMS standards. As this standard is developed almost completely by ITU-T, SC 27 agreed to send this document out as FCD (Final Committee Draft) ballot.

This document establishes the guidelines and general principles for initiating, implementing, maintaining, and improving information security management in telecommunications based on ISO/IEC 27002. The objectives outlined in this Recommendation provide general guidance on the commonly accepted goals of information security management for telecommunications.

### 3.3.11 Sector-Specific ISMS Standards for the World Lottery Association – Study Period (Type C-3)

The World Lottery Association (WLA) has sent a liaison statement to SC 27 to request SC 27 to consider the possibilities of developing WLA Security Control Standards sector-specific ISMS standards within SC 27. A study period to identify a consolidated SC 27 view on whether these WLA standards should be transformed into SC 27 sector-specific ISMS standards and to provide an overview of the types of changes required for this to happen was started from November 2006.

Since some of the requests from the WLA cannot be fulfilled by an ISO standard, SC 27 is now waiting for the response from the WLA. It was therefore agreed to continue the Study Period and WG 1 will consider the outcome of the Study for a New Work Item Proposal in this area at the Working Group meeting in October 2007.

### 3.3.12 Sector-Specific ISMS Standards for the Automotive Industry – Study Period (Type C-3)

At the SC 27 Working Group meetings in November 2006, SC 27/WG 1 discussed the requirements for sector specific ISMS standards, and agreed to start a Study Period to identify the requirements that might exist for ISMS standards specific for the automotive industry. A study period to identify a consolidated SC 27 view on whether there is a need for SC 27 automotive-sector-specific ISMS standards was started in November 2006, and it was agreed to continue this Study for another 6 months, to collect further input.

The purpose of this Study Period is to identify the activities in the member countries on ISMS/information security activities in the automotive industry and to collect as much input as possible about the activities on the various member countries and in other committees, which can then be reviewed at the Working Group meeting in October 2007 to determine whether there is a need for SC 27 to develop automotive-sector-specific ISMS standards.

## 4 Conclusion

The ISO/IEC 27000-ISO/IEC 27009 information security management system standards, which are currently under the scope of SC 27/WG 1, are ISO/IEC 27001 process specific. This is in contrast to the information security management system application and service specific standards (ISO/IEC 27002 control specific or technical standards that are technology specific), which are currently under the scope of SC 27 WG 4.

Through the specialisation of work scope, WG 1 could focus on the standard development related to the overall information security management system planning, operation and maintenance, plus any standardisation activities needed to facilitate, either the effective operation of the multi-level ISMS accreditation and certification framework, or the application of ISMS framework and controls to specific industry sector. In order to differentiate the latter, all sector-specific ISMS standards will be numbered from 27031 - 27039 [3].

## 5 References

- [1] International Register of ISMS Certificates website [Version 174 - end of August 2007], run by ISMS International User Group Ltd.  
- <http://www.iso27001certificates.com/>
- [2] Walter Fumy Comment : Information technology - Security and quality ISO Focus May 2007.
- [3] JTC1 SC 27 Document N5866 "WG 1 SD 1 Road Map" dated 14 June 2007.