

ABSTRACT

This paper summarizes the security standardization efforts and activities carried out by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T).

1. Introduction

The International Telecommunication Union - Telecommunication Standardization Sector or in short, ITU-T, is one of the three sectors within ITU. Its mission is to establish high quality standards (in ITU, standards are referenced as Recommendations) encompassing all fields of telecommunication timely and efficiently. With the advancement of technologies over the years, the types of threats and vulnerabilities that businesses faced in this well-connected world has increased many fold. Hence, security has played an increasing pertinent role to ensure that systems and processes are secure enough to perform business functions effectively and efficiently.

Within ITU-T, standardization work is being carried out by its 13 technical Study Groups (SGs), and SG 17 has been the designated lead study group for telecommunication security. This SG is responsible to centre its core activities on defining and maintaining the overall security frameworks, as well as to ensure the timely publication of communication system security Recommendations by managing projects involving coordination, assignment and prioritization of efforts.

2. Security Focus of SG 17

The main focus areas of SG 17 between 2001 and 2004 are:

- **Public Key and Attribute Certificate Frameworks (X.509) Revision 2005**
 - Ongoing enhancements as a result of more complex uses

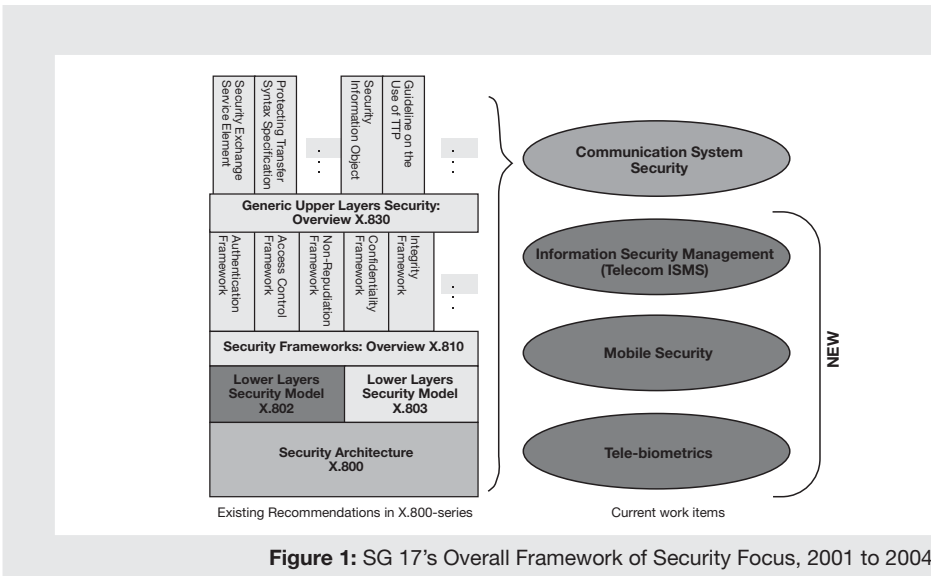
- **Security Architecture (X.805) New 2003**
 - For end-to-end communications

- **Security Management System (X.1051) New 2004**
 - For risk assessment, identification of assets and implementation characteristics

- **Mobile Security (X.1121 and X.1122) New 2004**
 - For mobile end-to-end data communications

- **Telebiometric Multimodal Model (X.1081) New 2004**
 - A framework for the specification of security and safety aspects of telebiometrics

The relationship between these five focus areas is depicted in the overall framework as shown in Figure 1.



Working Groups within SG 17 are called Questions (Qs), which are tasked to look into specific area of telecommunication security. An example is Question 7 or Q7 which looks into telecommunication security management, encompasses information security management system (ISMS), risk management, and incident management.

Figure 2 provides an overview of the Qs in SG 17, inter-relationship between the Qs, and the specific area that each Qs looks into from 2005 to 2008. Q4 has been identified as the coordinator for SG 17 on Telecommunication Security activities, and it will identify and develop security solutions in close co-operation with other SGs.

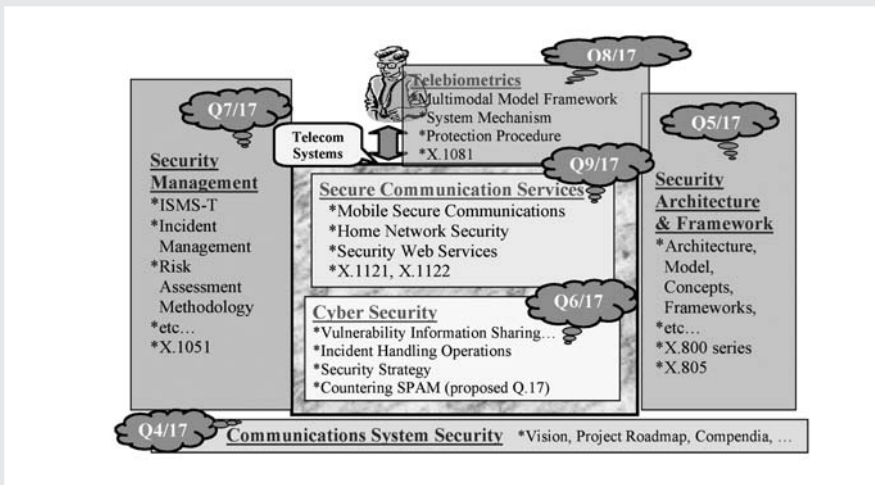


Figure 2: Overview of Questions in SG 17, 2005 to 2008

3. Additional Information on Recently Approved SG 17 Recommendations

3.1 X.805 - Security Architecture for End-to-End Communications

X.805 is the Recommendation that provides a holistic approach for defining comprehensive security architecture for providing end-to-end network security. The objective of this Recommendation is to serve as a foundation for developing the detailed recommendations for the end-to-end network security. The architecture can be applied independently of the network's underlying technology (be it wireless, wired, optical, voice, data, video, or converged networks) to various kinds of networks, which could be service providers networks, enterprise networks, or data center networks where the end-to-end security is a concern. This Recommendation defines the general security-related architectural elements that are necessary for providing end-to-end security. Figure 3 provides an illustration of the architecture.

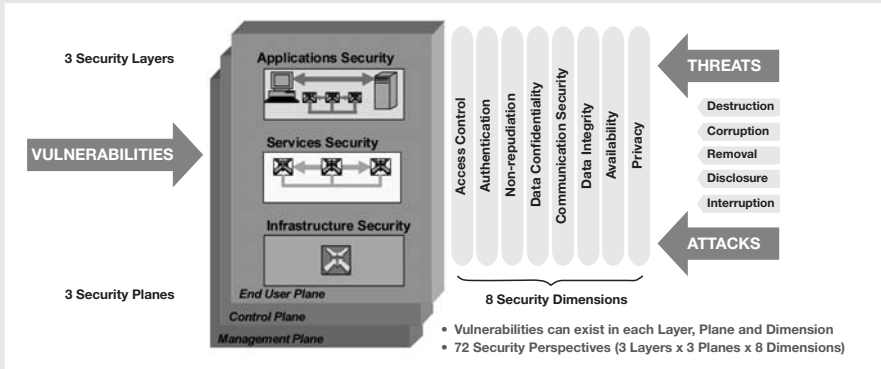


Figure 3: X.805, Security Architecture for End-to-End Communication

3.2 X.1051 - Security Management

The Information Security Management System (ISMS) for Telecommunications (also known as ISMS-T) specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the telecommunication's overall business risks. It is based on ISO/IEC 17799:2000, information technology, code of practice for information security management, and BS 7799-2:2002, Information security management systems - Specifications with guidance for use. Figure 4 shows the domain defined in ISO/IEC 17799.

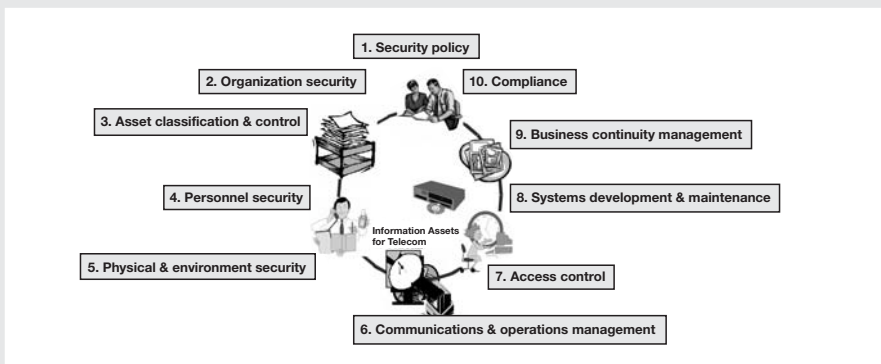


Figure 4: Domains Defined in ISO/IEC 17799

3.3. X.1121 and X.1122 - Mobile Security

The Recommendation on mobile security is a multi-part standard comprising of X.1121, X.1122 and a security policy which is currently under development. X.1121 is the Recommendation on the framework of security technologies for mobile end-to-end data communications, as shown in Figure 5. It describes the security threats, security requirements, and security functions for mobile end-to-end data communication, from both the perspectives of the mobile user and application service provider (ASP).

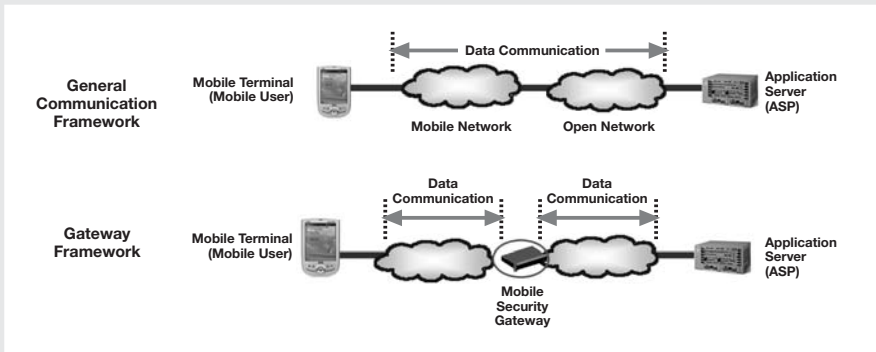


Figure 5: Framework of Security Technologies for Mobile End-to-End Data Communications

X.1122 is the guideline for implementing secure mobile systems based on public key infrastructure (PKI). PKI technology has been a useful security technology to realize many security functions such as digital signature and data integrity. However, it needs to be adapted for mobile end-to-end communications. As the method to construct and manage secure mobile systems using PKI technology has yet to be established, this specification provides guidelines on how to construct secure mobile systems based on PKI technology, as illustrated in Figure 6.

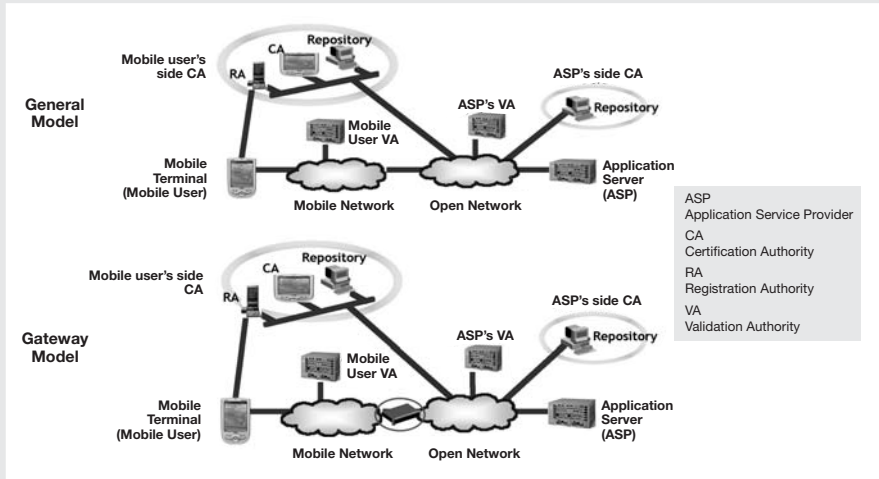


Figure 6: Secure Mobile Systems Based on PKI Technology

The security policy which is currently under development covers the different quality of security services needed to satisfy various requirements of security services for both users and Application Service Providers (ASPs).

3.4. X.1081 - The Telebiometric Multimodal Model A Framework for the Specification of Security and Safety Aspects of Telebiometrics

This Recommendation defines a multimodal model for security and public safety in telebiometrics, aimed at achieving the following:

- Assist with the derivation of safe limits for the operation of telecommunications systems and biometric devices;
- Provide a framework for developing a taxonomy of biometric devices; and
- Facilitate the development of authentication mechanisms, based on both static (for example fingerprints) and dynamic (for example gait, or signature pressure variation) attributes of a human being.

This model comprises a specification of a number of dimensions related to interactions in a set of specified modalities, in both directions and at various intensities, using the complete range of quantities and units specified in ISO 31 and IEC 60027-1. This provides a taxonomy for the interactions that can occur where the human body meets the devices capturing biometric parameters or impacting on the body.

4. Recommendations Planned for Approval in the Study Period

The following is a list of Recommendations planned for consent in the current study period and the corresponding Qs that are addressing each of these Recommendations:

- Q2: Directory services, Directory systems, and public-key/attribute certificates
 - Computerized directory assistance (E.115)

- Q5: Security Architecture and Framework
 - Draft of a version to ITU-T Rec.X.805

- Q7: Security Management
 - Code of practice for information security management (X.ism-1)
 - ISMS requirements specification (X.ism-2)

- Q8: Telebiometrics
 - Physiological quantities, their units and letter symbols (X.physiol)
 - General telebiometric system models, protocol and data contents (X.tsm-1)
 - Profile of client verification model on TSM (X.tsm-2)
 - The guideline of technical and managerial countermeasures for biometric data security (X.tpp)

- Q9: Secure Communication Service
 - Framework for security technologies for home network (X.homesec-1)
 - Certificate profile for the device in the home network (X.homesec-2)
 - General security value added service(policy) for mobile data communication (X.msec-3)

- Correlative reacting system in mobile network (X.crs)
- Authentication architecture in mobile end-to-end data communication (X.msec-4)
- Proposed Q17: Countering Spam
 - Guideline document on countering SPAM (X.gcs)
 - Technical framework for countering SPAM (X.fgs)
 - Technical means for countering SPAM (X.tcs)

5. Conclusion

Security has become an important issue in our lives that it is part and parcel of everybody's business. Information security requirements need to be identified and designed upfront and it should be a continuous ongoing effort to make it effective. Furthermore, a systematic way of addressing vulnerabilities (intrinsic properties of networks/systems) needs to be put in place so that protection can be provided independent of the risks, which are constantly changing and may be unknown.

6. References

- [1] ITU-T - <http://www.itu.int/ITU-T/>
- [2] Herbert Bertine and Koji Nakao, "Security Standardization in ITU-T", Cybersecurity Symposium II, 29 March 2005, Moscow, Russia

Note: Biography of Koji Nakao can be found in the paper on "**Introduction And Updates On Information Security Technologies Related Activities In Japan**" on page 27, and Meng-Chow Kang in the **Preface** on page 05.

ABSTRACT

This paper provides an overview of the ISO/IEC JTC 1/SC 27 work, as well as looking at the future programme of work in the specific area of information security management.

1. Introduction

In today's diverse range of business environments and markets being globally inter-connected across mobile, wireless and broadband networks, information security is playing an even more important role than ever before. Protection of important organizational information assets is critical, and the risks to this information are to be dealt with whilst enabling business to benefit from market opportunities to develop and grow its business.

International information and IT security standards provide a means for developing solutions and a basis for doing business securely. ISO/IEC JTC 1/SC 27 is an international centre of expertise in the field of information and IT security standards and has been at the forefront of this work for over a decade. SC27 is organized in three Working Groups (WGs). WG1 focuses on information and IT security management and related standards, including network security and incident response. WG2 predominantly focuses on cryptographic technology and security protocols, and WG3 focuses on security assurance related standards, such as the Common Criteria standard.

2. The ISO/IEC 27000 Family of Standards

In 2005, WG1 has embarked on a programme of work relating to the development of a family of information security management system (ISMS) standards referred to as the 27000 series of standards.

- ISO/IEC 27001
- ISO/IEC 27002 (ISO/IEC 17799 after 2007)
- ISO/IEC 27003 ISMS Implementation guidelines

- ISO/IEC 27004 Information security management metrics and measurements
- Others
 - Principals and vocabulary
 - ISMS risk management

Work on ISMS standards is being carried out in close collaboration with ITU-T and will result in joint publication of these standards. ITU-T already have an 'ISMS telecoms requirements' document (X.1001) based on BS 7799 Part 2:2002 and this is expected to be further developed in alignment with the ISO/IEC 27001 development. In addition ITU-T is in collaboration on ISO/IEC 27002 and is considering collaboration of the other ISMS developments - ISO/IEC 27003 and 27004.

3. ISO/IEC 27001 - ISMS Requirements

The first of these standards, ISO/IEC 27001, is expected to be published in November 2005. This standard is based on the existing standard BS 7799 Part 2, which is currently used world-wide for third party management system audits and certification. Both ISO/IEC 27001 (ISMS) and BS 7799 Part 2:2002 (ISMS) use the Plan-Do-Check-Act (PDCA) process model as adopted in ISO 9001 (QMS) and ISO 14001 (EMS). This PDCA process defines a cycle of activities for the establishment of an ISMS, the implementation and operational use of the ISMS, the regular monitoring and review of the ISMS, and the improving and updating of the ISMS, taking into account any changes necessary. This process cycle is designed to ensure that effective information security is implemented and it remains effective through a process of continual improvement.

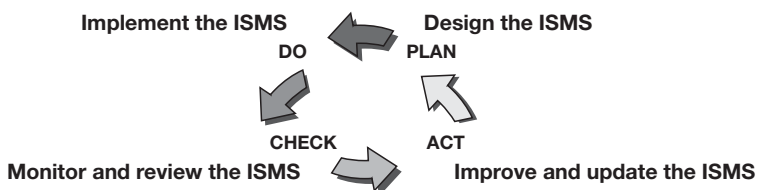


Figure 1: The PDCA Process Model

The PDCA process model in ISO/IEC 27001 has a set of risk management processes for identifying and assessing the risks and impacts, and determining appropriate management options for treating these risks. One of the risk treatment options is to reduce the risks by the appropriate selection of controls. Annex A of this standard contains the set of controls from ISO/IEC 17799:2005, which can be selected for implementation according to which risks need to be reduced.

4. ISMS Certification

It is important to note that ISO/IEC 17799:2005 is a code of practice for information security management and is not applicable for accredited certification - it was neither designed nor is it suitable for this purpose, whereas the specification standard ISO/IEC 27001 Information security management system (ISMS) - Requirements has been designed to be applicable for accreditation certification. ISO/IEC 27001 is a revised version of BS 7799 Part 2:2002, a standard that has been used for accreditation certification for the past seven years. The certification process used for this is exactly the same as that used for ISO 9001 for quality management system (QMS) assessments and ISO 14001 for environmental management system (EMS) assessments. Once ISO/IEC 27001 has been published and BS 7799 Part 2 has been withdrawn, future certification work (e.g. new certifications, surveillance audits on existing certifications and renewal of certifications) can be transferred over to using the ISO standard. National Accreditation Bodies that are involved in the process will be issuing a Certification Transition Statement which will give details of the time period during which organisations, working together with their Certification Body, will need to make the transition from BS 7799 Part 2:2002 to ISO/IEC 27001.

The current International Register for ISMS Accredited Certificates (www.xisec.com) will continue to exist and function as an International Register for the purpose of registering an organisation's ISMS certificate. Certification Bodies throughout the world should continue to provide the Registrar with the details of all new certificates as well any updates to existing certificates using the same notification process in operation today.

**5. ISO/IEC 27002 (ISO/IEC 17799:2005)
- Code of Practice for Information Security Management**

The revised version of ISO/IEC 17799 was published on the 15 June 2005. This new edition provides many new features and improvements in order to keep best practice for information security up-to-date with progress and trends and to include changes in ways of doing business. These new features include additional best practice:

- To cover the increase in the use of external services and outsourcing and how to manage the use of these services securely,
- To extend the controls and guidance on asset management and to cover issues such as 'acceptable use' and 'ownership',
- The introduction of new technologies and how these technologies are being used, such as the growing use of mobile and wireless networks,
- To address the problem of 'mobile code',
- The growing number of new threats and risks confronting business and extensions to incident management controls and guidance,
- To provide a comprehensive approach to human resource security, and
- To address the growing problem of vulnerability management, including patch management.

The new chapter structure is shown in figure 2:

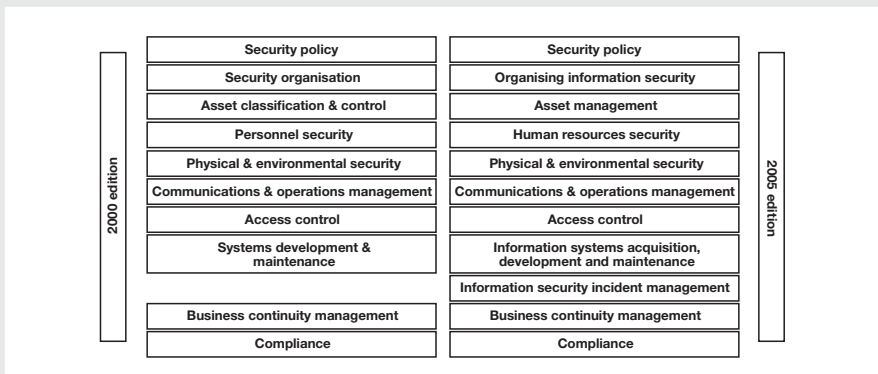


Figure 2: A Comparison of the 2000 and 2005 Version of ISO/IEC 17799

Improvements have been made to the 'user friendliness' of the standard, to make it easier for readers to distinguish what the control is in contrast to what the implementation guidance for the control is. Figure 3 shows this new 'user friendly' structure.

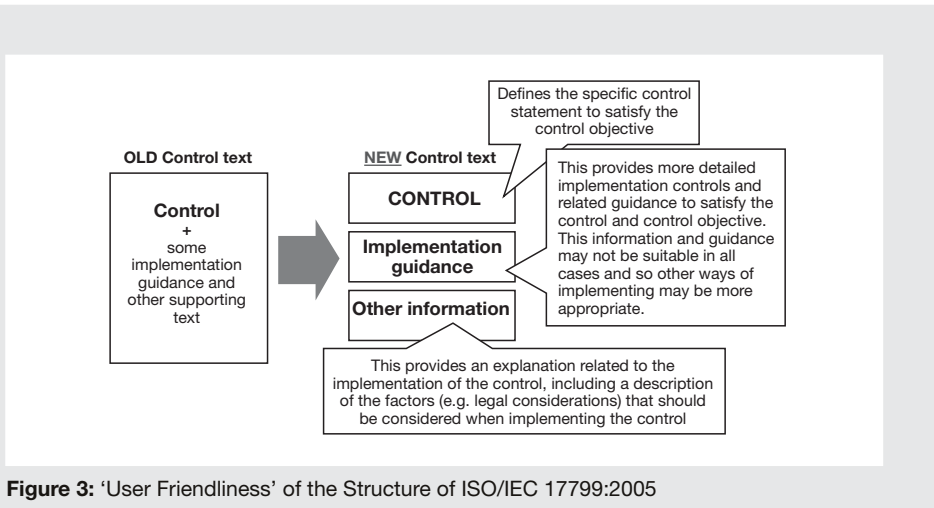


Figure 3: 'User Friendliness' of the Structure of ISO/IEC 17799:2005

The revised version provides business with an important tool for managing its information security risks and to enhance its ability at managing its incidents and to support its business continuity capability whilst maximising its investments and opportunities in the marketplace. The key objective of this code of practice is to enable business to protect the confidentiality, integrity and availability of its sensitive and critical information.

ISO/IEC 17799:2005 Code of practice for information security management is clearly related to the ISMS family of standards. However ISO/IEC 17799 will not change its number in the short term, but in April 2007, the proposal is to allocate the number ISO/IEC 27002 to the ISO/IEC 17799 standard. Given the existing success, uptake and market penetration of ISO/IEC 17799, this will enable the market to become familiar with this new series of numbers.

**6. ISO/IEC 27004
- Information Security Management Metrics and Measurements**

Besides the standard ISO/IEC 27001, there is also a standard ISO/IEC 27004 'Information security management metrics and measurement' being developed. This development is aimed at addressing how to measure the effectiveness of ISMS implementations (processes and controls) and will specify metrics and provide guidance concerning measurement techniques applicable for determining and describing the efficiency and effectiveness of information security management systems in support of ISO/IEC 27001 (see facing page). It includes resources (information security controls), and activities (information security processes and procedures). The metrics are used mainly for the measurement of the "Do" components of an ISMS (implement and operate the ISMS) as input to the "Check" (monitor and review) components of an ISMS, with the goal of providing a means for taking decisions at the "ACT" (maintain and improve the ISMS) stage, leading to continuous improvement of the ISMS cycle. This standard will provide a valuable tool for business generating a range of effectiveness indicators for benchmarking and setting performance targets.

7. ISO/IEC 27003 ISMS Implementation Guidelines

SC27 is undergoing development of 'ISMS Implementation guidance' standard with the intention of providing more help and guidance on implementing the processes and controls in ISO/IEC 27001. This is based on Annex B of BS 7799 Part 2:2002.

8. Future ISO/IEC 27000 Developments

In addition, there are proposals being discussed within SC 27 for other standards and guidelines being developed to support the use and implementation of ISO/IEC 27001. For example:

- A Principles and Vocabulary part, similar to ISO 9000.

- Development of 'ISMS Risk Assessment/Management' standard to help with implementing the risk processes in ISO/IEC 27001 - this work will need to be commensurate with and take cognisance of the standard "Management of information and communications technology security" (MICTS) Part 2, which is on information security risks.

9. Other SC27 Developments

a. MICTS (ISO/IEC 13335)

Part 1 of this standard addresses the concepts and models fundamental to a basic understanding of ICT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security.

Part 1 is now published.

Part 2 is under revision and is currently out for Committee Draft (CD) ballot, and it is now being re-titled to "information security risk". Part 2 considers techniques for ICT security risk management covering assets and their valuation, vulnerabilities related to these assets, the threats that might potentially be able to exploit these vulnerabilities and the resulting risks and impacts.

MICTS Part 1 is now the subject of study period to consider updating to align with MICTS Part 2 development to focus on information security risks.

b. IT Network Security (ISO/IEC 18028)

The IT Network Security Project progressed two of its standards to Final Draft International Standard (DIS) and two to Final Committee Draft (CD):

- Part 1 Network security management (FCD)
- Part 2 Network security architecture (FDIS)
- Part 3 Securing communications between networks using security gateways (FDIS)
- Part 4 Remote Access (published)
- Part 5 Securing communications across networks using Virtual Private Networks (FCD)

This work is carried out in close collaboration with ITU-T and will result in joint publication of these standards.

c. Information security incident management (ISO/IEC TR 18044)

This Technical Report (TR) has now been published and provides advice, guidance and a methodical planned approach on information security incident management for information security managers, and information system managers. Insufficient preparation by an organization for security incidents (and weaknesses) will make any actual response chaotic and thus ineffective.

d. Disaster Recovery Services

Business continuity and disaster recovery have always featured as two important issues in ISO/IEC 17799 and this is covered by an individual chapter giving high level best practice controls. SC27 is now launching a new project in this area to provide further advice and guidance at a more detailed implementation level. A New Work Item (NP) has been launched based on the Singapore standard SS 507 which covers business continuity/disaster recovery for service providers. If approved, work will start at the November meeting of WG1 in Kuala Lumpur, Malaysia.

10. Conclusion

In conclusion, SC27 is at the leading edge of standardisation work for both information and ICT systems. It has published many standards that are in use today around the world providing secure applications, services and networks to business and governments. These standards cover both management and technical aspects addressing a range of business and technological risks. It also liaises with other standards groups and user organisations to collaborate on joint work such as with ISO/TC68 in the area of banking, ITU-T on telecoms standards, and SC37 on biometrics. SC27 continues to work with experts and business around the world to ensure ISO security standards are up to date, appropriate and driven by market needs.

Mr Ted Humphreys

*Chartered Fellow of BCS CITP, CISM
Chair of ISO/IEC JTC 1/SC 27 WG 1*

*Director
XiSEC Consultants Ltd, UK*



Mr Ted Humphreys (Chartered Fellow of the BCS - FBCS CITP, CISM) is the Director of XiSEC Consultants Ltd, a UK company providing information security management consultancy services around the world. He has been an expert in the field of information security and risk management for more than 27 years. During this time, he has worked for major international companies (in Europe, North America and Asia), as well organisations such as the European Commission and the OECD.

Mr Ted Humphreys, the internationally acknowledged father and management guru (and some say spiritual leader) of the ISO/IEC 17799 and ISMS (BS 7799) standards and the global BS 7799 certification movement, has been the editor of BS 7799 Part 1:1999, ISO/IEC 17799:2000, the 1999 and 2002 editions of BS 7799 Part 2 the ISMS standard and the EA 7/03 the ISMS accreditation guidelines. He is the Founder and Director of the ISMS International User Group and is responsible for the International Register of BS 7799/ISMS Certificates. In 2002 he was honoured with the Secure Computing Lifetime Achievement Award. This international award recognises his noteworthy achievements in shaping and promoting the development and standardisation of information security management BS 7799 best practice standards.

Dr Angelika Plate

Co-Editor of ISO/IEC 17799:2005 and Editor of ISO/IEC 27003

*Director
ÆXIS Security Consultants*



Dr Angelika Plate runs the German based information security consulting company ÆXIS Security Consultants, and has worked with many companies in different ISO/IEC 17799 and BS 7799-2 projects to establish, implement, maintain and improve ISMS. Prior to establishing ÆXIS at the end of 1997, she was employed by BSI (the German Information Security Agency) as a senior information security expert.

Dr Angelika Plate has been involved in ISO activities for many years, where she was acting as the editor of two international standards dealing with risk assessment, control selection and risk management, and as an editor of the revised version of ISO/IEC 17799, which has now been published; she is now editing the new ISO/IEC 27003. Prior to that, she was involved in the revisions of BS 7799 Parts 1 and 2 in UK and has been supporting and contributing to the development of ISO/IEC 27001, the international version of BS 7799-2. She is also chairing the ISMS IUG Germany, which she founded in 2002.