ISO/IEC JTC 1 N9713

2009-09-13

Replaces:

ISO/IEC JTC 1
Information Technology

Document Type:	business plan
Document Title:	SC 27 Business Plan, October 2009-September 2010
Document Source:	SC 27 Chairman
Project Number:	
Document Status:	This document is forwarded to JTC 1 National Bodies for review and consideration at the October 2009 JTC 1 Plenary meeting in Tel Aviv.
Action ID:	ACT
Due Date:	
No. of Pages:	14

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Business Plan

TITLE: SC 27 Business Plan October 2009 – September 2010

SOURCE: Walter Fumy, SC 27 Chairman

DATE: 2009-09-10

PROJECT:

STATUS: for submission to JTC 1

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice Chair
T. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 11

Secretariat ISO/IEC JTC 1/SC 27 - DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; e-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

Business Plan for JTC 1/SC 27 'Security Techniques'

Period covered: October 2009 - September 2010

Submitted by: Walter Fumy, SC 27 Chairman

1 Management Summary

1.1 Chairman's Remarks

This Business Plan has been compiled in accordance with Resolution 47 of the SC 27 Plenary meeting held in Beijing, May 11-12, 2009.

1.2 JTC 1/SC 27 Statement of Scope

The development of standards for the protection of information and ICT. This includes 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, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

1.3 Project Report

1.3.1 Progress

The overall progress made over the past year again was excellent as shown by the number of documents that have been published (see section 2.2) and also by the target dates being kept in the majority of cases.

- total number of projects 123
- number of active projects 77
- number of publications: 85

SC 27 fully supports all its active projects. Details of the current status of all projects and their target dates can be found in SC 27 Standing Document SD 4, see also http://www.jtc1sc27.din.de/en .

1.3.2 New Projects and Study Periods

The following New Work Items for SC 27 have been approved over the past 12 months, all supported by substantial NB interest:

- NP 27013: *Guidance for the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001.*

  This standard will provide guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 Service management. This includes implementation advice on adopting an integrated management system, i.e. the processes, policies, and procedures for those organisations that are intending to implement ISO/IEC 27001 when ISO/IEC 20000-1 is already adopted, or vice versa; implement both ISO/IEC 27001 and ISO/IEC 20000-1 together; or align already existing ISO/IEC 27001 and ISO/IEC 20000-1 management systems implementations.

- NP 27014: *Information security governance framework.*

  Resolving strategic issues concerning the protection of corporate information assets and to support the organisation's corporate governance relies on effective information security governance (ISG). The standard will define an information security governance framework, establish its objectives, principles, and processes, and show how an ISG framework can be used to evaluate, direct, and monitor an information security management system.

- NP 27015: *Information security management system for financial and insurance services sector.*

  This standard is intended to provide guidance to the financial and insurance services sectors on how to adapt the 2700x Information Security Management System (ISMS) framework. It aims to support those sectors in fulfilling sector specific information security related legal and regulatory requirements through an internationally agreed and well-accepted framework. This standard should serve the financial and insurance sector as well as their business partners and customers.

- NP 27036: *Guidelines for security of outsourcing*.

  This standard will provide guidance to organizations on the evaluation of security risks involved in the procurement and use of outsourced services. It establishes security recommendations additional to the ISO/IEC 27002 security controls related to outsourcing and includes the following areas: strategic goals, objectives and business needs; risks and risk mitigation techniques; and assurance provision.

- NP 27037: *Guidelines for identification, collection and/or acquisition and preservation of digital evidence*.

  This standard will provide guidance on digital evidence management, describing the process of recognition and identification, collection and/or acquisition and preservation of digital data

which may contain information of potential evidential value. It is applicable to organisations needing to conduct the identification, collection and/or acquisition and preservation of digital evidence in the event of computer incidents; after the incidents happened or while the incidents happen in real time.

- NP 29190: *Privacy capability maturity model.*

  This standard will provide guidance to organizations for assessing how mature they are with respect to their processes for collecting, using, disclosing, retaining and disposing of personal information. The document may also be used by third parties for the purpose of maturity assessment.

- NP 29191: *Requirements on relative anonymity with identity escrow.*

  This standard will discuss a framework that provides measures against unauthorized access or manipulation of data without having the users to reveal their identity. It is based on a model for authentication and authorization using group signature techniques providing relative anonymity, i.e. users are anonymous to anyone but an escrow agent. Main objective of the document is to provide guidance for the use of group signatures for data minimization and user convenience.

- NP 29192: *Lightweight cryptography.*

  This standard will specify cryptographic mechanisms suitable for constrained environments, as regards to aspects such as chip area, power consumption, memory size, or communication bandwidth. Areas of application for lightweight cryptography include RFID tags, smart cards (in particular contactless applications), secure batteries, health-care systems (e.g. Body Area Networks), sensor networks, and many others.

- NP 29193: *Secure System Engineering Principles and Techniques.*

  This Technical Report will provide guidance on the principles, best practices and techniques for secure-system design for information and communication systems, complementing already existing design processes with security-specific engineering aspects. It will focus on the principles and techniques used to ensure that the security controls are effective and potential deficiencies of those controls can be handled within the system in a way that minimizes the security impact of such deficiencies.

In addition, SC 27 has established Study Periods on the following topics:

- *Object identifiers and ASN.1 syntax.*
- *Information security management economics.*
- *Secret sharing mechanisms.*
- *Mechanisms supporting anonymity.*
- *Tamper protection requirements and evaluation.*
- *Redaction.*
- *Access control.*
- *Review of ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

1.3 Co-operation and Competition

SC 27 enjoys a very large number of fruitful and valuable liaisons with many organizations within ISO/IEC JTC 1 including SC 6, SC 7, SC 17, SC 36, and SC 37, within ISO including TC 68, TC 215, ISO/CASCO, TMB/JTCG, TMB/SAG and to several external organizations including CCDB, ETSI, CEN/NISSG, ITU-T, FIRST, ICDPPC, ISSEA, ISACA, ISF and TCG.

Currently there are 24 internal and 26 external liaisons. A complete list is available at www.jtc1sc27.din.de/sbe/members .

Selected aspects related to these liaisons are highlighted below.

1.3.1 SC 37 'Biometrics'

Strong synergy exists between biometrics and IT security. The potential contribution of SC 27 to biometrics standards is evident. In particular, the areas of template protection techniques, algorithm security, and security evaluation are fields where SC 27 has the necessary experience to complement the mandate of SC 37. Therefore, SC 27 maintains close collaboration with SC 37 'Biometrics'.

1.3.2 TC 68 'Financial Services'

TC 68 and SC 27 collaborate on IT security standards of mutual interest. To encourage such cooperation, to share expertise and content, and to avoid overlap in standards development and manage New Work Item proposals that are relevant to both committees, a joint *'Coordination Committee on Security Work'* has been established. The latest meeting of this committee took place September 11, 2008 in Berlin where a number of cooperation topics have been agreed.

1.3.3 ITU-T Q10/SG17

ITU-T Q10/SG17 and SC 27 collaborate on several projects in order to progress common or twin text documents and to publish common standards. These projects include

- ISO/IEC 15816: *Security information objects for access control* (= ITU-T X.841)
- ISO/IEC 14516: *Guidelines on the use and management of Trusted Third Party services* (= ITU-T X.842)
- ISO/IEC 15945: *Specification of TTP services to support the application of digital signatures* (= ITU-T X.843)
- ISO/IEC 18028: *IT network security**
- ISO/IEC 27001: *ISMS requirements*
- ISO/IEC 27002: *Code of practice for information security management*
- ISO/IEC 27011: *Information security management guidelines for telecommunications* (= ITU-T X.1051)
- ISO/IEC 27032: Guidelines for cybersecurity
- ISO/IEC 29115: *Entity Authentication Assurance* (= ITU-T x.eea)

*) This work is also done in collaboration with JTC 1/SC 6.

1.3.4 The International Common Criteria Project (ICCP)

The ICCP and SC 27/WG 3 have had a long-standing technical liaison on projects related to IT Security Evaluation Criteria. Thus, Working Group 3 has been working in close co-operation with the Common Criteria Development Board (CCDB) on the development of the Common Criteria, which has been simultaneously published as ISO/IEC 15408. The co-operation has been extended to also involve the work on 18045 "Evaluation methodology for

IT security". This close cooperation allows NBs not represented in the ICCP to review, comment and contribute to the project. An update of 15408, to bring it in line with the recently updated version 3.1 within the ICCP, is now close to completion. The related standard on Evaluation Methodology, 18045, has already been aligned. Recently the WG has been contributing to the ICCP exploratory work on future development of Common Criteria.

2 Period Review

2.1 Market Requirements

Up until the 1970s, the use of security techniques to protect information and communications was largely restricted to some specific areas of application - such as banking - and to governments. With the advent of the Internet and the prospect of performing business on-line, IT security has been in the forefront of information and communications technology (ICT) have emerged high on the management agenda, have been the subject of new legislation and has made its way into many news headlines. E.g., organizations deploying electronic services (e.g., e-business, e-government) need to ensure control over who gets into applications and what users are allowed once they are in. User identification, authentication and authorization management technologies address these issues. Electronic signatures provide data integrity and non-repudiation and thus help to accelerate the growth in secure electronic business and subsequently to eliminate paper-based transactions.

At the same time, users need confidence in the effectiveness of the implemented security; an area where security evaluation and resulting assurance play an important part – here we have the Common Criteria (ISO/IEC 15408) for the security evaluation of products and systems and ISO/IEC 27001 for the third party certification of an organization's information security management system (ISMS) – similar to the model for ISO 9001 (Quality), ISO 14001 (Environment) and ISO 22000 (Food safety management).

In addition, users ask more and more about protection of their privacy and the related data. The relation between IT security and privacy is close, complex, and delicate. This can especially be seen in the area of Identity Management, e.g. pointing to the issue, who owns which very personal data about whom. SC 27 addresses this issue in its new Working Group 5 "Identity Management and Privacy Technologies", e.g. by ISO/IEC 24760 "A Framework for Identity Management" and ISO/IEC 29100 "Privacy Framework".

Standardized security techniques are becoming mandatory requirements for e-commerce, health-care, telecoms, automotive and many other application areas in both the commercial and government sectors. SC 27 addresses those market needs and provides a center of expertise for the standardization of security techniques.

The near future sees many market opportunities for SC 27 to expand the deployment of its standards as well as collaborating with other standards bodies on new projects and ideas. SC 27 as a centre of excellence on information security and IT security has always been at the forefront of security standardization. It has the right blend of skills and resources to deliver security standards to market requirements as borne out by its past track record. As applications of security technologies have broadened during the last years, so have both the membership of SC 27 and its programme of work.

A rapidly emerging and critical area of standardization to address corporate needs around the world is that of governance whether in the form of IT governance or information security governance (ISG). SC 27 is embarking on a programme of work into ISG in collaboration with other groups in JTC 1 dealing with other governance issues such as IT governance. Protecting corporate information assets cannot be solved by IT security solutions and technologies alone. Hence resolving strategic issues concerning the protection of corporate

information assets and to support the organization's corporate governance relies on effective information security governance.

The scope of information security governance is to:

- Help meet corporate governance requirements related to information security
- Align information security objectives with business objectives
- Ensure a risk-based approach is adopted for information security management
- Implement effective management controls for information security management
- Evaluate, direct, and monitor an information security management system
- Safeguard information of all types, including electronic, paper, and spoken
- Ensure good conduct of people in using information

2.2 Achievements

2.2.1 Publications

Since October 2008, the following International Standards and Technical Reports have been published:

- ISO/IEC 9798-2: *Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithm (3rd edition).*

  Publication date: 2008-12-15

  Part 2 of ISO/IEC 9798 specifies entity authentication mechanisms using symmetric encipherment. To prevent valid authentication information from being accepted at a later time, time variant parameters such as time stamps, sequence numbers, or random numbers are employed. Four of the six authentication mechanisms specified do not involve a trusted third party. Two of these four are concerned with unilateral authentication while the other two specify mechanisms for mutual authentication. In addition, two mechanisms involving a trusted third party are specified, which can be used for unilateral or mutual authentication depending on the number of messages exchanged.

- ISO/IEC 11889-1: *Trusted Platform Module - Part 1: Overview (Publicly available Specification).*

  Publication date: 2009-05-15

  Part 1 of ISO/IEC 11889 serves as an informative background document and contains no specifications or normative information. A Trusted Platform Module (TPM) is an implementation of a defined set of capabilities intended to provide authentication and attestation functionality for a computing device, and to protect information by controlling access to it. Trusted Platforms offer improved, hardware-based security in numerous applications, such as file and folder encryption, local password management, S-MIME email, VPN and PKI authentication, and wireless authentication.

- ISO/IEC 11889-2: *Trusted Platform Module - Part 2: Design principles (Publicly available Specification).*

  Publication date: 2009-05-15

  Part 2 of ISO/IEC 11889 defines the principles of TPM operation, in particular the base operating modes, the algorithms and key choices, along with basic interoperability requirements. The document is based on the Trusted Platform Module specification version 1.2.

- ISO/IEC 11889-3: *Trusted Platform Module - Part 3: Structures (Publicly available Specification).*

  Publication date: 2009-05-15

  Part 3 of ISO/IEC 11889 defines the structures and constants in use by the TPM. As the TPM must interoperate between various implementations, these structures enable the required interoperability. Another rationale for defining the structures is that some of the structures require security properties, either confidentiality or integrity calculations. The document is based on the Trusted Platform Module specification version 1.2.

- ISO/IEC 11889-4: *Trusted Platform Module - Part 4: Commands (Publicly available Specification).*

  Publication date: 2009-05-15

  Part 4 of ISO/IEC 11889 defines the commands that allow software to communicate to and use the TPM. This part defines the command format as both the TPM and calling software must agree on the exact command format, as many of the commands require cryptographic authorization and the format of the authorization must be standardized. The document is based on the Trusted Platform Module specification version 1.2.

- ISO/IEC 13888-1: *Non-repudiation - Part 1: General (3rd edition)*.

  Publication date: 2009-07-01

  This part of ISO/IEC 13888 serves as a general model for subsequent parts specifying non-repudiation mechanisms using cryptographic techniques. This multipart International Standard provides non-repudiation mechanisms for the following phases of non-repudiation: evidence generation, evidence transfer, storage and retrieval, and evidence verification. Dispute arbitration is outside the scope of this International Standard.

- ISO/IEC TR 15446: Guide for the production of Protection Profiles and Security Targets (2nd edition).

  Publication date: 2009-03-01

  ISO/IEC TR 15446 provides guidance related to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with ISO/IEC 15408:2008 or Common Criteria Version 3.1, a technically identical standard published by the Common Criteria Management Board. The document is primarily aimed at those who are involved in the development of PPs and STs. It will also be of interest to consumers and users of PPs and STs who wish to understand the contents of PPs and STs developed by others, and wish to confirm the relevance and accuracy of the information that they contain. The document is an informational ISO Technical Report intended for guidance only.

- ISO/IEC 19772: *Authenticated encryption.*

  Publication date: 2009-02-15

  ISO/IEC 19772 specifies six methods for authenticated encryption, i.e. defined ways of processing a data string with the combined security objectives of data confidentiality, data integrity, and data origin authentication. All six methods specified in this International Standard are based on a block cipher algorithm, and require the originator and the recipient of the protected data to share a secret key for this block cipher. Four of the mechanisms in this standard allow data to be authenticated which is not encrypted.

  See also http://www.iso.org/iso/pressrelease.htm?refid=Ref1221

- ISO/IEC 19792: *Security evaluation of biometrics*.

  Publication date: 2009-08-01

  ISO/IEC 19792 specifies the specific subjects to be addressed during the security evaluation of a biometric system seeking to conform to this International Standard. It covers the

biometric-specific aspects and principles to be considered during the security evaluation of a biometric system. It does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels).

- ISO/IEC 24761: *Authentication context for biometrics.*

  Publication date: 2009-05-15

  ISO/IEC 24761defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. This International Standard allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion.

- ISO/IEC 21827: *Systems Security Engineering - Capability Maturity Model (SSE-CMM) (2nd edition) .*

  Publication date: 2008-10-01

  ISO/IEC 21827 describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering. The SSE-CMM does not prescribe a particular process or sequence, but captures practices generally observed in industry. The model serves as a standard metric for security engineering practices.

- ISO/IEC 27000*: Information security management systems -- Overview and vocabulary.*

  Publication date: 2009-05-01

  ISO/IEC 27000 provides an introduction to information security management systems (ISMS); an overview of standards related to ISO/IEC 27001 (referred to as “ISMS Family Standards”) currently published or under development; and terms and definitions (vocabulary) used throughout ISMS Family Standards.

  See also http://www.iso.org/iso/pressrelease.htm?refid=Ref1223

- ISO/IEC 27011 (= ITU-T X.1051): *Information security management guidelines for telecommunications organizations*.

  Publication date: 2008-12-15

  This Recommendation | International Standard defines interpretation guidelines for the implementation and management of Information Security Management (ISM) in telecommunications organizations based on ISO/IEC 27002 (Code of practice for information security management).

In addition, a substantial number of Amendments and Technical Corrigenda have been published over the past 12 months.

2.2.2 Documents awaiting Publication

Currently there are no International Standards or Technical Reports developed by SC 27 which have been finalized and are awaiting publication.

2.3 Resources

The last SC 27 Plenary meeting took place April 11-12, 2009 in Beijing, China and was attended by 55 delegates from 22 of the current 42 P-members.

The five SC 27 Working Groups held meetings October 6-10, 2008 in Limassol, Cyprus, and May 4–8, 2009 in Beijing, China. In average, these WG meetings were attended by about 200 delegates in total.

The next Working Group meetings are scheduled for November 2-6 2009 in Redmond, USA and for April 19–23, 2010 in Melaka, Malaysia. The next SC 27 Plenary meeting is planned to take place April 26–27, 2010 in Melaka, Malaysia.

Overall, the resources and expertise prove to be sufficient to meet the many challenges, SC 27 is facing. In particular, the two newly established Working Groups have attracted additional experts from all regions worldwide. With the new multi-part project ISO/IEC 11889 on Trusted Platform Modules (JTC 1 PAS process) SC 27 is further expanding its range of expertise into security engineering.

3 Focus Next Work Period

3.1 Deliverables

Deliverables expected from the next work period (October 2009 - September 2010) include

- ISO/IEC 9797-1: *Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher (2nd edition)*.
- ISO/IEC 9797-2: *Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function (2nd edition)*.
- ISO/IEC 9798-1: *Entity authentication - Part 1: General (3rd edition)*.
- ISO/IEC 9798-5: *Entity authentication - Part 5: Mechanisms using zero knowledge techniques (3rd edition)*.
- ISO/IEC 13888-3: *Non-repudiation - Part 3: Mechanisms using asymmetric techniques (2nd edition)*.
- ISO/IEC 15408-1: *Evaluation criteria for IT Security – Part 1: Introduction and general model (3rd edition).*
- ISO/IEC 15946-5: *Cryptographic techniques based on elliptic curves – Part 5 : Elliptic curve generation*.
- ISO/IEC 18014-2: *Time-stamping services – Part 2: Mechanisms producing independent tokens (2nd edition).*
- ISO/IEC 18014-3: *Time-stamping services – Part 3: Mechanisms producing linked tokens (2nd edition).*
- ISO/IEC TR 19791: *Security assessment of operational systems (2nd edition)*.
- ISO/IEC 27003: *Information security management system implementation guidance*.
- ISO/IEC 27004: *Information security management – Measurement*.
- ISO/IEC 27033-1: *Network security - Part 1: Overview and concepts*.

3.2 Strategies

SC 27's Area of Work is the standardization of generic methods and techniques for IT security. Among its 'users' are other standardization groups that adopt these where appropriate, in whole or in part, and provide a selection of required options. An important

means to ensure the timely development of market-oriented methods and techniques for IT security is the cooperation with such users, such as SC 7, SC 37 and TC 68.

3.2.1 Risks

The time to develop market driven standards is not always consistent with the market needs and timeframe for these standards. Ways and means to continually improve the timely development and delivery of standards are reviewed on a regular basis.

3.2.2 Opportunities

Standardized security techniques are becoming mandatory requirements for e-commerce, health-care, and many other application areas. The use of security techniques and in particular of electronic signatures constitutes a core element in e-business, e-government and other on-line activities. Over the last years, SC 27's work programme has included the basic techniques required for these activities. The existing portfolio of SC 27 work items and standards can be used to define a security framework, e.g., for governance, the telecom sector, healthcare sector or for the financial/insurance sector.

3.2.3 Marketing Initiatives and Joint Standardization Events

SC 27 has established the position of a PR officer and produces and distributes a number of press releases each year. These aim at promoting the standards that SC 27 develops and publishes. The press releases are targeted at users, implementers and management in industry and commerce. The distribution channels include international user groups and associations interested in security standards, security journals, publications and news letters, the SC 27 Web site as well standards development bodies (within ISO/IEC, ITU-T, CEN, ETSI and other bodies such as IETF and IEEE).

SC27 chair, deputy-chair, convenors and experts are frequently presenting the work of SC27 at many conferences and workshops around the world. Some of those in 2008/2009 include:

- RSA conference Japan, Tokyo, April 2008
- International School on Foundations of Security Analysis and Design (FOSAD), Bertinoro, Italy, August 2008
- Industry Seminar, Cyprus, October 2008
- International Conference of Data Protection Commissioners, Strasbourg, October 2008
- Information Security Standardization International Forum, Beijing, May 2009.

Since 2005 thirteen articles have been published in the ISO publications: ISO Focus, ISO Journal and ISO Management Systems. To name a few we have four in ISO Focus (volume 6, no. 6 2009) bringing to the public attention achievements of successful standardization work in the area of Information Security Management Systems (ISMS) as well as new approaches being underway within the newly established Working Group 4 "Security Controls" and WG 5 "Identity Management and Privacy Technologies". Seven other articles have been published in ISO Management Systems, including an article jointly written with SC7/WG25 on the integration of the ISO/IEC 27001 information security management system requirements and ISO/IEC 20000-1 service management standards. 2009 saw the publication of two more acrticles for ISO Management Systems and more are planned for 2010.

Both WG 4 and WG 5 have on their agenda projects to be developed in close cooperation with their liaison organizations especially with ITU-T SG17 and ITU-T D but also with such liaison members as ICDPPC, Liberty Alliance, FIDIS, OASIS, The Open Group, PrimeLife, PICOS; ETSI/TISPAN, W3C.

SD11 provides a very accessible overview of the work of SC27. This includes a number of the SC27 articles that have been published by ISO in the publications ISO Focus, ISO Journal and ISO Management System. SD11 is freely available to everyone and is downloadable via the SC27 Web Site (http://www.jtc1sc27.din.de/sce/sd11).

The following are some of the collaborative workshops have taken place:

- Joint ITU-T SG17/Q.6 & SC 27/WG 4 Workshop on Cybersecurity Standards in Geneva on 26th October 2007. Further details can be found at http://www.jtc1sc27.din.de/sue/ws_cybersec.
- Joint ITU-T SG17/Q.6 /SC 27/WG 5 / FIDIS Workshop on Identity Management Standards in Lucerne on 30th September 2007. More details can be obtained from the workshop's web site at http://www.jtc1sc27.din.de/sue/ws_idm.

Tutorial and press material on SC 27, its projects, and its standardization roadmaps is available from http://www.jtc1sc27.din.de/

3.3 Work Programme Priorities

Priority tasks for Working Group 1 include to ensure that work on projects 27007: *Guidelines for information security management systems auditing*, 27008 *Guidelines for auditors on information security management systems controls* and 27014 *Information security governance framework* are progressed as planned, and keeping the WG1 Roadmap up-to-date. Revisions have also been commenced on 27001 *Information security management systems - Requirements* and 27002 *Code of practice for information security management*. In addition, WG 1's role in the cooperation with ITU-T is of strategic importance in particular on the topics of network security, information security governance, risk management profiles and the ISO 27000 ISMS family of standards.

For Working Group 2, priorities for the next work period include the successful completion of the WG 2 projects mentioned in section 3.1, as well as the development of standards by recently established projects: 29150 *Signcryption* (which will specify mechanisms combining digital signature and cipher functions), 29192 *Lightweight cryptography* (as mentioned in 1.3.2) and 11770-5 *Group key management*. WG 2 will also start working in the standardization of cryptographic mechanisms in support of WG 5's work in the area of anonymity (29191 mentioned in 1.3.2) and other aspects of privacy. In addition, WG 2's roles in the cooperation with TC 68 Banking and Related Financial Services are of strategic importance.

Priority for Working Group 3 is to ensure that the main security evaluation and testing standards progress and are complemented with appropriate guidance and technical reports on specific fields of application. WG 3's cooperation with the Common Criteria Development Board (CCDB) remains important, and synergies with the current efforts for the development of the Common Criteria v4 should be useful for the progress of the WG3 roadmap. Beyond the development of the already identified projects and roadmap, there are different sectoral and national initiatives to develop specific standards that are mostly based or derived on WG3 projects. An effort will be made to improve coordination with these initiatives to avoid a proliferation of similar standards.

Priorities for Working Group 4 for the next work period include the successful completion of the WG 4 projects listed in section 3.1, and to ensure that work on projects 27031 *ICT Readiness for Business Continuity*, 27032 *Guidelines for Cybersecurity*, 27033 *Network Security Part 2 and 3*, and 27034-1 *Application Security Part 1 - Overview and Concepts* progressed to completion as planned. In addition, WG 4 continues to seek contributions to further consolidate and support the scope of work detailed in the WG 4 Roadmap (SD1).

Priorities for Working Group 5 are to develop foundational frameworks and architectures (projects 24760 *A framework for identity management*, 29100 *Privacy framework, and*

29101 Privacy architecture), to consolidate progress on biometrics projects transferred from Working Group 2, which is also requested by SC 37, and to develop standards according to its standards development roadmap, that is being used to identify, promote, and prioritize future work on supporting technologies, models, and methodologies. Examples are 24745 *Biometric template protection,* 29146 *A framework for access management,* 29190: *Privacy capability maturity model, and* 29191: *Requirements on relative anonymity with identity escrow.*